

Guía del portal para tenants de VMware Cloud Director

Modificado el 4 de abril de 2021
VMware Cloud Director 10.2

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 © 2017-2021 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

Guía del portal para tenants de VMware Cloud Director™ 11

1 Introducción al portal para tenants de VMware Cloud Director 13

- Descripción general de VMware Cloud Director™ 13
- Iniciar sesión en el portal para tenants de VMware Cloud Director 15
- Funciones y derechos del portal para tenants de VMware Cloud Director 15
- Usar el portal para tenants de VMware Cloud Director 16
- Usar la búsqueda global de VMware Cloud Director 17
- Usar la búsqueda rápida de VMware Cloud Director 18
- Ver tareas 19
- Detener una tarea en curso 20
- Ver eventos 21
- Establecer preferencias de usuario 21

2 Trabajar con máquinas virtuales 23

- Arquitectura de máquina virtual 24
- Cifrar máquinas virtuales 25
- Ver máquinas virtuales 26
- Crear una nueva máquina virtual independiente 27
- Aprovisionamiento rápido de máquinas virtuales 29
- Abrir una consola de máquina virtual 29
 - Instalar VMware Remote Console en un cliente 29
 - Abrir una consola remota de máquina virtual 30
 - Abrir una consola web 31
- Realizar operaciones de encendido y apagado en las máquinas virtuales 32
 - Encender una máquina virtual 32
 - Apagar una máquina virtual 32
 - Desconectar un sistema operativo invitado 33
 - Restablecer una máquina virtual 33
 - Suspender una máquina virtual 34
 - Descartar el estado suspendido de una máquina virtual 34
 - Encender varias máquinas virtuales 35
 - Apagar varias máquinas virtuales 35
 - Descartar el estado suspendido de varias máquinas virtuales 35
 - Restablecer varias máquinas virtuales 36
- Instalar VMware Tools en una máquina virtual 36
- Actualizar la versión de hardware virtual de una máquina virtual 37
- Editar propiedades de una máquina virtual 38

Cambiar las propiedades generales de una máquina virtual	38
Cambiar las propiedades de hardware de una máquina virtual	40
Cambiar las propiedades de personalización del sistema operativo invitado de una máquina Virtual	42
Cambiar las propiedades avanzadas de una máquina virtual	47
Insertar medios	50
Expulsar medio	50
Copiar una máquina virtual en otra vApp	51
Mover una máquina virtual a otra vApp	51
Afinidad y antiafinidad de máquinas virtuales	52
Ver reglas de afinidad y antiafinidad	53
Crear una regla de afinidad	53
Crear una regla de antiafinidad	54
Editar una regla de afinidad o de antiafinidad	54
Eliminar una regla de afinidad o de antiafinidad	55
Supervisar máquinas virtuales	55
Trabajar con instantáneas	56
Tomar una instantánea de una máquina virtual	57
Revertir una máquina virtual a una instantánea	58
Quitar una instantánea de una máquina virtual	59
Renovar una concesión de máquina virtual	59
Eliminar una máquina virtual	60
Grupos de escalado automático	60
Crear un grupo de escalado	60
Agregar una regla de escalado automático	61

3 Trabajar con vApp 63

Ver vApps	64
Generar una nueva vApp	64
Crear una vApp a partir de un paquete OVF	67
Agregar una vApp desde un catálogo	69
Crear una vApp a partir de una plantilla de vApp	71
Importar una máquina virtual desde vCenter Server como vApp	73
Realizar operaciones de encendido y apagado en vApps	73
Encender una vApp	73
Apagar una vApp	74
Restablecer una vApp	74
Suspender una vApp	75
Descartar el estado de suspensión de una vApp	75
Encender varias vApps	76
Apagar varias vApps	76
Descartar el estado de suspensión de varias vApps	77

Restablecer varias vApps	77
Suspender varias vApps	78
Abrir una vApp	78
Editar propiedades de una vApp	78
Editar las propiedades generales de la vApp	79
Editar el orden de inicio y detención de las máquinas virtuales en una vApp	79
Editar las propiedades de invitado de una vApp	81
Compartir una vApp	81
Mostrar un diagrama de red de vApp	82
Trabajar con redes en una vApp	83
Ver las redes de una vApp	83
Colocar una barrera de red de vApp	84
Agregar una red a una vApp	85
Configuración de servicios de redes para una red de vApp	86
Eliminar una red de vApp	93
Trabajar con instantáneas	93
Tomar una instantánea de una vApp	94
Revertir una vApp a una instantánea	95
Quitar una instantánea de una vApp	95
Crear instantáneas de varias vApps	96
Eliminar las instantáneas de varias vApps	96
Revertir varias vApps a instantáneas	97
Cambiar el propietario de una vApp	97
Mover una vApp a otro centro de datos virtual	98
Copiar una vApp detenida en otro centro de datos virtual	98
Copiar una vApp encendida	99
Agregar una máquina virtual a una vApp	100
Guardar una vApp como plantilla de vApp en un catálogo	101
Descargar una vApp como un paquete OVF	102
Renovar una concesión de vApp	103
Eliminar una vApp	104
Eliminar varias vApps	104

4 Trabajar con clústeres de Kubernetes 105

Agregar una política de Kubernetes de VDC de organización	106
Editar una política de Kubernetes de VDC de organización	108
Crear un clúster de Tanzu Kubernetes	109
Crear un clúster de Kubernetes nativo	111
Crear un clúster de VMware Tanzu Kubernetes Grid Integrated Edition	113
Configurar el acceso externo a un servicio en un clúster de Tanzu Kubernetes	114

