

Guía del portal para administradores de proveedores de servicios 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

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

Copyright © 2018-2020 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

- 1 Acerca del vCloud Director Service Provider Admin Portal 8**
 - Información actualizada 9
- 2 Introducción a vCloud Director Service Provider Admin Portal 10**
 - Descripción general de la administración de vCloud Director 10
 - Iniciar sesión en el vCloud Director Service Provider Admin Portal 14
 - Ver tareas 15
 - Detener una tarea en curso 15
 - Ver eventos 16
- 3 Administrar recursos de vSphere 17**
 - Agregar recursos de NSX y vCenter Server 18
 - Adjuntar una instancia de vCenter Server sola o junto con una instancia de NSX Manager 18
 - Asignar la clave de licencia de NSX en vCenter Server 21
 - Registrar una instancia de NSX-T Manager 22
 - Ver las instancias de vCenter Server 22
 - Modificar la configuración de vCenter Server 23
 - Habilitar o deshabilitar una instancia de vCenter Server 24
 - Volver a conectar una instancia de vCenter Server 24
 - Actualizar una instancia de vCenter Server 24
 - Actualizar las políticas de almacenamiento de una instancia de vCenter Server 25
 - Eliminar del registro una instancia de vCenter Server 25
 - Modificar la configuración de NSX Manager 26
 - Modificar la configuración de NSX-T Manager 26
 - Eliminar una instancia de NSX-T Manager 26
 - Listas de recursos multisitio 27
- 4 Administrar centros de datos virtuales de proveedor 28**
 - Habilitar o deshabilitar un centro de datos virtual de proveedor 28
 - Eliminar un centro de datos virtual de proveedor 29
 - Editar la configuración general de un centro de datos virtual de proveedor 29
 - Fusionar centros de datos virtuales de proveedor 30
 - Ver los centros de datos virtuales de organización que corresponden a un centro de datos virtual de proveedor 30
 - Ver los almacenes de datos en un centro de datos virtual de proveedor 31
 - Ver las redes externas en un centro de datos virtual de proveedor 32

- Administrar las políticas de almacenamiento de máquina virtual en un centro de datos virtual de proveedor 33
- Agregar una política de almacenamiento de máquina virtual a un centro de datos virtual de proveedor 33
- Habilitar o deshabilitar una política de almacenamiento de máquina virtual en un centro de datos virtual de proveedor 34
- Eliminar una política de almacenamiento de máquina virtual de un centro de datos virtual de proveedor 34
- Modificar los metadatos de una política de almacenamiento de máquina virtual en un centro de datos virtual de proveedor 35
- Administrar los grupos de recursos en un centro de datos virtual de proveedor 35
 - Agregar un grupo de recursos a un centro de datos virtual de proveedor 35
 - Habilitar o deshabilitar un grupo de recursos en un centro de datos virtual de proveedor 36
 - Separar un grupo de recursos de un centro de datos virtual de proveedor 37
- Modificar los metadatos de un centro de datos virtual de proveedor 38

5 Administrar organizaciones 39

- Entender las concesiones 39
- Crear una organización 40
- Configurar catálogos de una organización 40
- Configurar las políticas de una organización 41

6 Administrar centros de datos virtuales de organización 43

- Introducción a los modelos de asignación 43
 - Uso sugerido de los modelos de asignación 45
 - Modelo de asignación Flex 46
 - Modelo de asignación de grupo de asignación 48
 - Modelo de asignación de pago por uso 49
 - Modelo de asignación de grupo de reserva 50
- Entender las políticas de recursos informáticos 51
 - Políticas de recursos informáticos de centro de datos virtual de proveedor 51
 - Políticas de recursos informáticos del centro de datos virtual 55
- Crear un centro de datos virtual de organización 59
- Habilitar o deshabilitar un centro de datos virtual de organización 63
- Eliminar un centro de datos virtual de organización 63
- Modificar el nombre y la descripción de un centro de datos virtual de organización 64
- Modificar la configuración de modelo de asignación de un centro de datos virtual de organización 64
- Modificar la configuración de almacenamiento de un centro de datos virtual de organización 64
 - Modificar la configuración de aprovisionamiento de máquinas virtuales de un centro de datos virtual de la organización 65
- Agregar una política de almacenamiento de máquina virtual a un centro de datos virtual de organización 65

Cambiar la política de almacenamiento predeterminada en un centro de datos virtual de organización	66
Editar el límite de una política de almacenamiento en un centro de datos virtual de organización	66
Modificar los metadatos de una política de almacenamiento de máquina virtual en un centro de datos virtual de organización	67
Habilitar o deshabilitar una política de almacenamiento en un centro de datos virtual de organización	68
Eliminar una política de almacenamiento de un centro de datos virtual de organización	68
Editar la configuración de red de un centro de datos virtual de organización	69
Modificar los metadatos de un centro de datos virtual de organización	70
Ver los grupos de recursos de un centro de datos virtual de organización	71
Administrar el firewall distribuido en un centro de datos virtual de organización	71
Habilitar el firewall distribuido en un centro de datos virtual de organización	71
Agregar una regla de firewall distribuido	72
Editar una regla de firewall distribuido	75
Objetos de agrupamiento personalizados	76
Trabajar con grupos de seguridad	79
Trabajar con etiquetas de seguridad	83

7 Administrar puertas de enlace Edge 88

Trabajar con clústeres de Edge	89
Agregar una puerta de enlace Edge	90
Configurar servicios de puerta de enlace Edge	93
Administrar un firewall de puerta de enlace Edge	93
Administrar DHCP de puerta de enlace Edge	97
Agregar una regla SNAT o DNAT	103
Configuración avanzada de enrutamiento	105
Equilibrio de carga	115
Acceso seguro mediante redes privadas virtuales	130
Administración de certificados SSL	158
Objetos de agrupamiento personalizados	166
Ver el uso de redes y las asignaciones de IP en una puerta de enlace Edge	169
Editar propiedades de puerta de enlace Edge	169
Habilitar o deshabilitar el enrutamiento distribuido en una puerta de enlace Edge	170
Modificar las redes externas y la configuración de una puerta de enlace Edge	170
Editar la configuración general de una puerta de enlace Edge	171
Editar la puerta de enlace predeterminada de una puerta de enlace Edge	171
Editar la configuración de IP de una puerta de enlace Edge	172
Editar los grupos de IP subasignados en una puerta de enlace Edge	172
Editar los límites de velocidad en una puerta de enlace Edge	173
Volver a implementar una puerta de enlace Edge	173
Eliminar una puerta de enlace Edge	174

	Estadísticas y logs para una puerta de enlace Edge	174
	Ver estadísticas	174
	Habilitar registro	175
	Habilitar el acceso de la línea de comandos SSH a una puerta de enlace Edge	177
8	Administrar redes de centros de datos virtuales de organización	178
	Administrar redes de centros de datos virtuales NSX-T de organización	178
	Agregar una red de centros de datos virtuales de organización NSX-T	178
	Editar una red de centros de datos virtuales de organización NSX-T	179
	Eliminar una red de centros de datos virtuales de organización de NSX-T	180
9	Administrar SDDC y servidores proxy de SDDC	181
10	Administrar funciones y administradores del sistema	183
	Administrar derechos y funciones	183
	Funciones predeterminadas y sus derechos	185
	Nuevos derechos en esta versión	194
	Administrar paquetes de derechos	194
	Administrar las funciones de tenant globales	197
	Administrar funciones de proveedor	200
	Administrar usuarios y grupos de proveedor	202
	Administrar usuarios de proveedor	202
	Administrar grupos de proveedores	205
11	Administrar la configuración del sistema	208
	Administrar proveedores de identidad	208
	Administrar las conexiones LDAP	208
	Configurar el sistema para usar un proveedor de identidad SAML	211
	Administrar complementos	213
	Cargar un complemento	214
	Habilitar o deshabilitar un complemento	214
	Eliminar un complemento	215
	Publicar o cancelar la publicación de un complemento de una organización	215
	Personalizar los portales de vCloud Director	215
12	Supervisar vCloud Director	218
	vCloud Director e informe de costes	218
	Ver información de uso de un centro de datos virtual de proveedor	219
13	Administrar servicios	220
	Integrar vRealize Orchestrator con vCloud Director	220

Registrar una instancia de vRealize Orchestrator en vCloud Director	221
Crear una categoría de servicios	222
Editar una categoría de servicios	222
Importar un servicio	223
Buscar un servicio	224
Ejecutar un servicio	224
Cambiar una categoría de servicios	225
Eliminar un servicio del registro	225
Publicar un servicio	226
14 Administrar entidades personalizadas	227
Buscar una entidad personalizada	227
Editar una definición de entidad personalizada	228
Agregar una definición de entidad personalizada	228
Instancias de entidades personalizadas	229
Asociar una acción a una entidad personalizada	230
Anular la asociación de una acción con una entidad personalizada	230
Publicar una entidad personalizada	231
Eliminar una entidad personalizada	232

Acerca del vCloud Director Service Provider Admin Portal

1

La *Guía del vCloud Director Service Provider Admin Portal* proporciona información sobre el uso del Service Provider Admin Portal. El service provider admin portal se utiliza para administrar y supervisar organizaciones, derechos, funciones, usuarios y grupos en la nube. También se pueden crear y administrar las redes de centros de datos virtuales de organización con respaldo de NSX-T.

Público objetivo

Esta guía está destinada a los administradores de proveedores de servicios que deseen usar las capacidades proporcionadas en el vCloud Director Service Provider Admin Portal.

Documentación relacionada

Consulte la *Guía del administrador de vCloud Director* para obtener información sobre las funciones y las capacidades disponibles para los administradores mediante la consola web de vCloud Director en lugar de con el service provider admin portal 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 consultar las definiciones de términos tal y como se utilizan en la documentación técnica de VMware, visite <https://docs.vmware.com>.

Información actualizada

Esta documentación sobre *Guía del portal para administradores de proveedores de servicios de vCloud Director* se actualiza con cada versión del producto o cuando sea necesario.

En esta tabla se muestra el historial de actualizaciones de *Guía del portal para administradores de proveedores de servicios de vCloud Director*.

Revisión	Descripción
5 de abril de 2019	Se ha mejorado la información de los capítulos Introducción a los modelos de asignación y Entender las políticas de recursos informáticos .
28 de marzo de 2019	Versión inicial.

Introducción a vCloud Director Service Provider Admin Portal

2

El vCloud Director Service Provider Admin Portal es una interfaz dedicada para administradores de proveedores de servicios.

Este capítulo incluye los siguientes temas:

- [Descripción general de la administración de vCloud Director](#)
- [Iniciar sesión en el vCloud Director Service Provider Admin Portal](#)
- [Ver tareas](#)
- [Detener una tarea en curso](#)
- [Ver eventos](#)

Descripción general de la administración de vCloud Director

Con VMware vCloud Director se pueden crear nubes seguras con varios tenants. Para ello, es necesario agrupar recursos de infraestructura virtual en centros de datos virtuales y exponer estos recursos a los usuarios a través de portales web e interfaces programáticas como un servicio completamente automatizado y basado en catálogos.

La *Guía del administrador de vCloud Director* proporciona información acerca de cómo agregar recursos al sistema, crear y aprovisionar organizaciones, gestionar recursos y organizaciones y supervisar el sistema.

Recursos de vSphere y NSX

vCloud Director cuenta con recursos de vSphere para proporcionar CPU y memoria a fin de ejecutar las máquinas virtuales. Además, los almacenes de datos vSphere proporcionan almacenamiento de archivos de la máquina virtual y otros archivos necesarios para el funcionamiento de la máquina virtual. vCloud Director también utiliza conmutadores distribuidos de vSphere, grupos de puertos de vSphere y NSX Data Center for vSphere para admitir las redes de máquinas virtuales.

vCloud Director también puede utilizar los recursos de NSX-T Data Center. Para obtener información sobre el registro de una instancia de NSX-T Manager con su nube, consulte *Guía del portal para administradores de proveedores de servicios de vCloud Director* o *Guía de programación de vCloud API para proveedores de servicios*.

Puede utilizar las instancias subyacentes de vSphere y los recursos de NSX para crear recursos de nube.

A partir de la versión 9.7, vCloud Director puede actuar como un servidor proxy HTTP, con el que se puede permitir que las organizaciones accedan al entorno de vSphere subyacente.

Recursos de nube

Los recursos de nube son una abstracción de sus recursos de vSphere subyacentes.

Proporcionan los recursos informáticos y de memoria para las máquinas virtuales y vApps de vCloud Director. Una vApp es un sistema virtual que contiene una o más máquinas virtuales individuales con parámetros que definen los detalles operativos. Los recursos de nube también proporcionan acceso al almacenamiento y a la conectividad de red.

Los recursos de nube incluyen centros de datos virtuales del proveedor y de la organización, redes externas, redes de centros de datos virtuales de organización y grupos de redes. Además, vCloud Director 9.7 introduce el centro de datos definido por software (Software-Defined Data Center, SDDC) y los servidores proxy de SDDC como recursos de nube que proporcionan acceso al entorno de vSphere subyacente desde vCloud Director.

Para poder agregar recursos de nube a vCloud Director, primero debe agregar recursos de vSphere.

SDDC y servidores proxy de SDDC

vCloud Director 9.7 introduce el SDDC como un recurso de nube que encapsula una instalación completa de vCenter Server. Un SDDC incluye uno o varios servidores proxy de SDDC que son puntos de acceso a diferentes componentes del entorno de vSphere subyacente. El proveedor puede crear y habilitar SDDC y servidores proxy. El proveedor puede publicar un SDDC y sus servidores proxy en los tenants.

Para crear y administrar SDDC y servidores proxy, debe utilizar vCloud OpenAPI. Consulte *Introducción a vCloud OpenAPI* en <https://code.vmware.com>.

Centros de datos virtuales de proveedor

Un centro de datos virtual de proveedor combina los recursos informáticos y de memoria de un solo grupo de recursos de vCenter Server con los recursos de almacenamiento de uno o más almacenes de datos disponibles en dicho grupo de recursos.

Un centro de datos virtual de proveedor puede usar recursos de red de una instancia de NSX Manager asociada con la instancia de vCenter Server o de una instancia de NSX-T Manager registrada en la nube.

Puede crear varios centros de datos virtuales de proveedor para usuarios en diferentes ubicaciones geográficas o unidades empresariales o para los usuarios con diferentes requisitos de rendimiento.

Centros de datos virtuales de organización

Un centro de datos virtual de organización proporciona recursos a una organización con particiones desde un centro de datos virtual de proveedor. Los centros de datos virtuales de organización proporcionan un entorno donde se pueden almacenar, implementar y manejar sistemas virtuales. También proporcionan almacenamiento a medios virtuales, como disquetes y CD ROMs.

Una sola organización puede tener varios centros de datos virtuales de organización.

Redes de vCloud Director

vCloud Director admite tres tipos de redes.

- Redes externas
- Redes de centros de datos virtuales de organización
- Redes de vApp

Algunas redes de centros de datos virtuales de organización y todas las redes de vApp se respaldan mediante grupos de redes.

Redes externas

Una red externa es una red lógica y diferenciada basada en un grupo de puertos de vSphere. Las redes de centros de datos virtuales de organización pueden conectarse a redes externas para proporcionar conectividad Internet en máquinas virtuales dentro de una vApp.

A partir de la versión 9.5, vCloud Director admite redes externas IPv6. Una red externa IPv6 es compatible con subredes IPv4 e IPv6, y una red externa IPv4 es compatible con subredes IPv4 e IPv6.

De manera predeterminada, solo los **administradores del sistema** crean y administran redes externas.

Redes de centros de datos virtuales de organización

Una red de centros de datos virtuales de organización pertenece a 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. Para proporcionar conectividad externa, puede conectar una red de centro de datos virtual de organización a una red externa. También puede crear una red de centros de datos virtuales de organización aislada que sea interna a la organización.

vCloud Director 9.5 incorpora compatibilidad con IPv6 para las redes de centros de datos virtuales de organización directas y enrutadas.

A partir de vCloud Director 9.5, los **administradores del sistema** pueden crear redes de centros de datos virtuales aisladas respaldadas por un conmutador lógico de NSX-T. Los **administradores de la organización** pueden crear redes de centros de datos virtuales aisladas respaldadas por grupos de redes.

vCloud Director 9.5 también incorpora Cross VDC Networking mediante la configuración de redes extendidas en grupos de centros de datos virtuales.

De forma predeterminada, solo los **administradores del sistema** pueden crear redes de centros de datos virtuales directas y cruzadas. Los **administradores del sistema** y los **administradores de la organización** pueden gestionar redes de centros de datos virtuales de organización, aunque hay algunos límites para lo que puede hacer un **administrador de la organización**.

Redes de vApp

Una red de vApp pertenece a una vApp y permite que las máquinas virtuales de la vApp se comuniquen entre sí. Para permitir que vApp se comunique con otras vApps en la organización, puede conectar la red de la vApp a una red de centros de datos virtuales de organización. Si la red de centros de datos virtuales de organización está conectada a una red externa, la vApp puede comunicarse con las vApps de otras organizaciones. Las redes de vApp están respaldadas por grupos de redes.

La mayoría de usuarios con acceso a vApp pueden crear y administrar sus propias redes de vApp. Para obtener información sobre cómo trabajar con redes en una vApp, consulte *Guía del portal para tenants de vCloud Director*.

Grupos de redes

Un grupo de redes es un grupo de redes no diferenciadas disponible para que lo use un centro de datos virtual de organización. Los recursos de red de vSphere respaldan los grupos de redes como ID de VLAN o grupos de puerto. vCloud Director utiliza los grupos de redes para crear redes de centros de datos virtuales de organización interna con enrutamiento NAT y todas las redes de vApp. El tráfico de red de cada red en un grupo se aísla a nivel de capa 2 del resto de redes.

Cada centro de datos virtual de organización en vCloud Director puede tener un grupo de redes. Varios centros de datos virtuales de organización pueden compartir un grupo de redes. El grupo de redes de un centro de datos virtual de organización proporciona redes creadas para satisfacer la cuota de red de un centro de datos virtual de organización.

Solo los **administradores del sistema** pueden crear y administrar grupos de redes.

Organizaciones

vCloud Director admite varios tenants a través de las organizaciones. Una organización es una unidad de administración de un grupo de usuarios, grupos y recursos informáticos. Los usuarios se autentican a nivel de organización, proporcionando las credenciales establecidas por un administrador de la organización al crear o importar el usuario. Los **administradores del sistema** crean y aprovisionan organizaciones, mientras que los **administradores de la organización** gestionan usuarios, grupos y catálogos de organización. Las tareas de los **administradores de la organización** se describen en *Guía del portal para tenants de vCloud Director*.

Usuarios y grupos

Una organización puede contener un número arbitrario de usuarios y grupos. Los **administradores de la organización** pueden crear usuarios e importar usuarios y grupos de un servicio de directorios como LDAP. El **administrador del sistema** gestiona el conjunto de derechos disponibles para cada organización. El **administrador del sistema** puede crear y publicar funciones de tenant globales en una o varias organizaciones. El **administrador de la organización** puede crear funciones locales en sus organizaciones.

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 las plantillas y los archivos de medios incluidos en la vApp para crear sus propias vApps. Un **administrador del sistema** puede permitir a una organización la publicación de un catálogo y hacer que esté disponible para otras organizaciones. Los **administradores de las organizaciones** pueden decidir los elementos del catálogo que proporcionarán a sus usuarios.

Iniciar sesión en el vCloud Director Service Provider Admin Portal

Puede acceder al Service Provider Admin Portal de vCloud Director mediante un navegador web.

Requisitos previos

Debe tener derechos de administrador del sistema para acceder al vCloud Director Service Provider Admin Portal.

Procedimiento

- 1 En un navegador, escriba la dirección URL del Service Provider Admin Portal del sitio de vCloud Director y presione Entrar.

Por ejemplo, escriba **`https://vcloud.ejemplo.com/proveedor`**.

- 2 Inicie sesión con el nombre de usuario y la contraseña del administrador del sistema.

Ver tareas

En el Service Provider Admin Portal, puede ver las tareas recientes y su estado.

La vista de tareas es útil para dar un vistazo al estado de las tareas en el portal para administradores de proveedores de servicios. La vista muestra cuándo se han ejecutado las tareas y si estas se realizaron correctamente. Esta herramienta puede utilizarse para dar un buen primer paso para solucionar los problemas del entorno.

Los recuadros informativos azules y rojos sobre el icono Tareas muestran, respectivamente, el número de tareas ejecutadas y con errores.

Procedimiento

- ◆ En el menú de la parte superior derecha, seleccione el icono Tareas ().

Resultados

Se muestra una lista de las tareas recientes junto con la hora a la que se ha ejecutado la tarea y el estado de esta.

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>vmUpdateVapp</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.

Administrar recursos de vSphere

3

vCloud Director deriva sus recursos de una infraestructura virtual de vSphere subyacente. Tras registrar los recursos de vSphere en vCloud Director, es posible asignar estos recursos a organizaciones dentro de la instalación de vSphere para su uso.

vCloud Director utiliza uno o varios entornos de vCenter Server para respaldar sus centros de datos virtuales. A partir de la versión 9.7, vCloud Director también puede utilizar un entorno de vCenter Server para encapsular un SDDC con uno o varios servidores proxy. Puede habilitar los tenants para que usen estos servidores proxy como puntos de acceso al entorno de vSphere subyacente desde vCloud Director con sus cuentas de vCloud Director.

Para poder usar una instancia de vCenter Server en vCloud Director, primero es necesario asociar esta instancia de vCenter Server.

Cuando se crea un centro de datos virtual de proveedor respaldado mediante una instancia de vCenter Server asociada, esta instancia de vCenter Server aparece como “publicada” en el proveedor de servicios, lo que también se denomina “en el ámbito de proveedor”. Para obtener información sobre la creación de un centro de datos virtual de proveedor, consulte *Guía del administrador de vCloud Director*.

Cuando se crea un SDDC que encapsula una instancia de vCenter Server asociada, esta instancia de vCenter Server aparece como “publicada” en los tenants, lo que también se denomina “en el ámbito de tenant”. Para obtener información sobre cómo crear un SDDC, consulte [Capítulo 9 Administrar SDDC y servidores proxy de SDDC](#).

Nota De forma predeterminada, con una instancia de vCenter Server asociada, se puede crear un VDC de proveedor o un SDDC. Si creó un VDC de proveedor respaldado por una instancia de vCenter Server, no puede utilizar esta instancia de vCenter Server para crear un SDDC y viceversa. Puede utilizar vCloud API para modificar la configuración del sistema de la instalación de vCloud Director, de modo que una instancia de vCenter Server pueda respaldar un VDC de proveedor y un SDDC.

Este capítulo incluye los siguientes temas:

- [Agregar recursos de NSX y vCenter Server](#)
- [Ver las instancias de vCenter Server](#)

- [Modificar la configuración de vCenter Server](#)
- [Habilitar o deshabilitar una instancia de vCenter Server](#)
- [Volver a conectar una instancia de vCenter Server](#)
- [Actualizar una instancia de vCenter Server](#)
- [Actualizar las políticas de almacenamiento de una instancia de vCenter Server](#)
- [Eliminar del registro una instancia de vCenter Server](#)
- [Modificar la configuración de NSX Manager](#)
- [Modificar la configuración de NSX-T Manager](#)
- [Eliminar una instancia de NSX-T Manager](#)
- [Listas de recursos multisitio](#)

Agregar recursos de NSX y vCenter Server

vCloud Director cuenta con recursos de vSphere para proporcionar CPU, memoria y almacenamiento a fin de ejecutar máquinas virtuales. Además, a partir de la versión 9.7, vCloud Director puede actuar como servidor HTTP entre los tenants y el entorno de vSphere subyacente.

Para obtener información sobre los requisitos del sistema de vCloud Director, y las versiones compatibles de vCenter Server y ESXi, consulte *Matrices de interoperabilidad de productos de VMware* en http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Adjuntar una instancia de vCenter Server sola o junto con una instancia de NSX Manager

Asocie una instancia de vCenter Server para que sus recursos estén disponibles para usarlos en vCloud Director. Puede asociar una instancia de vCenter Server junto con su instancia de NSX Manager relacionada o bien puede asociar una instancia de vCenter Server de forma independiente.

vCloud Director puede utilizar una instancia de vCenter Server con su instancia de NSX Manager asociada o con una instancia de NSX-T Manager.

Si desea que vCloud Director use esta instancia de vCenter Server con su instancia de NSX Manager asociada, debe adjuntar las instancias de vCenter Server y NSX Manager juntas.

Si desea que vCloud Director use esta instancia de vCenter Server con una instancia de NSX-T Manager, debe adjuntar la instancia de vCenter Server sola. Después de adjuntar la instancia de vCenter Server sola, debe [Registrar una instancia de NSX-T Manager](#).

Nota Después de adjuntar una instancia de vCenter Server sola, no puede agregar su instancia de NSX Manager asociada en una etapa posterior. Puede eliminar la instancia de vCenter Server del registro y volver a asociarla junto con su instancia de NSX Manager relacionada.

Puede adjuntar una instancia de vCenter Server a cualquier sitio desde el entorno de vCloud Director.

Requisitos previos

- Si configuró vCloud Director para comprobar certificados SSO de vCenter y vSphere, compruebe que ha cargado los certificados de vCenter Server en vCloud Director. Para obtener información sobre la configuración general del sistema, consulte la *Guía del administrador de vCloud Director*.
- Si configuró vCloud Director para comprobar certificados de NSX Manager, verifique que ha cargado los certificados de NSX Manager en vCloud Director. Para obtener información sobre la configuración general del sistema, consulte la *Guía del administrador de vCloud Director*.

Procedimiento

1 [Agregar la instancia de vCenter Server](#)

Para agregar una instancia de vCenter Server, introduzca los detalles de acceso de vCenter Server.


2 [\(Opcional\) Agregar la instancia de NSX Manager asociada](#)

Si desea que vCloud Director use esta instancia de vCenter Server con su instancia de NSX Manager asociada, debe agregar detalles de acceso de NSX Manager.

Agregar la instancia de vCenter Server

Para agregar una instancia de vCenter Server, introduzca los detalles de acceso de vCenter Server.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de vSphere**.
- 2 En el panel izquierdo, haga clic en **vCenters** y, a continuación, haga clic en **Agregar**.
- 3 Si tiene una implementación multisitio de vCloud Director, en el menú desplegable **Sitio**, seleccione el sitio al que desea agregar esta instancia de vCenter Server y haga clic en **Siguiente**.
- 4 Escriba un nombre y, si lo desea, una descripción para la instancia de vCenter Server en vCloud Director.
- 5 Introduzca la URL de la instancia de vCenter Server.

Si se utiliza el puerto predeterminado, puede omitir el número de puerto. Si se utiliza un puerto personalizado, incluya el número de puerto
Por ejemplo, **https://FQDN_or_IP_address:<custom_port_number>**.
- 6 Escriba el nombre de usuario y la contraseña de la cuenta de vCenter Server **administrador**.
- 7 (opcional) Para deshabilitar la instancia de vCenter Server después del registro, desactive el botón de alternancia **Habilitado**.

8 Configure la URL de vCenter Server Web Client.

Opción	Descripción
Usar servicios de vSphere para proporcionar URL	Para esta opción, debe usar la API de vCloud para configurar vCloud Director de manera que use el servicio de búsqueda de vSphere.
URL de vSphere Web Client	Para usar esta opción, debe introducir la URL de vSphere Web Client. Por ejemplo, https://ejemplo.vmware.com/cliente-vsphere .

9 Haga clic en **Siguiente**.

10 (opcional) Omita el paso para agregar la instancia de NSX Manager que está asociada a la instancia de vCenter Server y finalice el registro.

Si desea que vCloud Director use esta instancia de vCenter Server con una instancia de NSX-T Manager, debe agregar solo la instancia de vCenter Server.

Nota No se puede agregar la instancia de NSX Manager asociada en una etapa posterior. Puede eliminar la instancia de vCenter Server del registro y volver a asociarla junto con su instancia de NSX Manager relacionada.

- En la página **Configuración de NSX-V Manager**, desactive el botón de alternancia **Configurar ajustes** y haga clic en **Siguiente**.
- En la página **Listo para completar**, revise los detalles de registro y haga clic en **Finalizar**.

(Opcional) Agregar la instancia de NSX Manager asociada

Si desea que vCloud Director use esta instancia de vCenter Server con su instancia de NSX Manager asociada, debe agregar detalles de acceso de NSX Manager.

Procedimiento

1 En la página **Configuración de NSX-V Manager**, deje activado el botón de alternancia **Configurar ajustes**.

2 Introduzca la URL de la instancia de NSX Manager.

Si se utiliza el puerto predeterminado, puede omitir el número de puerto. Si se utiliza un puerto personalizado, incluya el número de puerto

Por ejemplo, **https://FQDN_o_dirección_IP:<número_de_puerto_personalizado>**.

3 Escriba el nombre de usuario y la contraseña de la cuenta de **administrador** de NSX.

- 4 (opcional) Para habilitar Cross VDC Networking para los centros de datos virtuales que respalda esta instancia de vCenter Server, active el botón de alternancia **Cross VDC Networking** e introduzca las propiedades de implementación de máquina virtual de control y un nombre para el alcance del proveedor de red.

Las propiedades de implementación de la máquina virtual de control se utilizan a fin de implementar un dispositivo en la instancia de NSX Manager para componentes de Cross VDC Networking, como un enrutador universal.

Opción	Descripción
Ruta de acceso del grupo de recursos	La ruta de acceso jerárquica a un grupo de recursos específico en la instancia de vCenter Server que comienza en el clúster, <i>Clúster/Elemento_principal_de_grupo_de_recursos/Recurso_de_destino</i> . Por ejemplo, TestbedCluster1/mgmt-rp . Como alternativa, puede introducir el identificador de referencia de objeto administrado del grupo de recursos. Por ejemplo, resgroup-1476 .
Nombre de almacén de datos	El nombre del almacén de datos que alojará los archivos del dispositivo. Por ejemplo, shared-disk-1 .
Interfaz de administración	El nombre de la red en vCenter Server o el grupo de puertos usado para la interfaz de administración de DLR de HA. Por ejemplo, TestbedPG1 .
Alcance de proveedor de red	Corresponde al dominio de error de red en las topologías de red de los grupos de centros de datos. Por ejemplo, boston-fault1 . Para obtener información sobre la administración de grupos entre centros de datos virtuales, consulte la <i>Guía del portal para tenants de vCloud Director</i> .

- 5 En la página **Listo para completar**, revise los detalles de registro y haga clic en **Finalizar**.

Pasos siguientes

- [Asignar la clave de licencia de NSX en vCenter Server](#).
- Para obtener información sobre la creación de un centro de datos virtual de proveedor, consulte la *Guía del administrador de vCloud Director*.

Asignar la clave de licencia de NSX en vCenter Server

Si adjuntó una instancia de vCenter Server junto con su instancia de NSX Manager asociada, debe usar vSphere Client para asignar una clave de licencia a la instancia de NSX Manager que admite redes de vCloud Director.

Requisitos previos

Esta operación está limitada a los administradores del sistema.

Procedimiento

- 1 Desde una instancia de vSphere Client conectada al sistema vCenter Server, seleccione **Inicio > Licencia**.


- 2 Para la vista de informe, seleccione **Activo**.
- 3 Haga clic con el botón secundario en el activo NSX Manager y seleccione **Cambiar clave de licencia**.
- 4 Seleccione **Asignar una clave de licencia nueva** y haga clic en **Introducir la clave**.
- 5 Introduzca la clave de licencia, introduzca una etiqueta opcional para la clave y haga clic en **Aceptar**.

Utilice la clave de licencia de NSX Manager que recibió al adquirir vCloud Director. Puede usar esta clave de licencia en varias instancias de vCenter Server.
- 6 Haga clic en **Aceptar**.

Registrar una instancia de NSX-T Manager

Puede registrar una instancia de NSX-T Manager en vCloud Director para que vCloud Director pueda utilizar sus recursos de red. Un centro de datos virtual de proveedor puede utilizar recursos de red de NSX Data Center for vSphere o de NSX-T Data Center.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de vSphere**.
- 2 En el panel izquierdo, haga clic en **NSX-T Manager** y, a continuación, haga clic en **Agregar**.
- 3 Si tiene una implementación multisitio de vCloud Director, en el menú desplegable **Sitio**, seleccione el sitio al que desea agregar esta instancia de NSX-T Manager y haga clic en **Siguiente**.
- 4 Escriba un nombre y, si lo desea, una descripción para la instancia de NSX-T Manager en vCloud Director.
- 5 Introduzca la URL de la instancia de NSX-T Manager.