5 Trabajar con redes 117

- Administrar redes de centros de datos virtuales de organización 120
 - Ver las redes de VDC de organización disponibles 121
 - Agregar una red de centros de datos virtuales de organización aislada 122
 - Agregar una red de centros de datos virtuales de organización enrutada 123
 - Agregar una red de centros de datos virtuales de organización directa 125
 - Agregar una red de VDC de organización con un conmutador lógico de NSX-T Data Center importado 126
 - Editar la configuración general de una red de centros de datos virtuales de organización 127
 - Conectar una red de centros de datos virtuales de organización a una puerta de enlace Edge 128
 - Desconectar una red de VDC de organización de una puerta de enlace Edge 129
 - Convertir la interfaz de una red de VDC de organización enrutada 129
 - Ver las direcciones IP usadas para una red de centros de datos virtuales de organización 130
 - Agregar direcciones IP a un grupo de direcciones IP de red de centros virtuales de organización 130
 - Editar o eliminar rangos de IP utilizados en una red de centros de datos virtuales de organización 131
 - Editar la configuración de DNS de una red de centros de datos virtuales de organización 132
 - Configurar las opciones de DHCP para una red de centros de datos virtuales de organización aislada 132
 - Agregar un grupo DHCP a una red enrutada de centros de datos virtuales de organización respaldada por NSX-T Data Center 133
 - Editar o eliminar un grupo DHCP existente para una red de centros de datos virtuales de organización aislada respaldada por NSX Data Center for vSphere 134
 - Restablecer una red de centros de datos virtuales de organización 135
 - Eliminar una red de centros de datos virtuales de organización 135
- Administrar redes de grupo de centros de datos con NSX-T Data Center 135
 - Administrar grupos de centros de datos con el tipo de proveedor de red NSX-T Data Center 136
 - Usar el firewall distribuido en un grupo de centros de datos con el tipo de proveedor de red NSX-T Data Center 139
 - Administrar redes de grupo de centros de datos con el tipo de proveedor de red NSX-T Data Center 144
 - Administrar puntos de salida para grupos de centros de datos con el tipo de proveedor de red NSX-T Data Center 149
- Administrar redes de grupo de centros de datos con NSX Data Center for vSphere 151
 - Administrar grupos de centros de datos con tipo de proveedor de red NSX Data Center for vSphere 153
 - Administrar redes de grupo de centros de datos respaldadas por NSX Data Center for vSphere 168
- Administrar servicios de puerta de enlace Edge de NSX Data Center for vSphere 170

Introducción a las redes avanzadas de VMware Cloud Director con NSX Data Center for vSphere	171
Configuración del firewall de tenant con NSX Data Center for vSphere	172
Administrar DHCP de puerta de enlace Edge de NSX Data Center for vSphere	184
Administrar la traducción de direcciones de red en una puerta de enlace Edge de NSX Data Center for vSphere	190
Configuración avanzada de enrutamiento para puertas de enlace Edge de NSX Data Center for vSphere	193
Equilibrio de carga con NSX Data Center for vSphere	203
Configurar el acceso seguro mediante VPN en una puerta de enlace Edge de NSX Data Center for vSphere	218
Administración de certificados SSL en una puerta de enlace Edge de NSX Data Center for vSphere	245
Objetos de agrupamiento personalizados para puertas de enlace Edge de NSX Data Center for vSphere	252
Estadísticas y logs de una puerta de enlace Edge de NSX Data Center for vSphere	256
Habilitar el acceso de la línea de comandos SSH a una puerta de enlace Edge de NSX Data Center for vSphere	258
Trabajar con etiquetas de seguridad para puertas de enlace Edge de NSX Data Center for vSphere	258
Trabajar con grupos de seguridad para puertas de enlace Edge de NSX Data Center for vSphere	263
Administrar puertas de enlace Edge de NSX-T Data Center	267
Agregar un conjunto de direcciones IP a una puerta de enlace Edge de NSX-T Data Center	267
Agregar una regla de firewall de puerta de enlace Edge de NSX-T Data Center	268
Agregar una regla SNAT o una regla DNAT a una puerta de enlace NSX-T Edge	269
Configurar un servicio de reenviador de DNS en una puerta de enlace NSX-T Edge	272
Crear perfiles de puerto de aplicación personalizados	273
VPN de IPSec basada en políticas para puertas de enlace Edge de NSX-T Data Center	274
Configurar servicios de red externa dedicada	277
Trabajar con equilibrio de carga avanzado de NSX	283

6 Usar discos con nombre y revisar políticas de almacenamiento 291

Crear y usar discos con nombre	291
Crear un disco con nombre	292
Editar un disco con nombre	292
Asociar un disco con nombre a una máquina virtual	293
Eliminar un disco con nombre	293
Revisar las propiedades de la política de almacenamiento	294

7 Revisar y editar las propiedades del centro de datos virtual 295

Revisar las propiedades del centro de datos virtual	295
Revisar los metadatos del centro de datos virtual	295

Limitar el acceso a un VDC de organización a usuarios y grupos específicos de la organización 296

8 Trabajar con instancias de vCenter Server dedicadas, endpoints y servidores proxy 298

Usar Chrome Browser Extension for VMware Cloud Director 299

Configurar el navegador con la configuración de proxy 299

Iniciar sesión en la interfaz de usuario de un componente mediante un endpoint 300

9 Trabajar con plantillas de vApp 302

Ver una plantilla de vApp 302

Crear una plantilla de vApp desde un archivo OVF 303

Importar una máquina virtual desde vCenter Server como plantilla de vApp 304

Asignar una política de colocación de máquinas virtuales y una política de tamaño de máquina virtual a una plantilla de vApp 305

Descargar una plantilla de vApp 306

Eliminar una plantilla de vApp 306

10 Trabajar con archivos de medios 308

Cargar archivos de medios 308

Eliminar un archivo de medios 309

Descargar un archivo de medios 309

11 Trabajar con catálogos 311

Ver catálogos 312

Crear un catálogo 312

Compartir un catálogo 313

Eliminar un catálogo 314

Cambiar el propietario de un catálogo 315

Administrar metadatos de un catálogo 315

Publicar un catálogo 316

Suscribirse a un catálogo externo 317

Actualizar la dirección URL de ubicación y la contraseña de un catálogo suscrito 317

Sincronizar un catálogo suscrito 318

12 Trabajar con plantillas de centros de datos virtuales de organización 319

Ver plantillas disponibles del centro de datos virtual 319

Crear instancias de un centro de datos virtual desde una plantilla 320

13 Administración de usuarios, grupos y funciones 322

Administración de usuarios 322

Crear un usuario 322

Importar usuarios	324
Modificar un usuario	325
Desactivar o activar una cuenta de usuario	326
Eliminar un usuario	326
Desbloquear una cuenta de usuario bloqueada	327
Administrar las cuotas de recursos de un usuario	327
Administración de grupos	328
Importar un grupo	328
Eliminar un grupo	329
Editar un grupo	329
Administrar las cuotas de recursos de un grupo	330
Funciones y derechos	331
Funciones predeterminadas y sus derechos	331
Derechos en funciones globales de tenant predefinidas	333
Crear una función de tenant personalizada	339
Editar una función de tenant personalizada	340
Eliminar una función	341
14 Configurar proveedores de identidad	342
Habilitar el uso de un proveedor de identidad SAML en la organización	342
Editar la configuración LDAP de una organización	344
Configurar, probar y sincronizar una conexión LDAP	345
15 Administrar certificados	348
Importar certificados de confianza	348
Importar certificados en la biblioteca de certificados	349
16 Administrar la organización	351
Editar el nombre y la descripción de la organización	351
Modificar la configuración de correo electrónico	352
Probar la configuración SMTP	353
Modificar la configuración de dominio para las máquinas virtuales de la organización	353
Trabajar con varios sitios	354
Configurar y administrar implementaciones multisitio	354
Entender las concesiones	355
Modificar las políticas de concesión de la vApp y la plantilla de vApp dentro de la organización	356
Modificar las políticas de cuenta de usuario y contraseña en la organización	357
Crear un panel de control de avisos	358
17 Trabajar con Biblioteca de servicios	359
Buscar un servicio	359

Ejecutar un servicio 360

18 Administrar entidades definidas 361

Trabajar con definiciones de entidad personalizada 363

 Buscar una entidad personalizada 364

 Editar una definición de entidad personalizada 364

 Agregar una definición de entidad personalizada 365

 Instancias de entidades personalizadas 366

 Asociar una acción a una entidad personalizada 366

 Anular la asociación de una acción de una entidad personalizada 367

 Publicar una entidad personalizada 368

 Eliminar una entidad personalizada 368

Guía del portal para tenants de VMware Cloud Director™

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

Público objetivo

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

Glosario de publicaciones técnicas de VMware

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

Términos y condiciones de uso

VMware le otorga permiso para modificar esta guía de usuario para tenants (la “Guía”) según sea razonablemente necesario para adaptarla a sus procesos operativos y después reproducir y distribuir la Guía modificada a sus clientes. No puede cobrar a sus clientes una cantidad por el acceso a la Guía modificada. USTED ACEPTA QUE LA GUÍA SE LE PROPORCIONA SIN CARGO, “TAL CUAL” SIN GARANTÍA DE NINGÚN TIPO Y SOLO PARA EL PROPÓSITO DESCRITO ANTERIORMENTE. POR CONSIGUIENTE, LA RESPONSABILIDAD TOTAL DE VMWARE Y SUS PROVEEDORES QUE RESULTEN DE O ESTÉN RELACIONADOS CON EL HECHO DE PROPORCIONARLE ACCESO A LA GUÍA NO EXCEDERÁ DE 100 DÓLARES. EN NINGÚN CASO VMWARE O SUS PROVEEDORES TENDRÁN RESPONSABILIDAD POR CUALQUIER DAÑO INDIRECTO, INCIDENTAL, ESPECÍFICO O CONSECUENTE (INCLUYENDO, SIN LIMITACIÓN, DAÑOS POR PÉRDIDA DE GANANCIAS EMPRESARIALES, INTERRUPCIÓN COMERCIAL O

PÉRDIDA DE INFORMACIÓN EMPRESARIAL), AUNQUE VMWARE O SUS PROVEEDORES HAYAN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS. ESTAS LIMITACIONES SE APLICARÁN INDEPENDIENTEMENTE DE CUALQUIER FALLO EN EL PROPÓSITO ESENCIAL DE CUALQUIER RECURSO LIMITADO.

Introducción al portal para tenants de VMware Cloud Director

1

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

Este capítulo incluye los siguientes temas:

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

Descripción general de VMware Cloud Director™

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

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

Organizaciones

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

Usuarios y grupos

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

Centros de datos virtuales

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

Redes de centros de datos virtuales de organización

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

Redes de vApp

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

Catálogos

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

Instancias (SDDC) de vCenter Server dedicadas y servidores proxy

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

Iniciar sesión en el portal para tenants de VMware Cloud Director

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

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

Procedimiento

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

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

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

Funciones y derechos del portal para tenants de VMware Cloud Director

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

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

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

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

Usar el portal para tenants de VMware Cloud Director

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

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

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

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

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

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

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

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

En la barra de navegación superior, puede desplazarse hasta los diferentes elementos del menú.

Elemento del menú	Descripción
Centros de datos	Le dirige a los recursos Centro de datos virtual , Grupos de centros de datos y Centros de datos de vSphere dedicados de la organización.
Centro de datos virtuales	Le dirige a la pantalla Centro de datos virtual en la que se muestran los centros de datos virtuales dentro de la organización.
Centros de datos de vSphere dedicados	Le dirige a la pantalla en la que se muestran los centros de datos de vSphere dedicados que el proveedor de servicios ha publicado en la organización.