Por ejemplo, **`https://FQDN_o_dirección_IP`**.
- 6 Escriba el nombre de usuario y la contraseña de la cuenta de NSX-T Manager **administrador**.
- 7 Haga clic en **Guardar**.


Pasos siguientes

Para obtener información sobre la creación de un centro de datos virtual de proveedor respaldado por NSX-T Data Center, consulte *Guía de programación de vCloud API para proveedores de servicios* en <https://code.vmware.com>.

Ver las instancias de vCenter Server

Puede ver una lista de las instancias de vCenter Server en todos los sitios de la instalación de vCloud Director. Puede ver de qué modo vCloud Director utiliza cada instancia de vCenter Server.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de vSphere**.
- 2 En el panel izquierdo, haga clic en **vCenters**.

Resultados

Se muestra una lista de todas las instancias de vCenter Server asociadas. La lista contiene la siguiente información para cada instancia de vCenter Server.


	Descripción
Nombre	El nombre de la instancia de vCenter Server en vCloud Director.
Estado	Habilitado o deshabilitado. Consulte Habilitar o deshabilitar una instancia de vCenter Server .
Conexión	Conectado o no a vCloud Director. Consulte Volver a conectar una instancia de vCenter Server .
Host de VC	FQDN de la instancia de vCenter Server.
Versión	La versión de vCenter Server.
Proveedor de servicios	Publicado o no para el uso por parte de los centros de datos virtuales.
Tenant	Publicado o no para su uso como un centro de datos definido por software (Software-Defined Data Center, SDDC).
Sitio	El FQDN de vCloud Director del sitio al que pertenece la instancia de vCenter Server.

Modificar la configuración de vCenter Server

Si la información de conexión de una instancia de vCenter Server adjuntada se modifica, o si desea cambiar su nombre o descripción en vCloud Director, puede modificar la configuración.

Puede modificar la configuración que definió al agregar la instancia de vCenter Server. Consulte [Agregar la instancia de vCenter Server](#).

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de vSphere**.
- 2 En el panel izquierdo, haga clic en **vCenter** y, a continuación, haga clic en el nombre de la instancia de vCenter Server que desea modificar.
- 3 En la esquina superior derecha de la sección **Información de vCenter**, haga clic en **Editar**.
- 4 Edite la configuración de vCenter Server y haga clic en **Guardar**.


Pasos siguientes

Si modificó la información de conexión, debe [Volver a conectar una instancia de vCenter Server](#).

Habilitar o deshabilitar una instancia de vCenter Server

Antes de realizar un mantenimiento o eliminar del registro una instancia de vCenter Server, debe deshabilitar la instancia de vCenter Server de destino. Para proporcionar sus recursos a centros de datos virtuales en vCloud Director, debe habilitar la instancia de vCenter Server.

Procedimiento


- 1 En el menú principal () , seleccione **Recursos de vSphere**.
- 2 En el panel izquierdo, haga clic en **vCenters**.
- 3 Haga clic en el botón de radio ubicado junto a la instancia de vCenter Server de destino y, a continuación, haga clic en **Habilitar** o **Deshabilitar**.
- 4 Para confirmar, haga clic en **Aceptar**.

Volver a conectar una instancia de vCenter Server

Si una instancia de vCenter Server aparece como desconectada, o si modificó la configuración de conexión, puede intentar restablecer la conexión.

Nota Al establecer la nueva conexión, la instancia de vCenter Server no estará disponible para las operaciones.


Procedimiento

- 1 En el menú principal () , seleccione **Recursos de vSphere**.
- 2 En el panel izquierdo, haga clic en **vCenters**.
- 3 Haga clic en el botón de radio ubicado junto al nombre de la instancia de vCenter Server de destino y, a continuación, haga clic en **Volver a conectar**.
- 4 Para confirmar, haga clic en **Aceptar**.

Actualizar una instancia de vCenter Server

Para actualizar la información de la base de datos de vCloud Director sobre los recursos de vCenter Server subyacentes, debe actualizar la instancia de vCenter Server.

Procedimiento


- 1 En el menú principal () , seleccione **Recursos de vSphere**.
- 2 En el panel izquierdo, haga clic en **vCenters**.

- 3 Haga clic en el botón de radio ubicado junto al nombre de la instancia de vCenter Server de destino y, a continuación, haga clic en **Actualizar**.
- 4 Para confirmar, haga clic en **Aceptar**.

Actualizar las políticas de almacenamiento de una instancia de vCenter Server

Para actualizar la información de la base de datos de vCloud Director sobre las políticas de almacenamiento de máquina virtual en el entorno de vSphere subyacente, debe actualizar las políticas de almacenamiento de la instancia de vCenter Server.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de vSphere**.
- 2 En el panel izquierdo, haga clic en **vCenters**.
- 3 Haga clic en el botón de radio ubicado junto al nombre de la instancia de vCenter Server de destino y, a continuación, haga clic en **Actualizar políticas**.
- 4 Para confirmar, haga clic en **Aceptar**.


Eliminar del registro una instancia de vCenter Server

Para dejar de utilizar los recursos de una instancia de vCenter Server, puede quitar esta instancia de vCenter Server de la instalación de vCloud Director.

Requisitos previos

- Deshabilite la instancia de vCenter Server. Consulte [Habilitar o deshabilitar una instancia de vCenter Server](#).
- Elimine todos los centros de datos virtuales de proveedor que usan grupos de recursos de esta instancia de vCenter Server. Consulte [Eliminar un centro de datos virtual de proveedor](#).

Procedimiento


- 1 En el menú principal () , seleccione **Recursos de vSphere**.
- 2 En el panel izquierdo, haga clic en **vCenters**.
- 3 Haga clic en el botón de radio ubicado junto al nombre de la instancia de vCenter Server de destino y, a continuación, haga clic en **Anular registro**.
- 4 Para confirmar, haga clic en **Aceptar**.

Modificar la configuración de NSX Manager

Si la información de conexión de una instancia registrada de NSX Manager se modifica, o si desea cambiar su nombre o descripción en vCloud Director, puede modificar su configuración.

Puede modificar la configuración que definió al agregar la instancia de NSX Manager. Consulte [\(Opcional\) Agregar la instancia de NSX Manager asociada](#).

Procedimiento


- 1 En el menú principal () , seleccione **Recursos de vSphere**.
- 2 En el panel izquierdo, haga clic en **vCenters** y, a continuación, haga clic en el nombre de la instancia de vCenter Server que está asociada a la instancia de NSX Manager de destino.
- 3 En la esquina superior derecha de la sección **Información de NSX-V Manager**, haga clic en **Editar**.
- 4 Edite la configuración de vCenter Server y haga clic en **Guardar**.

Modificar la configuración de NSX-T Manager

Si la información de conexión de una instancia registrada de NSX-T Manager se modifica, o si desea cambiar su nombre o descripción en vCloud Director, puede modificar su configuración.

Puede modificar la configuración que definió al agregar la instancia de vCenter Server. Consulte [Registrar una instancia de NSX-T Manager](#).

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de vSphere**.
- 2 En el panel izquierdo, haga clic en **NSX-T Manager** y, a continuación, haga clic en el nombre de la instancia de NSX-T Manager que desea modificar.
- 3 En la esquina superior derecha de la pestaña **General**, haga clic en **Editar**.
- 4 Edite la configuración de NSX-T Manager y haga clic en **Guardar**.


Eliminar una instancia de NSX-T Manager

Para dejar de utilizar los recursos de una instancia de NSX-T Manager, puede quitar esta instancia de vCenter Server de la instalación de vCloud Director.

Requisitos previos

Elimine todos los centros de datos virtuales de proveedor que usen recursos de esta instancia de NSX-T Manager. Consulte [Eliminar un centro de datos virtual de proveedor](#).

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de vSphere**.
- 2 En el panel izquierdo, haga clic en **NSX-T Manager**.
- 3 Haga clic en el botón de radio ubicado junto al nombre de la instancia de NSX-T Manager que desea eliminar y haga clic en **Eliminar**.
- 4 Para confirmar, haga clic en **Eliminar**.

Listas de recursos multisitio

Si trabaja con implementaciones de vCloud Director en varias ubicaciones, puede ver listas de recursos que incluyen información sobre objetos de todos los sitios conectados.

Para facilitar la navegación por vSphere y los recursos de nube desde Service Provider Admin Portal, a partir de la versión 9.7, vCloud Director incluye listas de recursos multisitio.

Puede acceder a las listas de recursos a través de los menús **Recursos de vSphere** y **Recursos de nube**.

Puede acceder a información detallada sobre objetos desde los diferentes sitios y también crear objetos en el sitio local y en sitios remotos.

Las listas de recursos multisitio de vSphere son compatibles con instancias de vCenter Server, instancias de NSX-T Manager, grupos de recursos, almacenes de datos, hosts, conmutadores distribuidos, grupos de puertos, elementos deshabilitados y políticas de almacenamiento.

Las listas de recursos de nube multisitio se admiten para VDC de organización, plantillas de VDC de organización, VDC de proveedor, celdas de nube, puertas de enlace Edge, redes externas y grupos de redes.

Nota No se admiten las listas de organizaciones multisitio.

Administrar centros de datos virtuales de proveedor

4

Después de crear un centro de datos virtual de proveedor, es posible modificar sus propiedades, deshabilitarlo o eliminarlo, y administrar sus políticas de almacenamiento y grupos de recursos.

Para crear un centro de datos virtual de proveedor, es necesario usar vCloud Director Web Console o vCloud API. Para obtener información sobre el uso de vCloud Director Web Console, consulte *Guía del administrador de vCloud Director*. Para obtener información sobre el uso de vCloud API, consulte *Guía de programación de vCloud API para proveedores de servicios*.

Este capítulo incluye los siguientes temas:


- [Habilitar o deshabilitar un centro de datos virtual de proveedor](#)
- [Eliminar un centro de datos virtual de proveedor](#)
- [Editar la configuración general de un centro de datos virtual de proveedor](#)
- [Fusionar centros de datos virtuales de proveedor](#)
- [Ver los centros de datos virtuales de organización que corresponden a un centro de datos virtual de proveedor](#)
- [Ver los almacenes de datos en un centro de datos virtual de proveedor](#)
- [Ver las redes externas en un centro de datos virtual de proveedor](#)
- [Administrar las políticas de almacenamiento de máquina virtual en un centro de datos virtual de proveedor](#)
- [Administrar los grupos de recursos en un centro de datos virtual de proveedor](#)
- [Modificar los metadatos de un centro de datos virtual de proveedor](#)

Habilitar o deshabilitar un centro de datos virtual de proveedor

Para deshabilitar todos los centros de datos virtuales de organización que utilizan los recursos de un centro de datos virtual de proveedor, se puede deshabilitar este centro de datos virtual de proveedor. No se pueden crear centros de datos virtuales de organización que utilicen los recursos de un centro de datos virtual de proveedor deshabilitado.

Las vApp en ejecución y las máquinas virtuales encendidas se siguen ejecutando en los centros de datos virtuales de organización existentes respaldados por este centro de datos virtual de proveedor, pero no se pueden crear ni iniciar vApps o máquinas virtuales adicionales.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de proveedor**.
- 3 Haga clic en el botón de radio ubicado junto al centro de datos virtual de proveedor de destino y, a continuación, haga clic en **Habilitar** o **Deshabilitar**.
- 4 Para confirmar, haga clic en **Aceptar**.

Eliminar un centro de datos virtual de proveedor


Para eliminar los recursos de un centro de datos virtual de proveedor de vCloud Director, puede eliminar este centro de datos virtual de proveedor.

Los recursos subyacentes en vSphere permanecen inalterados.

Requisitos previos

- Deshabilite el centro de datos virtual del proveedor de destino. Consulte [Habilitar o deshabilitar un centro de datos virtual de proveedor](#).
- Elimine todos los centros de datos virtuales de organización que utilicen recursos de este centro de datos virtual de proveedor. Consulte [Eliminar un centro de datos virtual de organización](#).


Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de proveedor**.
- 3 Haga clic en el botón de radio ubicado junto al nombre del centro de datos virtual de proveedor que desea eliminar y haga clic en **Eliminar**.
- 4 Para confirmar, haga clic en **Aceptar**.

Editar la configuración general de un centro de datos virtual de proveedor

Puede modificar el nombre y la descripción de un centro de datos virtual de proveedor. Si el grupo de recursos de respaldo admite una versión de hardware virtual mayor, es posible actualizar al hardware virtual más alto que admite un centro de datos virtual de proveedor.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de proveedor** y, a continuación, haga clic en el nombre del centro de datos virtual de proveedor que desea modificar.
- 3 En la pestaña **Configurar > General**, en la esquina superior derecha, haga clic en **Editar**.
- 4 (opcional) Modifique el nombre y la descripción del centro de datos virtual de proveedor.
- 5 (opcional) En el menú desplegable, seleccione la versión de hardware mayor que admite este centro de datos virtual de proveedor y haga clic en **Guardar**.

La versión más alta que se puede seleccionar depende de los hosts ESXi en el grupo de recursos que respalda el centro de datos virtual de proveedor.

Nota Solo puede actualizar la versión de hardware que admite un centro de datos virtual de proveedor. No se puede cambiar la versión de hardware a una anterior.

- 6 Haga clic en **Guardar**.


Fusionar centros de datos virtuales de proveedor

Para combinar los recursos de dos centros de datos virtuales de proveedor, puede fusionar estos dos centros de datos virtuales de proveedor en uno solo.

Requisitos previos

- Los centros de datos virtuales de proveedor de destino pertenecen al mismo sitio.
- Los centros de datos virtuales de proveedor de destino contienen solo centros de datos virtuales de organización elásticos.


Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de proveedor**.
- 3 Haga clic en el botón de radio ubicado junto al nombre del centro de datos virtual de proveedor que desea expandir y, a continuación, haga clic en **Fusionar**.
- 4 Haga clic en el botón de radio junto al nombre del centro de datos virtual de proveedor con el que desea fusionar los recursos y, a continuación, haga clic en **Fusionar**.

Ver los centros de datos virtuales de organización que corresponden a un centro de datos virtual de proveedor

Puede ver una lista de los centros de datos virtuales de organización que utilizan recursos de un centro de datos virtual de proveedor.


Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de proveedor** y, a continuación, haga clic en el nombre del centro de datos virtual de proveedor de destino.
- 3 Haga clic en la pestaña **VDC de organización**.

Resultados

Se muestra la lista de los centros de datos virtuales de organización que consumen los recursos de este centro de datos virtual de proveedor. Para cada VDC de organización, la lista incluye información sobre el estado, la condición, el modelo de asignación, la organización, la instancia de vCenter Server, la cantidad de redes, la cantidad de vApps, la cantidad de políticas de almacenamiento y la cantidad de grupos de recursos.


Pasos siguientes

- Puede ir a la vista de centro de datos virtual de organización en el vCloud Director Tenant Portal haciendo clic en el icono **emergente** () que aparece junto al nombre del centro de datos virtual de organización de destino.
- Al hacer clic en el botón de radio ubicado junto al nombre de un centro de datos virtual de organización, puede realizar operaciones de administración similares a las que se describen en [Capítulo 6 Administrar centros de datos virtuales de organización](#).

Ver los almacenes de datos en un centro de datos virtual de proveedor

Puede ver detalles acerca de los almacenes de datos que proporcionan la capacidad de almacenamiento a un centro de datos virtual de proveedor.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de proveedor** y, a continuación, haga clic en el nombre del centro de datos virtual de proveedor de destino.
- 3 Haga clic en la pestaña **Almacén de datos**.

Se muestra una lista de todos los almacenes de datos en el centro de datos virtual de proveedor. La lista contiene la siguiente información para cada almacén de datos.


Título	Descripción
Nombre	El nombre del almacén de datos
Estado	Habilitado o deshabilitado

Título	Descripción
Tipo	El tipo del sistema de archivos que utiliza el almacén de datos: Virtual Machine File System (VMFS) o Network File System (NFS)
Utilizado	El espacio del almacén de datos que ocupan los archivos de máquina virtual, incluidos los archivos de log, las instantáneas y los discos virtuales. Cuando se enciende una máquina virtual, el espacio de almacenamiento utilizado incluye también los archivos de log.
Aprovisionado	El espacio de almacén de datos garantizado para las máquinas virtuales. Si alguna de las máquinas virtuales utiliza el aprovisionamiento fino, es posible que parte del espacio aprovisionado no se utilice y otras máquinas virtuales lo ocupen. Este valor puede ser mayor que la capacidad del almacén de datos real si se usa el aprovisionamiento fino.
Almacenamiento solicitado	<p>El almacenamiento aprovisionado que solo utilizan los objetos de vCloud Director en el almacén de datos, entre ellos:</p> <ul style="list-style-type: none"> ■ Máquinas virtuales aprovisionadas en vCloud Director ■ Elementos del catálogo (plantillas y medios) ■ Instancias de NSX Edge. ■ Requisitos de intercambio de memoria utilizados y sin utilizar para máquinas virtuales <p>Este valor no incluye el almacenamiento solicitado por las máquinas virtuales instantáneas o los discos intermedios en un árbol de clon vinculado.</p>
vCenter	La instancia de vCenter Server asociada con el almacén de datos.

Ver las redes externas en un centro de datos virtual de proveedor

Puede ver una lista de las redes externas a las que puede acceder un centro de datos virtual de proveedor.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de proveedor** y, a continuación, haga clic en el nombre del centro de datos virtual de proveedor de destino.
- 3 Haga clic en la pestaña **Redes externas**.

Resultados

Puede ver una lista de las redes externas disponibles con información sobre la configuración de CIDR de puerta de enlace y el uso del grupo de direcciones IP.

Administrar las políticas de almacenamiento de máquina virtual en un centro de datos virtual de proveedor

Es posible agregar, habilitar, deshabilitar y eliminar políticas de almacenamiento de máquina virtual de un centro de datos virtual de proveedor. También es posible agregar, editar y eliminar metadatos de una política de almacenamiento de máquina virtual en un centro de datos virtual de proveedor.

Agregar una política de almacenamiento de máquina virtual a un centro de datos virtual de proveedor


Puede agregar una política de almacenamiento de máquina virtual a un centro de datos virtual de proveedor. A continuación, puede configurar los centros de datos virtuales de organización que este centro de datos virtual de proveedor respalda para admitir la política de almacenamiento agregada.

Importante vCloud Director no admite políticas de almacenamiento de máquina virtual para los servicios de datos basados en host, como el cifrado y Storage I/O Control.

Requisitos previos

- El administrador de vSphere creó la política de almacenamiento de máquina virtual de destino. Para obtener información sobre la administración basada en políticas de almacenamiento (Storage Policy Based Management, SPBM), consulte la documentación de *almacenamiento de vSphere*.
- [Actualizar las políticas de almacenamiento de una instancia de vCenter Server](#).

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de proveedor** y, a continuación, haga clic en el nombre del centro de datos virtual de proveedor de destino.
- 3 En la pestaña **Políticas de almacenamiento**, haga clic en **Agregar**.
- 4 Seleccione una o varias políticas de almacenamiento que desea agregar y haga clic en **Agregar**.

Si selecciona * (**Cualquiera**), vCloud Director agregará y eliminará almacenes de datos de forma dinámica conforme se agreguen o eliminen de los clústeres de almacenes de datos del centro de datos virtual de proveedor.


Pasos siguientes

Configure centros de datos virtuales de organización respaldados por el centro de datos virtual de proveedor para admitir la directiva de almacenamiento. Consulte [Agregar una política de almacenamiento de máquina virtual a un centro de datos virtual de organización](#).

Habilitar o deshabilitar una política de almacenamiento de máquina virtual en un centro de datos virtual de proveedor

Después de deshabilitar una política de almacenamiento de máquina virtual en un centro de datos virtual de proveedor, sus centros de datos virtuales de organización ya no pueden utilizar dicha política.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de proveedor** y, a continuación, haga clic en el nombre del centro de datos virtual de proveedor de destino.
- 3 Haga clic en la pestaña **Políticas de almacenamiento**.
- 4 Haga clic en el botón de radio ubicado junto a la política de almacenamiento de máquina virtual de destino y, a continuación, haga clic en **Habilitar** o **Deshabilitar**.
- 5 Para confirmar, haga clic en **Aceptar**.


Eliminar una política de almacenamiento de máquina virtual de un centro de datos virtual de proveedor

Puede eliminar una política de almacenamiento de máquina virtual de un centro de datos virtual de proveedor.

Requisitos previos

Deshabilite la política de almacenamiento de máquina virtual de destino. Consulte [Habilitar o deshabilitar una política de almacenamiento de máquina virtual en un centro de datos virtual de proveedor](#).

Procedimiento


- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de proveedor** y, a continuación, haga clic en el nombre del centro de datos virtual de proveedor de destino.
- 3 Haga clic en la pestaña **Políticas de almacenamiento**.
- 4 Haga clic en el botón de radio ubicado junto a la política de almacenamiento de máquina virtual de destino y haga clic en **Quitar**.
- 5 Para confirmar, haga clic en **Quitar**.

Modificar los metadatos de una política de almacenamiento de máquina virtual en un centro de datos virtual de proveedor

Puede agregar, editar y eliminar metadatos de una política de almacenamiento en un centro de datos virtual de proveedor.

Si se usan metadatos de objeto, se pueden asociar pares de *name=value* definidos por el usuario con una política de almacenamiento en un centro de datos virtual de proveedor. Los metadatos de objeto también se pueden usar en expresiones de filtro de consultas de vCloud API.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de proveedor** y, a continuación, haga clic en el nombre del centro de datos virtual de proveedor de destino.
- 3 Haga clic en la pestaña **Políticas de almacenamiento**.
- 4 Haga clic en el botón de radio ubicado junto a la política de almacenamiento de máquina virtual de destino y haga clic en **Metadatos**.
- 5 Haga clic en **Editar**.
- 6 (opcional) Para agregar un par clave-valor, haga clic en **Agregar**, introduzca un nombre y un valor, y seleccione un tipo para el nuevo par clave-valor.
- 7 (opcional) Para editar un par clave-valor, introduzca un nuevo nombre y un valor, y seleccione un nuevo tipo para el par clave-valor.
- 8 (opcional) Para eliminar un par clave-valor, en el extremo derecho de la fila, haga clic en el icono **Eliminar**.
- 9 Haga clic en **Guardar** y, a continuación, haga clic en **Aceptar**.

Administrar los grupos de recursos en un centro de datos virtual de proveedor

Es posible agregar, habilitar, deshabilitar y separar grupos de recursos secundarios de un centro de datos virtual de proveedor. No se puede deshabilitar ni separar el grupo de recursos principal de un centro de datos virtual de proveedor.

Agregar un grupo de recursos a un centro de datos virtual de proveedor

Puede agregar uno o varios grupos de recursos secundarios a un centro de datos virtual de proveedor, de modo que se puedan expandir sus centros de datos virtuales de organización de pago por uso y grupo de asignaciones.


Cuando los recursos informáticos están respaldados por varios grupos de recursos, se pueden expandir para tener en cuenta a más máquinas virtuales.

Puede agregar grupos de recursos respaldados por clústeres de vSphere configurados de forma óptima para alojar instancias de NSX Edge que tengan vínculos superiores de VLAN. vCloud Director puede utilizar metadatos para indicar que el sistema debe colocar puertas de enlace Edge de VDC de organización en grupos de recursos respaldados por dichos clústeres. Para obtener más información, consulte el artículo <https://kb.vmware.com/kb/2151398> de la base de conocimientos de VMware.

Requisitos previos

El administrador de vSphere creó el grupo de recursos secundario de destino en la instancia de vCenter Server que respalda al grupo de recursos principal del centro de datos virtual de proveedor.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de proveedor** y, a continuación, haga clic en el nombre del centro de datos virtual de proveedor de destino.
- 3 En la pestaña **Grupos de recursos**, haga clic en **Agregar**.
- 4 Seleccione uno o varios grupos de recursos para agregarlos y haga clic en **Agregar**.

Resultados

vCloud Director agrega el grupo de recursos para que lo utilice un centro de datos virtual de proveedor. De este modo, se vuelven elásticos todos los centros de datos virtuales de organización de pago por uso y grupo de asignación respaldados por el centro de datos virtual de proveedor.

vCloud Director agrega también un grupo de recursos de VDC de sistema debajo del nuevo grupo de recursos. Este grupo de recursos se utiliza para crear recursos del sistema, como máquinas virtuales Edge de NSX y máquinas virtuales que actúan como plantillas para los clones vinculados.

Importante No modifique ni elimine el grupo de recursos de VDC de sistema.


Habilitar o deshabilitar un grupo de recursos en un centro de datos virtual de proveedor

Cuando se deshabilita un grupo de recursos, los recursos informáticos y de memoria del grupo dejan de estar disponibles para el centro de datos virtual de proveedor.

Los procesos que ya están en curso no dejan de usar recursos del grupo de recursos deshabilitado.

Nota No se puede deshabilitar el grupo de recursos principal en un centro de datos virtual de proveedor.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de proveedor** y, a continuación, haga clic en el nombre del centro de datos virtual de proveedor de destino.
- 3 Haga clic en la pestaña **Grupos de recursos**.
- 4 Haga clic en el botón de radio ubicado junto al grupo de recursos de destino y, a continuación, haga clic en **Habilitar** o **Deshabilitar**.
- 5 Para confirmar, haga clic en **Aceptar**.


Separar un grupo de recursos de un centro de datos virtual de proveedor

Si un centro de datos virtual de proveedor tiene varios grupos de recursos, es posible separar un grupo de recursos secundario del centro de datos virtual de proveedor. No se puede desconectar el grupo de recursos principal del centro de datos virtual de proveedor.

Requisitos previos

- Deshabilite el grupo de recursos de destino en el centro de datos virtual de proveedor. Consulte [Habilitar o deshabilitar un grupo de recursos en un centro de datos virtual de proveedor](#).
- Migre cualquier máquina virtual de ese grupo de recursos a un grupo de recursos habilitado. Para obtener información sobre la migración de máquinas virtuales entre grupos de recursos en un centro de datos virtual de proveedor, consulte *Guía del administrador de vCloud Director*.
- Vuelva a implementar cualquier red que se haya visto afectada por el grupo de recursos deshabilitado.
- Vuelva a implementar cualquier puerta de enlace Edge que se haya visto afectada por el grupo de recursos deshabilitado.

Procedimiento


- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de proveedor** y, a continuación, haga clic en el nombre del centro de datos virtual de proveedor de destino.
- 3 Haga clic en la pestaña **Grupos de recursos**.
- 4 Seleccione el botón de radio situado junto al grupo de recursos de destino y haga clic en **Separar**.
- 5 Para confirmar, haga clic en **Aceptar**.

Modificar los metadatos de un centro de datos virtual de proveedor

Es posible agregar, editar y eliminar metadatos de un centro de datos virtual de proveedor.

Mediante los metadatos de objeto, es posible asociar pares *nombre=valor* definidos por el usuario con un centro de datos virtual de proveedor. Puede utilizar metadatos de objeto en las expresiones de filtro de consulta de vCloud API.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de proveedor** y, a continuación, haga clic en el nombre del centro de datos virtual de proveedor de destino.
- 3 En la esquina superior derecha de la pestaña **Configurar > Metadatos**, haga clic en **Editar**.
- 4 (opcional) Para agregar un par clave-valor, haga clic en **Agregar**, introduzca un nombre y un valor, y seleccione un tipo para el nuevo par clave-valor.
- 5 (opcional) Para editar un par clave-valor, introduzca un nuevo nombre y un valor, y seleccione un nuevo tipo para el par clave-valor.
- 6 (opcional) Para eliminar un par clave-valor, en el extremo derecho de la fila, haga clic en el icono **Eliminar**.
- 7 Haga clic en **Guardar** y, a continuación, haga clic en **Aceptar**.

Administrar organizaciones

5

El vCloud Director Service Provider Admin Portal permite crear, configurar y administrar las organizaciones de vCloud Director.

Utilice el vCloud Director Service Provider Admin Portal para administrar organizaciones, establecer políticas para determinar el modo en el que los usuarios consumen recursos asignados a una organización, y administrar la publicación y el uso compartido de los catálogos.

Este capítulo incluye los siguientes temas:

- [Entender las concesiones](#)
- [Crear una organización](#)
- [Configurar catálogos de una organización](#)
- [Configurar las políticas de una organización](#)

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 la 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 directiva de organización que haya establecido.

Crear una organización

Puede crear una nueva organización desde el vCloud Director Service Provider Admin Portal.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
 - a En el panel de la izquierda, seleccione **Organizaciones**.

La lista de organizaciones existentes se muestra en una vista de cuadrícula.
- 2 Para crear una nueva organización, haga clic en el botón **+Agregar**.
Se abrirá el cuadro de diálogo **Nueva organización**.
- 3 Introduzca los siguientes valores.


Opción	Descripción
Nombre de la organización	El identificador único que constituye la dirección URL para acceder al portal para tenants de la organización.
Nombre completo de la organización	El nombre completo de la organización.
Descripción	Una descripción opcional de la organización.


- 4 Haga clic en el botón **Crear** para completar la creación.

Configurar catálogos de una organización

Puede configurar el modo en el que una organización comparte sus catálogos de servicios.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
 - a En el panel de la izquierda, seleccione **Organizaciones**.

La lista de organizaciones existentes se muestra en una vista de cuadrícula.
- 2 Utilice la barra de listas () que se encuentra a la izquierda de cada elemento para mostrar las acciones que se pueden realizar para cada organización.
- 3 Haga clic en **Catálogos**.
Se abrirá el cuadro de diálogo **Configuración del catálogo** de la organización.

4 Configure las siguientes opciones de uso compartido y publicación.

Opción	Descripción
Compartir	Permite a los administradores de la organización compartir los catálogos de esta organización con otras organizaciones en esta instancia de vCloud Director. Si no selecciona esta opción, los administradores de la organización podrán seguir compartiendo catálogos dentro de la organización.
Permitir publicación en catálogos externos	Permite que los administradores de la organización publiquen catálogos en organizaciones externas a esta instancia de vCloud Director.
Permitir suscripción a catálogos externos	Permite que los administradores de la organización se suscriban a catálogos externos a esta instancia de vCloud Director.



Configurar las políticas de una organización

Las concesiones, las cuotas y los límites reducen la capacidad de los usuarios de la organización de consumir recursos de almacenamiento y de procesamiento. Puede modificar estas configuraciones para evitar que los usuarios agoten o monopolicen los recursos de una organización.

Requisitos previos

Consulte [Entender las concesiones](#).

Procedimiento

- En el menú principal () , seleccione **Recursos de nube**.
 - En el panel de la izquierda, seleccione **Organizaciones**.
La lista de organizaciones existentes se muestra en una vista de cuadrícula.
- Utilice la barra de listas () que se encuentra a la izquierda de cada elemento para mostrar las acciones que se pueden realizar para cada organización.
- Haga clic en **Políticas** para editar concesiones, cuotas, límites de recursos y políticas de contraseña de la organización.
- Configure las concesiones de vApp con los siguientes ajustes.

Opción	Descripción
Concesión máxima de tiempo de ejecución	Tiempo durante el que las vApps funcionan antes de detenerse de manera automática.
Concesión máxima de almacenamiento	Tiempo durante el que las vApps detenidas están disponibles antes de limpiarse de manera automática.
Limpieza de almacenamiento	El modo en el que se procesan las vApps después de detenerlas y limpiarlas.

5 Configure las concesiones de plantilla de vApp con los siguientes ajustes.

Opción	Descripción
Concesión máxima de almacenamiento	Tiempo que las plantillas de vApp están disponibles antes de limpiarse de manera automática.
Limpieza de almacenamiento	El modo en el que se procesan las plantillas de vApp caducadas después de limpiarlas.

6 Configure las cuotas con los siguientes ajustes.

Opción	Descripción
Cuota de todas las MV	Número total de máquinas virtuales disponibles que un usuario puede almacenar en esta organización.
Cuota de MV en ejecución	Número total de máquinas virtuales que un usuario puede encender en esta organización.

7 Configure los límites con los siguientes ajustes.

Opción	Descripción
Número de operaciones intensivas en recursos por usuario	Escriba el número máximo de operaciones simultáneas que requieren un uso intensivo de los recursos por usuario o seleccione Heredar límite del sistema .
Número de operaciones intensivas en recursos para poner en cola por usuario	Escriba el número máximo de operaciones en cola que requieren un uso intensivo de los recursos por usuario o seleccione Heredar límite del sistema .
Número de operaciones intensivas en recursos por organización	Escriba el número máximo de operaciones simultáneas que requieren un uso intensivo de los recursos por organización o seleccione Heredar límite del sistema .
Número de operaciones intensivas en recursos para poner en cola por organización	Escriba el número máximo de operaciones en cola que requieren un uso intensivo de los recursos por organización o seleccione Heredar límite del sistema .
Número de conexiones simultáneas por MV	Escriba el número máximo de conexiones simultáneas de la consola por máquina virtual o seleccione Heredar límite del sistema .
Número de centros de datos virtuales por organización	Escriba el número máximo de centros de datos virtuales de organización por organización o seleccione Heredar cuota del sistema .

8 Configure las políticas de contraseña con los siguientes ajustes.

Opción	Descripción
Bloqueo de cuenta habilitado	Habilite el bloqueo de cuentas de usuario tras un número determinado de intentos de inicio de sesión no válidos.
Inicios de sesión no válidos antes del bloqueo	Número de intentos de inicio de sesión no válidos antes de que se bloquee la cuenta de usuario.
Intervalo de bloqueo de cuenta	Período durante el cual una cuenta de usuario bloqueada no puede iniciar sesión.

Administrar centros de datos virtuales de organización

6

Para proporcionar recursos a una organización, es necesario crear uno o varios centros de datos virtuales de organización para esta organización. Después de crear un centro de datos virtual de organización, es posible modificar sus propiedades, deshabilitarlo o eliminarlo, y administrar su modelo de asignación, almacenamiento y configuración de red.

Este capítulo incluye los siguientes temas:

- [Introducción a los modelos de asignación](#)
- [Entender las políticas de recursos informáticos](#)
- [Crear un centro de datos virtual de organización](#)
- [Habilitar o deshabilitar un centro de datos virtual de organización](#)
- [Eliminar un centro de datos virtual de organización](#)
- [Modificar el nombre y la descripción de un centro de datos virtual de organización](#)
- [Modificar la configuración de modelo de asignación de un centro de datos virtual de organización](#)
- [Modificar la configuración de almacenamiento de un centro de datos virtual de organización](#)
- [Editar la configuración de red de un centro de datos virtual de organización](#)
- [Modificar los metadatos de un centro de datos virtual de organización](#)
- [Ver los grupos de recursos de un centro de datos virtual de organización](#)
- [Administrar el firewall distribuido en un centro de datos virtual de organización](#)

Introducción a los modelos de asignación

Un modelo de asignación determina cómo y cuándo los recursos informáticos y de memoria del centro de datos virtual (Virtual Data Center, VDC) de proveedor asignados se confirman en el VDC de organización.

En la siguiente tabla se muestra la configuración de distribución de recursos de vSphere en el nivel del grupo de recursos o de la máquina virtual (MV) según el modelo de asignación de VDC de organización.

	Modelo de asignación Flex	Modelo de grupo de asignación elástico	Modelo de grupo de asignación no elástico	Modelo de pago por uso	Modelo de grupo de reserva
Elástico	Con base en la configuración de VDC de organización.	Sí	No	Sí	No
Velocidad de vCPU	Si un límite de CPU de máquina virtual no está definido en una política de recursos informáticos de VDC, la velocidad de vCPU podría afectar al límite de CPU de la máquina virtual dentro del VDC.	Afecta a la cantidad de vCPU en ejecución en el VDC de organización.	No aplicable	Afecta al límite de CPU de máquina virtual	No aplicable
Límite de CPU de grupo de recursos	Límite de CPU de VDC de organización prorrateado en función de la cantidad de máquinas virtuales en el grupo de recursos.	Asignación de CPU de VDC de organización	Asignación de CPU de VDC de organización	Sin límite	Asignación de CPU de VDC de organización
Reserva de CPU del grupo de recursos	La reserva de CPU del VDC de organización se prorratea en función de la cantidad de vCPU en el grupo de recursos. La reserva de CPU de VDC de organización es igual a la asignación de CPU de VDC de organización multiplicada por la garantía de CPU.	La suma de las máquinas virtuales encendidas. Es igual a la garantía de CPU multiplicada por la velocidad y el número de vCPU.	Asignación de CPU de VDC de organización multiplicada por la garantía de CPU	Ninguno, ampliable	Asignación de CPU de VDC de organización
Límite de memoria del grupo de recursos	El límite de memoria de VDC de organización se prorratea en función de la cantidad de máquinas virtuales en el grupo de recursos.	Sin límite	Asignación de RAM del VDC de organización	Sin límite	Asignación de RAM del VDC de organización
Reserva de memoria del grupo de recursos	La reserva de RAM del VDC de organización se prorratea en función de la cantidad de máquinas virtuales en el grupo de recursos. La reserva de RAM del VDC de organización es igual a la asignación de RAM del VDC de organización multiplicada por la garantía de RAM.	La suma de la garantía de RAM multiplicada por la vRAM de todas las máquinas virtuales encendidas en el grupo de recursos. La reserva de RAM del grupo de recursos es ampliable.	Asignación de RAM del VDC de organización multiplicada por la garantía de RAM	Ninguno, ampliable	Asignación de RAM del VDC de organización

	Modelo de asignación Flex	Modelo de grupo de asignación elástico	Modelo de grupo de asignación no elástico	Modelo de pago por uso	Modelo de grupo de reserva
Límite de CPU de máquina virtual	En función de la política de recursos informáticos de VDC de la máquina virtual.	Sin límite	Sin límite	Velocidad de vCPU multiplicada por la cantidad de vCPU	Personalizada
Reserva de CPU de la máquina virtual	En función de la política de recursos informáticos de VDC de la máquina virtual.	0	0	Es igual a la velocidad de la CPU multiplicada por la velocidad y la cantidad de vCPU.	Personalizada
Límite de RAM de máquina virtual	En función de la política de recursos informáticos de VDC de la máquina virtual.	Sin límite	Sin límite	vRAM	Personalizada
Reserva de RAM de máquina virtual	En función de la política de recursos informáticos de VDC de la máquina virtual.	0	Es igual a la vRAM multiplicada por la garantía de RAM y sumada a la sobrecarga de RAM.	Es igual a la vRAM multiplicada por la garantía de RAM y sumada a la sobrecarga de RAM.	Personalizada

Uso sugerido de los modelos de asignación

Cada modelo de asignación se puede utilizar para distintos niveles de control y administración del rendimiento.

La siguiente tabla contiene información sobre el uso sugerido de cada modelo de asignación.

Modelo de asignación	Uso sugerido
Modelo de asignación Flex	Con el modelo de asignación Flex, puede conseguir un control de rendimiento detallado en el nivel de cargas de trabajo. Usando el modelo de asignación Flex, los administradores del sistema de vCloud Director pueden administrar la elasticidad de VDC de organización individuales. El modelo de asignación Flex utiliza la administración de cargas de trabajo basada en políticas. Con el modelo de asignación Flex, los proveedores de nube tienen un mejor control sobre la sobrecarga de memoria en un VDC de organización y pueden hacer cumplir un uso de capacidad de ráfaga estricto de los tenants.
Modelo de asignación de grupo de asignación	Utilice el modelo de asignación de grupo de asignación para cargas de trabajo estables de larga duración, en las que los tenants se suscriben a un consumo fijo de recursos informáticos y los proveedores de nube pueden predecir y administrar la capacidad de los recursos informáticos. El modelo de asignación de grupo de asignación es ideal para cargas de trabajo con requisitos de rendimiento variados. Con el modelo de asignación de grupo de asignación, todas las cargas de trabajo comparten los recursos asignados de los grupos de recursos de vCenter Server. Independientemente de si se habilita o deshabilita la elasticidad, los tenants reciben una cantidad limitada de recursos informáticos. Con el modelo de asignación de grupo de asignación, los proveedores de nube habilitan o deshabilitan la elasticidad en el nivel del sistema y la configuración se aplica a todos los VDC de organización del grupo de asignación. Si se utiliza la asignación de grupo de asignación no elástico, el VDC de organización reserva de antemano el grupo de recursos de VDC y los tenants pueden sobreconfirmar vCPU, pero no pueden sobreconfirmar ninguna cantidad de memoria. Si se utiliza la asignación de grupo elástico, el VDC de organización no reserva de antemano ningún recurso informático y la capacidad puede abarcar varios clústeres. Los proveedores de nube administran la sobreconfirmación de recursos informáticos físicos y los tenants no pueden sobreconfirmar vCPU ni memoria.
Pago por uso	Utilice el modelo de pago por uso cuando no tenga que asignar recursos informáticos por adelantado en vCenter Server. La reserva, el límite y los recursos compartidos se aplican a cada carga de trabajo que los tenants implementan en el VDC. Con el modelo de asignación de pago por uso, cada carga de trabajo del VDC de organización recibe el mismo porcentaje de recursos informáticos configurados que se reservaron. vCloud Director considera que la velocidad de CPU de cada vCPU para cada carga de trabajo es la misma, y solo se puede definir la velocidad de CPU en el nivel del VDC de organización. Desde el punto de vista del rendimiento, debido a que no se puede cambiar la configuración de reserva de cargas de trabajo individuales, cada carga de trabajo recibe la misma preferencia. El modelo de asignación de pago por uso es ideal para los tenants que necesitan ejecutar cargas de trabajo con requisitos de rendimiento diferentes en el mismo VDC de organización. Debido a la elasticidad, el modelo de pago por uso es adecuado para cargas de trabajo genéricas de corta duración que forman parte de aplicaciones de escalado automático. Con el pago por uso, los tenants pueden hacer coincidir los picos en la demanda de recursos informáticos dentro de un VDC de organización.
Grupo de reserva	Utilice el modelo de asignación de grupo de reserva cuando necesite un control detallado sobre el rendimiento de las cargas de trabajo que se ejecutan en el VDC de organización. Desde una perspectiva de proveedor de nube , el modelo de asignación de grupo de reserva requiere una asignación por adelantado de todos los recursos informáticos en vCenter Server. El modelo de asignación de grupo de reserva no es elástico. El modelo de asignación de grupo de reserva es ideal para las cargas de trabajo que se ejecutan en hardware dedicado a un tenant específico. En tales casos, los usuarios tenant pueden administrar el uso y la sobreconfirmación de recursos informáticos.

Modelo de asignación Flex

A partir de vCloud Director 9.7, los **administradores del sistema** pueden crear centros de datos virtuales (Virtual Data Center, VDC) de organización con el modelo de asignación Flex. Con la

combinación de las políticas de recursos informáticos de VDC y asignación Flex, los **administradores del sistema** pueden controlar el consumo de CPU y de RAM tanto en el VDC como en los niveles de máquinas virtuales individuales. El modelo de asignación Flex admite todas las configuraciones de asignación disponibles en los modelos de asignación existentes.

Si crea un VDC de organización no flexible en vCloud Director 9.7, puede volver a configurar el VDC de organización para que utilice el modelo de asignación Flex. Si crea un VDC de organización con una versión de vCloud Director anterior a 9.7, no puede volver a configurar los centros de datos de la organización para utilizar el modelo de asignación Flex.

Al crear un VDC de organización flexible, los **administradores del sistema** controlan los siguientes atributos del VDC de organización:

- Habilitar o deshabilitar la función de grupo elástico
- Incluya o excluya la sobrecarga de memoria.
- Especificar una política de recursos informáticos de VDC predeterminada para el VDC de organización
- Asignación y garantía de memoria y CPU
- Cuota de red
- Perfil de almacenamiento

Como **administrador del sistema de vCloud Director**, puede configurar un VDC de organización Flex para que sea elástico o no elástico. Cuando los VDC de organización flexibles tienen habilitada la función de grupo elástico, el VDC de organización se amplía y utiliza todos los grupos de recursos asociados con su VDC de proveedor. En vCloud Director 9.7, si convierte un VDC de organización no elástico en un VDC de organización elástico, no podrá volver a convertir el mismo VDC de organización en uno no elástico.

El modelo de asignación Flex admite las capacidades de las políticas de recursos informáticos de VDC de la organización sin ninguna de las restricciones que presentan los demás modelos de asignación. En el modelo de asignación Flex, la asignación de recursos informáticos de máquina virtual depende de las políticas de recursos informáticos de VDC de organización. Si no define una política de recursos informáticos de VDC para un VDC de organización, la asignación de recursos informáticos dependerá del modelo de asignación del VDC de organización. Mediante la combinación del modelo de asignación Flex y las políticas de recursos informáticos de VDC de organización, un solo VDC de organización puede alojar máquinas virtuales que utilicen la configuración común de todos los demás modelos de asignación. Para obtener más información, consulte [Descripción de las políticas de recursos informáticos](#).

Para crear un VDC de organización flexible, puede utilizar vCloud Director Service Provider Admin Portal o vCloud API. Para obtener información acerca de vCloud API, consulte *Guía de programación de vCloud API para proveedores de servicios*.

Modelo de asignación de grupo de asignación

Con el modelo de asignación de grupo de asignación, un porcentaje de los recursos que asigne desde el centro de datos virtual (Virtual Datacenter, VDC) de proveedor se confirman en el VDC de organización. Puede especificar el porcentaje de la CPU y de la memoria. Este porcentaje se conoce como el factor de garantía de porcentaje y permite sobreasignar recursos.

A partir de vCloud Director 5.1.2, los administradores del sistema pueden configurar VDC de organización de grupo de asignación para que sean elásticos o no elásticos. La elasticidad es una configuración global que afecta a todos los VDC de organización de grupo de asignación. Para obtener información sobre la modificación de la configuración general del sistema, consulte la *Guía del administrador de vCloud Director*.

Los VDC de organización de grupo de asignación tienen habilitado un grupo de asignación elástico de forma predeterminada. Los sistemas actualizados desde vCloud Director 5.1 que tienen VDC de organización de grupo de asignación con máquinas virtuales que abarcan varios grupos de recursos tienen habilitado el grupo de asignación elástico de forma predeterminada.

Cuando los VDC de grupo de asignación tienen habilitada la función de grupo de asignación elástico, el VDC de organización se amplía y utiliza todos los grupos de recursos asociados a su VDC de proveedor. Debido a ello, la frecuencia de la vCPU es ahora un parámetro obligatorio para un grupo de asignación.

Establezca la frecuencia y el factor de garantía de porcentaje de la vCPU de manera que se puedan implementar suficientes máquinas virtuales en el VDC de organización sin que la CPU constituya un factor de cuello de botella.

Cuando se crea una máquina virtual, el motor de colocación la sitúa en el grupo de recursos de VDC de proveedor que mejor se ajusta a los requisitos de la máquina virtual. Se crea un grupo de subrecursos para este VDC de organización en el grupo de recursos de VDC de proveedor, y la máquina virtual se sitúa en ese grupo de subrecursos.

Al encender la máquina virtual, el motor de colocación comprueba el grupo de recursos de VDC de proveedor para asegurarse de que sigue teniendo capacidad para encender la máquina virtual. En caso contrario, el motor de colocación mueve la máquina virtual a un grupo de recursos de VDC de proveedor con suficientes recursos para ejecutarla. Se crea un grupo de subrecursos para el VDC de organización si no existe.

El grupo de subrecursos se configura con suficientes recursos para ejecutar la nueva máquina virtual. La reserva de memoria del grupo de subrecursos aumenta en función del tamaño de la memoria configurada de la máquina virtual por el factor de garantía de porcentaje del VDC de organización. La reserva de CPU del grupo de subrecursos aumenta en función del número de vCPU con el que se ha configurado la máquina virtual por la vCPU especificada en el nivel de VDC de organización por el factor de garantía de garantía de porcentaje de la CPU establecido en el nivel de VDC de organización. Si la función de grupo de asignación elástico está habilitada, el límite de memoria del grupo de subrecursos aumenta según el tamaño de memoria configurado de la máquina virtual, y el límite de CPU del grupo de subrecursos aumenta en

función de la cantidad de vCPU con que se ha configurado la máquina virtual por la frecuencia de vCPU especificada en el nivel de VDC de organización. La máquina virtual se configura de nuevo para establecer su memoria y reserva de CPU en cero, y el motor de colocación de máquina virtual sitúa la máquina virtual en un grupo de recursos de VDC de proveedor.

Con el modelo elástico de asignación de grupos de asignación, solo vCloud Director supervisa y administra los límites. Si se deshabilita la función elástica, el límite del grupo de recursos se establece adicionalmente.

Las ventajas del modelo de grupo de asignación son que una máquina virtual puede aprovechar los recursos de una máquina virtual inactiva en el mismo grupo de subrecursos. Este modelo puede aprovechar los nuevos recursos incorporados al VDC de proveedor.

En casos excepcionales, una máquina virtual se cambia del grupo de recursos al que se asignó en el momento de su creación a un grupo de recursos diferente durante el encendido debido a la falta de recursos en el grupo de recursos original. Este cambio puede hacer que mover los archivos de disco de máquina virtual a un nuevo grupo de recursos suponga unos costes bajos.

Cuando la función de grupo de asignación elástico está deshabilitada, el comportamiento de los VDC de organización de grupo de asignación es similar al del modelo de asignación de grupo en vCloud Director 1.5. En este modelo, la frecuencia de vCPU no se puede configurar. La sobreconfirmación se controla mediante el establecimiento del porcentaje de recursos garantizados.

De forma predeterminada, en un VDC de grupo de asignación las máquinas virtuales obtienen de la configuración del VDC los ajustes de reservas, límites y recursos compartidos. Para crear o volver a configurar una máquina virtual con una configuración de asignación de recursos personalizados para CPU y memoria, puede utilizar vCloud API. Consulte la *Guía de programación de vCloud API para proveedores de servicios*.

Modelo de asignación de pago por uso

Con el modelo de asignación de pago por uso, los recursos solo se confirman cuando los usuarios crean vApps en el VDC de organización. Puede especificar un porcentaje de los recursos para garantizar, lo que le permite sobreconfirmar recursos. Puede agregar varios grupos de recursos al VDC de proveedor para hacer que el VDC de organización de pago por uso sea flexible.

Los recursos confirmados en la organización se aplican en el nivel de máquina virtual.

Cuando se enciende una máquina virtual, si el grupo de recursos original no puede alojar la máquina virtual, el motor de colocación revisa el grupo de recursos y asigna la máquina virtual a otro grupo de recursos. Si no existe ningún grupo de subrecursos disponible para el grupo de recursos, vCloud Director crea uno con un límite infinito y una velocidad cero. La velocidad de la máquina virtual se establece en su límite multiplicado por sus recursos confirmados. El motor de colocación de máquina virtual sitúa la máquina virtual en un grupo de recursos del VDC de proveedor.

La ventaja del modelo de pago por uso es que aprovecha los nuevos recursos agregados al VDC de proveedor.

En casos excepcionales, una máquina virtual se cambia del grupo de recursos al que se asignó en el momento de su creación a un grupo de recursos diferente durante el encendido debido a la falta de recursos en el grupo de recursos original. Este cambio puede hacer que mover los archivos de disco de máquina virtual a un nuevo grupo de recursos suponga unos costes bajos.

En el modelo de pago por uso, no se reserva ningún recurso por adelantado, por lo que es posible que una máquina virtual no se encienda si no hay suficientes recursos. Las máquinas virtuales que funcionan con este modelo tampoco pueden aprovechar los recursos de las máquinas virtuales inactivas en el mismo grupo de subrecursos, puesto que los recursos se establecen en el nivel de máquina virtual.

De forma predeterminada, en un VDC de pago por uso, las máquinas virtuales obtienen sus ajustes de reservas, límites y recursos compartidos de la configuración del VDC. Para crear o volver a configurar una máquina virtual con una configuración de asignación de recursos personalizados para CPU y memoria, puede utilizar vCloud API. Consulte la *Guía de programación de vCloud API para proveedores de servicios*.

Modelo de asignación de grupo de reserva

Con el modelo de asignación de grupo de reserva, todos los recursos que se asignen se confirman inmediatamente en el VDC de organización. Para controlar la sobreconfirmación, los usuarios de la organización pueden especificar ajustes de reservas, límites y prioridades para máquinas virtuales individuales.

Dado que este modelo tiene solo un grupo de recursos y un grupo de subrecursos, el motor de colocación no reasigna un grupo de recursos de la máquina virtual cuando se enciende. La velocidad y el límite de la máquina virtual no se modifican.

Con el modelo de grupo de reserva, los recursos están disponibles siempre que se necesitan. Este modelo también ofrece un control preciso sobre la velocidad, el límite y los recursos compartidos de la máquina virtual, lo cual puede producir un uso óptimo de los recursos reservados si se realiza una planificación cuidadosa. Para obtener información sobre cómo configurar los ajustes de asignación de recursos de máquinas virtuales en VDC de grupos de reserva, consulte *Guía del usuario de vCloud Air Virtual Private Cloud OnDemand*.

En este modelo, la reserva se realiza siempre en el clúster principal. Si no existen recursos suficientes para crear un VDC de organización en el clúster principal, se produce un error en la creación del VDC de organización.

Otras limitaciones de este modelo es que no es flexible y es posible que los usuarios de la organización no configuren de forma óptima los recursos compartidos, las velocidades y los límites de las máquinas virtuales, lo cual lleva consigo una infrautilización de los recursos.

Entender las políticas de recursos informáticos

A partir de vCloud Director 9.7, puede controlar la asignación de recursos y la colocación de máquinas virtuales mediante políticas de recursos informáticos. Con base en el alcance y la función, existen dos tipos de políticas de recursos informáticos: políticas de recursos informáticos del centro de datos virtual (Virtual Data Center, VDC) de proveedor y políticas de recursos informáticos de VDC.

Política de recursos informáticos de VDC de proveedor

Una política de recursos informáticos de VDC de proveedor define reglas de afinidad entre máquinas virtuales y hosts que afectan directamente a la colocación de cargas de trabajo de tenants. Los usuarios tenant no tienen visibilidad sobre las políticas de recursos informáticos de VDC de proveedor.

El alcance de las políticas de recursos informáticos de VDC de proveedor se encuentra en el nivel de VDC de proveedor.

Política de recursos informáticos de VDC

Las políticas de recursos informáticos de VDC controlan las características de recursos informáticos de una máquina virtual en el nivel de VDC de organización. Debido a que los usuarios tenants no tienen visibilidad sobre las políticas de recursos informáticos de VDC de proveedor, si se desean exponer las reglas de afinidad entre máquinas virtuales y hosts para uso de los tenants, se debe hacer referencia a la política de recursos informáticos de VDC de proveedor dentro de la política de recursos informáticos de VDC.

Políticas de recursos informáticos de centro de datos virtual de proveedor

Usando las políticas de recursos informáticos de centro de datos virtual (VDC) de proveedor, los **administradores del sistema** de vCloud Director pueden exponer grupos de máquinas virtuales y grupos de máquinas virtuales lógicas a los tenants.

Las políticas de recursos informáticos de VDC de proveedor pueden contener una recopilación de los siguientes elementos:

- Grupos de máquinas virtuales que contienen máquinas virtuales similares. Cada grupo de máquinas virtuales pertenece a un clúster diferente.
- Grupos de máquinas virtuales lógicas que son adecuadas para diversas funcionalidades.
- Grupos de máquinas virtuales y grupos de máquinas virtuales lógicas.

Políticas de recursos informáticos de VDC de proveedor y grupos de máquinas virtuales lógicas

Los **administradores del sistema** pueden exponer reglas de afinidad entre máquinas virtuales y hosts de Distributed Resource Scheduler (DRS) de vSphere a los tenants mediante grupos de máquinas virtuales y grupos de máquinas virtuales lógicas. Las reglas de afinidad entre máquinas virtuales y hosts de DRS se exponen en el nivel de proveedor en vCloud Director como grupos de máquinas virtuales. Las reglas de afinidad entre máquinas virtuales y hosts se enlazan a un clúster específico. Debido a que los VDC de proveedor elásticos se pueden expandir a varios clústeres de vSphere, los grupos de máquinas virtuales lógicas proporcionan una abstracción de reglas de afinidad entre máquinas virtuales y hosts de DRS que funciona en varios clústeres mediante la agrupación de grupos de máquinas virtuales enlazados al clúster que son lógicamente equivalentes. Para administrar grupos de máquinas virtuales lógicas, utilice vCloud OpenAPI. Para obtener información sobre vCloud OpenAPI, consulte *Primeros pasos con vCloud OpenAPI* en <https://code.vmware.com>.

Para exponer las reglas de afinidad entre máquinas virtuales y hosts, agregue grupos de máquinas virtuales y grupos de máquinas virtuales lógicas a una política de recursos informáticos de VDC de proveedor y cree una referencia entre la política de recursos informáticos de VDC de proveedor y una política de recursos informáticos de VDC.

En el contexto de la política de recursos informáticos de VDC de proveedor, los grupos de máquinas virtuales lógicas tienen una relación AND entre ellos.

Con las políticas de recursos informáticos de VDC de proveedor y los grupos de máquinas virtuales lógicas, los **administradores del sistema de vCloud Director** pueden exponer varios grupos de máquinas virtuales a usuarios tenant dentro de un VDC de organización. Por ejemplo, considere un entorno que contenga dos clústeres: *clúster1* y *clúster2*. En *clúster1* reside el host *SQL_host_1*, mientras que en *clúster2* residen los hosts *SQL_fast_host* y *Fast_host*.

1 En *cluster1*, se crean *SQL_host_group1* y *VM_group1*.

Se crea una afinidad positiva entre *VM_group1* y *SQL_host_group1*.

2 En *clúster2*, se crean cuatro grupos.

- Se crean *SQL_host_group2* y *VM_group2*.

Se crea una afinidad positiva entre *VM_group2* y *SQL_host_group2*.

- Se crean *fast_host_group* y *VM_group3*.

Se crea una afinidad positiva entre *VM_group3* y *fast_host_group*.

Se crea *PVDC_compute_policy1* que se compone de *logical_VM_group1* y *logical_VM_group2*. El elemento *logical_VM_group1* consta de *VM_group1* y *VM_group2*. El elemento *logical_VM_group2* consta de *VM_group3*.

Se crea y publica la política de recursos informáticos de VDC *SQL_and_fast* en un VDC de organización y se agrega una referencia a *PVDC_compute_policy1*. Al crear una referencia entre la política de recursos informáticos de VDC *SQL_and_fast* y el elemento *PVDC_compute_policy1*, se expone la información de los grupos de máquinas virtuales lógicas y los grupos de máquinas virtuales a los usuarios tenant dentro del VDC de organización. Como resultado, cuando un tenant aplica la política de recursos informáticos de VDC *SQL_and_fast* a una máquina virtual, el motor de colocación agrega la máquina virtual al elemento *SQL_fast_host* en *cluster2*.

El flujo de trabajo es el siguiente.

- 1 El **administrador de vCenter Server** crea grupos de hosts mediante vSphere Client.
Para obtener información, consulte el tema *Crear un grupo de DRS de host (MSCS)* en la *Documentación de VMware vSphere ESXi y vCenter Server*.
- 2 El **administrador de vCenter Server** o el **administrador del sistema de vCloud Director** crea grupos de máquinas virtuales.
Para obtener información, consulte el tema *Crear o actualizar un grupo de máquinas virtuales* en la *Guía del administrador de vCloud Director*.
- 3 El **administrador del sistema de vCloud Director** crea las reglas de afinidad adecuadas entre los grupos de máquinas virtuales y los grupos de hosts.
Para obtener información, consulte *Administrar reglas de afinidad de máquina virtual-host* en la *Guía del administrador de vCloud Director*.
- 4 El **administrador del sistema de vCloud Director** agrupa de forma lógica los grupos de máquinas virtuales equivalentes en grupos de máquinas virtuales lógicas mediante vCloud OpenAPI.
- 5 El **administrador del sistema de vCloud Director** crea una política de recursos informáticos de VDC de proveedor y agrega los grupos de máquinas virtuales lógicas mediante vCloud OpenAPI.
- 6 El **administrador del sistema de vCloud Director** crea una política de recursos informáticos de VDC que hace referencia a la política de recursos informáticos de VDC de proveedor y publica la política de recursos informáticos de VDC en un VDC de organización mediante vCloud OpenAPI.

Cuando un tenant crea una máquina virtual en el VDC de organización y selecciona la política de recursos informáticos de VDC, vCloud Director agrega la máquina virtual al grupo de máquinas virtuales al que se hace referencia en la política de recursos informáticos de VDC. Como resultado, vCloud Director crea la máquina virtual en el host adecuado.

Políticas de recursos informáticos de VDC de proveedor y grupos de máquinas virtuales

Una política de recursos informáticos de VDC de proveedor puede tener un grupo de máquinas virtuales de cada clúster o ninguno. Por ejemplo, la política de recursos informáticos de VDC de proveedor *oracle_license* puede estar compuesta de los grupos de máquinas virtuales *oracle_license1* y *oracle_license2*, donde el grupo de máquinas virtuales *oracle_license1* pertenece al clúster *oracle_cluster1* y el grupo de máquinas virtuales *oracle_license2* pertenece al clúster *oracle_cluster2*.

Cuando se asigna una política de recursos informáticos de VDC de proveedor a una máquina virtual, el motor de colocación agrega esta máquina virtual al grupo de máquinas virtuales correspondiente del clúster en el que reside. Por ejemplo, si se decide implementar una máquina virtual en el clúster *oracle_cluster1* y asignar la política de recursos informáticos de VDC de proveedor *oracle_license* a esta máquina virtual, el motor de colocación agregará la máquina virtual al grupo de máquinas virtuales *oracle_license1*.

El flujo de trabajo es el siguiente.

- 1 El **administrador del sistema** crea una o varias políticas de recursos informáticos de VDC de proveedor mediante vCloud OpenAPI.
- 2 El **administrador del sistema** crea una o varias políticas de recursos informáticos de VDC mediante vCloud OpenAPI.

Una política de recursos informáticos de VDC puede asociarse a ninguna o una política de recursos informáticos de VDC de proveedor. Las políticas de recursos informáticos de VDC tienen nombres y políticas de recursos informáticos de VDC de proveedor únicos.

- 3 El **administrador del sistema** publica la política de recursos informáticos de VDC en uno o varios VDC de organización mediante vCloud OpenAPI.

Los tenants solo pueden ver las políticas de recursos informáticos de VDC que se publican en los VDC de organización. Las políticas de recursos informáticos de VDC de proveedor no están disponibles en el nivel de tenant.

- 4 Los tenants pueden utilizar vCloud API o el portal para tenants de vCloud Director para asignar una política de recursos informáticos de VDC de organización a una máquina virtual al crear o actualizar una máquina virtual.

Inicialmente, el sistema no contiene ninguna política de recursos informáticos de VDC de proveedor, y cada VDC de organización solo contiene una política de recursos informáticos predeterminada, que no está asociada a una política de recursos informáticos de VDC de proveedor.

Para crear y administrar políticas de recursos informáticos de VDC globales y de proveedor, debe utilizar vCloud OpenAPI. Consulte *Primeros pasos con vCloud OpenAPI* en <https://code.vmware.com>.

Políticas de recursos informáticos del centro de datos virtual

Las políticas de recursos informáticos del centro de datos virtual (Virtual Data Center, VDC) controlan la asignación de recursos informáticos físicos para las cargas de trabajo de los tenants. Para asignar recursos físicos en función de requisitos de carga de trabajo específicos, los usuarios tenant pueden seleccionar políticas de recursos informáticos de VDC predeterminadas o personalizadas.

Una política de recursos informáticos de VDC agrupa atributos que definen la asignación de recursos informáticos para las máquinas virtuales dentro de un VDC de organización. La asignación de recursos informáticos incluye las reservas, los límites, los recursos compartidos y la asignación de CPU y de memoria.

Los **administradores del sistema** de vCloud Director crean y administran políticas de recursos informáticos a nivel global y pueden publicar políticas de recursos informáticos individuales en uno o varios VDC de organización. Cuando se publica una política de recursos informáticos de VDC en un VDC de organización, la política pasa a estar disponible para los usuarios de la organización. Al crear y administrar máquinas virtuales en el VDC de organización, los **administradores de tenants** pueden asignar las políticas de recursos informáticos de VDC disponibles a las máquinas virtuales. Los usuarios y los **administradores de tenants** del VDC de organización no pueden consultar la configuración específica de una política de recursos informáticos de VDC.