Elemento del menú	Descripción
Aplicaciones	Le dirige a los recursos Aplicaciones virtuales y Máquinas virtuales de la organización.
Bibliotecas	Le dirige a una vista consolidada de plantillas de vApp, catálogos, medios y otros tipos de archivos. Utilice estas plantillas y archivos para implementar máquinas virtuales o vApps.
Red	Le dirige a las redes, las puertas de enlace Edge y los grupos de centros de datos de su organización.
Administración	Le dirige a las pantallas de configuración Control de acceso y Proveedor de identidad , así como a la configuración general, de correo electrónico, de personalización de invitado, de metadatos, de multisitio y de políticas de la organización.
Supervisar	Le dirige a las pantallas Tareas y Eventos . La pantalla Tareas muestra las tareas de las que informa VMware Cloud Director. La pantalla Eventos muestra los eventos de los que informa VMware Cloud Director.

Puede personalizar el portal para tenants de VMware Cloud Director con las instancias de Cloud Director OpenAPI de **Branding**. Para obtener información sobre el uso de Cloud Director OpenAPI, consulte el documento en el que se describen los *primeros pasos con Cloud Director OpenAPI* en <https://code.vmware.com>.

Usar la búsqueda global de VMware Cloud Director

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

La lista de objetos predefinidos es:

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

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

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

Procedimiento

- 1 En la esquina superior derecha del portal para tenants de VMware Cloud Director, haga clic en el icono **Buscar**.
- 2 (opcional) Para anclar el panel de búsqueda, haga clic en el icono **Anclar**.

- 3 En el cuadro de texto **Buscar**, introduzca un símbolo, una parte de un nombre o una dirección IP para buscar los nombres de objetos que coincidan o las direcciones IP estáticas de las máquinas virtuales.
- 4 Si emplea un entorno multisitio, seleccione los sitios en los que desea realizar la búsqueda.
- 5 Pulse **Entrar**.

Resultados

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

Pasos siguientes

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

Usar la búsqueda rápida de VMware Cloud Director

Puede usar la búsqueda rápida de VMware Cloud Director para buscar pantallas, entidades y acciones. Los resultados dependen de su ubicación en la interfaz de usuario.

Los resultados dependen del contexto, de si se seleccionó una entidad y de las acciones disponibles para una entidad en particular. Los resultados de la búsqueda se agrupan en secciones.

- Navegación global: los resultados de esta sección no están relacionados con una entidad específica, por ejemplo, puertas de enlace Edge, LDAP, tareas, certificados de confianza, máquinas virtuales, etc. Estos resultados se obtienen con independencia de dónde se encuentre usted en la interfaz de usuario.
- Navegación contextual: los resultados de esta sección dependen de la entidad seleccionada en la interfaz de usuario. Por ejemplo, vistas específicas de vApp, como máquinas virtuales, diagrama de red, etc. Si selecciona una entidad como una vApp, la búsqueda muestra los resultados de navegación globales y contextuales, así como cualquier acción que pueda aplicarse a la entidad.
- Acciones contextuales: los resultados de esta sección dependen de la entidad seleccionada en la interfaz de usuario. En función de la ubicación en la que usted se encuentre en la interfaz de usuario y de la entidad que seleccione, mediante los resultados de la búsqueda rápida, puede realizar una acción relacionada con la entidad. Por ejemplo, la búsqueda en la vista de detalles de una máquina virtual muestra los resultados de las vistas globales, las vistas contextuales y las acciones que puede realizar en la máquina virtual seleccionada.

- Búsqueda de entidades por nombre: si está viendo una lista de entidades, los resultados de la búsqueda pueden incluir también nombres de entidades del mismo tipo que las de la lista. Por ejemplo, si está viendo una lista de máquinas virtuales, los resultados de la búsqueda incluyen coincidencias de navegación globales y nombres coincidentes de máquinas virtuales. Si hay más de una página de entidades en la lista que está viendo, la búsqueda comprueba la lista completa de entidades y puede mostrar un nombre que no está visible en la página actual.

Procedimiento

- 1 Abra la ventana **Búsqueda rápida**.
 - En la barra de navegación superior, haga clic en el menú **Ayuda** y seleccione **Búsqueda rápida**.
 - Pulse Ctrl+. o Cmd+., según su sistema operativo.

- 2 Introduzca los criterios de búsqueda.

- 3 Examine los resultados y seleccione una opción, o realice una acción haciendo clic o presionando Entrar.

Puede usar las teclas de dirección arriba y abajo para examinar los resultados de la búsqueda.


Ver tareas

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

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

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Supervisar y Tareas**.
Se muestra la lista de todas las tareas, junto con la hora de ejecución y el estado de la tarea.
- 2 Haga clic en el icono de editor () para cambiar los detalles que desea ver acerca de las tareas.
- 3 (opcional) Para ver los detalles de la tarea, haga clic en el nombre de la tarea.
Entre los detalles de la tarea se incluye información como el motivo del error, cuándo falló la tarea, entre otros datos.

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

Detener una tarea en curso

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

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

Requisitos previos

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

Procedimiento

- 1 Inicie una operación de ejecución prolongada.

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

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

Resultados

La operación se detiene.

Ver eventos


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

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Supervisar y Eventos**.

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

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

- 3 (opcional) Haga clic en un evento para ver sus detalles.

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

Establecer preferencias de usuario

Puede establecer ciertas preferencias de alertas del sistema o de visualización que se implementarán cada vez que inicie sesión en el sistema.

Para obtener más información acerca de las concesiones, consulte [Entender las concesiones](#).

Procedimiento

- 1 En la barra de navegación superior, haga clic en su nombre de usuario y seleccione **Preferencias del usuario**.
- 2 Seleccione la página que desea que aparezca al iniciar sesión.
 - a Seleccione el botón de radio situado junto a **Página de inicio** y haga clic en **Editar**.
 - b Seleccione una opción del menú desplegable y haga clic en **Guardar**.
- 3 Configure una notificación por correo electrónico para las ocasiones en que caduque la concesión de tiempo de ejecución.
 - a Seleccione el botón de radio situado junto a **Tiempo de alerta de concesión de implementación** y haga clic en **Editar**.
 - b Introduzca un valor en segundos y haga clic en **Guardar**.
- 4 Configure una notificación por correo electrónico para las ocasiones en que caduque la concesión de almacenamiento.
 - a Seleccione el botón de radio situado junto a **Tiempo de alerta de concesión de almacenamiento** y haga clic en **Editar**.
 - b Introduzca un valor en segundos y haga clic en **Guardar**.