Gracias a las políticas de recursos informáticos de VDC, los proveedores de nube pueden definir perfiles de consumo de memoria y CPU con nombre que los tenants pueden asociar a las máquinas virtuales dentro de un VDC de organización. El uso de políticas de recursos informáticos de VDC es un mecanismo para que los proveedores de nube definan y ofrezcan niveles diferenciados de servicio (por ejemplo, un perfil de uso intensivo de CPU o un perfil de uso elevado de memoria). Gracias a las políticas de recursos informáticos de VDC, los proveedores de nube también pueden limitar o restringir el consumo de CPU y memoria de las máquinas virtuales de un VDC de organización.

Gracias a las políticas de recursos informáticos de VDC, los administradores del sistema de vCloud Director pueden controlar los siguientes aspectos del consumo de recursos informáticos en el nivel de máquina virtual:

- Cantidad de vCPU y velocidad de reloj de vCPU
- Cantidad de memoria asignada a la máquina virtual
- Reserva, límite y recursos compartidos de memoria y CPU

Atributos de las políticas de recursos informáticos del centro de datos virtual

Al crear una política de recursos informáticos del centro de datos virtual (VDC), puede especificar un subconjunto de todos los atributos disponibles. El único atributo obligatorio es el nombre de la política de recursos informáticos de VDC.

En la siguiente tabla se enumeran todos los atributos que puede definir en una política de recursos informáticos de VDC.

Tabla 6-1. Atributos de políticas de recursos informáticos de VDC

Atributo de política de recursos informáticos de VDC	Parámetro de API	Descripción
Name	name	Parámetro obligatorio que se utiliza como identificador de la política de recursos informáticos de VDC.
Description	description	Representa una breve descripción de la política de recursos informáticos de VDC.
vCPU Speed	cpuSpeed	Define la velocidad de vCPU de una máquina virtual (MV) en MHz.
Memory	memory	Define la memoria configurada para una máquina virtual en MB. Cuando un tenant asigna la política de recursos informáticos de VDC a una máquina virtual, esta recibe la cantidad de memoria que se define mediante este atributo.
Number of vCPUs	cpuCount	Define el número de vCPU que se configuran para una máquina virtual. Cuando un tenant asigna la política de recursos informáticos de VDC a una máquina virtual, esta recibe la cantidad de vCPU que se define mediante este atributo.
Cores per Socket	coresPerSocket	La cantidad de núcleos por socket para una máquina virtual. La cantidad de vCPU que se define en la política de recursos informáticos de VDC debe ser divisible por el número de núcleos por socket. Si la cantidad de vCPU no es divisible por el número de núcleos por socket, la cantidad de núcleos por socket deja de ser válida.
Memory Reservation Guarantee	memoryReservationGuarantee	Define la cantidad reservada de memoria configurada para una máquina virtual. El valor del atributo puede ser 0 o 1. Si el valor de la garantía de reserva de memoria es 0, no se define ninguna garantía de memoria. Si el valor es uno, se define el 100% de memoria reservada.
CPU Reservation Guarantee	cpuReservationGuarantee	Define cuántos de los recursos de CPU de una máquina virtual están reservados. La CPU asignada para una máquina virtual es igual a la cantidad de vCPU multiplicada por la velocidad de vCPU en MHz. El valor del atributo puede ser 0 o 1. Si el valor de la garantía de reserva de CPU es 0, no se define ninguna reserva de CPU. El valor 1 define el 100% de CPU reservada.
CPU Limit	cpuLimit	Define el límite de CPU en MHz para una máquina virtual. Si el valor es menos uno (-1), no se define ningún límite de CPU. Si no se define en la política de recursos informáticos de VDC, el límite de CPU es igual a la CPU asignada para la máquina virtual.
Memory Limit	memoryLimit	Define el límite de memoria en MB para una máquina virtual. El valor menos uno (-1) define que no hay límite de memoria. Si no se define en la política de recursos informáticos de VDC, el límite de memoria es igual a la memoria asignada para la máquina virtual.
CPU Shares	cpuShares	Define la cantidad de recursos compartidos de CPU para una máquina virtual. Si no se define en la política de recursos informáticos de VDC, se aplican recursos compartidos normales a la máquina virtual.
Memory Shares	memoryShares	Define la cantidad de recursos compartidos de memoria para una máquina virtual. Si no se define en la política de recursos informáticos de VDC, se aplican recursos compartidos normales a la máquina virtual.

Tabla 6-1. Atributos de políticas de recursos informáticos de VDC (continuación)

Atributo de política de recursos informáticos de VDC	Parámetro de API	Descripción
Extra Configurations	extraConfigs	Representa una asignación entre pares de clave y valor que se aplican como valores de configuración adicionales en una máquina virtual.
Provider VDC Compute Policy	pvmcComputePolicy	Define la referencia de la política de recursos informáticos de VDC a una política de recursos informáticos de VDC de proveedor.

Trabajo con políticas de recursos informáticos del centro de datos virtual

vCloud Director genera una política de recursos informáticos predeterminada para todos los centros de datos virtuales (VDC). La política de recursos informáticos de VDC predeterminada solo contiene un nombre y una descripción. Todos los atributos restantes de esta política están vacíos.

Asimismo, puede definir otra política de recursos informáticos de VDC como política predeterminada para un VDC de organización. La política de recursos informáticos de VDC predeterminada controla la asignación y el consumo de recursos de las máquinas virtuales (MV) que los tenants crean en el VDC de organización, a menos que un tenant asigne otra política específica de recursos informáticos de VDC a la máquina virtual.

Para limitar el número máximo de recursos informáticos que los tenants pueden asignar a las máquinas virtuales individuales dentro de un VDC de organización, los proveedores de nube pueden definir una política máxima de recursos informáticos de VDC. Cuando se la asigna a un VDC de organización, la política máxima de recursos informáticos de VDC actúa como un límite superior para la configuración de recursos informáticos en todas las máquinas virtuales dentro del VDC de organización. La política máxima de recursos informáticos de VDC no está disponible para los usuarios tenant al crear una máquina virtual. Cuando se define una política de recursos informáticos de VDC como la política máxima de recursos informáticos de VDC, vCloud Director copia internamente el contenido de la política y utiliza el contenido copiado como política máxima de recursos informáticos de VDC. Como consecuencia, el VDC de organización no depende de la política de recursos informáticos de VDC utilizada inicialmente.

Si publica varias políticas de recursos informáticos de VDC en un VDC de organización, los usuarios tenant pueden seleccionar de entre todas las políticas personalizadas y la política predeterminada al crear y administrar máquinas virtuales en el VDC de organización.

Estas son las operaciones de políticas de recursos informáticos de VDC disponibles para los proveedores de nube:

- Crear una política de recursos informáticos de VDC.
- Publicar una política de recursos informáticos de VDC en uno o varios VDC de organización.
- Cancelar la publicación de una política de recursos informáticos de VDC de un VDC de organización.

- Eliminar una política de recursos informáticos de VDC.

Los usuarios que tengan el derecho **ORG_VDC_MANAGE_COMPUTE_POLICIES** pueden crear, actualizar y publicar políticas de recursos informáticos de VDC. Para crear políticas de recursos informáticos de VDC, debe utilizar vCloud API.

En la siguiente tabla se enumeran las operaciones de políticas de recursos informáticos de VDC disponibles para los usuarios tenant.

Tabla 6-2. Operaciones de políticas de recursos informáticos de VDC para usuarios tenant

Operación	Descripción
Asigne una política de recursos informáticos de VDC a una máquina virtual durante la creación de una máquina virtual.	Los usuarios tenant que están autorizados para crear máquinas virtuales en un VDC de organización de manera opcional pueden asignar políticas de recursos informáticos de VDC a las máquinas virtuales. Como resultado, los parámetros definidos en la política de recursos informáticos de VDC controlan el consumo de memoria y CPU de la máquina virtual. La asignación de una política de recursos informáticos de VDC no es un requisito para los tenants durante la creación de una máquina virtual. Si un tenant no selecciona de manera explícita una política de recursos informáticos de VDC para asignarla a una máquina virtual, la política de VDC predeterminada se aplica a la máquina virtual. Los usuarios tenant pueden asignar una política de recursos informáticos de VDC a una máquina virtual durante la creación de una máquina virtual mediante el portal para tenants de vCloud Director.
Asigne una política de recursos informáticos de VDC a una máquina virtual existente.	Los usuarios tenant que están autorizados para administrar máquinas virtuales en un VDC de organización pueden actualizar la asociación entre una máquina virtual y una política de recursos informáticos de VDC. Como resultado, el sistema vuelve a configurar la máquina virtual para que consuma los recursos informáticos que se especifican en la nueva política de recursos informáticos de VDC. Los usuarios tenant pueden asignar una política de recursos informáticos de VDC a la máquina virtual existente mediante el portal para tenants de vCloud Director.

Mediante las políticas de recursos informáticos de VDC, los proveedores de nube pueden restringir el consumo de recursos informáticos para todas las máquinas virtuales dentro de un VDC de organización a, por ejemplo, tres tamaños predefinidos (como *tamaño pequeño*, *tamaño mediano* y *tamaño grande*). El flujo de trabajo es el siguiente.

- 1 Un **administrador del sistema** crea tres políticas de recursos informáticos de VDC con los siguientes atributos:

Nombre	Atributos
Tamaño pequeño	<ul style="list-style-type: none"> ■ Descripción: política de máquina virtual de tamaño pequeño ■ Nombre: Tamaño pequeño ■ Memoria: 1024 ■ Cantidad de vCPU: 1
Tamaño mediano	<ul style="list-style-type: none"> ■ Descripción: política de máquina virtual de tamaño mediano ■ Nombre: Tamaño mediano ■ Memoria: 2048 ■ Cantidad de vCPU: 2
Tamaño grande	<ul style="list-style-type: none"> ■ Descripción: política de máquina virtual de tamaño grande ■ Nombre: Tamaño grande ■ Memoria: 4096 ■ Cantidad de vCPU: 4

- 2 Publique las nuevas políticas de recursos informáticos de VDC en un VDC de organización.

La publicación de una política de recursos informáticos de VDC en un VDC de organización pone la política a disposición de los usuarios tenant en el VDC de organización.

- 3 Como alternativa, defina una de las políticas de recursos informáticos de VDC como una política de VDC predeterminada para el VDC de organización.

Si define una política predeterminada para el VDC de organización y si los usuarios tenant no especifican otra política durante la creación de una máquina virtual, la política predeterminada se aplica a la máquina virtual.

Para ver y modificar las políticas de recursos informáticos de VDC, debe utilizar vCloud API.


Crear un centro de datos virtual de organización

Para asignar recursos a una organización, es necesario crear un centro de datos virtual de organización. Un centro de datos virtual de organización obtiene sus recursos de un centro de datos virtual de proveedor. Una organización puede tener varios centros de datos virtuales de organización.

Requisitos previos

Cree un centro de datos virtual de proveedor. Consulte la *Guía del administrador de vCloud Director*.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de organización** y, a continuación, en **Nuevo**.
- 3 Introduzca un nombre y, si lo desea, una descripción para el nuevo centro de datos virtual de organización.
- 4 (opcional) Para deshabilitar el nuevo centro de datos virtual de organización después de la creación, desactive el botón de alternancia **Habilitar el VDC de organización**.

Los usuarios no pueden implementar vApps en un centro de datos virtual de organización deshabilitado.

- 5 Haga clic en **Siguiente**.
- 6 Seleccione el botón de radio junto al nombre de la organización a la que desea agregar este centro de datos virtual y haga clic en **Siguiente**.
- 7 Seleccione el botón de radio junto al nombre del centro de datos virtual de proveedor desde el cual el centro de datos virtual de organización debe obtener recursos informáticos y de almacenamiento, y haga clic en **Siguiente**.

La lista de centros de datos virtuales de proveedor muestra todos los centros de datos virtuales de proveedor habilitados en el sitio con información sobre los recursos disponibles. La lista de redes muestra información sobre las redes disponibles para el centro de datos virtual de proveedor seleccionado.

- 8 Seleccione un modelo de asignación para este centro de datos virtual de organización y haga clic en **Siguiente**.

Opción	Descripción
Grupo de asignación	Un porcentaje de los recursos que asigne desde el centro de datos virtual de proveedor se confirman en el centro de datos virtual de organización. Puede especificar el porcentaje de la CPU y de la memoria.
Pago por uso	Los recursos solo se confirman cuando los usuarios crean vApps en el centro de datos virtual de organización.
Grupo de reserva	Todos los recursos que asigne se confirmarán inmediatamente en el centro de datos virtual de organización.
Flex	Puede controlar el consumo de recursos tanto en el VDC como en los niveles de máquinas virtuales individuales. El modelo de asignación Flex admite las capacidades de las políticas de recursos informáticos de VDC de organización. El modelo de asignación Flex admite todas las configuraciones de asignación disponibles en los otros modelos de asignación.

- 9 Configure las opciones de asignación para el modelo de asignación que seleccionó y haga clic en **Siguiente**.

Opción	Descripción	Modelo de asignación
Elasticidad	Habilite o deshabilite la función de grupo elástico. Un VDC de organización elástico abarca y utiliza todos los grupos de recursos asociados con su VDC de proveedor.	Flex
Incluir sobrecarga de memoria de máquina virtual	Incluya o excluya la sobrecarga de memoria.	Flex
Asignación de CPU	La cantidad máxima de CPU que desea asignar a las máquinas virtuales que se ejecutan en este centro de datos virtual de organización.	<ul style="list-style-type: none"> ■ Grupo de asignación ■ Grupo de reserva ■ Flex
Permitir que los recursos de CPU aumenten por encima de	Para proporcionar recursos de CPU ilimitados a este centro de datos virtual de organización, active este botón de alternancia.	Grupo de reserva
Cuota de CPU	La cantidad máxima de consumo de CPU para este centro de datos virtual de organización.	<ul style="list-style-type: none"> ■ Pago por uso ■ Flex
Recursos de CPU garantizados	<p>El porcentaje de recursos de CPU que desea garantizar a una máquina virtual que se ejecuta en este centro de datos virtual de organización. Puede garantizar menos del 100% para controlar la sobreasignación de recursos de CPU.</p> <p>En el caso de un modelo de asignación de grupo de asignación, la garantía de porcentaje también determina el porcentaje de asignación de CPU que se confirma para este centro de datos virtual de organización.</p>	<ul style="list-style-type: none"> ■ Grupo de asignación ■ Pago por uso ■ Flex
Velocidad de vCPU	La velocidad de la vCPU. Se asigna esta cantidad de GHz por vCPU a las máquinas virtuales que se ejecutan en el centro de datos virtual de organización.	<ul style="list-style-type: none"> ■ Pago por uso ■ Flex
Asignación de memoria	La cantidad máxima de memoria que desea asignar a las máquinas virtuales que se ejecutan en el centro de datos virtual de organización.	<ul style="list-style-type: none"> ■ Grupo de asignación ■ Grupo de reserva
Cuota de memoria	La cantidad máxima de consumo de memoria para este centro de datos virtual de organización.	<ul style="list-style-type: none"> ■ Pago por uso ■ Flex
Recursos de memoria garantizados	<p>El porcentaje de recursos de memoria que desea garantizar a las máquinas virtuales que se ejecutan en el centro de datos virtual de organización. Puede sobreasignar recursos garantizando menos del 100%.</p> <p>En el caso de un modelo de asignación de grupo de asignación, la garantía de porcentaje también determina el porcentaje de asignación de memoria que se confirma para este centro de datos virtual de organización.</p>	<ul style="list-style-type: none"> ■ Grupo de asignación ■ Pago por uso ■ Flex
Cantidad máxima de máquinas virtuales	La cantidad máxima de máquinas virtuales que pueden existir en el centro de datos virtual de organización.	<ul style="list-style-type: none"> ■ Grupo de asignación ■ Pago por uso ■ Grupo de reserva ■ Flex

- 10** Configure las opciones de almacenamiento para este centro de datos virtual de organización y haga clic en **Siguiente**.

La lista contiene las políticas de almacenamiento habilitadas en el centro de datos virtual de proveedor de origen.

- a Active las casillas de verificación de las políticas de almacenamiento que desea agregar a este centro de datos virtual de organización.
- b (opcional) Para limitar la cantidad de capacidad de almacenamiento asignada a una política de almacenamiento seleccionada, seleccione **Limitado** en el menú desplegable de la celda **Tipo de asignación** e introduzca la capacidad máxima en la celda **Almacenamiento asignado**.

- c (opcional) Para cambiar la política de almacenamiento predeterminada, en el menú desplegable **Política de creación de instancias predeterminada**, seleccione la política de almacenamiento predeterminada de destino.

vCloud Director utiliza la política de almacenamiento predeterminada para todas las operaciones de aprovisionamiento de máquinas virtuales cuando no se ha especificado una política de almacenamiento a nivel de plantilla de vApp o máquina virtual.

- d (opcional) Para habilitar el aprovisionamiento fino de las máquinas virtuales en el centro de datos virtual de organización, active el botón de alternancia **Aprovisionamiento fino**.
- e (opcional) Para deshabilitar el aprovisionamiento fino de las máquinas virtuales en el centro de datos virtual de organización, desactive el botón de alternancia **Aprovisionamiento rápido**.

- 11** Configure las opciones de grupos de redes para este centro de datos virtual de organización y haga clic en **Siguiente**.

vCloud Director utiliza el grupo de redes para crear redes de vApp y redes internas de centros de datos virtuales de organización.

- Para omitir la adición de un grupo de redes en esta etapa, desactive el botón de alternancia **Usar grupo de redes**.
- Para configurar un grupo de redes, seleccione el botón de radio junto al nombre del grupo de redes de destino e introduzca la cuota para este centro de datos virtual de organización.


La cuota es la cantidad máxima de redes aprovisionadas en el centro de datos virtual de organización que respalda este grupo de redes. No debe superar el número de redes disponibles para el grupo de redes seleccionado.

- 12** Revise la página **Listo para completar** y haga clic en **Finalizar**.

Habilitar o deshabilitar un centro de datos virtual de organización

Para evitar que vApps y máquinas virtuales adicionales utilicen recursos informáticos y de almacenamiento de un centro de datos virtual de organización, se puede deshabilitar este centro de datos virtual de organización. Las vApp en ejecución y las máquinas virtuales encendidas se continúan ejecutando, pero no puede crear ni iniciar vApp ni máquinas virtuales adicionales.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de organización**.
- 3 Seleccione el botón de radio junto al nombre del centro de datos virtual de organización de destino y, a continuación, haga clic en **Habilitar** o **Deshabilitar**.
- 4 Para confirmar, haga clic en **Aceptar**.

Eliminar un centro de datos virtual de organización


Para eliminar todos los recursos de un centro de datos virtual de organización de una organización, es posible eliminar este centro de datos virtual de organización. Los recursos permanecerán invariables en el centro de datos virtual de proveedor de origen.

Importante Esta operación elimina de forma permanente el centro de datos virtual de organización y todas sus máquinas virtuales, vApps, redes de centros de datos virtuales de organización y puertas de enlace Edge.

Requisitos previos

Si desea conservar ciertas máquinas virtuales, vApps, plantillas de vApp o archivos de medios que pertenecen al centro de datos virtual de organización de destino, mueva estos elementos a otro centro de datos virtual de organización.

Procedimiento


- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de organización**.
- 3 Seleccione el botón de radio ubicado junto al nombre del centro de datos virtual de organización que desea eliminar y haga clic en **Eliminar**.
- 4 Si este centro de datos virtual de organización contiene algún recurso, como máquinas virtuales, vApps, redes de centros de datos virtuales de organización y puertas de enlace Edge, seleccione la casilla de verificación de cada tipo de recurso para confirmar su eliminación.

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

Modificar el nombre y la descripción de un centro de datos virtual de organización

A medida que se expande la instalación de vCloud Director, se recomienda asignar una descripción o un nombre más significativo a un centro de datos virtual de organización existente.

Procedimiento


- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de organización** y, a continuación, haga clic en el nombre del centro de datos virtual de organización de destino.
- 3 En la pestaña **General**, en la esquina superior derecha, haga clic en **Editar**.
- 4 Introduzca un nombre y una descripción nuevos, y haga clic en **Guardar**.

Modificar la configuración de modelo de asignación de un centro de datos virtual de organización

No puede cambiar el modelo de asignación de un centro de datos virtual de organización, pero puede cambiar algunos de los ajustes del modelo de asignación especificados durante la creación del centro de datos virtual de organización.

Puede modificar la configuración de asignación para el modelo de asignación que configuró durante la creación del centro de datos virtual de organización. Consulte [Paso 9](#).

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de organización** y, a continuación, haga clic en el nombre del centro de datos virtual de organización de destino.
- 3 En la pestaña **Asignación**, en la esquina superior derecha, haga clic en **Editar**.
- 4 Edite la configuración del modelo de asignación y haga clic en **Guardar**.


Modificar la configuración de almacenamiento de un centro de datos virtual de organización

Es posible modificar la configuración de almacenamiento que se configuró durante la creación del centro de datos virtual de organización.

Modificar la configuración de aprovisionamiento de máquinas virtuales de un centro de datos virtual de la organización

Puede modificar la configuración de aprovisionamiento fino y aprovisionamiento rápido de máquinas virtuales que estableció al crear el centro de datos virtual de la organización.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de organización** y, a continuación, haga clic en el nombre del centro de datos virtual de organización de destino.
- 3 En la esquina superior derecha de la pestaña **Almacenamiento**, haga clic en **Editar**.
- 4 (opcional) Modifique la configuración de aprovisionamiento fino.
 - Para deshabilitar el aprovisionamiento fino de máquinas virtuales en el centro de datos virtual de la organización, desactive el botón de alternancia **Aprovisionamiento fino**.
 - Para habilitar el aprovisionamiento fino de máquinas virtuales en el centro de datos virtual de la organización, active el botón de alternancia **Aprovisionamiento fino**.
- 5 (opcional) Modifique la configuración de aprovisionamiento rápido.
 - Para habilitar el aprovisionamiento rápido de máquinas virtuales en el centro de datos virtual de la organización, active el botón de alternancia **Aprovisionamiento rápido**.
 - Para deshabilitar el aprovisionamiento fino de las máquinas virtuales en el centro de datos virtual de organización, desactive el botón de alternancia **Aprovisionamiento rápido**.
- 6 Haga clic en **Editar**.


Agregar una política de almacenamiento de máquina virtual a un centro de datos virtual de organización

Puede configurar un centro de datos virtual de organización para que admita una política de almacenamiento de máquina virtual que haya agregado previamente al centro de datos virtual del proveedor de respaldo.

Requisitos previos

Agregó la política de almacenamiento de máquina virtual de destino al centro de datos virtual de proveedor de origen. Consulte [Agregar una política de almacenamiento de máquina virtual a un centro de datos virtual de proveedor](#).

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de organización** y, a continuación, haga clic en el nombre del centro de datos virtual de organización de destino.

- 3 Haga clic en la pestaña **Almacenamiento** y, a continuación, en **Agregar**.

Puede ver una lista de las políticas de almacenamiento adicionales disponibles en el centro de datos virtual de proveedor de origen.

- 4 Active las casillas de verificación de las políticas de almacenamiento que desea agregar y haga clic en **Agregar**.

Cambiar la política de almacenamiento predeterminada en un centro de datos virtual de organización


Es posible cambiar la política de almacenamiento predeterminada que se configuró durante la creación de un centro de datos virtual de organización.

vCloud Director utiliza la política de almacenamiento predeterminada para todas las operaciones de aprovisionamiento de máquinas virtuales cuando no se ha especificado una política de almacenamiento a nivel de plantilla de vApp o máquina virtual.

Requisitos previos

- Se agregó la política de almacenamiento predeterminada de destino al centro de datos virtual de organización. Consulte [Agregar una política de almacenamiento de máquina virtual a un centro de datos virtual de organización](#).
- Se habilitó la política de almacenamiento predeterminada de destino en el centro de datos virtual de organización. Consulte [Habilitar o deshabilitar una política de almacenamiento en un centro de datos virtual de organización](#).

Procedimiento


- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de organización** y, a continuación, haga clic en el nombre del centro de datos virtual de organización de destino.
- 3 Haga clic en la pestaña **Almacenamiento**.
- 4 Haga clic en el botón de radio junto al nombre de la política de almacenamiento predeterminada de destino y haga clic en **Establecer como predeterminado**.
- 5 Para confirmar, haga clic en **Aceptar**.

Editar el límite de una política de almacenamiento en un centro de datos virtual de organización

Es posible cambiar el límite de la capacidad de almacenamiento asignada que se configuró para una política de almacenamiento durante la creación de un centro de datos virtual de organización.

Se puede establecer la capacidad de almacenamiento asignada como sin límite o configurar una cantidad máxima de capacidad de almacenamiento asignada para una política de almacenamiento en un centro de datos virtual de organización.

Procedimiento


- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de organización** y, a continuación, haga clic en el nombre del centro de datos virtual de organización de destino.
- 3 Haga clic en la pestaña **Almacenamiento**.
- 4 Haga clic en el botón de radio junto al nombre de la política de almacenamiento de destino y haga clic en **Editar límite**.
- 5 Configure la opción de límite para esta política de almacenamiento.
 - Para establecer un límite, seleccione el botón de radio superior e introduzca la cantidad máxima de recursos de almacenamiento para esta política de almacenamiento en este centro de datos virtual de organización.
 - Para no establecer ningún límite, seleccione el botón de radio **Sin límite**.
- 6 Haga clic en **Editar**.

Modificar los metadatos de una política de almacenamiento de máquina virtual en un centro de datos virtual de organización

Es posible agregar, editar y eliminar metadatos de una política de almacenamiento en un centro de datos virtual de organización.

Mediante los metadatos de objeto, es posible asociar pares *name=va lue* definidos por el usuario con una política de almacenamiento en un centro de datos virtual de organización. Puede utilizar metadatos de objeto en las expresiones de filtro de consulta de vCloud API.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de organización** y, a continuación, haga clic en el nombre del centro de datos virtual de organización de destino.
- 3 Haga clic en la pestaña **Almacenamiento**.
- 4 Haga clic en el botón de radio junto al nombre de la política de almacenamiento de destino y haga clic en **Metadatos**.
- 5 Haga clic en **Editar**.
- 6 (opcional) Para agregar un par clave-valor, haga clic en **Agregar**, introduzca un nombre y un valor, y seleccione un tipo para el nuevo par clave-valor.
- 7 (opcional) Para editar un par clave-valor, introduzca un nuevo nombre y un valor, y seleccione un nuevo tipo para el par clave-valor.
- 8 (opcional) Para eliminar un par clave-valor, en el extremo derecho de la fila, haga clic en el icono **Eliminar**.

9 Haga clic en **Guardar** y, a continuación, haga clic en **Aceptar**.

Habilitar o deshabilitar una política de almacenamiento en un centro de datos virtual de organización


Para evitar que vApps y máquinas virtuales adicionales utilicen una política de almacenamiento en un centro de datos virtual de organización, se puede deshabilitar esta política de almacenamiento en el centro de datos virtual de organización. Las vApps en ejecución y las máquinas virtuales encendidas se siguen ejecutando, pero no se pueden crear ni iniciar vApps ni máquinas virtuales adicionales en esta política de almacenamiento.

No se puede deshabilitar la política de almacenamiento predeterminada.

Requisitos previos

Si desea deshabilitar la política de almacenamiento predeterminada, [Cambiar la política de almacenamiento predeterminada en un centro de datos virtual de organización](#).

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de organización** y, a continuación, haga clic en el nombre del centro de datos virtual de organización de destino.
- 3 Haga clic en la pestaña **Almacenamiento**.
- 4 Haga clic en el botón de radio junto a la política de almacenamiento de destino y, a continuación, haga clic en **Habilitar** o **Deshabilitar**.
- 5 Para confirmar, haga clic en **Aceptar**.


Eliminar una política de almacenamiento de un centro de datos virtual de organización

Para evitar que un centro de datos virtual de organización use una política de almacenamiento, es posible eliminar esta política del centro de datos virtual de organización. Las vApps en ejecución y las máquinas virtuales encendidas se siguen ejecutando, pero no se pueden crear ni iniciar vApps ni máquinas virtuales adicionales en esta política de almacenamiento.

Requisitos previos

Deshabilite la política de almacenamiento que desea eliminar. Consulte [Habilitar o deshabilitar una política de almacenamiento en un centro de datos virtual de organización](#).

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de organización** y, a continuación, haga clic en el nombre del centro de datos virtual de organización de destino.

- 3 Haga clic en la pestaña **Almacenamiento**.
- 4 Haga clic en el botón de radio junto al nombre de la política de almacenamiento de destino y haga clic en **Quitar**.
- 5 Para confirmar, haga clic en **Quitar**.

Editar la configuración de red de un centro de datos virtual de organización

Es posible cambiar el grupo de redes desde el cual se aprovisionan las redes nuevas en un centro de datos virtual de organización. También puede habilitar centros de datos virtuales de organización de modo que sean elegibles para Cross VDC Networking.


Un grupo de redes es un grupo de redes no diferenciadas que puede utilizar para crear redes de vApp, redes de VDC de organización enrutadas y redes de VDC de organización internas. Puede cambiar el grupo de redes para las redes nuevas. Las redes existentes continúan usando los grupos de redes anteriores.

Con centros de datos virtuales de organización que están habilitados para Cross VDC Networking, los usuarios de la organización con derechos pertinentes pueden crear grupos de centros de datos y redes de capa 2 extendidas en estos grupos.

Requisitos previos

Si desea habilitar Cross-VDC Networking para un centro de datos virtual de organización, compruebe que configuró Cross-vCenter NSX en el centro de datos virtual de proveedor de respaldo.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de organización** y, a continuación, haga clic en el nombre del centro de datos virtual de organización de destino.
- 3 En la pestaña **Grupo de redes**, en la esquina superior derecha, haga clic en **Editar**.
Puede ver el número de redes que utiliza este centro de datos virtual de organización.
- 4 (opcional) Configure los ajustes del grupo de redes para este centro de datos virtual de organización.
 - Si no desea un grupo de redes para este centro de datos virtual de organización, desactive el botón de alternancia **Usar grupo de redes**.
 - Si desea configurar un grupo de redes para este centro de datos virtual de organización, siga estos pasos:
 - a Active el botón de alternancia **Usar grupo de redes**.

Puede ver una lista de los grupos de redes disponibles con información sobre su uso, las redes disponibles y su capacidad.

- b Seleccione el botón de radio ubicado junto al nombre del grupo de recursos de destino.
- c Configure la cuota para este grupo de redes en este centro de datos virtual de organización.

La cuota es la cantidad máxima de redes aprovisionadas. No debe superar el número de redes disponibles para el grupo de redes seleccionado.

- 5 Si desea habilitar Cross VDC Networking para este centro de datos virtual de organización, active el botón de alternancia **Cross VDC Networking**.

- 6 Haga clic en **Guardar**.

Resultados


En el portal para tenants de vCloud Director, los centros de datos virtuales que se habilitaron para Cross VDC Networking aparecen en la lista de centros de datos para crear un grupo de centros de datos. Para obtener información sobre cómo crear grupos de centros de datos, consulte la *Guía del portal para tenants de vCloud Director*.

Modificar los metadatos de un centro de datos virtual de organización

Es posible agregar, editar y eliminar metadatos de un centro de datos virtual de organización.

Mediante los metadatos de objeto, es posible asociar pares *nombre=valor* definidos por el usuario con un centro de datos virtual de organización. Puede utilizar metadatos de objeto en las expresiones de filtro de consulta de vCloud API.

Procedimiento


- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de organización** y, a continuación, haga clic en el nombre del centro de datos virtual de organización de destino.
- 3 Haga clic en la pestaña **Metadatos**.
- 4 Haga clic en **Editar**.
- 5 (opcional) Para agregar un par clave-valor, haga clic en **Agregar**, introduzca un nombre y un valor, y seleccione un tipo para el nuevo par clave-valor.
- 6 (opcional) Para editar un par clave-valor, introduzca un nuevo nombre y un valor, y seleccione un nuevo tipo para el par clave-valor.
- 7 (opcional) Para eliminar un par clave-valor, en el extremo derecho de la fila, haga clic en el icono **Eliminar**.