Trabajar con máquinas virtuales

2

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

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

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

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

Este capítulo incluye los siguientes temas:

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

- [Copiar una máquina virtual en otra vApp](#)
- [Mover una máquina virtual a otra vApp](#)
- [Afinidad y antiafinidad de máquinas virtuales](#)
- [Supervisar máquinas virtuales](#)
- [Trabajar con instantáneas](#)
- [Renovar una concesión de máquina virtual](#)
- [Eliminar una máquina virtual](#)
- [Grupos de escalado automático](#)

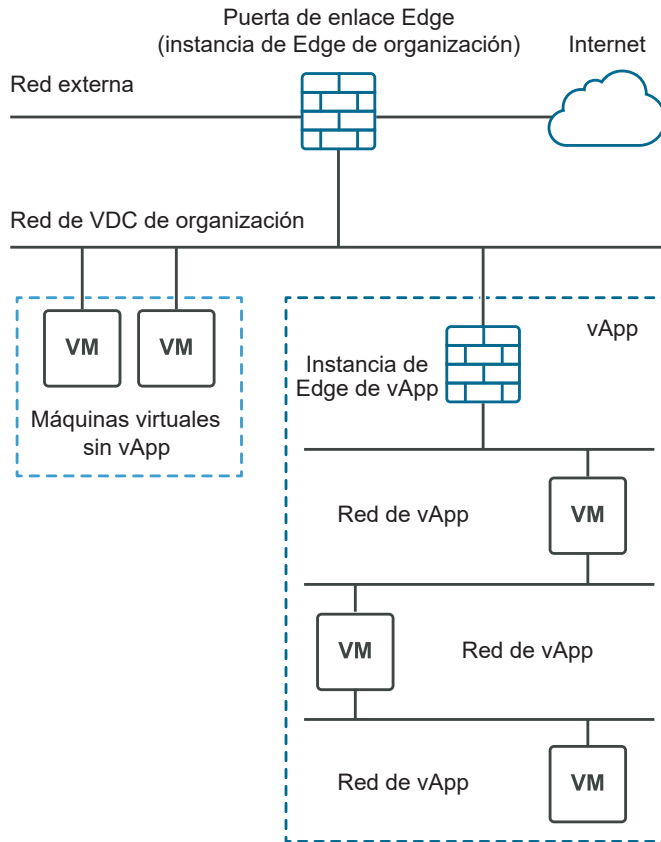
Arquitectura de máquina virtual

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

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

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

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



Cifrar máquinas virtuales

A partir de VMware Cloud Director 10.1, puede mejorar la seguridad de los datos mediante el cifrado de máquinas virtuales. Puede cifrar máquinas virtuales y discos si los asocia a políticas de almacenamiento que tengan la funcionalidad de cifrado de máquinas virtuales.

El cifrado no solo protege la máquina virtual, sino también los discos y otros archivos de las máquinas virtuales. Puede ver las funcionalidades de las políticas de almacenamiento y el estado de cifrado de tanto las máquinas virtuales como los discos en la API y la interfaz de usuario. Puede realizar todas las operaciones en los discos y las máquinas virtuales cifrados que sean compatibles con la versión de vCenter Server correspondiente.

Si el VDC de organización tiene una política de almacenamiento en la que se haya habilitado el cifrado de máquinas virtuales, puede cifrar máquinas virtuales y discos. Consulte el tema [Habilitar cifrado de máquinas virtuales en políticas de almacenamiento de un centro de datos virtual de organización](#) en la *Guía del portal para administradores de proveedores de servicios de VMware Cloud Director*. Para cifrar una máquina virtual o un disco, asícielos a una política de almacenamiento en la que se haya habilitado el cifrado de máquinas virtuales. Para las máquinas

virtuales, consulte [Crear una nueva máquina virtual independiente](#) o [Cambiar las propiedades generales de una máquina virtual](#). Para los discos con nombre, consulte [Crear un disco con nombre](#) o [Editar un disco con nombre](#). Para descifrar una máquina virtual o un disco, asócielos a una política de almacenamiento en la que no se haya habilitado el cifrado.

Limitaciones del cifrado de máquinas virtuales

Las siguientes acciones no se admiten en VMware Cloud Director:

- Cifrar o descifrar una máquina virtual encendida o sus discos.
- Exportar un OVF de una máquina virtual cifrada.
- Cifrar y descifrar los discos de una máquina virtual con una instantánea si los discos forman parte de la instantánea.
- Descifrar una máquina virtual cuando su disco está en una política cifrada.
- Agregar un disco cifrado a una máquina virtual sin cifrar.
- Cifrar un disco existente en una máquina virtual sin cifrar.
- Agregar un disco con nombre cifrado a una máquina virtual sin cifrar.
- Crear un clon vinculado cifrado.
- Cifrar una máquina virtual de clon vinculado o sus discos.
- Crear instancias de máquinas virtuales (o bien moverlas o clonarlas) entre instancias de vCenter Server cuando la máquina virtual de origen está cifrada.

Nota En un VDC de organización con aprovisionamiento rápido, si la máquina virtual de origen o destino está cifrada y desea crear un clon, VMware Cloud Director siempre crea un clon completo.

Identificar una funcionalidad de almacenamiento de cifrado de máquinas virtuales

De forma predeterminada, los **administradores del sistema** y los **administradores de la organización** tienen los derechos necesarios para ver las funcionalidades de almacenamiento de VDC de organización, así como para ver si los discos y las máquinas virtuales están cifrados. Los **autores de vApp** pueden ver el estado de cifrado de una máquina virtual y sus discos en la página **Detalles** de la máquina virtual. Para obtener más información sobre las funciones y los derechos, consulte [Funciones predeterminadas y sus derechos](#).



Ver máquinas virtuales

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

Procedimiento


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

2 Elija una de las siguientes opciones.

- Para ver las máquinas virtuales en una vista de cuadrícula, haga clic en .
- Para ver las máquinas virtuales en una vista de tarjeta, haga clic en .

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

3 (opcional) Organice la lista de máquinas virtuales desde el menú desplegable **Ordenar por**.

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

Por ejemplo, puede apagar una máquina virtual.

5 Para acceder a la interfaz del sistema operativo invitado de la máquina virtual, haga clic en el icono de escritorio en la esquina superior derecha de la vista de tarjetas.


6 Para ver y editar los detalles de una máquina virtual, haga clic en **Detalles**.

Crear una nueva máquina virtual independiente

Puede crear una nueva máquina virtual independiente.

Procedimiento

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

2 Haga clic en  para ver la lista en una vista de tarjetas y, si lo desea, organizar la lista de máquinas virtuales desde el menú desplegable **Ordenar por**.

3 Haga clic en **Nueva máquina virtual**.

4 Introduzca el nombre y el nombre del equipo de la máquina virtual.

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

5 (opcional) Introduzca una descripción significativa.

6 Seleccione si desea que la máquina virtual se encienda inmediatamente después de crearse.

7 Seleccione cómo desea implementar la máquina virtual.

Opción	Acción
Nuevo	<p>Implementa una nueva máquina virtual con una configuración personalizable.</p> <ul style="list-style-type: none"> a Seleccione una familia de sistema operativo y un sistema operativo. b (Opcional) Seleccione una imagen de arranque. c (Opcional) Seleccione una política de colocación y una política de tamaño de máquina virtual. <p>Los menús desplegables de las políticas de colocación y tamaño de la máquina virtual solo están visibles si el proveedor de servicios publicó dichas políticas en el VDC de organización.</p> <ul style="list-style-type: none"> d (Opcional) Seleccione el tamaño de la máquina virtual en las opciones de tamaño predefinidas o haga clic en Opciones de tamaño personalizadas para introducir manualmente la cantidad de CPU virtuales, núcleos por socket y configuración de memoria. <p>Si selecciona una política de tamaño de máquina virtual que defina el tamaño de la máquina virtual, esta opción no estará visible.</p> <p>Los tamaños predefinidos de la máquina virtual son: Pequeño, Mediano y Grande.</p> <ul style="list-style-type: none"> e Especifique la configuración de almacenamiento para la máquina virtual, como la política de almacenamiento y el tamaño en GB. f Especifique la configuración de red para la máquina virtual, como red, modo de IP, dirección IP y NIC primaria.
A partir de plantilla	<p>Implementa una máquina virtual a partir de una plantilla seleccionada del catálogo de plantillas.</p> <ul style="list-style-type: none"> a Seleccione una plantilla de máquina virtual a partir de la lista de plantillas disponibles. b (Opcional) Seleccione una política de colocación y una política de tamaño de máquina virtual. <p>Los menús desplegables de las políticas de colocación y tamaño de la máquina virtual solo están visibles si el proveedor de servicios publicó dichas políticas en el VDC de organización. Si la plantilla seleccionada tiene políticas asignadas, es posible que se limiten a las políticas de plantilla predefinidas.</p> <ul style="list-style-type: none"> c (Opcional) Seleccione esta opción para usar una política de almacenamiento personalizada y seleccione la política de almacenamiento que desea usar del menú desplegable Política de almacenamiento personalizada que se usará. d Lea y acepte el contrato de licencia de usuario final, si lo hubiere.

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

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

Aprovisionamiento rápido de máquinas virtuales

El aprovisionamiento rápido ahorra tiempo al utilizar clones vinculados para las operaciones de aprovisionamiento de la máquina virtual.

Un clon vinculado es un duplicado de la máquina virtual que utiliza el mismo disco virtual que el original, con una cadena de discos delta para hacer un seguimiento de las diferencias entre el original y el clon. Si desactiva el aprovisionamiento rápido, todas las operaciones de aprovisionamiento producen clones completos.

Un clon vinculado no puede existir en un centro de datos o un almacén de datos de vCenter Server diferente al de la máquina virtual original.

Al aprovisionar rápidamente una máquina virtual, VMware Cloud Director crea una máquina virtual instantánea para admitir la creación de clones vinculados entre centros de datos de vCenter Server y almacenes de datos para las máquinas virtuales que están asociadas con una plantilla de vApp específica.

Una máquina virtual instantánea es una copia exacta de la máquina virtual original. La máquina virtual instantánea se crea en el centro de datos y en el almacén de datos en el que se genera el clon vinculado.

Importante La consolidación local de una máquina virtual con aprovisionamiento rápido no se admite en los contenedores de almacenamiento que emplean snapshots nativos. Los almacenes de datos habilitados para VVOL y VAAI usan snapshots nativos, por lo que es posible que las máquinas virtuales con aprovisionamiento rápido implementadas en uno de estos contenedores de almacenamiento no puedan consolidarse. Si necesita consolidar una máquina virtual con aprovisionamiento rápido implementada en un almacén de datos habilitado para VVOL o VAAI, deberá reubicarla en un contenedor de almacenamiento diferente.

Abrir una consola de máquina virtual

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

Requisitos previos

La máquina virtual debe estar encendida.

Instalar VMware Remote Console en un cliente

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

Requisitos previos

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

Procedimiento

1 Descargue el instalador.

- Desplácese hasta la página de descargas de VMware Remote Console y seleccione el vínculo para su plataforma.

www.vmware.com/go/download-vmrc

- En la pantalla del panel de control **Centro de datos virtual** del VMware Cloud Director Tenant Portal, haga clic en la tarjeta del centro de datos virtual que desea explorar. Seleccione una máquina virtual y, en el menú **Acciones**, seleccione **Descargar VMRC**.