8 Haga clic en **Guardar** y, a continuación, haga clic en **Aceptar**.

Ver los grupos de recursos de un centro de datos virtual de organización

Puede ver una lista de los grupos de recursos de vCenter Server que utiliza un centro de datos virtual de organización.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de organización** y, a continuación, haga clic en el nombre del centro de datos virtual de organización de destino.
- 3 Haga clic en la pestaña **Grupos de recursos**.

Resultados

Puede ver una tabla con los grupos de recursos que utiliza el centro de datos virtual de organización, así como la instancia de vCenter Server a la que pertenece cada grupo de recursos.

Administrar el firewall distribuido en un centro de datos virtual de organización

Para proporcionar seguridad de red de capa 2 y capa 3 en un centro de datos virtual de organización, es posible habilitar y crear reglas para el firewall distribuido en este centro de datos virtual de organización. Con las reglas de firewall distribuido, se puede proteger el tráfico que se transmite entre las máquinas virtuales de un centro de datos virtual de organización.

vCloud Director admite servicios de firewall distribuido en centros de datos virtuales de organización respaldados por NSX Data Center for vSphere.

Para crear las reglas de firewall distribuido, puede utilizar diversos grupos de seguridad y objetos de agrupamiento. Consulte [Objetos de agrupamiento personalizados](#) y [Trabajar con grupos de seguridad](#).


Para obtener información sobre la protección del tráfico hacia y desde una puerta de enlace Edge, consulte [Administrar un firewall de puerta de enlace Edge](#).

Habilitar el firewall distribuido en un centro de datos virtual de organización

Para poder administrar la configuración de firewall distribuido en un centro de datos virtual de organización, primero es necesario habilitar el firewall distribuido en este centro de datos virtual de organización.

vCloud Director admite servicios de firewall distribuido en centros de datos virtuales de organización respaldados por NSX Data Center for vSphere.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de organización**.
- 3 Haga clic en el botón de radio junto al nombre del centro de datos virtual de organización de destino y, a continuación, haga clic en **Administrar firewall**.
- 4 En la pestaña **Firewall distribuido > General**, active el botón de alternancia **Habilitar firewall distribuido**.

Resultados

Se mostrarán las reglas de firewall distribuido predeterminadas, las que permiten que todo el tráfico de capa 3 y capa 2 pase por el centro de datos virtual de organización.

- En la pestaña **Firewall distribuido > General**, se puede ver la regla de firewall distribuido predeterminada para el tráfico de capa 3, denominada regla Permitir predeterminada.
- En la pestaña **Firewall distribuido > Ethernet**, se puede ver la regla de firewall distribuido predeterminada para el tráfico de capa 2, denominada regla Permitir 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](#)
- 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 el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de organización**.

- 3 Haga clic en el botón de radio junto al nombre del centro de datos virtual de organización de destino y, a continuación, haga clic en **Administrar firewall**.

- 4 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**.

- 5 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.

- 6 Haga clic en la celda **Nombre** y escriba un nombre.
- 7 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 General . Escriba el valor de origen que desea utilizar. Los valores válidos son direcciones IP, CIDR, un rango de direcciones IP o la palabra clave cualquiera . 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"> ■ Utilice la ventana Seleccionar objetos para agregar objetos que coincidan con los elementos seleccionados y haga clic en Conservar para agregarlos a la regla. ■ Para excluir un origen de la regla, agréguelo a esta regla mediante la ventana Seleccionar objetos y, a continuación, seleccione el icono para habilitar o deshabilitar la exclusión para excluir dicho origen de esta regla. <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 Seleccionar objetos.</p>

8 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 General . Escriba el valor de destino que desea utilizar. Los valores válidos son direcciones IP, CIDR, un rango de direcciones IP o la palabra clave cualquiera . 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"> ■ Utilice la ventana Seleccionar objetos para agregar objetos que coincidan con los elementos seleccionados y haga clic en Conservar para agregarlos a la regla. ■ Para excluir un origen de la regla, agréguelo a esta regla mediante la ventana Seleccionar objetos y, a continuación, seleccione el icono para habilitar o deshabilitar la exclusión para excluir dicho origen de esta regla. <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 Seleccionar objetos.</p>

9 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"> a Seleccione el protocolo de servicio. b Escriba los números de puerto de los puertos de origen y destino (o especifique cualquiera), y haga clic en Conservar.
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"> a Seleccione uno o varios objetos, y añádalos al filtro. b Haga clic en Conservar.

10 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.

11 En la celda **Dirección** de la nueva regla, determine si la regla se aplica al tráfico entrante, al tráfico saliente o a ambos.

12 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**.

- 13 Seleccione la celda **Aplicado a** y use el icono **+** para definir el alcance de objetos al que se aplica esta regla.

Nota 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.


- 14 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 el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de organización**.
- 3 Haga clic en el botón de radio junto al nombre del centro de datos virtual de organización de destino y, a continuación, haga clic en **Administrar firewall**.
- 4 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.
- 5 Haga clic en **Guardar cambios**.

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**. Para abrir esta página, debe desplazarse hasta la configuración de firewall distribuido del VDC de organización o la configuración de servicios de una puerta de enlace Edge que pertenezca al VDC de organización.


Procedimiento

- 1 Abra la página **Objetos de agrupamiento**.

Opción	Acción
Desde la configuración de firewall distribuido del VDC de organización	<ol style="list-style-type: none"> a En el menú principal () , seleccione Recursos de nube. b En el panel izquierdo, haga clic en VDC de organización. c Seleccione el botón de radio junto al nombre del centro de datos virtual de organización de destino y, a continuación, haga clic en Administrar firewall. d Haga clic en la pestaña Objetos de agrupamiento.
Desde la configuración de servicios de una puerta de enlace Edge en el VDC de organización	<ol style="list-style-type: none"> a En el menú principal () , seleccione Recursos de nube. b En el panel izquierdo, haga clic en Puertas de enlace Edge. c Seleccione el botón de radio junto al nombre de una puerta de enlace Edge que pertenece al centro de datos virtual de organización de destino y haga clic en Servicios. d Haga clic en la pestaña Objetos de agrupamiento.

- 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 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, se usa la página **Objetos de agrupamiento**. Para abrir esta página, debe desplazarse hasta la configuración del firewall distribuido del VDC de organización, o bien a la configuración de servicios de una puerta de enlace Edge que pertenezca al VDC de organización.


Procedimiento

- 1 Abra la página **Objetos de agrupamiento**.

Opción	Acción
Desde la configuración de firewall distribuido del VDC de organización	<ol style="list-style-type: none"> a En el menú principal () , seleccione Recursos de nube. b En el panel izquierdo, haga clic en VDC de organización. c Seleccione el botón de radio junto al nombre del centro de datos virtual de organización de destino y, a continuación, haga clic en Administrar firewall. d Haga clic en la pestaña Objetos de agrupamiento.
Desde la configuración de servicios de una puerta de enlace Edge en el VDC de organización	<ol style="list-style-type: none"> a En el menú principal () , seleccione Recursos de nube. b En el panel izquierdo, haga clic en Puertas de enlace Edge. c Seleccione el botón de radio junto al nombre de una puerta de enlace Edge que pertenece al centro de datos virtual de organización de destino y haga clic en Servicios. d Haga clic en la pestaña Objetos de agrupamiento.

- 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 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 mediante la página **Objetos de agrupamiento**. Para abrir esta página, debe desplazarse hasta la configuración del firewall distribuido del VDC de organización, o bien a la configuración de servicios de una puerta de enlace Edge que pertenezca al VDC de organización.

Procedimiento

- 1 Abra la página **Objetos de agrupamiento**.

Opción	Acción
Desde la configuración de firewall distribuido del VDC de organización	<ol style="list-style-type: none"> a En el menú principal () , seleccione Recursos de nube. b En el panel izquierdo, haga clic en VDC de organización. c Seleccione el botón de radio junto al nombre del centro de datos virtual de organización de destino y, a continuación, haga clic en Administrar firewall. d Haga clic en la pestaña Objetos de agrupamiento.
Desde la configuración de servicios de una puerta de enlace Edge en el VDC de organización	<ol style="list-style-type: none"> a En el menú principal () , seleccione Recursos de nube. b En el panel izquierdo, haga clic en Puertas de enlace Edge. c Seleccione el botón de radio junto al nombre de una puerta de enlace Edge que pertenece al centro de datos virtual de organización de destino y haga clic en Servicios. d Haga clic en la pestaña Objetos de agrupamiento.

- 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 mediante la página **Objetos de agrupamiento**. Para abrir esta página, debe desplazarse hasta la configuración del firewall distribuido del VDC de organización, o bien a la configuración de servicios de una puerta de enlace Edge que pertenezca al VDC de organización.

Procedimiento

1 Abra la página **Objetos de agrupamiento**.

Opción	Acción
Desde la configuración de firewall distribuido del VDC de organización	<ul style="list-style-type: none"> a En el menú principal () , seleccione Recursos de nube. b En el panel izquierdo, haga clic en VDC de organización. c Seleccione el botón de radio junto al nombre del centro de datos virtual de organización de destino y, a continuación, haga clic en Administrar firewall. d Haga clic en la pestaña Objetos de agrupamiento.
Desde la configuración de servicios de una puerta de enlace Edge en el VDC de organización	<ul style="list-style-type: none"> a En el menú principal () , seleccione Recursos de nube. b En el panel izquierdo, haga clic en Puertas de enlace Edge. c Seleccione el botón de radio junto al nombre de una puerta de enlace Edge que pertenece al centro de datos virtual de organización de destino y haga clic en Servicios. d Haga clic en la pestaña Objetos de agrupamiento.

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.

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 En el menú principal () , seleccione **Recursos de nube**.


- 2 En el panel izquierdo, haga clic en **VDC de organización**.
- 3 Haga clic en el botón de radio junto al nombre del centro de datos virtual de organización de destino y, a continuación, haga clic en **Administrar firewall**.
- 4 Haga clic en la pestaña **Objetos de agrupamiento > Grupos de seguridad**.

- 5 Haga clic en el botón **Crear** ().

- 6 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.

- 7 (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**.

- 8 (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.

- 9 (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.

- 10 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 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de organización**.
- 3 Haga clic en el botón de radio junto al nombre del centro de datos virtual de organización de destino y, a continuación, haga clic en **Administrar firewall**.
- 4 Haga clic en la pestaña **Objetos de agrupamiento > Grupos de seguridad**.
- 5 Seleccione el grupo de seguridad que desea editar.
Debajo de la lista de grupos de seguridad se muestran los detalles del grupo de seguridad.
- 6 (opcional) Edite el nombre y la descripción del grupo de seguridad.
- 7 (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**.
- 8 (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**.
- 9 (opcional) Para eliminar un conjunto de miembros dinámicos, haga clic en el icono **Eliminar** () que aparece junto al conjunto de miembros que desee borrar.

- 10** (opcional) Para editar la lista de miembros incluidos, haga clic en el icono **Editar** () que aparece junto a la lista Incluir miembros.
- 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**.
 - 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.
 - 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.
- 11** (opcional) Para editar la lista de miembros excluidos, haga clic en el icono **Editar** () que aparece junto a la lista Excluir miembros.
- 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**.
 - 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.
 - 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.
- 12** 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

- En el menú principal () , seleccione **Recursos de nube**.
- En el panel izquierdo, haga clic en **VDC de organización**.
- Haga clic en el botón de radio junto al nombre del centro de datos virtual de organización de destino y, a continuación, haga clic en **Administrar firewall**.
- Haga clic en la pestaña **Objetos de agrupamiento > Grupos de seguridad**.
- Seleccione el grupo de seguridad que desea eliminar.
- Haga clic en el botón **Eliminar** () .
- Para confirmar la eliminación, haga clic en **Aceptar**.

Resultados

Se eliminará el grupo de seguridad.

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 el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de organización**.
- 3 Haga clic en el botón de radio junto al nombre del centro de datos virtual de organización de destino y, a continuación, haga clic en **Administrar firewall**.
- 4 Haga clic en la pestaña **Etiquetas de seguridad**.
- 5 Haga clic en el botón **Crear** () e introduzca un nombre para la etiqueta de seguridad.
- 6 (opcional) Escriba una descripción para la etiqueta de seguridad.

- 7 (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.

- 8 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 el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de organización**.
- 3 Haga clic en el botón de radio junto al nombre del centro de datos virtual de organización de destino y, a continuación, haga clic en **Administrar firewall**.
- 4 Haga clic en la pestaña **Etiquetas de seguridad**.
- 5 En la lista de etiquetas de seguridad, seleccione la etiqueta de seguridad que desea editar y haga clic en el botón **Editar** ().

- 6 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.

- 7 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.

- 8 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 el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de organización**.
- 3 Haga clic en el botón de radio junto al nombre del centro de datos virtual de organización de destino y, a continuación, haga clic en **Administrar firewall**.
- 4 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**.

5 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 el menú principal () , seleccione **Recursos de nube**.
- 2** En el panel izquierdo, haga clic en **VDC de organización**.
- 3** Haga clic en el botón de radio junto al nombre del centro de datos virtual de organización de destino y, a continuación, haga clic en **Administrar firewall**.
- 4** Haga clic en la pestaña **Etiquetas de seguridad**.
- 5** En la lista de etiquetas de seguridad, seleccione la etiqueta de seguridad que desea editar.
- 6** Haga clic en el botón **Editar** () .
- 7** Edite el nombre y la descripción de la etiqueta de seguridad.
- 8** Asigne la etiqueta a las máquinas virtuales que seleccione o elimine la asignación de estas.
- 9** 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 el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de organización**.
- 3 Haga clic en el botón de radio junto al nombre del centro de datos virtual de organización de destino y, a continuación, haga clic en **Administrar firewall**.
- 4 Haga clic en la pestaña **Etiquetas de seguridad**.
- 5 En la lista de etiquetas de seguridad, seleccione la etiqueta de seguridad que desea eliminar.
- 6 Haga clic en el botón **Eliminar** () .
- 7 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](#).

Administrar puertas de enlace Edge

7

Las puertas de enlace Edge proporcionan una red de centros de datos virtuales de organización enrutada con conectividad a redes externas. Además, pueden brindar servicios, como el equilibrio de carga, la traducción de direcciones de red y un firewall. vCloud Director es compatible con puertas de enlace Edge IPv4 e IPv6.

Las puertas de enlace Edge requieren NSX Data Center for vSphere. Para obtener información, consulte la *Guía de administración de NSX*.

A partir de vCloud Director 9.7, la carga de trabajo de recursos informáticos y la carga de trabajo de redes se aíslan mediante diferentes grupos de recursos y políticas de almacenamiento de vSphere. Las puertas de enlace Edge residen en los clústeres de Edge que se deben crear previamente. Consulte [Trabajar con clústeres de Edge](#).

Puede migrar las puertas de enlace Edge heredadas a los clústeres de Edge correspondientes si vuelve a implementar estas puertas de enlace Edge. Consulte [Volver a implementar una puerta de enlace Edge](#).

Importante A partir de la versión 9.7, vCloud Director solo admite puertas de enlace Edge avanzadas. Debe convertir todas las puertas de enlace Edge no avanzadas heredadas en puertas de enlace avanzadas. Consulte <https://kb.vmware.com/kb/66767>.

Este capítulo incluye los siguientes temas:

- [Trabajar con clústeres de Edge](#)
- [Agregar una puerta de enlace Edge](#)
- [Configurar servicios de puerta de enlace Edge](#)
- [Ver el uso de redes y las asignaciones de IP en una puerta de enlace Edge](#)
- [Editar propiedades de puerta de enlace Edge](#)
- [Volver a implementar una puerta de enlace Edge](#)
- [Eliminar una puerta de enlace Edge](#)
- [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 clústeres de Edge

Para aislar las cargas de trabajo de recursos informáticos de las cargas de trabajo de redes, vCloud Director 9.7 introduce el objeto de clúster de Edge. Un clúster de Edge consta de una política de almacenamiento y un grupo de recursos de vSphere que se utilizan solo para puertas de enlace Edge de VDC de organización. Los centros de datos virtuales de proveedor no pueden utilizar recursos dedicados a los clústeres Edge, y los clústeres de Edge no pueden utilizar recursos dedicados a centros de datos virtuales de proveedor.

Los clústeres de Edge proporcionan un dominio de difusión de capa 2 dedicado, que reduce la proliferación de VLAN y garantiza la seguridad y el aislamiento de la red. Por ejemplo, el clúster de Edge puede contener VLAN adicionales para el emparejamiento con enrutadores físicos.

Puede crear cualquier cantidad de clústeres de Edge. Puede asignar un clúster de Edge a un VDC de organización como un clúster de Edge principal o secundario.

- El clúster de Edge principal de un VDC de organización se utiliza para el dispositivo Edge principal de una puerta de enlace Edge de VDC de organización.
- El clúster de Edge secundario de un VDC de organización se utiliza para el dispositivo Edge en espera cuando una puerta de enlace Edge está en modo de HA.

Diferentes VDC de organización pueden compartir clústeres de Edge o pueden tener sus propios clústeres de Edge dedicados.

Con la versión vCloud Director 9.7, el proceso anterior de uso de metadatos para controlar la colocación de puertas de enlace Edge quedó obsoleto. Consulte <https://kb.vmware.com/kb/2151398>.

Puede migrar las puertas de enlace Edge heredadas a los clústeres de Edge creados recientemente si vuelve a implementar estas puertas de enlace Edge. Consulte [Volver a implementar una puerta de enlace Edge](#).

Preparar el entorno para un clúster de Edge

- 1 En vSphere, cree el grupo de recursos para el clúster de Edge de destino.

Si un centro de datos virtual de organización utiliza un grupo de redes VLAN, el grupo de redes VLAN y el clúster de Edge para este centro de datos virtual de organización deben residir en el mismo conmutador distribuido de vSphere.
- 2 Si un centro de datos virtual de organización utiliza un grupo de redes VXLAN, en NSX, agregue el clúster de Edge a la zona de transporte VXLAN y, posteriormente, sincronice el grupo de redes VXLAN en vCloud Director.
- 3 En vSphere, cree el perfil de almacenamiento del clúster de Edge.

Crear y administrar clústeres de Edge

Después de preparar el entorno, para crear y administrar clústeres de Edge, es necesario usar los métodos `EdgeClusters` de vCloud OpenAPI. Consulte *Introducción a vCloud OpenAPI* en <https://code.vmware.com>.

Para ver clústeres de Edge, se requiere el derecho **Vista de clústeres de Edge**. Para crear, actualizar y eliminar clústeres de Edge, se requiere el derecho **Administración de clústeres de Edge**.

Al crear un clúster de Edge, debe especificar el nombre, el grupo de recursos de vSphere y el nombre del perfil de almacenamiento.

Después de crear un clúster de Edge, puede modificar su nombre y su descripción. Después de eliminar o mover las puertas de enlace Edge que contiene, puede eliminar el clúster de Edge.

Asignar un clúster de Edge a un VDC de organización

Después de crear un clúster de Edge, puede asignarlo a un VDC de organización si actualiza el perfil de red del VDC de organización. Puede asignar un clúster de Edge a un VDC de organización como un clúster de Edge principal o secundario.

Si no asigna un clúster de Edge secundario, el dispositivo Edge en espera de una puerta de enlace Edge en el modo de HA se implementa en el clúster de Edge principal, pero en un host diferente del que ejecuta el dispositivo Edge principal.

Para actualizar, ver y eliminar perfiles de red de VDC de organización, es necesario usar los métodos `VdcNetworkProfile` de vCloud OpenAPI. Consulte *Introducción a vCloud OpenAPI* en <https://code.vmware.com>.

Consideraciones:

- Los clústeres de Edge principal y secundario deben residir en el mismo conmutador distribuido de vSphere.
- Si el VDC de organización utiliza un grupo de redes VXLAN, la zona de transporte NSX debe expandir los recursos informáticos y los clústeres de Edge.
- Si el VDC de organización utiliza un grupo de redes VLAN, los clústeres de Edge y los clústeres de recursos informáticos deben estar en el mismo conmutador distribuido de vSphere.

Si vuelve a actualizar el clúster de Edge principal o secundario de un VDC de organización, para mover una puerta de enlace Edge existente al nuevo clúster, debe volver a implementar esta puerta de enlace Edge. Consulte [Volver a implementar una puerta de enlace Edge](#).

Agregar una puerta de enlace Edge

Las puertas de enlace Edge proporcionan una red de centros de datos virtuales de organización con enrutamiento y conectividad a redes externas y pueden suministrar servicios, como el equilibrio de carga, la traducción de direcciones de red y un firewall.

A partir de vCloud Director 9.7, las puertas de enlace Edge se implementan en los clústeres de Edge que se crearon y se asignaron previamente al centro de datos virtual de organización.


Puede agregar una puerta de enlace Edge IPv4 o IPv6 que se conecta a una o varias redes externas.

Nota Las puertas de enlace Edge IPv6 admiten servicios limitados. Las puertas de enlace Edge IPv6 admiten firewalls de Edge, firewalls distribuidos y enrutamiento estático.

Requisitos previos

- Para obtener información sobre los requisitos del sistema para implementar una puerta de enlace Edge, consulte *Guía de administración de NSX*.
- Si desea implementar la puerta de enlace Edge en un clúster de Edge dedicado, cree y asigne un clúster de Edge al centro de datos virtual de organización. Consulte [Trabajar con clústeres de Edge](#).

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **Puertas de enlace Edge** y, a continuación, haga clic en **Nueva**.
- 3 Haga clic en el botón de radio ubicado junto al nombre del centro de datos virtual de organización en el que desea crear la puerta de enlace Edge y, a continuación, haga clic en **Siguiente**.
- 4 Introduzca un nombre y, si lo desea, una descripción para la nueva puerta de enlace Edge.
- 5 Active o deje desactivados cada uno de estos ajustes generales de la puerta de enlace Edge.

Configuración general	Descripción
Enrutamiento distribuido	Configura la puerta de enlace Edge para que proporcione enrutamiento lógico distribuido.
Modo FIPS	Configura la puerta de enlace Edge para que use el modo FIPS de NSX.
Alta disponibilidad	Habilita la conmutación por error automática a una puerta de enlace Edge de respaldo.

- 6 Seleccione la configuración de la puerta de enlace Edge para los recursos del sistema y haga clic en **Siguiente**.

Opción	Descripción
Compacta	Requiere menos memoria y recursos informáticos.
Grande	Proporciona una capacidad y un rendimiento mayores que los que se obtienen con la opción Compacta. Las configuraciones Grande y Extragrande proporcionan funciones de seguridad idénticas.

Opción	Descripción
Extragrande	Se utiliza para entornos que tienen un equilibrador de carga con un gran número de sesiones simultáneas.
Cuádruple	Se utiliza para entornos de alto rendimiento. Requiere una alta velocidad de conexión.

- 7 Seleccione una o varias subredes de las redes externas a las que se puede conectar la puerta de enlace Edge y haga clic en **Siguiente**.

Si asignó un clúster de Edge al VDC de organización, la lista que se muestra contiene las redes externas a las que puede acceder este clúster de Edge.

- 8 (opcional) Configure una red como puerta de enlace predeterminada.
 - a Active el botón de alternancia **Configurar puerta de enlace predeterminada**.
 - b Seleccione el botón de radio ubicado junto al nombre de la red externa de destino y seleccione el botón de radio ubicado junto a la dirección IP de destino.
 - c (opcional) Active el botón de alternancia **Utilizar la puerta de enlace predeterminada para retransmisión de DNS**.

- 9 Haga clic en **Siguiente**.

- 10 Active o deje desactivados cada uno de estos ajustes avanzados de la puerta de enlace Edge y haga clic en **Siguiente**.

Configuración avanzada	Descripción
Configuración de IP	Puede especificar manualmente una dirección IP para cada subred de la puerta de enlace Edge.
Subasignar grupos de IP	Puede subasignar varios grupos de direcciones IP estáticas de los grupos de direcciones IP disponibles de cada red externa en la puerta de enlace Edge.
Límites de velocidad	Puede configurar los límites de velocidad de entrada y salida de cada red externa de la puerta de enlace Edge.

- 11** (opcional) Si habilitó una o varias opciones de configuración avanzada en el [Paso Paso 10](#), configure cada opción habilitada.

Configuración avanzada	Pasos
Configuración de IP	<p>Para cada red de la puerta de enlace Edge, en la celda Direcciones IP, introduzca una dirección IP y haga clic en Siguiente.</p> <p>Si no introduce una dirección IP para una red, el sistema asignará una dirección IP arbitraria a esta red.</p>
Subasignar grupos de IP	<ol style="list-style-type: none"> Haga clic en el botón de radio ubicado junto al nombre de una red externa y haga clic en Editar. Puede ver los grupos de direcciones IP disponibles para esta red externa y los grupos de IP subasignados actuales, si están configurados. Edite los grupos de IP subasignados para esta red externa y haga clic en Guardar. Puede agregar rangos y direcciones IP a partir de los rangos de los grupos de direcciones IP disponibles. Haga clic en Guardar. El sistema combina rangos de direcciones IP que se superponen. Haga clic en Siguiente. <p>Nota La asignación de direcciones IP a una puerta de enlace Edge es un proceso en el que el proveedor asigna la propiedad de las direcciones IP a la puerta de enlace. vCloud Director configura automáticamente la interfaz de puerta de enlace adecuada con las direcciones secundarias durante el proceso de asignación. Si alguna de las direcciones IP se utiliza fuera de vCloud Director, esto puede provocar conflictos de direcciones IP.</p>
Límites de velocidad	<p>Para cada red externa de la puerta de enlace Edge, active el botón de alternancia Habilitar, introduzca los límites en las celdas Velocidad de entrada y Velocidad de salida, y haga clic en Siguiente.</p>

- 12** Revise la página **Listo para completar** y haga clic en **Finalizar**.

Configurar servicios de puerta de enlace Edge

Es posible configurar servicios, como DHCP, firewall, traducción de direcciones de red (Network Address Translation, NAT) y VPN en una puerta de enlace Edge.

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 el firewall distribuido en un centro de datos virtual de organización](#).

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.


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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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 cualquiera. 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"> ■ Utilice la ventana Seleccionar objetos para agregar objetos que coincidan con los elementos seleccionados y haga clic en Conservar para agregarlos a la regla. ■ Para excluir un origen de la regla, agréguelo a esta regla mediante la ventana Seleccionar objetos y, a continuación, seleccione el icono para habilitar o deshabilitar la exclusión para excluir dicho origen de esta regla. <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 Seleccionar objetos.</p>

- 6 Haga clic en la celda **Destino** y realice una de las siguientes acciones:

Opción	Descripción
Hacer clic en el icono IP	<p>Escriba el valor de destino que desea utilizar. Los valores válidos son direcciones IP, CIDR, un rango de direcciones IP o la palabra clave cualquiera. 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"> ■ Utilice la ventana Seleccionar objetos para agregar objetos que coincidan con los elementos seleccionados y haga clic en Conservar para agregarlos a la regla. ■ Para excluir un origen de la regla, agréguelo a esta regla mediante la ventana Seleccionar objetos y, a continuación, seleccione el icono para habilitar o deshabilitar la exclusión para excluir dicho origen de esta regla. <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 Seleccionar objetos.</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:
 - a Seleccione el protocolo de servicio.
 - b Escriba los números de puerto de los puertos de origen y destino, o bien especifique **cualquiera**.
 - c 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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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**.

Aplicar la configuración del servidor syslog a una puerta de enlace Edge

Si se habilitó el registro para una o varias reglas de firewall de puerta de enlace Edge, la puerta de enlace Edge se conecta al servidor syslog. Si se creó una puerta de enlace Edge antes de la configuración inicial del servidor syslog o si se cambió la configuración del servidor syslog, es necesario sincronizar la configuración del servidor syslog para esta puerta de enlace Edge.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
- 3 Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge y haga clic en **Sincronizar syslog**.
- 4 Para confirmar, haga clic en **Aceptar**.

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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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 Servidor de nombres principal y Servidor de nombres secundario se establecen como Automático .
Servidor de nombres principal	Si no habilita Autoconfigurar DNS , 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 Autoconfigurar DNS , 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, Tiempo de concesión 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).
Nota No se puede especificar un tiempo de concesión cuando se selecciona La concesión no caduca nunca .	

- 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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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 Servidor de nombres principal y Servidor de nombres secundario se establecen como Automático .
Servidor de nombres principal	Si no selecciona Autoconfigurar DNS , 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 Autoconfigurar DNS , 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.

Opción	Descripción
Puerta de enlace predeterminada	<p>Escriba la dirección de puerta de enlace predeterminada.</p> <p>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.</p>
La concesión no caduca nunca	<p>Habilite este botón de alternancia para conservar la dirección IP enlazada con esa dirección MAC por un tiempo indefinido.</p> <p>Cuando se selecciona esta opción, Tiempo de concesión se establece como infinito.</p>
Tiempo de concesión (segundos)	<p>Periodo de tiempo (en segundos) que las direcciones IP asignadas por DHCP se otorgan como concesión a los clientes.</p> <p>El tiempo de concesión predeterminado es un día (86.400 segundos).</p> <p>Nota No se puede especificar un tiempo de concesión cuando se selecciona La concesión no caduca nunca.</p>

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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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**.

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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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 Cualquiera .
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 Protocolo como ICMP o Cualquiera .
Tipo de ICMP	<p>Si selecciona ICMP (una utilidad de informe y diagnóstico de errores usada entre dispositivos para comunicar información de errores) en Protocolo, seleccione un valor de Tipo de ICMP 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>

Opción	Descripción
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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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 Normal o NSSA.</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"> ■ Ninguna <p>No se requiere autenticación.</p> ■ Contraseña <p>Con esta opción, la contraseña que se especifica en el campo Valor de autenticación de área se incluye en el paquete transmitido.</p> ■ MD5 <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 Valor de autenticación de área.</p>

- 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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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
Habilitar reinicio correcto	Especifica que el reenvío de paquetes no debe interrumpirse cuando se reinicien los servicios de BGP.
Habilitar el origen predeterminado	Permite que la puerta de enlace Edge se anuncie como puerta de enlace predeterminada ante los vecinos de BGP.
AS local	<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
Dirección IP	Escriba la dirección IP de un vecino de BGP para esta puerta de enlace Edge.
AS remoto	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.
Ponderación	La ponderación predeterminada de la conexión de vecino. Ajuste este valor según las necesidades de la organización.
Tiempo de conexión persistente	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.
Tiempo de espera de recuperación	<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>
Contraseña	<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>
Filtros de BGP	<p>Utilice esta tabla para especificar el filtrado de rutas mediante una lista de prefijos de este vecino de BGP.</p> <p>Precaución 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 Conservar para guardar cada filtro.</p> <ul style="list-style-type: none"> ■ Seleccione la dirección para indicar si se filtrará el tráfico que va hacia el vecino o que viene desde él. ■ Seleccione la acción para indicar si permitirá o denegará el tráfico. ■ Escriba la red que desea filtrar hacia el vecino o desde él. Escriba ANY o una red con formato CIDR. ■ Escriba el GE de prefijo de IP y el LE de prefijo de IP para utilizar las palabras clave 1e y ge en la lista de prefijos de IP.

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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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 Cualquiera para aplicar los criterios a todas las rutas de red.
Protocolo de aprendizaje	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 Protocolo de aprendiz.
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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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.</p> <p>Habilite Aceleración habilitada 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>Nota 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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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
Tipo	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.
Habilitar acceso directo SSL	Haga clic aquí para habilitar la autenticación SSL que se transferirá al servidor virtual. De lo contrario, la autenticación SSL se realizará en la dirección de destino.
URL de redirección HTTP	HTTP y HTTPS: escriba la dirección URL a la que debe redirigirse el tráfico que llega a la dirección de destino.