2 Ejecute la instalación para su plataforma.

- Si utiliza Windows, haga doble clic en el instalador `.msi` y siga las indicaciones.
- Si utiliza Linux, inicie sesión con privilegios de **raíz**, ejecute el instalador `.bundle` y siga las indicaciones.
- Si utiliza Mac OS, haga doble clic en el archivo `.dmg` para abrirlo y, a continuación, haga doble clic en el icono de VMware Remote Console que se encuentra en él para copiarlo en la carpeta Aplicaciones.

Resultados

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

Abrir una consola remota de máquina virtual


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

Requisitos previos

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

Procedimiento

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

- Haga clic en  para ver la lista en una vista de tarjetas y, si lo desea, organizar la lista de máquinas virtuales desde el menú desplegable **Ordenar por**.
- En el menú **Acciones** de la máquina virtual, seleccione **Iniciar consola remota de MV**.

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

Resultados

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

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


Abrir una consola web

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

Requisitos previos

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

Procedimiento

- En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **Máquinas virtuales**.
- Haga clic en  para ver la lista en una vista de tarjetas y, si lo desea, organizar la lista de máquinas virtuales desde el menú desplegable **Ordenar por**.
- En el menú **Acciones** de la máquina virtual, seleccione **Iniciar consola web**.

Resultados

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

Pasos siguientes

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

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

Realizar operaciones de encendido y apagado en las máquinas virtuales

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

Encender una máquina virtual


Encender una máquina virtual equivale a encender una máquina física.

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

Requisitos previos

La máquina virtual debe estar apagada.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **Máquinas virtuales**.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, si lo desea, organizar la lista de máquinas virtuales desde el menú desplegable **Ordenar por**.
- 3 En el menú **Acciones** de la máquina virtual que desea iniciar, seleccione **Encender**.

Resultados

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


Apagar una máquina virtual

Apagar una máquina virtual equivale a apagar una máquina física.

Requisitos previos

La máquina virtual debe estar encendida.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **Máquinas virtuales**.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, si lo desea, organizar la lista de máquinas virtuales desde el menú desplegable **Ordenar por**.
- 3 En el menú **Acciones** de la máquina virtual que desea apagar, seleccione **Apagar**.

Resultados

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


Desconectar un sistema operativo invitado

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

Requisitos previos

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

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **Máquinas virtuales**.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, si lo desea, organizar la lista de máquinas virtuales desde el menú desplegable **Ordenar por**.
- 3 En el menú **Acciones** de la máquina virtual, seleccione **Desconectar SO invitado**.

Resultados

El SO invitado se desconectará.

Restablecer una máquina virtual


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

Requisitos previos

Su máquina virtual está encendida.

Procedimiento

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

-
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, si lo desea, organizar la lista de máquinas virtuales desde el menú desplegable **Ordenar por**.
- 3 En el menú **Acciones** de la máquina virtual que desea restablecer, seleccione **Restablecer**.

Resultados

Se borrará el estado de la máquina virtual.

Suspender una máquina virtual


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

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

Requisitos previos

La máquina virtual debe estar encendida.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **Máquinas virtuales**.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, si lo desea, organizar la lista de máquinas virtuales desde el menú desplegable **Ordenar por**.
- 3 En el menú **Acciones** de la máquina virtual que desea suspender, seleccione **Suspender**.

Resultados

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

Descartar el estado suspendido de una máquina virtual


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

Requisitos previos

Debe haber una máquina virtual suspendida.

Procedimiento

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

- 2 Haga clic en  para ver la lista en una vista de tarjetas y, si lo desea, organizar la lista de máquinas virtuales desde el menú desplegable **Ordenar por**.
- 3 En el menú **Acciones** de la máquina virtual, seleccione **Descartar estado de suspensión**.

Resultados

El estado se descarta y la máquina virtual se apaga.

Encender varias máquinas virtuales

Puede encender varias máquinas virtuales al mismo tiempo.

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

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **Máquinas virtuales**.
- 2 Alterne la opción de **selección múltiple**.
- 3 Seleccione las máquinas virtuales que desea encender.
- 4 En el menú **Acciones**, seleccione **Encender**.
- 5 Haga clic en **Aceptar** para confirmar.

Apagar varias máquinas virtuales

Puede apagar varias máquinas virtuales al mismo tiempo.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **Máquinas virtuales**.
- 2 Alterne la opción de **selección múltiple**.
- 3 Seleccione las máquinas virtuales que desea apagar.
- 4 En el menú **Acciones**, seleccione **Apagar**.
- 5 Haga clic en **Aceptar** para confirmar.

Descartar el estado suspendido de varias máquinas virtuales

Si varias máquinas virtuales se encuentran en estado de suspensión y ya no es necesario reanudar su uso, puede descartar este estado de las máquinas virtuales al mismo tiempo. Al hacerlo, se elimina la memoria guardada y las máquinas virtuales vuelven a apagarse.

Requisitos previos

Compruebe que las máquinas virtuales se encuentren en estado de suspensión.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **Máquinas virtuales**.
- 2 Alterne la opción de **selección múltiple**.
- 3 Seleccione las máquinas virtuales para las que desea descartar el estado de suspensión.
- 4 En el menú **Acciones**, seleccione **Descartar estado de suspensión**.
- 5 Haga clic en **Aceptar** para confirmar.

Restablecer varias máquinas virtuales

Cuando se restablecen varias máquinas virtuales al mismo tiempo, se borran sus estados (de memoria, memoria caché, etc.), aunque se mantienen en ejecución.

Restablecer una máquina virtual equivale a presionar el botón de restablecimiento en una máquina física. Inicia un restablecimiento completo del sistema operativo sin cambiar el estado de encendido de la máquina virtual.