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"> ■ IP de origen <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> <ul style="list-style-type: none"> ■ MSRDP <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>
Nombre de cookie	<p>HTTP y HTTPS: Si ha especificado Cookie como el mecanismo de persistencia, escriba 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"> ■ Insertar <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> ■ Prefijo <p>Seleccione esta opción cuando el cliente no admite más de una cookie.</p> <p>Nota 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> ■ Sesión de aplicación: para esta opción, el servidor no envía una cookie, sino que envía la información de sesión del usuario como una dirección 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.
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>Nota 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 Insertar encabezado HTTP X-Forwarded-For 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 Habilitar SSL del lado de grupo 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
Certificados del servidor virtual	Seleccione el certificado, las CA o las CRL utilizadas para descifrar el tráfico HTTPS.
Certificados del grupo	Defina el certificado, las CA o las CRL utilizadas para autenticar el equilibrador de carga del lado servidor. Nota Seleccione Habilitar SSL del lado de grupo para habilitar esta pestaña.
Cifrado	Seleccione los algoritmos de cifrado (o conjunto de cifrado) que se han negociado durante el protocolo de enlace SSL/TLS.
Autenticación de cliente	Especifique si la autenticación de cliente se ignorará o será obligatoria. Nota Si se establece como obligatoria, 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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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 Método 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 Método 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 Nueva supervisión del servicio 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>Nota Cuando se selecciona el método POST, debe especificar un valor para Enviar.</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>Nota Cuando Esperado no coincide, la supervisión no intenta hacer coincidir el contenido de Recibir.</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><extension>delay=2 critical=3 escape</extension></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 7-1. 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. Nota 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 SECONDS. 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 STRING en el ejemplo.
eregi= <i>STRING</i>	Busca en la página una expresión regular que no distingue mayúsculas de minúsculas que reemplaza a STRING 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 7-2. 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 7-3. 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= <i>STRING</i>	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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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
ROUND-ROBIN	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.
IP-HASH	Selecciona un servidor en función de un hash de la dirección IP de origen y de destino de cada paquete.
LEASTCONN	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.
URI	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=<name></code> . Por ejemplo, puede utilizar host 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=<url></code> .

6 Agregue miembros al grupo.

- Haga clic en el botón **Agregar** (.
- Introduzca el nombre del miembro de grupo.
- Introduzca la dirección IP del miembro de grupo.
- Introduzca el puerto en el que el miembro recibirá el tráfico desde el equilibrador de carga.
- Introduzca el puerto de supervisión en el que el miembro recibirá las solicitudes de supervisión de estado.
- En el cuadro de texto **Ponderación**, escriba la proporción de tráfico que gestionará este miembro. Debe ser un número entero entre 1 y 256.
- (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.
- (opcional) En el cuadro de texto **Conexiones mínimas**, escriba el número mínimo de conexiones simultáneas que un miembro siempre debe aceptar.
- 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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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 Perfil de aplicación 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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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
Rango de IP	<p>Introduzca un rango de direcciones IP para este grupo de direcciones IP (por ejemplo, 127.0.0.1–127.0.0.9).</p> <p>Estas direcciones IP se asignarán a los clientes VPN cuando se autenticuen y se conecten al túnel VPN de SSL.</p>
Máscara de red	<p>Introduzca la máscara de red del grupo de direcciones IP (por ejemplo, 255.255.255.0).</p>
Puerta de enlace	<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 Rango de IP.</p>
Descripción	(Opcional) Introduzca una descripción para este grupo de direcciones IP.
Estado	Seleccione si desea habilitar o deshabilitar este grupo de direcciones IP.
DNS primario	(Opcional) Introduzca el nombre del servidor DNS primario que se utilizará para la resolución de nombres de estas direcciones IP virtuales.
DNS secundario	(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, 192169.1.0/24).</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"> ■ A través del túnel <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> ■ Omitir el túnel <p>El cliente VPN omite la puerta de enlace Edge y envía el tráfico directamente al servidor privado.</p>
Habilitar optimización de TCP	<p>(Opcional) Para optimizar la velocidad de Internet de la mejor manera, cuando selecciona A través del túnel para enviar el tráfico, también debe seleccionar Habilitar optimización de TCP</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 Habilitar optimización de TCP elimina el riesgo de que se produzca este problema de TCP sobre TCP.</p> <p>Nota Cuando se habilita la optimización de TCP:</p> <ul style="list-style-type: none"> ■ Debe especificar los números de puerto para los que se optimizará el tráfico de Internet. ■ 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.

Opción	Acción
Puertos	Si selecciona A través del túnel , escriba el rango de números de puertos que desea abrir para que el usuario remoto acceda a los servidores internos, como 20–21 para el tráfico de FTP y 80–81 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
Habilitar política de contraseñas	Active la aplicación de la configuración de la política de contraseñas que configure aquí.
Longitud de la contraseña	Introduzca las cantidades mínima y máxima de caracteres que se permiten para la contraseña.
Cantidad mínima de letras	(Opcional) Escriba la cantidad mínima de caracteres alfabéticos que se requieren en la contraseña.
Cantidad mínima de dígitos	(Opcional) Escriba la cantidad mínima de caracteres numéricos que se requieren en la contraseña.
Cantidad mínima de caracteres especiales	(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.
La contraseña no debe contener el ID de usuario	(Opcional) Habilite esta opción para exigir que la contraseña no contenga el identificador de usuario.
La contraseña caduca en	(Opcional) Escriba la cantidad máxima de días de vigencia de la contraseña, antes de que el usuario deba cambiarla.
Notificación de caducidad en	(Opcional) Escriba la cantidad de días antes del valor de La contraseña caduca en 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
Habilitar política de bloqueo de cuentas	Active la aplicación de la configuración de la política de bloqueo de cuentas que configure aquí.
Recuento de reintentos	Introduzca la cantidad de veces que un usuario puede intentar acceder a la cuenta.
Duración del reintento	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 Recuento de reintentos como 5 y Duración del reintento como 1 minuto, la cuenta del usuario se bloqueará tras 5 intentos de inicio de sesión incorrectos en 1 minuto.
Duración del bloqueo	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

- 1 En la pestaña **VPN-Plus de SSL**, haga clic en **Usuarios**.

- 2 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 Agregar () 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
Habilitar funcionamiento en modo silencioso	Se oculta la ventana en la que se indica que se completó la instalación.
Validación del certificado de seguridad del servidor	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 Tiempo de espera forzado .
Tiempo de espera forzado	Escriba el período de tiempo de espera en minutos. Este campo se muestra cuando se activa el botón de alternancia Habilitar tiempo de espera forzado .

- 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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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 En la pestaña **VPN de IPsec**, haga clic en **Sitios de VPN de IPsec**.
- 2 Haga clic en el botón **Agregar** (.
- 3 Configure los ajustes de la conexión de VPN de IPsec.

Opción	Acción
Habilitado	Habilite esta conexión entre los dos endpoints de VPN.
Habilitar confidencialidad directa total (PFS)	<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>Importante 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>
Nombre	(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, 192.168.99.0/24).</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>Nota 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, 192.168.99.0/24).</p>
Algoritmo de cifrado	<p>Seleccione el tipo de algoritmo de cifrado del menú desplegable.</p> <p>Nota 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"> ■ PSK <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> ■ Certificado <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 Configuración global de la pestaña VPN de IPsec.</p>
Cambiar clave compartida	(Opcional) Al actualizar la configuración de una conexión existente, puede activar esta opción para que el campo Clave compartida previamente esté disponible, de modo que pueda actualizar la clave compartida.
Clave compartida previamente	<p>Si ha seleccionado PSK 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>Nota 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>Nota 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"> ■ <code>securelocaltrafficbyip=IPAddress</code>: permite redirigir el tráfico local de la puerta de enlace Edge a través del túnel VPN de IPsec. <p>Este el valor predeterminado.</p> <ul style="list-style-type: none"> ■ <code>passthroughSubnets=PeerSubnet/IPAddress</code>: permite admitir la superposición de subredes.

4 Haga clic en **Conservar**.

5 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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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.

Procedimiento

1 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**.

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.

3 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).


4 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.

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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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.

- 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 Cambiar certificado del servidor para seleccionar el certificado que se enlazaré al servidor VPN de capa 2. En la ventana Cambiar certificado del servidor , active Validar certificado de servidor , seleccione un certificado de servidor de la lista y haga clic en Aceptar .

- Para configurar los sitios del mismo nivel, haga clic en la pestaña **Sitios de servidor**.

- Haga clic en el botón **Agregar** (.

- 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 Contraseña Confirmar contraseña	Introduzca el nombre de usuario y la contraseña con los que se autenticará el sitio del mismo nivel. Las credenciales de usuario en el sitio del mismo nivel deben ser las mismas que las del lado cliente.
Interfaces extendidas	Seleccione al menos una subinterfaz que se extenderá con el cliente. 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.
Dirección de puerta de enlace de optimización de salida	(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.

- Haga clic en **Conservar**.
- 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	Introduzca el puerto del servidor VPN de capa 2 al que se debe conectar el cliente. El puerto predeterminado es 443.
Algoritmo de cifrado	Seleccione el algoritmo de cifrado para comunicarse con el servidor.
Interfaces extendidas	Seleccione las subinterfaces que se ampliarán al servidor. 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.
Dirección de puerta de enlace de optimización de salida	(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.
Detalles del usuario	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
Habilitar proxy seguro	Seleccione esta opción para habilitar el proxy seguro.
Dirección	Introduzca la dirección IP del servidor proxy.
Puerto	Introduzca el puerto del servidor proxy.
Nombre de usuario	Introduzca las credenciales de autenticación del servidor proxy.
Contraseña	

- 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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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
Nombre común	<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>
Unidad de organización	<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>
Nombre de organización	<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>
Localidad	<p>Escriba la ciudad o localidad donde se registró legalmente la empresa.</p>
Nombre del estado o de la provincia	<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>
Código de país	<p>Escriba el nombre del país donde se registró legalmente la empresa.</p>
Algoritmo de clave privada	<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>Nota VPN-Plus de SSL admite solamente certificados RSA.</p>
Tamaño de clave	<p>Escriba el tamaño de la clave en bits.</p> <p>El valor mínimo es de 2048 bits.</p>
Descripción	<p>(Opcional) Escriba una descripción para el certificado.</p>

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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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**. Para abrir esta página, debe desplazarse hasta la configuración de firewall distribuido del VDC de organización o la configuración de servicios de una puerta de enlace Edge que pertenezca al VDC de organización.

Procedimiento

- 1 Abra la página **Objetos de agrupamiento**.

Opción	Acción
Desde la configuración de firewall distribuido del VDC de organización	<ol style="list-style-type: none"> a En el menú principal () , seleccione Recursos de nube. b En el panel izquierdo, haga clic en VDC de organización. c Seleccione el botón de radio junto al nombre del centro de datos virtual de organización de destino y, a continuación, haga clic en Administrar firewall. d Haga clic en la pestaña Objetos de agrupamiento.
Desde la configuración de servicios de una puerta de enlace Edge en el VDC de organización	<ol style="list-style-type: none"> a En el menú principal () , seleccione Recursos de nube. b En el panel izquierdo, haga clic en Puertas de enlace Edge. c Seleccione el botón de radio junto al nombre de una puerta de enlace Edge que pertenece al centro de datos virtual de organización de destino y haga clic en Servicios. d Haga clic en la pestaña Objetos de agrupamiento.

- 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 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, se usa la página **Objetos de agrupamiento**. Para abrir esta página, debe desplazarse hasta la configuración del firewall distribuido del VDC de organización, o bien a la configuración de servicios de una puerta de enlace Edge que pertenezca al VDC de organización.


Procedimiento

- 1 Abra la página **Objetos de agrupamiento**.

Opción	Acción
Desde la configuración de firewall distribuido del VDC de organización	<ol style="list-style-type: none"> a En el menú principal () , seleccione Recursos de nube. b En el panel izquierdo, haga clic en VDC de organización. c Seleccione el botón de radio junto al nombre del centro de datos virtual de organización de destino y, a continuación, haga clic en Administrar firewall. d Haga clic en la pestaña Objetos de agrupamiento.
Desde la configuración de servicios de una puerta de enlace Edge en el VDC de organización	<ol style="list-style-type: none"> a En el menú principal () , seleccione Recursos de nube. b En el panel izquierdo, haga clic en Puertas de enlace Edge. c Seleccione el botón de radio junto al nombre de una puerta de enlace Edge que pertenece al centro de datos virtual de organización de destino y haga clic en Servicios. d Haga clic en la pestaña Objetos de agrupamiento.

- 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 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 mediante la página **Objetos de agrupamiento**. Para abrir esta página, debe desplazarse hasta la configuración del firewall distribuido del VDC de organización, o bien a la configuración de servicios de una puerta de enlace Edge que pertenezca al VDC de organización.

Procedimiento

- 1 Abra la página **Objetos de agrupamiento**.

Opción	Acción
Desde la configuración de firewall distribuido del VDC de organización	<ol style="list-style-type: none"> a En el menú principal () , seleccione Recursos de nube. b En el panel izquierdo, haga clic en VDC de organización. c Seleccione el botón de radio junto al nombre del centro de datos virtual de organización de destino y, a continuación, haga clic en Administrar firewall. d Haga clic en la pestaña Objetos de agrupamiento.
Desde la configuración de servicios de una puerta de enlace Edge en el VDC de organización	<ol style="list-style-type: none"> a En el menú principal () , seleccione Recursos de nube. b En el panel izquierdo, haga clic en Puertas de enlace Edge. c Seleccione el botón de radio junto al nombre de una puerta de enlace Edge que pertenece al centro de datos virtual de organización de destino y haga clic en Servicios. d Haga clic en la pestaña Objetos de agrupamiento.

- 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 mediante la página **Objetos de agrupamiento**. Para abrir esta página, debe desplazarse hasta la configuración del firewall distribuido del VDC de organización, o bien a la configuración de servicios de una puerta de enlace Edge que pertenezca al VDC de organización.

Procedimiento

1 Abra la página **Objetos de agrupamiento**.

Opción	Acción
Desde la configuración de firewall distribuido del VDC de organización	<ul style="list-style-type: none"> a En el menú principal () , seleccione Recursos de nube. b En el panel izquierdo, haga clic en VDC de organización. c Seleccione el botón de radio junto al nombre del centro de datos virtual de organización de destino y, a continuación, haga clic en Administrar firewall. d Haga clic en la pestaña Objetos de agrupamiento.
Desde la configuración de servicios de una puerta de enlace Edge en el VDC de organización	<ul style="list-style-type: none"> a En el menú principal () , seleccione Recursos de nube. b En el panel izquierdo, haga clic en Puertas de enlace Edge. c Seleccione el botón de radio junto al nombre de una puerta de enlace Edge que pertenece al centro de datos virtual de organización de destino y haga clic en Servicios. d Haga clic en la pestaña Objetos de agrupamiento.

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.

Ver el uso de redes y las asignaciones de IP en una puerta de enlace Edge

Es posible ver las redes en una puerta de enlace Edge con información sobre sus subredes y su uso del grupo de direcciones IP. También se puede ver la dirección IP asignada a cada red.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **Puertas de enlace Edge** y, a continuación, haga clic en el nombre de la puerta de enlace Edge de destino.
- 3 Para ver las redes externas con información sobre sus subredes y su uso del grupo de direcciones IP, haga clic en la pestaña **Redes externas > Redes y subredes**.
- 4 Para ver las redes externas con información sobre sus categorías y direcciones IP, haga clic en la pestaña **Redes externas > Asignaciones de IP**.

Editar propiedades de puerta de enlace Edge


Habilitar o deshabilitar el enrutamiento distribuido en una puerta de enlace Edge

Después de habilitar el enrutamiento distribuido de vCloud Director en una puerta de enlace Edge, el administrador de la organización puede crear varias redes de centros de datos virtuales de organización enrutadas con interfaces distribuidas conectadas a esta puerta de enlace Edge. El tráfico en esas redes se optimiza para la comunicación entre máquinas virtuales.

Requisitos previos

La instancia de NSX Manager de respaldo se configura con un clúster de NSX Controller. Consulte la *Guía de administración de NSX*.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
- 3 Seleccione el botón de radio junto al nombre de la puerta de enlace Edge de destino y, a continuación, haga clic en **Habilitar enrutamiento distribuido** o **Deshabilitar enrutamiento distribuido**.
- 4 Para confirmar, haga clic en **Aceptar**.


Modificar las redes externas y la configuración de una puerta de enlace Edge

Para modificar las redes externas y la configuración de la puerta de enlace Edge, puede usar el asistente **Editar puerta de enlace Edge**, que contiene las mismas páginas que el asistente que usó para crear la puerta de enlace Edge.

Puede modificar la configuración que definió al agregar la puerta de enlace Edge. Consulte [Agregar una puerta de enlace Edge](#).

Para modificar la configuración de enrutamiento distribuido, consulte [Habilitar o deshabilitar el enrutamiento distribuido en una puerta de enlace Edge](#).


Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
- 3 Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge que desea modificar y, luego, haga clic en **Editar**.
- 4 Para modificar la configuración de la puerta de enlace Edge, pase por las páginas del asistente **Editar puerta de enlace Edge** con la opción **Siguiente** y, en la página **Listo para completar**, haga clic en **Finalizar**.

Editar la configuración general de una puerta de enlace Edge

Es posible modificar el nombre y la descripción de una puerta de enlace Edge, habilitar o deshabilitar el modo FIPS y el estado de alta disponibilidad, y cambiar la configuración de tamaño de la puerta de enlace Edge.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **Puertas de enlace Edge** y, a continuación, haga clic en el nombre de la puerta de enlace Edge de destino.
- 3 En la pestaña **General**, en la esquina superior derecha, haga clic en **Editar**.
- 4 (opcional) Edite el nombre y la descripción de la puerta de enlace Edge.
- 5 (opcional) Active o desactive cada ajuste de configuración general de la puerta de enlace Edge.

Configuración general	Descripción
Modo FIPS	Configura la puerta de enlace Edge para que use el modo FIPS de NSX.
Alta disponibilidad	Habilita la conmutación por error automática a una puerta de enlace Edge de respaldo.

- 6 (opcional) Cambie la configuración de la puerta de enlace Edge para los recursos del sistema.


Opción	Descripción
Compacta	Requiere menos memoria y recursos informáticos.
Grande	Proporciona una capacidad y un rendimiento mayores que los que se obtienen con la opción Compacta. Las configuraciones Grande y Extragrande proporcionan funciones de seguridad idénticas.
Extragrande	Se utiliza para entornos que tienen un equilibrador de carga con un gran número de sesiones simultáneas.
Cuádruple	Se utiliza para entornos de alto rendimiento. Requiere una alta velocidad de conexión.

- 7 Para confirmar los cambios, haga clic en **Guardar**.

Editar la puerta de enlace predeterminada de una puerta de enlace Edge

Es posible cambiar la red que una puerta de enlace Edge utiliza como puerta de enlace predeterminada.

Procedimiento


- 1 En el menú principal () , seleccione **Recursos de nube**.

- 2 En el panel izquierdo, haga clic en **Puertas de enlace Edge** y, a continuación, haga clic en el nombre de la puerta de enlace Edge de destino.
- 3 En la pestaña **Redes externas > Puerta de enlace predeterminada**, en la esquina superior derecha, haga clic en **Editar**.
- 4 (opcional) Configure una red como puerta de enlace predeterminada.
 - a Active el botón de alternancia **Configurar puerta de enlace predeterminada**.
 - b Seleccione el botón de radio ubicado junto al nombre de la red externa de destino y seleccione el botón de radio ubicado junto a la dirección IP de destino.
 - c (opcional) Active el botón de alternancia **Utilizar la puerta de enlace predeterminada para retransmisión de DNS**.
- 5 Para confirmar los cambios, haga clic en **Guardar**.

Editar la configuración de IP de una puerta de enlace Edge

Es posible modificar la configuración de IP para redes externas en una puerta de enlace Edge.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **Puertas de enlace Edge** y, a continuación, haga clic en el nombre de la puerta de enlace Edge de destino.
- 3 En la pestaña **Redes externas > Configuración de IP**, haga clic en **Editar**.
- 4 Para cada red de la puerta de enlace Edge, en la celda **Direcciones IP**, introduzca una dirección IP o deje la celda en blanco.


Si no introduce una dirección IP para una red, el sistema asignará una dirección IP arbitraria a esta red.
- 5 Para confirmar los cambios, haga clic en **Guardar**.

Editar los grupos de IP subasignados en una puerta de enlace Edge

Puede subasignar varios grupos de direcciones IP estáticas de los grupos de direcciones IP disponibles de una red externa en una puerta de enlace Edge.

Nota La asignación de direcciones IP a una puerta de enlace Edge mediante subasignación es un proceso en el que el proveedor asigna la propiedad de las direcciones IP a la puerta de enlace. vCloud Director configura automáticamente la interfaz de puerta de enlace adecuada con las direcciones secundarias durante el proceso de subasignación, lo que puede provocar conflictos de direcciones IP si se utiliza alguna de las direcciones IP fuera de vCloud Director.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.

- 2 En el panel izquierdo, haga clic en **Puertas de enlace Edge** y, a continuación, haga clic en el nombre de la puerta de enlace Edge de destino.
- 3 Haga clic en la pestaña **Redes externas > Grupos de IP subasignados**.
Puede ver los grupos de IP subasignados actuales para cada red externa en esta puerta de enlace Edge.
- 4 Haga clic en el botón de radio ubicado junto al nombre de una red externa y haga clic en **Editar**.
Puede ver los grupos de direcciones IP disponibles para esta red externa y los grupos de IP subasignados actuales, si están configurados.
- 5 Edite los grupos de IP subasignados para esta red externa y haga clic en **Guardar**.
Puede agregar, modificar y eliminar direcciones IP y rangos de direcciones IP a partir de los rangos de los grupos de direcciones IP disponibles.

Resultados


El sistema combina los rangos de direcciones IP solapadas.

Editar los límites de velocidad en una puerta de enlace Edge

Puede configurar los límites de velocidad de entrada y salida de cada red externa de la puerta de enlace Edge.

Los límites de velocidad se aplican solo a las redes externas respaldadas mediante grupos de puertos distribuidos con enlace estático.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **Puertas de enlace Edge** y, a continuación, haga clic en el nombre de la puerta de enlace Edge de destino.
- 3 En la pestaña **Redes externas > Límites de velocidad**, en la esquina superior derecha, haga clic en **Editar**.
Puede ver los límites de velocidad actuales de cada red externa en esta puerta de enlace Edge.
- 4 Edite los límites de velocidad y haga clic en **Guardar**.
Para cada red externa de la puerta de enlace Edge, puede habilitar o deshabilitar los límites de velocidad, así como cambiar las velocidades de entrada y de salida.

Volver a implementar una puerta de enlace Edge


Es posible eliminar e implementar un nuevo dispositivo de puerta de enlace Edge con las configuraciones más recientes.

Si los servicios de Edge no funcionan según lo esperado, puede volver a implementar el dispositivo de puerta de enlace Edge.

Puede volver a implementar puertas de enlace Edge heredadas para migrar las puertas de enlace Edge a clústeres de Edge creados recientemente.

Al volver a implementar una puerta de enlace Edge, vCloud Director la elimina y la vuelve a crear con las configuraciones más recientes.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
- 3 Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **Volver a implementar**.
- 4 Para confirmar, haga clic en **Aceptar**.

Resultados

La máquina virtual de la puerta de enlace Edge se reemplaza con una nueva máquina virtual y se restauran todos los servicios.


Eliminar una puerta de enlace Edge

Es posible quitar una puerta de enlace Edge del centro de datos virtual de organización.

Requisitos previos

Elimine todas las redes de centros de datos virtuales de organización que utilicen la puerta de enlace Edge de destino.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
- 3 Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **Eliminar**.
- 4 Para confirmar, haga clic en **Eliminar**.


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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **Servicios**.
- 2 Haga clic en la pestaña **Estadísticas**.
- 3 Desplácese por las pestañas en función del tipo de estadísticas que desee ver.

Opción	Descripción
Conexiones	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.
VPN de IPsec	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.
VPN de capa 2	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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **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 En el menú principal () , seleccione **Recursos de nube**.
 - b En el panel izquierdo, haga clic en **Puertas de enlace Edge**.
 - c Haga clic en el botón de radio junto al nombre de la puerta de enlace Edge de destino y haga clic en **Servicios**.
- 2 Haga clic en la pestaña **Configuración de Edge**.
- 3 Configure los ajustes de SSH.

Opción	Descripción
Nombre de usuario	Introduzca las credenciales para el acceso de SSH a esta puerta de enlace Edge.
Contraseña	
Vuelva a escribir la contraseña	De forma predeterminada, el nombre de usuario de SSH es admin .
Caducidad de contraseña	Introduzca el período de caducidad de la contraseña (en días).
Titular de inicio de sesión	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 que correspondan para permitir el acceso de SSH a esta puerta de enlace Edge.

Administrar redes de centros de datos virtuales de organización

8

Este capítulo incluye los siguientes temas:

- [Administrar redes de centros de datos virtuales NSX-T de organización](#)

Administrar redes de centros de datos virtuales NSX-T de organización

Solo los administradores del sistema pueden crear, modificar y eliminar redes de centros de datos virtuales de organización que se basan en conmutadores lógicos NSX-T.

Para administrar redes de centros de datos virtuales de organización, los administradores del sistema deben iniciar sesión en Service Provider Admin Portal y desplazarse hasta el portal para tenants de vCloud Director de la organización de destino.

Para obtener información sobre la administración de redes de centros de datos virtuales de organización que se basan en NSX Data Center for vSphere, consulte la *Guía del portal para tenants de vCloud Director*.

Agregar una red de centros de datos virtuales de organización NSX-T

Como un administrador del sistema, puede crear una red de centros de datos virtuales de organización mediante la importación de un conmutador lógico desde una instancia de NSX-T Manager asociada.

Nota Con un conmutador lógico de NSX-T, puede crear solo una red de organización aislada IPv4. No se puede crear una red de organización directa o enrutada basada en un conmutador lógico de NSX-T.


Requisitos previos

- El centro de datos virtual del proveedor que respalda el centro de datos virtual de organización de destino debe asociarse con una instancia de NSX-T Manager.
- Se ha creado al menos un conmutador lógico de NSX-T que otras redes de centros de datos virtuales de organización no emplean.

Para obtener información sobre la configuración de conmutadores lógicos de NSX-T, consulte la *Guía de administración de NSX-T*. Para obtener información sobre la creación de un VDC de proveedor respaldado por una instancia de NSX-T Manager, consulte *Guía de programación de vCloud API para proveedores de servicios*.

Procedimiento

- 1 Desplácese hasta el portal para tenants de vCloud Director de la organización de destino.

- a En el menú principal () , seleccione **Recursos de nube**.
- b En **Organizaciones**, haga clic en el nombre de la organización de destino.

Se lo redirigirá a la vista **Centros de datos** del portal para tenants de vCloud Director para esta organización.

- 2 Si hay varios VDC en la organización, haga clic en la tarjeta del VDC de destino de la organización.

- 3 En el panel izquierdo, en **Redes**, haga clic en **Red**.

- 4 Haga clic en **Importar**.

Aparece el asistente **Importar conmutador lógico**.

- 5 Introduzca un nombre y, si lo desea, una descripción de la nueva red de VDC de organización y haga clic en **Siguiente**.

- 6 En la lista de conmutadores lógicos de NSX-T disponibles, seleccione el conmutador de destino haciendo clic en el botón de radio junto al nombre del conmutador y haga clic en **Siguiente**.

- 7 Introduzca la configuración de enrutamiento entre dominios sin clases (Classless Inter-Domain Routing, CIDR) de red.

Utilice el formato *dirección_IP_de_puerta_de_enlace_de_red/longitud_de_prefijo_de_subred* (por ejemplo, **192.167.1.1/24**).

Si el conmutador está configurado con una subred, esta información se rellena previamente.

- 8 (opcional) Ajuste la configuración de DNS y el grupo de direcciones IP estáticas.

Puede agregar varias direcciones IP y rangos de direcciones IP.


- 9 Haga clic en **Siguiente**.

- 10 Revise la página Listo para completar y haga clic en **Finalizar**.

Editar una red de centros de datos virtuales de organización NSX-T

Puede modificar el nombre, la descripción, la configuración de DNS y el grupo de direcciones IP estáticas de una red de centros de datos virtuales de organización que se base en un conmutador lógico NSX-T. Sin embargo, no puede editar la configuración de enrutamiento entre dominios sin clases (Classless Inter-Domain Routing, CIDR) para la red.


Procedimiento

- 1 Desplácese hasta el portal para tenants de vCloud Director de la organización de destino.
 - a En el menú principal () , seleccione **Recursos de nube**.
 - b En **Organizaciones**, haga clic en el nombre de la organización de destino.Se lo redirigirá a la vista **Centros de datos** del portal para tenants de vCloud Director para esta organización.
- 2 Si hay varios VDC en la organización, haga clic en la tarjeta del VDC de destino de la organización.
- 3 En el panel izquierdo, en **Redes**, haga clic en **Red**.
- 4 Haga clic en el botón de radio junto al nombre de la red de destino y haga clic en **Modificar**.
Aparecerá el asistente **Editar red de VDC de organización**.
- 5 (opcional) En la pestaña **General**, edite el nombre y la descripción de la red.
- 6 (opcional) En la pestaña **Configurar red**, edite la configuración de DNS y el grupo de direcciones IP estáticas de la red.
Puede agregar, modificar y eliminar direcciones IP y rangos de IP.
- 7 Haga clic en **Guardar**.

Eliminar una red de centros de datos virtuales de organización de NSX-T

Si ya no utiliza una red de centros de datos virtuales de organización NSX-T, puede eliminarla.

Procedimiento

- 1 Desplácese hasta el portal para tenants de vCloud Director de la organización de destino.
 - a En el menú principal () , seleccione **Recursos de nube**.
 - b En **Organizaciones**, haga clic en el nombre de la organización de destino.Se lo redirigirá a la vista **Centros de datos** del portal para tenants de vCloud Director para esta organización.
- 2 Si hay varios VDC en la organización, haga clic en la tarjeta del VDC de destino de la organización.
- 3 En el panel izquierdo, en **Redes**, haga clic en **Red**.
- 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 **Aceptar**.

Administrar SDDC y servidores proxy de SDDC

9

A partir de la versión 9.7, vCloud Director puede actuar como un servidor proxy HTTP entre los tenants y el entorno de vSphere subyacente. Un centro de datos definido por software (Software-Defined Data Center, SDDC) encapsula la infraestructura de una instancia de vCenter Server asociada. Un servidor proxy de SDDC es un punto de acceso a un componente de un SDDC, por ejemplo, una instancia de vCenter Server, un host ESXi o una instancia de NSX Manager.

Con la función SDDC, se puede usar vCloud Director como punto central de administración para todos los entornos de vSphere.

- Es posible dedicar los recursos de una instancia de vCenter Server a un solo tenant mediante la publicación del SDDC correspondiente solo en su organización. El tenant no comparte estos recursos con otros tenants. El tenant puede acceder a este SDDC mediante una interfaz de usuario o un proxy de API sin necesidad de una VPN.
- Es posible usar vCloud Director como directorio ligero para registrar todas las instancias de vCenter Server.
- Es posible usar vCloud Director como endpoint de API para todas las instancias de vCenter Server.

Antes de crear un SDDC, debe asociar la instancia de vCenter Server de destino a vCloud Director. Consulte [Adjuntar una instancia de vCenter Server sola o junto con una instancia de NSX Manager](#).

Nota De forma predeterminada, con una instancia de vCenter Server asociada, se puede crear un VDC de proveedor o un SDDC. Si creó un VDC de proveedor respaldado por una instancia de vCenter Server, no puede utilizar esta instancia de vCenter Server para crear un SDDC y viceversa. Puede utilizar vCloud API para modificar la configuración del sistema de la instalación de vCloud Director, de modo que una instancia de vCenter Server pueda respaldar un VDC de proveedor y un SDDC.

Puede crear y publicar servidores proxy de SDDC y SDDC en las organizaciones de su nube. Los usuarios pueden utilizar los servidores proxy de SDDC para acceder al entorno de vSphere subyacente. Los usuarios pueden iniciar sesión en la interfaz de usuario o la API de los componentes con proxy mediante sus cuentas de vCloud Director.

Los SDDC en vCloud Director eliminan el requisito de que vCenter Server sea accesible públicamente. Para controlar el acceso, puede habilitar y deshabilitar un SDDC en vCloud Director, y puede habilitar y deshabilitar un servidor proxy de SDDC.

Crear y administrar servidores proxy de SDDC y SDDC

Para crear y administrar SDDC y servidores proxy, debe utilizar vCloud OpenAPI. Consulte *Introducción a vCloud OpenAPI* en <https://code.vmware.com>.

Importante vCloud Director requiere una conexión de red directa a cada instancia de vCenter Server para utilizarla como SDDC. Si la instancia de vCenter Server utiliza una instancia externa de Platform Services Controller, vCloud Director requiere también una conexión de red directa a la instancia de Platform Services Controller.

Para usar VMware OVF Tool en un SDDC con proxy, vCloud Director requiere una conexión directa a cada host ESXi.

- 1 Cree un SDDC respaldado por una instancia de vCenter Server asociada y habilitada.
vCloud Director crea el SDDC con un proxy predeterminado para la instancia de vCenter Server. Si la instancia de vCenter Server utiliza una instancia externa de Platform Services Controller, vCloud Director crea también un proxy para la instancia de Platform Services Controller.
- 2 Obtenga el certificado y la huella digital de los servidores proxy creados, y compruebe que el certificado y la huella digital estén presentes y sean correctos.
- 3 Habilite el SDDC.
- 4 Publique el SDDC en una o varias organizaciones.
- 5 Para permitir que los usuarios accedan a los SDDC y los servidores proxy de SDDC desde vCloud Director Tenant Portal, debe publicar el complemento **Extensión de CPOM** en sus organizaciones. Consulte [Publicar o cancelar la publicación de un complemento de una organización](#).

Después de crear y publicar un SDDC, puede agregar, editar, habilitar, deshabilitar y quitar sus servidores proxy de SDDC.

Nota Al agregar un servidor proxy a un SDDC, debe cargar el certificado y la huella digital para que los tenants puedan recuperar el certificado y la huella digital si el componente con proxy utiliza certificados autofirmados.

Administrar funciones y administradores del sistema

10

Mediante el uso de la consola web de vCloud Director, puede agregar administradores del sistema 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.

Nota A partir de vCloud Director 9.5, los proveedores de servicios pueden crear funciones de proveedor y administrar grupos y usuarios de proveedor mediante el portal para administradores de proveedor de servicios de vCloud Director o a través de vCloud OpenAPI. Para obtener información sobre la administración de grupos, usuarios y funciones de proveedor, consulte la *Guía del portal para administradores de proveedores de servicios de vCloud Director*. Para consultar la documentación de vCloud OpenAPI, desplácese hasta https://nombre_de_host_o_dirección_IP_de_vCloud_Director/docs.

Este capítulo incluye los siguientes temas:

- [Administrar derechos y funciones](#)
- [Administrar usuarios y grupos de proveedor](#)

Administrar derechos y funciones

Un derecho es la unidad fundamental de control de acceso en vCloud Director. Una función asocia un nombre de función a un conjunto de derechos. Cada organización puede tener distintos derechos y funciones.

vCloud Director utiliza funciones y sus derechos asociados para determinar si un usuario o grupo tiene autorización para realizar una operación. Muchos de los procedimientos documentados en las guías de vCloud Director incluyen una función de requisitos previos. Estos requisitos previos dan por hecho que la función con nombre es la función predefinida sin modificar o una función que incluye un conjunto de derechos equivalente.

vCloud Director 9.5 presenta paquetes de derechos y funciones globales de tenant que los administradores del sistema pueden utilizar para administrar los derechos y las funciones que están disponibles para cada organización.

Después de instalar vCloud Director, el sistema solo contiene el paquete de derechos del sistema, que incluye todos los derechos que están disponibles en el sistema. El paquete de derechos del sistema no está publicado en ninguna organización. El sistema también contiene las funciones globales de tenant integradas que se publican en todas las organizaciones. Para obtener información sobre las funciones predefinidas, consulte [Funciones predeterminadas y sus derechos](#).

Después de actualizar vCloud Director desde la versión 9.1 o una versión anterior, además del paquete de derechos del sistema, el sistema contiene un paquete de derechos heredado para cada organización existente. Cada paquete de derechos heredado incluye los derechos que están disponibles en la organización asociada en el momento de la actualización y se publica solo para esa organización.

Nota Para comenzar a usar el modelo de paquetes de derechos para una organización existente, debe eliminar el paquete de derechos heredado correspondiente.

Si actualizó vCloud Director desde la versión 9.1 o anterior, las plantillas de funciones existentes se publican en todas las organizaciones como funciones globales de tenant y las funciones existentes que no estén vinculadas a plantillas de funciones están disponibles como funciones específicas de tenant para sus organizaciones.

Terminología de derechos

Derecho

Cada derecho proporciona acceso para ver o administrar un tipo de objeto concreto en vCloud Director. Los derechos pertenecen a distintas categorías en función de los objetos con los que se relacionan como, por ejemplo, vApp, Catálogo, Organización, etc. La organización de proveedor contiene todos los derechos disponibles en el sistema. El administrador del sistema define los derechos que están disponibles para cada organización. No puede crear ni modificar los derechos incluidos en vCloud Director.

Paquete de derechos

Los administradores del sistema pueden utilizar paquetes de derechos para administrar los derechos que están disponibles para cada organización. Un paquete de derechos es un conjunto de derechos que el administrador del sistema puede publicar en una o varias organizaciones. El administrador del sistema puede crear y publicar los paquetes de derechos que corresponden a los niveles de servicio, funcionalidad monetizable por separado o cualquier otro agrupamiento arbitrario de derechos. Solo los administradores del sistema pueden ver y administrar los paquetes de derechos. Puede publicar varios paquetes en la misma organización.

Derechos de organización

Derechos de organización son el conjunto completo de derechos que están disponibles para una organización. Los derechos de organización pueden constar de varios paquetes de derechos, pero los administradores y los usuarios de cada organización ven un conjunto

plano de derechos que pueden utilizar para crear y modificar funciones específicas para tenants.

Terminología de funciones

Función

Una función es un conjunto de derechos que se puede asignar a uno o varios usuarios y grupos. Al crear o importar un usuario o un grupo, se les debe asignar una función.

Funciones de proveedor

Las funciones de proveedor son el conjunto de funciones que solo están disponibles para la organización de proveedor. Las funciones de proveedor únicamente pueden asignarse a usuarios Proveedor. Los administradores del sistema pueden crear funciones de proveedor personalizadas.

Funciones de tenant

Las funciones de tenant son el conjunto de funciones disponibles en una organización.

Los administradores del sistema pueden crear y editar funciones globales de tenant y publicarlas en una o varias organizaciones. Las funciones globales de tenant pueden asignarse a los usuarios tenant de las organizaciones en las que están publicadas. Los administradores de organización no pueden editar las funciones globales de tenant.

Nota Los usuarios tenant solo pueden utilizar los derechos de sus funciones que se publican para sus organizaciones.

Funciones específicas para tenants

Los administradores de organización pueden crear y modificar las funciones específicas para tenants que sean locales para sus organizaciones. Las funciones específicas para tenants pueden asignarse solo los usuarios tenant de la organización a la que pertenecen. Las funciones específicas para tenants pueden contener un subconjunto de solo los derechos de la organización.

Para obtener información acerca de las funciones de administración específicas para tenants, consulte la *Guía del portal para tenants de vCloud Director*.

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 10-1. 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				
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	

Tabla 10-1. 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
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				
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				

Tabla 10-1. 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: 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				
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				

Tabla 10-1. 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
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				
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				

Tabla 10-1. 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: Editar regla de afinidad de MV y MV	X	X	X		
VDC de organización: Editar propiedades ampliadas de VDC de organización	X				
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				

Tabla 10-1. 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
Supervisión de MV: Ver métricas históricas para el VDC de organización	X				
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 [Nuevos derechos en esta versión](#).

Nuevos derechos en esta versión

vCloud Director 9.7 introduce nuevos derechos, que se recomienda agregar a cualquier función global existente publicada en los tenants.

Derecho	Descripción	Función predeterminada
SDDC: Ver SDDC	Permite ver todos los SDDC publicados en la organización. El administrador del sistema puede ver todos los SDDC.	Administrador del sistema y Administrador de organización
SDDC: Administrar SDDC	Permite agregar, quitar y editar SDDC.	Administrador del sistema
SDDC: Administrar proxy de SDDC	Permite agregar, quitar, habilitar y deshabilitar servidores proxy de SDDC.	Administrador del sistema
Aplicaciones de servicio: Ver aplicaciones de servicio	Permite ver la lista de aplicaciones de servicio registradas. Se utiliza para las cuentas VMC.	Administrador del sistema
Aplicaciones de servicio: Registrar SDDC de VMC	Permite crear, ver, editar y eliminar aplicaciones de servicio. Se utiliza para las cuentas VMC.	Administrador del sistema
Aplicaciones de servicio: Administrar aplicaciones de servicio	Permite registrar aplicaciones de servicio. Se utiliza para las cuentas VMC.	Administrador del sistema
Clúster de Edge: Ver clúster de Edge	Permite ver una lista de clústeres de Edge y recuperar un clúster de Edge individual.	Administrador del sistema y Administrador de organización
Clúster de Edge: Administrar clúster de Edge	Permite crear, editar y eliminar clústeres de Edge.	Administrador del sistema y Administrador de organización
vApp: Editar política de recursos informáticos de la máquina virtual	Permite que los usuarios cambien la política de recursos informáticos de una máquina virtual.	Administrador del sistema, Administrador de organización, Autor de catálogo y Autor de vApp
Puerta de enlace: Importar puerta de enlace Edge	Permite importar un enrutador de nivel 1 como una puerta de enlace Edge.	Administrador del sistema y Administrador de organización

Para obtener información sobre la administración de derechos y funciones, consulte la *Guía del portal para administradores de proveedores de servicios de vCloud Director*.


Administrar paquetes de derechos

Como administrador del sistema, puede crear paquetes de derechos y publicarlos en una o varias organizaciones en su nube. Puede editar y eliminar los paquetes de derechos existentes. Puede cancelar la publicación de paquetes de derechos de organizaciones en la nube.

Crear un paquete de derechos

Puede agrupar un conjunto de derechos como un paquete de derechos que se puede publicar en una o varias organizaciones del sistema.

Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, en **Control de acceso de tenants**, haga clic en **Paquetes de derechos**.
- 3 Haga clic en **Agregar**.
- 4 Introduzca un nombre y, si lo desea, una descripción para el nuevo paquete de derechos.
- 5 Seleccione los derechos que desea asociar con este paquete.

Los derechos se agrupan en categorías y subcategorías para ver o administrar el acceso al objeto con los que se relacionan.

Puede seleccionar los derechos de forma individual, por vista o administración según la subcategoría, o bien por vista o administración de forma global.

Categoría	Descripción
Control de acceso	Contiene los derechos para ver y administrar organizaciones, derechos, funciones y usuarios.
Administración	Contiene los derechos para ver y administrar la configuración general y multisitio.
Proceso	Contiene los derechos para ver y administrar los VDC de organización y de proveedor, las vApps, las plantillas de VDC de organización y la supervisión de máquinas virtuales.
Extensiones	Contiene los derechos para ver y administrar los complementos y las extensiones de vCloud Director.
Infraestructura	Contiene los derechos para ver y administrar los recursos de vSphere.
Bibliotecas	Contiene los derechos para ver y administrar los catálogos y sus elementos.
Red	Contiene los derechos para ver y administrar los recursos de red.

- 6 Haga clic en **Guardar**.

Pasos siguientes


Puede publicar el paquete de derechos recién creado en una o varias organizaciones del sistema. Consulte [Publicar o cancelar la publicación de un paquete de derechos](#).

Publicar o cancelar la publicación de un paquete de derechos

Puede publicar un paquete de derechos en una o varias organizaciones del sistema. Después de publicar un paquete de derechos en una organización, los derechos incluidos en este paquete pasan a formar parte del conjunto de derechos de esa organización.

Los derechos de organización pueden constar de varios paquetes de derechos, pero los administradores y los usuarios de cada organización ven un conjunto plano de derechos que pueden utilizar para crear y modificar funciones.

Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, en **Control de acceso de tenants**, haga clic en **Paquetes de derechos**.
- 3 Seleccione el botón de radio que hay al lado del paquete de destino y haga clic en **Publicar**.
- 4 Para publicar el paquete:
 - a Seleccione **Publicar en tenants**.
 - b Seleccione las organizaciones para las que desea publicar la función.
 - Si desea publicar el paquete en todas las organizaciones existentes y recién creadas en el sistema, seleccione **Publicar en todos los tenants**.
 - Si desea publicar el paquete en algunas organizaciones en particular del sistema, seleccione esas organizaciones de forma individual.
- 5 Para cancelar la publicación del paquete:
 - Si desea cancelar la publicación del paquete en todas las organizaciones del sistema, anule la selección de **Publicar en tenants**.
 - Si desea cancelar la publicación del paquete en algunas organizaciones en particular del sistema, anule la selección de **Publicar en todos los tenants** y anule la selección de las organizaciones de forma individual.
- 6 Haga clic en **Guardar**.

Resultados


Los derechos incluidos en el paquete publicado están disponibles en las organizaciones seleccionadas y pueden utilizarse en las funciones de esas organizaciones.

Los derechos incluidos en la función cuya publicación se ha cancelado se eliminan de las organizaciones seleccionadas y no pueden utilizarse en las funciones de estas organizaciones.

Ver y editar un paquete de derechos

Puede ver los derechos que se incluyen en un paquete de derechos. Puede modificar el nombre, la descripción y los derechos de un paquete.

Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, en **Control de acceso de tenants**, haga clic en **Paquetes de derechos**.
- 3 Haga clic en el nombre del paquete de destino.
Puede ver los derechos que están asociados con el paquete al expandir las categorías de la derecha.
- 4 Edite el paquete y haga clic en **Conservar**.


Resultados

Si ha modificado los derechos del paquete, el nuevo conjunto de derechos se aplica a todas las organizaciones en la que se publica este paquete de derechos.

Eliminar un paquete de derechos

Puede quitar un paquete de derechos que ya no utilice en las organizaciones.

Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, en **Control de acceso de tenants**, haga clic en **Paquetes de derechos**.
- 3 Active el botón de radio junto al paquete de destino y haga clic en **Eliminar**.
- 4 Para confirmar, haga clic en **Aceptar**.

Administrar las funciones de tenant globales

Como administrador del sistema, puede crear funciones de tenant globales y publicarlas en una o varias organizaciones en la nube. Puede editar y eliminar las funciones de tenant globales existentes. Puede cancelar la publicación de funciones de tenant globales de organizaciones individuales en la nube.

Después de la instalación inicial y la configuración de vCloud Director, el sistema contiene un conjunto de tenants globales predefinidos que se publican en todas las organizaciones. Consulte [Funciones predeterminadas y sus derechos](#).


Crear una función de tenant global

Puede crear una función de tenant global que se puede publicar en una o varias organizaciones del sistema.

Tras la instalación y la configuración iniciales de vCloud Director, el sistema contiene funciones de tenant globales predefinidas que se publican en todas las organizaciones. Para obtener información sobre las funciones predefinidas, consulte [Funciones predeterminadas y sus derechos](#).

Puede agregar funciones globales personalizadas al sistema.

Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, en **Control de acceso de tenants**, haga clic en **Funciones globales**.
- 3 Haga clic en **Agregar**.
- 4 Introduzca un nombre y, si lo desea, una descripción para la nueva función.
- 5 Seleccione los derechos que desea asociar con la función.

Los derechos se agrupan en categorías y subcategorías para ver o administrar el acceso al objeto con los que se relacionan.

Puede seleccionar los derechos de forma individual, por vista o administración según la subcategoría, o bien por vista o administración de forma global.

Categoría	Descripción
Control de acceso	Contiene los derechos para ver y administrar organizaciones, derechos, funciones y usuarios.
Administración	Contiene los derechos para ver y administrar la configuración general y multisitio.
Proceso	Contiene los derechos para ver y administrar los VDC de organización y de proveedor, las vApps, las plantillas de VDC de organización y la supervisión de máquinas virtuales.
Extensiones	Contiene los derechos para ver y administrar los complementos y las extensiones de vCloud Director.
Infraestructura	Contiene los derechos para ver y administrar los recursos de vSphere.
Bibliotecas	Contiene los derechos para ver y administrar los catálogos y sus elementos.
Red	Contiene los derechos para ver y administrar los recursos de red.

- 6 Haga clic en **Conservar**.

Resultados

Tras crearlo, el nuevo derecho de tenant global solo está disponible para la organización del proveedor de vCloud Director.

Pasos siguientes

Puede publicar la función recién creada en una o varias organizaciones del sistema. Consulte [Publicar o cancelar la publicación de una función global de tenant](#).


Publicar o cancelar la publicación de una función global de tenant

Puede publicar una función global de tenant para una o varias organizaciones del sistema. Después de publicar una función en una organización, esa función pasa a formar parte del conjunto de funciones de tenant de la organización.

Requisitos previos

Si desea cancelar en una organización la publicación de una función global de tenant, compruebe que no se haya asignado a ningún usuario esa función en la organización.

Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, en **Control de acceso de tenants**, haga clic en **Funciones globales**.
- 3 Seleccione el botón de radio situado junto a la función de destino y haga clic en **Publicar**.
- 4 Para publicar la función:
 - a Seleccione **Publicar en tenants**.
 - b Seleccione las organizaciones para las que desea publicar la función.
 - Si desea publicar la función en todas las organizaciones existentes y de nueva creación en el sistema, seleccione **Publicar en todos los tenants**.
 - Si desea publicar la función para organizaciones particulares del sistema, seleccione esas organizaciones de forma individual.
- 5 Para cancelar la publicación de la función:
 - Si desea cancelar la publicación de la función en todas las organizaciones existentes en el sistema, anule la selección de **Publicar en tenants**.
 - Si desea cancelar la publicación de la función en algunas organizaciones en particular del sistema, anule la selección de **Publicar en todos los tenants** y anule de forma individual la selección de las organizaciones.
- 6 Haga clic en **Guardar**.

Resultados


La función publicada está disponible en las organizaciones seleccionadas y puede asignarse a los usuarios de esas organizaciones. Los administradores de organización no pueden editar las funciones globales de tenant que se publican para sus organizaciones.

La función cuya publicación se ha cancelado se elimina de las organizaciones seleccionadas y no se puede asignar a los usuarios de esas organizaciones.

Ver y editar una función global de tenant

Puede ver los derechos incluidos en una función global de tenant. Puede modificar el nombre, la descripción y los derechos de una función global tenant.

Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, en **Control de acceso de tenants**, haga clic en **Funciones globales**.
- 3 Haga clic en el nombre de la función de destino.
Puede ver los derechos que están asociados con la función al expandir las categorías de la derecha.
- 4 Para modificar el nombre, la descripción o los derechos de la función, haga clic en **Editar**.
- 5 Edite la función y haga clic en **Conservar**.

Resultados

Si ha modificado los derechos de la función, el nuevo conjunto de derechos se aplica a los usuarios de todas las organizaciones a las que se haya asignado esta función.


Eliminar una función de tenant global

Puede quitar una función de tenant global que ya no utilice en las organizaciones.

Requisitos previos

La función de tenant global que desea eliminar no debe estar asignada a ningún usuario en ninguna de las organizaciones.

Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, en **Control de acceso de tenants**, haga clic en **Funciones globales**.
- 3 Seleccione el botón de radio situado junto a la función de destino y haga clic en **Eliminar**.
- 4 Para confirmar, haga clic en **Aceptar**.

Administrar funciones de proveedor

Puede crear y administrar las funciones de la organización de proveedor de vCloud Director.

Para obtener información sobre la administración de funciones de tenant, consulte la *Guía del portal para tenants de vCloud Director*.


Crear una función de proveedor

Puede crear una función en la organización del proveedor de vCloud Director.

Tras la instalación y la configuración iniciales de vCloud Director, el sistema contiene funciones predefinidas que son locales para la organización del proveedor y globales para todas las organizaciones. Para obtener información sobre las funciones predefinidas, consulte [Funciones predeterminadas y sus derechos](#).

Puede agregar funciones de proveedor personalizadas a la organización del proveedor.

Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, en **Control de acceso de proveedores**, haga clic en **Funciones**.
- 3 Haga clic en **Nuevo**.
- 4 Introduzca un nombre y, si lo desea, una descripción para la nueva función.
- 5 Seleccione los derechos que desea asociar con la función.

Los derechos se agrupan en categorías y subcategorías para ver o administrar el acceso al objeto con los que se relacionan.

Puede seleccionar los derechos de forma individual, por vista o administración según la subcategoría, o bien por vista o administración de forma global.

Categoría	Descripción
Control de acceso	Contiene los derechos para ver y administrar organizaciones, derechos, funciones y usuarios.
Administración	Contiene los derechos para ver y administrar la configuración general y multisitio.
Proceso	Contiene los derechos para ver y administrar los VDC de organización y de proveedor, las vApps, las plantillas de VDC de organización y la supervisión de máquinas virtuales.
Extensiones	Contiene los derechos para ver y administrar los complementos y las extensiones de vCloud Director.
Infraestructura	Contiene los derechos para ver y administrar los recursos de vSphere.
Bibliotecas	Contiene los derechos para ver y administrar los catálogos y sus elementos.
Red	Contiene los derechos para ver y administrar los recursos de red.

- 6 Haga clic en **Guardar**.


Resultados

La función recién creada está disponible para asignarla a los usuarios de la organización del proveedor.

Ver o editar una función de proveedor

Puede ver los derechos incluidos en una función que es local para la organización de proveedor de vCloud Director. Puede modificar el nombre, la descripción y los derechos de una función.

Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, en **Control de acceso de proveedores**, haga clic en **Funciones**.
- 3 Haga clic en el nombre de la función de destino.
Puede ver los derechos que están asociados con la función al expandir las categorías de la derecha.
- 4 Para modificar el nombre, la descripción o los derechos de la función, haga clic en **Editar**.
- 5 Edite la función y haga clic en **Guardar**.

Resultados

Si ha modificado los derechos de la función, el nuevo conjunto de derechos se aplica a los usuarios a los que se haya asignado esta función.


Eliminar una función de proveedor

Puede quitar una función que ya no utilice en la organización del proveedor de vCloud Director.

Requisitos previos

La función que desea eliminar no debe estar asignada a ningún usuario.

Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, en **Control de acceso de proveedores**, haga clic en **Funciones**.
- 3 Seleccione el botón de radio situado junto a la función de destino y haga clic en **Eliminar**.
- 4 Para confirmar, haga clic en **Aceptar**.

Administrar usuarios y grupos de proveedor

Puede agregar e importar usuarios y grupos a su organización de proveedor vCloud Director.

Para obtener información sobre la administración de grupos y usuarios de la organización, consulte la *Guía del portal para tenants de vCloud Director*.

Administrar usuarios de proveedor

Puede administrar los usuarios de la organización de proveedor mediante el uso del Service Provider Admin Portal.


Para obtener información sobre la administración de usuarios del tenant de organizaciones, consulte la *Guía del portal para tenants de vCloud Director*.

Crear un usuario de proveedor

Puede crear un usuario en la organización del proveedor de vCloud Director.

Durante la instalación y la configuración de vCloud Director, se crea una cuenta de **administrador del sistema**. Tras la configuración inicial, puede crear usuarios y administradores adicionales en la organización del proveedor.

Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, en **Control de acceso de proveedores**, haga clic en **Usuarios**.
- 3 Haga clic en **Nuevo**.
- 4 Introduzca un nombre de usuario y una contraseña para el nuevo usuario.
La contraseña debe tener al menos seis caracteres.
- 5 Seleccione si desea habilitar el usuario tras la creación.
- 6 En el menú desplegable **Funciones disponibles**, seleccione una función para el usuario.
La lista de funciones disponibles consta de las funciones globales y las funciones que son locales para la organización del sistema.
- 7 (opcional) Introduzca la información de contacto para el usuario.
Puede introducir el nombre completo, la dirección de correo electrónico, el número de teléfono y el identificador de mensajería instantánea.
- 8 (opcional) Establezca las cuotas para el usuario.
 - a Puede establecer un límite de máquinas virtuales que pertenecen al usuario o seleccionar **Sin límite**.
 - b Puede establecer un límite de máquinas virtuales en ejecución que pertenecen al usuario o seleccionar **Sin límite**.


Importar usuarios de proveedor

Puede importar usuarios a su organización de proveedor de vCloud Director desde un proveedor de identidad LDAP o SAML previamente configurado.

Requisitos previos

[Configurar una conexión LDAP de sistema](#) o [Configurar el sistema para usar un proveedor de identidad SAML](#).

Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, en **Control de acceso de proveedores**, haga clic en **Usuarios**.

3 Haga clic en **Importar usuarios**.

4 En el menú desplegable **Origen**, seleccione el tipo de proveedor de identidad.

Puede ser **LDAP** o **SAML**.

Si configuró solo un proveedor de identidad, esta opción está preprogramada.

5 Especifique los usuarios.

Opción	Descripción
LDAP	<p>a Escriba un nombre completo o parcial de un usuario y haga clic en Buscar.</p> <p>b En los resultados de búsqueda, seleccione los usuarios que desee importar.</p> <p>c En el menú desplegable de Asignar función, seleccione una función para los usuarios importados.</p>
SAML	<p>a Escriba los nombres de usuario de los usuarios que desea importar en el formato de identificador de nombre admitido por el proveedor de identidad SAML.</p> <p>Utilice una línea nueva para cada nombre de usuario.</p> <p>b En el menú desplegable de Asignar función, seleccione una función para los usuarios importados.</p>

6 Haga clic en **Guardar**.


Resultados

Puede ver los usuarios importados en la lista de usuarios.

Editar un usuario de proveedor

Puede cambiar la contraseña, la función, la información de contacto y las cuotas de un usuario de la organización de proveedor. Sin embargo, no puede cambiar el nombre de usuario.


Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, en **Control de acceso de proveedores**, haga clic en **Usuarios**.
- 3 Haga clic en el botón de radio junto al nombre del usuario de destino y haga clic en **Editar**.
- 4 Edite los detalles del usuario y haga clic en **Guardar**.

Deshabilitar o habilitar un usuario de proveedor

Después de deshabilitar a un usuario, este no puede iniciar sesión en vCloud Director.

Procedimiento

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

- 2 En el panel izquierdo, en **Control de acceso de proveedores**, haga clic en **Usuarios**.
- 3 Haga clic en el botón de radio junto al nombre del usuario de destino y haga clic en **Habilitar** o **Deshabilitar**.
- 4 Si deshabilita un usuario, haga clic en **Aceptar** para confirmar.


Eliminar un usuario de proveedor

Puede quitar un usuario de la organización del proveedor de vCloud Director si elimina la cuenta de usuario.

Requisitos previos

Deshabilite el usuario que desea eliminar. Consulte [Deshabilitar o habilitar un usuario de proveedor](#).

Procedimiento


- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, en **Control de acceso de proveedores**, haga clic en **Usuarios**.
- 3 Haga clic en el botón de radio junto al nombre del usuario de destino y haga clic en **Eliminar**.
- 4 Para confirmar, haga clic en **Aceptar**.

Desbloquear un usuario proveedor

Si se habilitó el bloqueo de cuenta en la configuración del sistema de políticas de contraseñas, los usuarios podrían bloquear sus cuentas tras un número determinado de intentos de inicio de sesión fallidos. Incluso si el bloqueo se ha establecido con un intervalo de bloqueo de cuenta, se puede desbloquear una cuenta de usuario sin esperar a que caduque el bloqueo.

Para obtener información sobre cómo configurar la política de bloqueo de cuenta, consulte la *Guía del administrador de vCloud Director*.

Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, en **Control de acceso de proveedores**, haga clic en **Usuarios**.
- 3 Haga clic en el botón de radio junto al nombre de usuario de destino y haga clic en **Desbloquear**.

Administrar grupos de proveedores

Puede importar, editar y eliminar grupos de la organización del proveedor mediante el Service Provider Admin Portal.

Para obtener información sobre la administración de grupos en las organizaciones, consulte la *Guía del portal para tenants de vCloud Director*.


Importar un grupo de proveedor

Puede importar grupos a su organización de proveedor de vCloud Director desde un proveedor de identidad LDAP o SAML previamente configurado.

Requisitos previos

[Configurar una conexión LDAP de sistema](#) o [Configurar el sistema para usar un proveedor de identidad SAML](#).

Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, en **Control de acceso de proveedores**, haga clic en **Grupos**.
- 3 Haga clic en **Importar grupos**.
- 4 En el menú desplegable **Origen**, seleccione el tipo de proveedor de identidad.

Puede ser **LDAP** o **SAML**.

Si configuró solo un proveedor de identidad, esta opción está preprogramada.

- 5 Especifique los usuarios.


Opción	Descripción
LDAP	<ol style="list-style-type: none"> a Escriba un nombre completo o parcial de un grupo y haga clic en Buscar. b En los resultados de búsqueda, seleccione los grupos que desee importar. c En el menú desplegable de Asignar función, seleccione una función para los usuarios de los grupos importados.
SAML	<ol style="list-style-type: none"> a Escriba los nombres de los grupos que desea importar en el formato de identificador de nombre admitido por el proveedor de identidad SAML. Utilice una línea nueva para cada nombre de grupo. b En el menú desplegable de Asignar función, seleccione una función para los usuarios de los grupos importados.

- 6 Haga clic en **Guardar**.

Editar un grupo de proveedor

Puede modificar la descripción y cambiar la función de los miembros de un grupo que importó con anterioridad a su organización de proveedor vCloud Director.

Procedimiento


- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, en **Control de acceso de proveedores**, haga clic en **Grupos**.
- 3 Haga clic en el botón de radio junto al nombre del grupo de destino y haga clic en **Editar**.

- 4 Edite los detalles del grupo y haga clic en **Guardar**.

Eliminar un grupo de proveedores

Se puede quitar un grupo de la organización del proveedor de vCloud Director.

Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, en **Control de acceso de proveedores**, haga clic en **Grupos**.
- 3 Haga clic en el botón de radio junto al nombre del grupo de destino y haga clic en **Eliminar**.
- 4 Para confirmar, haga clic en **Aceptar**.

Administrar la configuración del sistema

11

Un administrador del sistema de vCloud Director puede controlar la configuración de todo el sistema relacionada con LDAP, la notificación de correo electrónico, las licencias y las preferencias generales del sistema.

Este capítulo incluye los siguientes temas:

- [Administrar proveedores de identidad](#)
- [Administrar complementos](#)
- [Personalizar los portales de vCloud Director](#)

Administrar proveedores de identidad

Puede integrar su nube con un proveedor de identidad externo e importar usuarios y grupos a las organizaciones. Puede configurar una conexión de servidor LDAP en el nivel de sistema o de organización. Puede configurar una integración de SAML al nivel de la organización.


Administrar las conexiones LDAP

Como administrador del sistema, puede configurar la organización del sistema vCloud Director y cualquier otra organización en el sistema para utilizar un servidor LDAP como origen de los usuarios y grupos. Las organizaciones pueden usar la conexión LDAP del sistema o una conexión LDAP privada.

Configurar una conexión LDAP de sistema

Para proporcionar a vCloud Director y a sus organizaciones acceso compartido a los usuarios y los grupos, puede configurar una conexión LDAP en el nivel del sistema.

Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, en **Proveedores de identidad**, haga clic en **LDAP**.

Se mostrará la configuración de LDAP actual.



Pasos siguientes

[Configurar, probar y sincronizar una conexión LDAP.](#)

Configurar una conexión LDAP de organización

Puede configurar una organización para que utilice la conexión LDAP de sistema como un origen compartido de usuarios y grupos. Asimismo, puede configurar una organización para que utilice una conexión LDAP independiente como un origen privado de usuarios y grupos.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **Organizaciones**.
- 3 Haga clic en el nombre de la organización de destino.
Se lo redirigirá al portal para tenants de vCloud Director de la organización.
- 4 En el menú principal () , seleccione **Administración**.
- 5 En el panel izquierdo, en **Proveedores de identidad**, haga clic en **LDAP**.
Se mostrará la configuración de LDAP actual.
- 6 En la pestaña **Opciones LDAP**, haga clic en **Editar**.
- 7 Configure el origen de usuarios y grupos de LDAP para esta organización, y haga clic en **Guardar**.

Opción	Descripción
No utilizar LDAP	La organización no utiliza un servidor LDAP como un origen de usuarios y grupos de organización.
Servicio LDAP del sistema VCD	La organización utiliza la conexión LDAP del sistema de vCloud Director que se ha configurado previamente. Consulte Configurar una conexión LDAP de sistema .
Servicio LDAP personalizado	La organización utiliza un servidor LDAP privado como un origen de usuarios y grupos de organización. Haga clic en la pestaña LDAP personalizado y siga los pasos descritos en Configurar, probar y sincronizar una conexión LDAP .

Configurar, probar y sincronizar una conexión LDAP

Para configurar una conexión LDAP de sistema u organización, se configuran los detalles del servidor LDAP. Puede probar la conexión para asegurarse de que haya introducido la configuración correcta, y de que los atributos de usuario y grupo estén asignados correctamente. Cuando una conexión LDAP se establece correctamente, puede sincronizar vCloud Director con el servidor LDAP en cualquier momento.

Requisitos previos

Si tiene pensado conectarse a un servidor LDAPS, compruebe que tiene un certificado generado correctamente para la compatibilidad mejorada de LDAP en Java 8 (actualización 181). Para obtener más información, consulte los *Cambios de la versión Java 8* en <https://www.java.com>.

Procedimiento

- 1 En la pestaña **Conexión**, escriba la información necesaria para la conexión LDAP.

Información necesaria	Descripción
Servidor	El nombre de host o la dirección IP del servidor LDAP.
Puerto	El número de puerto en el que el servidor LDAP está realizando la escucha. Para LDAP, el número de puerto predeterminado es 389. Para LDAPS, el número de puerto predeterminado es 636.
Nombre distintivo de la base	<p>El nombre distintivo (Distinguished Name, DN) de la base es la ubicación en el directorio LDAP en el que se conecta vCloud Director.</p> <p>Para conectarse en la raíz, introduzca solo los componentes de dominio (por ejemplo, DC=example,DC=com).</p> <p>Para conectarse a un nodo en el árbol, introduzca el nombre distintivo de dicho nodo (por ejemplo, OU=ServiceDirector,DC=example,DC=com).</p> <p>La conexión a un nodo limita el alcance del directorio disponible para vCloud Director.</p>
Tipo de conector	El tipo de servidor LDAP. Puede ser Active Directory u OpenLDAP .
Utilizar SSL	Si su servidor es LDAPS, active esta casilla de verificación.
Aceptar todos los certificados	Si su servidor es LDAPS, active esta casilla de verificación o cargue el certificado SSL de LDAP.
Almacén de confianza personalizado	Si su servidor es LDAPS, haga clic en el icono de carga () e importe un certificado SSL de LDAP, o bien seleccione Aceptar todos los certificados .
Método de autenticación	<p>La autenticación simple consiste en enviar al servidor LDAP el DN y la contraseña del usuario. Si utiliza LDAP, la contraseña LDAP se envía por la red en un texto no cifrado.</p> <p>Si desea usar Kerberos, debe configurar la conexión LDAP mediante el cliente web de vCloud Director. Para obtener más información, consulte la <i>Guía del administrador de vCloud Director</i>.</p>
Nombre de usuario	<p>El nombre de usuario de DN de LDAP completo para conectarse al servidor LDAP.</p> <p>Si la compatibilidad de lectura anónima está habilitada en su servidor LDAP, puede dejar estos cuadros de texto en blanco.</p>
Contraseña	<p>La contraseña para conectarse al servidor LDAP.</p> <p>Si la compatibilidad de lectura anónima está habilitada en su servidor LDAP, puede dejar estos cuadros de texto en blanco.</p>

- 2 Haga clic en la pestaña **Atributos de usuario**, examine los valores predeterminados de los atributos de usuario y, si el directorio LDAP utiliza un esquema diferente, modifique los valores.

- 3 Haga clic en la pestaña **Atributos de grupo**, examine los valores predeterminados de los atributos de grupo y, si el directorio LDAP utiliza un esquema diferente, modifique los valores.
- 4 Haga clic en **Guardar**.
- 5 Realice lo siguiente para probar la configuración de conexión LDAP y las asignaciones de atributos LDAP:

- a Haga clic en **Probar**.
- b Introduzca la contraseña del usuario del servidor LDAP que ha configurado y haga clic en **Probar**.

Si se ha conectado correctamente, se muestra una marca de verificación de color verde.

Los valores de atributos de grupo y usuario recuperados se muestran en una tabla. Los valores que se asignan correctamente a atributos LDAP están señalados con marcas de verificación de color verde. Los valores que no se asignan a atributos LDAP se dejan en blanco y se señalan con signos de exclamación de color rojo.

- c Para salir, haga clic en **Cancelar**.
- 6 Para sincronizar vCloud Director con el servidor LDAP configurado, haga clic en **Sincronizar**.
vCloud Director sincroniza la información de grupo y usuario con el servidor LDAP de forma periódica según el intervalo de sincronización que se haya establecido en la configuración general del sistema.

Espere unos minutos hasta que finalice la sincronización.

Resultados

Puede importar usuarios y grupos del servidor LDAP recién configurado.

Configurar el sistema para usar un proveedor de identidad SAML

Si desea importar usuarios y grupos desde un proveedor de identidad SAML a la organización del sistema, debe configurar la organización del sistema con dicho proveedor de identidad SAML. Los usuarios importados pueden iniciar sesión en la organización del sistema con las credenciales establecidas en el proveedor de identidad SAML.

Para configurar vCloud Director con un proveedor de identidad SAML, establezca una confianza mutua mediante el intercambio de metadatos de proveedor de identidad y proveedor de servicios SAML.

Cuando un usuario importado intenta iniciar sesión, el sistema extrae los siguientes atributos del token SAML (si está disponible) y los utiliza para interpretar los datos correspondientes sobre el usuario.

- email address = "EmailAddress"
- user name = "UserName"
- full name = "FullName"

- `user's groups = "Groups"`
- `user's roles = "Roles"` (este atributo puede configurarse)

Se utiliza la información del grupo si el usuario no se ha importado directamente, pero se espera que inicie sesión debido a que pertenece a grupos importados. Un usuario puede pertenecer a varios grupos, por lo que 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 se puede configurar mediante la API y solo 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

- Compruebe que tiene acceso a un proveedor de identidad compatible con SAML 2.0.
- Obtenga un archivo XML con los siguientes metadatos de su proveedor de identidad SAML.
 - 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 SAML.

Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel de la izquierda, en Proveedores de identidad, haga clic en **SAML** y luego en **Editar**.

Se muestra la configuración de SAML actual.

- 3 En la pestaña **Proveedor de servicios**, descargue los metadatos de proveedor de servicios SAML de vCloud Director.

- a Introduzca un identificador de entidad para la organización del sistema.

El identificador de entidad identifica de manera exclusiva la organización del sistema en el proveedor de identidad.

- b Examine la fecha de caducidad del certificado y, si caduca pronto, haga clic en **Volver a generar** para volver a generar el certificado.

El certificado se incluye en los metadatos de SAML y se utiliza para el cifrado y la firma. Uno de estos o ambos pueden ser necesarios dependiendo de cómo se establezca la confianza entre su organización y el IDP de SAML.


- c Haga clic en el vínculo **Metadatos**.

El vínculo es similar a `https://nombre_de_host_de_VCD/cloud/org/System/saml/metadata/alias/vcd`.

El navegador descarga los metadatos del proveedor de servicios SAML como un archivo XML, el cual debe proporcionar al proveedor de identidad.

- 4 En la pestaña **Proveedor de identidad**, cargue los metadatos de SAML que recibió anteriormente del proveedor de identidad.

- a Seleccione **Utilizar proveedor de identidad SAML**.

- b Haga clic en el icono **Examinar** () y cargue el archivo, o bien copie y pegue el contenido de este en el cuadro de texto **XML de metadatos**.

- 5 Haga clic en **Guardar**.

Resultados

Administrar complementos

Los complementos de vCloud Director amplían las funciones de Service Provider Admin Portal y vCloud Director Tenant Portal. Es posible cargar, deshabilitar y eliminar complementos de Service Provider Admin Portal. Es posible publicar un complemento en el proveedor de servicios y en organizaciones individuales.

Algunos complementos se instalan como parte de vCloud Director.

Extensión de CPOM

Proporciona la capacidad para ver y administrar SDDC y servidores proxy de SDDC mediante vCloud Director Tenant Portal.

Personalizar portal

Proporciona la capacidad para personalizar vCloud Director Service Provider Admin Portal y vCloud Director Tenant Portal.

vCloud Availability

El complemento VMware vCloud® Availability™ proporciona la capacidad de acceder directamente a vCloud Availability Portal directamente desde la interfaz de usuario de vCloud Director. Para obtener más información, consulte la [documentación de vCloud Availability](#).


Cargar un complemento

Puede cargar más complementos en el vCloud Director Service Provider Admin Portal para que el proveedor de servicios y las organizaciones en la nube puedan usarlos.

Requisitos previos

Descargue el archivo de instalación del complemento.

Procedimiento

- 1 En el menú principal () , seleccione **Personalizar portal**.
- 2 Haga clic en **Cargar**.
- 3 Haga clic en **Seleccionar archivo de complemento**, desplácese al archivo de instalación de destino y haga clic en **Abrir**.
- 4 Haga clic en **Siguiente**.
- 5 Seleccione el ámbito de este complemento.


Opción	Descripción
Proveedores de servicios	La función del complemento está disponible en el vCloud Director Service Provider Admin Portal.
Tenants	La función del complemento está disponible en el vCloud Director Service Provider Admin Portal de las organizaciones que seleccione.

- 6 Si el ámbito del complemento está establecido en Tenants, seleccione las organizaciones en las que desea publicar este complemento.
- 7 Repase la página **Revisar y finalizar** y haga clic en **Finalizar**.

Habilitar o deshabilitar un complemento

Para evitar que todas las organizaciones utilicen un complemento, es posible deshabilitarlo.


Procedimiento

- 1 En el menú principal () , seleccione **Personalizar portal**.
- 2 Seleccione las casillas de verificación junto a los nombres de los complementos de destino y haga clic en **Habilitar** o **Deshabilitar**.

Eliminar un complemento

Es posible quitar uno o varios complementos de vCloud Director Service Provider Admin Portal.

Procedimiento


- 1 En el menú principal () , seleccione **Personalizar portal**.
- 2 Seleccione las casillas de verificación junto a los nombres de los complementos que desea quitar y haga clic en **Eliminar**.
- 3 Para confirmar, haga clic en **Guardar**.

Publicar o cancelar la publicación de un complemento de una organización

Es posible modificar el conjunto de organizaciones que pueden utilizar la función que proporciona un complemento.

Es posible modificar el conjunto de organizaciones para varios complementos.

Procedimiento

- 1 En el menú principal () , seleccione **Personalizar portal**.
- 2 Seleccione las casillas de verificación junto a los nombres de los complementos de destino y haga clic en **Publicar**.
- 3 Seleccione el alcance de este complemento.

Opción	Descripción
Proveedores de servicios	La función de complemento se vuelve disponible en vCloud Director Service Provider Admin Portal.
Tenants	La función de complemento se vuelve disponible en el elemento vCloud Director Service Provider Admin Portal de las organizaciones que se seleccionen.

- 4 Si el alcance del complemento abarca a los tenants, seleccione las organizaciones en las que desea publicar este complemento.
- 5 Haga clic en **Guardar**.

Personalizar los portales de vCloud Director

Para respetar los criterios corporativos de personalización de marca y crear una experiencia de nube totalmente personalizada, es posible establecer el logotipo y el tema de vCloud Director Service Provider Admin Portal y vCloud Director Tenant Portal de cada organización. Además, es

posible modificar y agregar vínculos personalizados a los dos menús de la parte superior derecha de los portales de vCloud Director.

Nota Para personalizar los vínculos y los atributos de personalización de marca, es necesario usar los métodos branding de vCloud OpenAPI. Consulte *Introducción a vCloud OpenAPI* en <https://code.vmware.com>.

Personalización de marca de portales

Como parte de la instalación, vCloud Director contiene dos temas: predeterminado y oscuro. Puede crear, administrar y aplicar temas personalizados. Además, puede cambiar el nombre, el logotipo y el icono de explorador de los portales. Asimismo, el título del explorador adopta el nombre del portal que se haya establecido.

Configure los atributos de personalización de marca en un nivel del sistema para personalizar vCloud Director Service Provider Admin Portal. El elemento vCloud Director Tenant Portal de cada organización adopta los atributos de personalización de marca del sistema, a menos que se hayan configurado atributos de personalización de marca para el tenant específico.

Para un tenant específico, puede reemplazar de forma selectiva cualquier combinación de nombre de portal, color de fondo, logotipo, icono, tema y vínculos personalizados. Todo valor que no se establezca utiliza el valor predeterminado del sistema correspondiente.

Nota De forma predeterminada, la personalización de marca de un tenant individual no se muestra fuera de una sesión iniciada. La personalización de marca de un tenant individual no aparece en las páginas de inicio y cierre de sesión, para que los tenants no puedan detectar la existencia de otros tenants. Puede habilitar la personalización de marca fuera de las sesiones iniciadas mediante la herramienta de administración de celdas:

```
manage-config -n backend.branding.requireAuthForBranding -v false
```

Para obtener información sobre el uso de la herramienta de administración de celdas, consulte *Guía del administrador de vCloud Director*.

Vínculos personalizados

Los vínculos personalizados son un componente de la personalización de marca de los portales. Existen dos tipos de vínculos personalizados:

- Los elementos de menú override reemplazan los vínculos existentes para los elementos de menú **Ayuda**, **Acerca de** y **Descargar VMRC**. De forma predeterminada, **Descargar VMRC** redirige a los usuarios a <https://my.vmware.com> para descargar VMRC, lo que requiere que los usuarios tengan cuentas registradas para descarga. Al anular este vínculo, es posible reubicar el instalador de VMRC en un servidor propio.
- Los elementos de menú link son nuevos vínculos que se agregan al elemento de menú **Cerrar sesión** en la esquina superior derecha del portal. Los nuevos vínculos personalizados aparecen en el orden indicado en la llamada de API.

Puede organizar estos vínculos personalizados mediante los elementos de menú `section` y `separator`. Un elemento de menú `section` agrega un encabezado al menú, un elemento de menú `separator` agrega una línea al menú.

Los vínculos personalizados admiten variables personalizadas que se pueden utilizar para transmitir información de identificación a otras aplicaciones en forma de parámetros de consulta.

vCloud Director admite las siguientes variables personalizadas en el valor `url` para un vínculo personalizado:

Tabla 11-1. Variables personalizadas para vínculos personalizados

Variable	Descripción
<code>\${TENANT_NAME}</code>	Nombre de la organización
<code>\${TENANT_ID}</code>	Identificador de la organización
<code>\${SESSION_TOKEN}</code>	Token x-vcloud-authorization

Por ejemplo,

```
url: https://host:puerto/tenant/${TENANT_NAME}/vdcs
```

en vCloud Director Tenant Portal para la organización `myorg` se convierte en:

```
url: https://host:puerto/tenant/myorg/vdcs
```

Supervisar vCloud Director

12

Los administradores del sistema pueden supervisar las operaciones completadas y en curso y visualizar la información de uso de recursos al nivel de centro de datos virtual de proveedor, de centro de datos virtual de organización y de almacén de datos.

Este capítulo incluye los siguientes temas:

- [vCloud Director e informe de costes](#)
- [Ver información de uso de un centro de datos virtual de proveedor](#)

vCloud Director e informe de costes

Puede usar la VMware vRealize Operations Tenant App de vCloud Director para configurar un sistema de informes de costes para vCloud Director.

La VMware vRealize Operations Tenant App incluye funcionalidades de medición que permiten a los proveedores de servicios ofrecer servicios de contracargo a su base de clientes.

La VMware vRealize Operations Tenant App también es una aplicación para tenants, lo cual permite a los administradores de tenants ver su entorno y sus datos de facturación.

Para obtener información sobre la compatibilidad entre vCloud Director y la VMware vRealize Operations Tenant App, consulte las *matrices de interoperabilidad de productos de VMware* en http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.


Puede descargar la VMware vRealize Operations Tenant App en <https://marketplace.vmware.com/vsx/solutions/management-pack-for-vcloud-director>.

Para obtener información sobre cómo utilizar la VMware vRealize Operations Tenant App, consulte *Utilizar vRealize Operations Tenant App for vCloud Director como proveedor de servicios* y *Utilizar vRealize Operations Tenant App for vCloud Director como tenant*.

Ver información de uso de un centro de datos virtual de proveedor

Los centros de datos virtuales de proveedor proporcionan recursos informáticos, de memoria y de almacenamiento a sus centros de datos virtuales de organización. Puede supervisar el uso de los recursos del centro de datos virtual de proveedor para decidir si desea agregar más recursos.

Procedimiento

- 1 En el menú principal () , seleccione **Recursos de nube**.
- 2 En el panel izquierdo, haga clic en **VDC de proveedor** y, a continuación, haga clic en el nombre del centro de datos virtual de proveedor de destino.
- 3 Haga clic en la pestaña **Configurar > Métricas**.
- 4 Para obtener más detalles sobre cada parámetro, haga clic en cada icono de información.

La vista Bibliotecas de contenido del vCloud Director Service Provider Admin Portal proporciona una interfaz para la integración con vRealize Orchestrator. Los flujos de trabajo de vRealize Orchestrator están disponibles como un catálogo de servicios que los administradores de proveedores de servicios pueden publicar en los tenants o en otros proveedores de servicios para ampliar el conjunto de funciones y capacidades de administración que ofrecen.

Este capítulo incluye los siguientes temas:

- [Integrar vRealize Orchestrator con vCloud Director](#)
- [Crear una categoría de servicios](#)
- [Editar una categoría de servicios](#)
- [Importar un servicio](#)
- [Buscar un servicio](#)
- [Ejecutar un servicio](#)
- [Cambiar una categoría de servicios](#)
- [Eliminar un servicio del registro](#)
- [Publicar un servicio](#)

Integrar vRealize Orchestrator con vCloud Director

vRealize Orchestrator se integra con vCloud Director mediante el vCloud Director Service Provider Admin Portal.

La integración de vRealize Orchestrator con vCloud Director amplía la funcionalidad básica de vCloud Director al permitir que los administradores de proveedores de servicios desarrollen tareas de automatización complejas mediante la orquestación de flujos de trabajo y el uso de complementos de terceros.

Gracias al vCloud Director Service Provider Admin Portal, los administradores de proveedores de servicios son capaces de ver, importar y ejecutar flujos de trabajo de instancias del servidor de vRealize Orchestrator registradas.

En el vCloud Director Service Provider Admin Portal, los flujos de trabajo de vRealize Orchestrator se pueden publicar en los proveedores de servicios o los tenants, lo que permite control de acceso y ejecución rápidos de servicios personalizados e integrados.

vRealize Orchestrator cuenta con una amplia biblioteca de flujos de trabajo que contiene tareas creadas previamente diseñadas para resolver desafíos específicos y realizar tareas administrativas comunes. Los complementos de terceros también están disponibles en [VMware Solution Exchange](#).



Registrar una instancia de vRealize Orchestrator en vCloud Director

Para aprovechar la orquestación de flujos de trabajo y la automatización de tareas mediante vRealize Orchestrator en vCloud Director, se debe registrar una instancia de vRealize Orchestrator en el vCloud Director Service Provider Admin Portal.


Requisitos previos

- Implemente y configure una instancia del servidor de vRealize Orchestrator. Para obtener más información, consulte la sección correspondiente a la *instalación y la configuración de VMware vRealize Orchestrator* en la documentación de vRealize Orchestrator.
- Configure vRealize Orchestrator para que utilice vSphere como proveedor de autenticación.
- Compruebe que vCloud Director esté registrado en el servicio de búsqueda de la misma instancia de Platform Services Controller que la instancia de vCenter Single Sign-On que vRealize Orchestrator utiliza para la autenticación.

Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas de contenido**.
 - a En el panel de la izquierda, seleccione **Administración de servicios**.
Aparecerá la lista de servidores de vRealize Orchestrator registrados.
- 2 Para registrar un nuevo servidor de vRealize Orchestrator, haga clic en el botón  .
Aparecerá el cuadro de diálogo **Registrar vRealize Orchestrator**.
- 3 Introduzca los siguientes valores.

Opción	Descripción
Nombre	Nombre de la instancia de vRealize Orchestrator registrada.
Descripción	Descripción de la instancia del servidor de vRealize Orchestrator registrada.
Nombre de host	El nombre de dominio completo y el puerto de servidor del servidor de vRealize Orchestrator. El valor del puerto HTTPS predeterminado es 8281. Nota vCloud Director se conecta a la interfaz de la API de vRealize Orchestrator.
Nombre de usuario	Una cuenta de usuario que pertenece al grupo de administradores de vRealize Orchestrator.

Opción	Descripción
Contraseña	La contraseña de la cuenta de administrador de vRealize Orchestrator.
Anclaje de veracidad	El certificado SSL del servidor de vRealize Orchestrator en formato PEM.
	Haga clic en el icono de carga () para buscar y seleccionar el archivo .pem.


- 4 Haga clic en **Aceptar** para completar el registro.


El servidor de vRealize Orchestrator se registrará en vCloud Director.

Crear una categoría de servicios

Los servicios se pueden organizar en categorías de servicios.

Procedimiento

- 1 En el menú principal (), seleccione **Bibliotecas de contenido**.
 - a En el panel de la izquierda, seleccione **Administración de servicios**.
 - b Desplácese hasta la pestaña **Categorías de servicio**.


Aparecerá la lista de categorías de servidor existentes.
- 2 Para crear una nueva categoría de servicios, haga clic en el botón  .
Aparecerá el cuadro de diálogo **Nueva categoría de servicios**.
- 3 Introduzca los siguientes valores.

Opción	Descripción
Nombre	Nombre de la categoría de servicios.
Icono	Importa el icono que se muestra para la categoría de servicios.
Descripción	Breve descripción de la categoría de servicios.


Editar una categoría de servicios

Puede editar categorías de servicios existentes.

Procedimiento

- 1 En el menú principal (), seleccione **Bibliotecas de contenido**.
 - a En el panel de la izquierda, seleccione **Administración de servicios**.
 - b Desplácese hasta la pestaña **Categorías de servicio**.

Aparecerá la lista de categorías de servidor existentes.

- 2 Utilice la barra de listas () que se encuentra a la izquierda de una categoría de servicios seleccionada y haga clic en **Editar**.
- 3 Edite los siguientes valores.

Opción	Descripción
Nombre	Nombre de la categoría de servicios.
Icono	Importa el icono que se muestra para la categoría de servicios.
Descripción	Breve descripción de la categoría de servicios.


Importar un servicio

Puede importar servicios de la biblioteca de flujos de trabajo de una instancia de vRealize Orchestrator que esté registrada en vCloud Director.

Requisitos previos

- Registre una instancia de vRealize Orchestrator. Consulte [Registrar una instancia de vRealize Orchestrator en vCloud Director](#).
- Cree una categoría de servicios. Consulte [Crear una categoría de servicios](#).

Procedimiento

- 1 En el menú principal (), seleccione **Bibliotecas de contenido**.
 - a En el panel de la izquierda, seleccione **Biblioteca de servicios**.

Los servicios disponibles se muestran en una vista de tarjetas con doce elementos por página organizados por nombre y en orden alfabético. Cada tarjeta indica que el elemento es un flujo de trabajo de vRealize Orchestrator, y muestra el nombre del servicio y una etiqueta que corresponde a la categoría del servicio en la que se ha importado el flujo de trabajo.

- 2 Para importar un nuevo servicio, haga clic en el botón **Importar**.
- 3 Siga los pasos del asistente de **importación**.

Opción	Descripción
Importar en biblioteca de destino	Seleccione la categoría de servicios en la que se importará el servicio.
Seleccionar origen	Seleccione la instancia de vRealize Orchestrator desde la que se importarán los flujos de trabajo.
Seleccionar flujos de trabajo	Expanda la vista de árbol de jerarquía para seleccionar uno o varios flujos de trabajo e importarlos.
Revisar	Revise los detalles y haga clic en Listo para completar la importación.

Los flujos de trabajo importados aparecerán en la vista de tarjetas **Biblioteca de servicios**.

Buscar un servicio

Puede buscar un servicio por su nombre o por la categoría de servicios a la que pertenece.

Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas de contenido**.

- a En el panel de la izquierda, seleccione **Biblioteca de servicios**.

Los servicios disponibles se muestran en una vista de tarjetas con doce elementos por página organizados por nombre y en orden alfabético. Cada tarjeta indica que el elemento es un flujo de trabajo de vRealize Orchestrator, y muestra el nombre del servicio y una etiqueta que corresponde a la categoría del servicio en la que se ha importado el flujo de trabajo.

- 2 En el cuadro de texto **Buscar** de la parte superior de la página, introduzca una palabra o un carácter del nombre del servicio o la categoría de servicios que desea buscar.

- 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

Puede ejecutar flujos de trabajo de vRealize Orchestrator como servicios importados.

Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas de contenido**.

- a En el panel de la izquierda, seleccione **Biblioteca de servicios**.

Los servicios disponibles se muestran en una vista de tarjetas con doce elementos por página organizados por nombre y en orden alfabético. Cada tarjeta indica que el elemento es un flujo de trabajo de vRealize Orchestrator, y muestra el nombre del servicio y una etiqueta que corresponde a la categoría del servicio en la que se ha importado el flujo de trabajo.

- 2 Para ejecutar un servicio, haga clic en **Ejecutar** en la tarjeta del servicio seleccionado.

Aparecerá el asistente de **ejecución de un servicio**.

- 3 Rellene los parámetros de entrada del servicio necesarios y haga clic en **Finalizar**.

Resultados

Puede supervisar el estado de la ejecución en la vista **Tareas recientes**. Para obtener más información, consulte [Ver tareas](#).

Nota Cuando se inicia un flujo de trabajo de vRealize Orchestrator como un servicio de vCloud Director, vCloud Director agrega varios parámetros personalizados al contexto de ejecución del flujo de trabajo.

Propiedad personalizada	Descripción
_vcd_orgName	Nombre de la organización a la que pertenece el usuario que ejecuta el servicio.
_vcd_orgId	Identificador de la organización a la que pertenece el usuario que ejecuta el servicio.
_vcd_username	Nombre del usuario que ejecuta el servicio.
_vcd_isAdmin	Tiene el valor True si el usuario que ejecuta el servicio es un administrador .
_vdc_isAdmin	Obsoleto. Tiene el valor True si el usuario que ejecuta el servicio es un administrador .
_vdc_username	Obsoleto. Nombre del usuario que ejecuta el servicio.
_vcd_sessionToken	Token de autenticación que recibió tras la autenticación correcta en vCloud Director
_vcd_apiEndpoint	Endpoint de vCloud Director REST API

Cambiar una categoría de servicios

Puede cambiar la categoría a la que pertenece un servicio.

Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas de contenido**.

- a En el panel de la izquierda, seleccione **Biblioteca de servicios**.

Los servicios disponibles se muestran en una vista de tarjetas con doce elementos por página organizados por nombre y en orden alfabético. Cada tarjeta indica que el elemento es un flujo de trabajo de vRealize Orchestrator, y muestra el nombre del servicio y una etiqueta que corresponde a la categoría del servicio en la que se ha importado el flujo de trabajo.

- 2 En la tarjeta del servicio seleccionado, seleccione **Administrar > Cambiar categoría**.

Se abrirá el cuadro de diálogo **Cambiar categoría**.

- 3 Seleccione la categoría en la que desea colocar el servicio y haga clic en **Guardar**.

Eliminar un servicio del registro

Puede retirar el acceso a un servicio para los proveedores de servicios y los tenants eliminando el servicio del registro.

Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas de contenido**.

- a En el panel de la izquierda, seleccione **Biblioteca de servicios**.

Los servicios disponibles se muestran en una vista de tarjetas con doce elementos por página organizados por nombre y en orden alfabético. Cada tarjeta indica que el elemento es un flujo de trabajo de vRealize Orchestrator, y muestra el nombre del servicio y una etiqueta que corresponde a la categoría del servicio en la que se ha importado el flujo de trabajo.

- 2 En la tarjeta del servicio seleccionado, elija **Administrar > Eliminar flujo de trabajo del registro**.

Se abrirá el cuadro de diálogo **Eliminar flujo de trabajo del registro**.

- 3 Para quitar el servicio de la biblioteca de servicios, haga clic en **Eliminar**.

Publicar un servicio

Puede controlar el acceso de los tenants y los proveedores de servicios a los servicios mediante la publicación de un servicio.

Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas de contenido**.

- a En el panel de la izquierda, seleccione **Biblioteca de servicios**.

Los servicios disponibles se muestran en una vista de tarjetas con doce elementos por página organizados por nombre y en orden alfabético. Cada tarjeta indica que el elemento es un flujo de trabajo de vRealize Orchestrator, y muestra el nombre del servicio y una etiqueta que corresponde a la categoría del servicio en la que se ha importado el flujo de trabajo.

- 2 En la tarjeta del servicio seleccionado, elija **Administrar > Publicar flujo de trabajo**.

Aparecerá el cuadro de diálogo **Publicar flujo de trabajo**.

- 3 Para publicar en los proveedores de servicios, seleccione **Publicar en proveedores de servicios** y haga clic en **Guardar**.

- 4 Para publicar en una organización de tenants específica, seleccione el botón **Publicar en tenants**.

- a Aparecerá una lista con las organizaciones de tenants disponibles. Seleccione la organización de tenants en la que desea publicar el flujo de trabajo y haga clic en **Guardar**.

- 5 Para publicar en todas las organizaciones de tenants, seleccione **Publicar en todos los tenants** y haga clic en **Guardar**.

Administrar entidades personalizadas

14

Las definiciones de entidad personalizada de vCloud Director son tipos de objeto enlazados a tipos de objeto de vRealize Orchestrator. Cuando un proveedor de servicios publica definiciones de una entidad personalizada en otro proveedor de servicios, o en uno o varios tenants, la instancia de vCloud Director de los usuarios puede poseer, administrar y cambiar estos tipos según se necesite. Mediante la ejecución de los servicios, los usuarios del proveedor de servicios y 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 con una entidad personalizada](#)
- [Publicar una entidad personalizada](#)
- [Eliminar una entidad personalizada](#)

Buscar una entidad personalizada

Puede buscar una entidad personalizada por su nombre.

Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas de contenido**.
 - a En el panel de la izquierda, seleccione **Definiciones de entidades personalizadas**.

La lista de entidades personalizadas se muestra en una vista de tarjetas con doce 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 se puede cambiar el tipo de la entidad ni el tipo de objeto de vRealize Orchestrator al cual la entidad está enlazada. Estas 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.

Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas de contenido**.
 - a En el panel de la izquierda, seleccione **Definiciones de entidades personalizadas**.


La lista de entidades personalizadas se muestra en una vista de tarjetas con doce 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.


Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas de contenido**.
 - a En el panel de la izquierda, seleccione **Definiciones de entidades personalizadas**.

La lista de entidades personalizadas se muestra en una vista de tarjetas con doce 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	<p>Escriba un nombre y, si lo desea, una descripción para la nueva entidad.</p> <p>Introduzca un nombre para el tipo de entidad (por ejemplo, sshHost).</p>
VRO	<p>En el menú desplegable, seleccione la instancia de vRealize Orchestrator que va a utilizar para asignar la definición de entidad personalizada.</p> <p>Nota Si hay más de un servidor de vRealize Orchestrator, debe crear una definición de entidad personalizada para cada uno de ellos de manera independiente.</p>
Tipo	<p>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, SSH > Host.</p> <p>Si conoce el nombre del tipo, puede introducirlo directamente en el cuadro de texto. Por ejemplo, SSH:Host.</p>
Revisar	<p>Revise los detalles que ha especificado y haga clic en Listo para completar la creación.</p>


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.

Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas de contenido**.
 - a En el panel de la izquierda, seleccione **Definiciones de entidades personalizadas**.

La lista de entidades personalizadas se muestra en una vista de tarjetas con doce 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.

Procedimiento

- 1 En el menú principal (), seleccione **Bibliotecas de contenido**.
 - a En el panel de la izquierda, seleccione **Definiciones de entidades personalizadas**.
 La lista de entidades personalizadas se muestra en una vista de tarjetas con doce 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 Biblioteca de servicios .
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 Listo 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 con una entidad personalizada

Puede quitar un flujo de trabajo de vRealize Orchestrator de la lista de acciones asociadas.


Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas de contenido**.
 - a En el panel de la izquierda, seleccione **Definiciones de entidades personalizadas**.
 La lista de entidades personalizadas se muestra en una vista de tarjetas con doce 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.

Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas de contenido**.
 - a En el panel de la izquierda, seleccione **Definiciones de entidades personalizadas**.
 La lista de entidades personalizadas se muestra en una vista de tarjetas con doce 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.

Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas de contenido**.

- a En el panel de la izquierda, seleccione **Definiciones de entidades personalizadas**.

La lista de entidades personalizadas se muestra en una vista de tarjetas con doce 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.