Requisitos previos

Compruebe que las máquinas virtuales estén encendidas.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **Máquinas virtuales**.
- 2 Alterne la opción de **selección múltiple**.
- 3 Seleccione las máquinas virtuales que desee restablecer.
- 4 En el menú **Acciones**, seleccione **Restablecer**.
- 5 Haga clic en **Aceptar** para confirmar.

Instalar VMware Tools en una máquina virtual

VMware Cloud Director depende de VMware Tools para personalizar el sistema operativo invitado.


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

Requisitos previos

- Compruebe que la máquina virtual esté encendida.

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

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **Máquinas virtuales**.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, si lo desea, organizar la lista de máquinas virtuales desde el menú desplegable **Ordenar por**.
- 3 En el menú **Acciones** de la máquina virtual donde desea instalar VMware Tools, seleccione **Instalar VMware Tools**.

VMware Tools se instala en el sistema operativo invitado de destino. Si se produce un error durante la instalación, se muestra un mensaje de error. También puede consultar el progreso de la operación de instalación en la ventana **Tareas**.
- 4 Para abrir la consola web de la máquina virtual, desde el menú **Acciones**, seleccione **Iniciar la consola web**.
- 5 Siga las instrucciones en el [artículo 1014294 de la Base de conocimientos de VMware](#) para configurar VMware Tools para su sistema operativo específico.

Resultados

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

Actualizar la versión de hardware virtual de una máquina virtual

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

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

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


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

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

Requisitos previos

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

Procedimiento

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

Resultados

La máquina virtual se actualizará a la versión más reciente.

Editar propiedades de una máquina virtual

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


Cambiar las propiedades generales de una máquina virtual

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

Requisitos previos

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

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **Máquinas virtuales**.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, si lo desea, organizar la lista de máquinas virtuales desde el menú desplegable **Ordenar por**.
- 3 En la tarjeta de la máquina virtual que desea editar, haga clic en **Detalles**.

- 4 La lista de propiedades que puede ver o editar en **General** se expande de forma predeterminada.


Opción	Acción
Nombre de máquina virtual	<p>Edite el nombre de la máquina virtual.</p> <p>Esta propiedad se puede editar con la máquina virtual encendida.</p>
Nombre de equipo	<p>Edite el nombre del equipo y del host establecido en el sistema operativo invitado que identifica la máquina virtual en una red. Este campo está restringido a 15 caracteres debido a la limitación del SO Windows en los nombres de equipo.</p> <p>Esta propiedad se puede editar con la máquina virtual encendida.</p>
Descripción	<p>Edite la descripción opcional de la máquina virtual.</p> <p>Esta propiedad se puede editar con la máquina virtual encendida.</p>
Familia del sistema operativo	<p>Seleccione la familia de sistema operativo en el menú desplegable.</p> <p>Esta propiedad se puede editar con la máquina virtual apagada. Además, no puede editar esta propiedad si ya hay un sistema operativo en la máquina virtual.</p>
Sistema operativo	<p>Seleccione un sistema operativo en el menú desplegable.</p> <p>Esta propiedad se puede editar con la máquina virtual apagada. Además, no puede editar esta propiedad si ya hay un sistema operativo en la máquina virtual.</p>
Retardo de inicio	<p>Especifique el tiempo en milisegundos para retrasar la operación de arranque.</p> <p>Puede transcurrir poco tiempo entre el momento en que la máquina virtual se enciende y en el que sale de BIOS e inicia el software del sistema operativo invitado. Puede cambiar el retraso de arranque para proporcionar más tiempo.</p>
Directiva de almacenamiento	<p>Seleccione en el menú desplegable una directiva de almacenamiento para utilizarla en la máquina virtual.</p> <p>Esta propiedad se puede editar con la máquina virtual encendida.</p>
Centro de datos virtuales	<p>Vea el nombre del centro de datos virtual al que pertenece esta máquina virtual.</p>
VMware Tools	<p>Compruebe si VMware Tools está instalado en la máquina virtual.</p>
Versión del hardware virtual	<p>Observe la versión del hardware virtual de la máquina virtual.</p>
Actualizar a:	<p>Para realizar la actualización, seleccione una versión en el menú desplegable.</p>
Hora de inicio de la sincronización	<p>Active esta casilla de verificación para habilitar la sincronización de hora entre el sistema operativo invitado de la máquina virtual y el centro de datos virtual en el que se está ejecutando.</p>
Introducir configuración de BIOS	<p>Seleccione si desea forzar la entrada a la pantalla de configuración de BIOS la próxima vez que arranque la máquina virtual.</p> <p>Esta propiedad se puede editar mientras la máquina virtual está apagada.</p>

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

Cambiar las propiedades de hardware de una máquina virtual

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

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **Máquinas virtuales**.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, si lo desea, organizar la lista de máquinas virtuales desde el menú desplegable **Ordenar por**.
- 3 En la tarjeta de la máquina virtual que desea editar, haga clic en **Detalles**.
- 4 Haga clic en **Hardware** para expandir la lista de propiedades de hardware que puede ver y editar.

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

Opción	Descripción
Agregado en caliente de la CPU virtual	Si habilita el agregado en caliente de CPU virtual, es posible agregar CPU virtuales a la máquina virtual mientras esta está encendida. Solo puede agregar múltiplos del número de núcleos por socket. Esta función solo la admiten ciertos sistemas operativos invitados y versiones de hardware de máquinas virtuales.
Número de sockets	Observe el número de sockets. El número de sockets se determina en función del número de CPU virtuales disponibles. El número cambia cuando se actualiza la cantidad de CPU virtuales.
Medios extraíbles	Observe los medios extraíbles disponibles, como la unidad de CD/DVD y de disquete conectada.

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

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

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

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

Opción	Descripción
NIC primario	Se muestra una marca cuando se selecciona el NIC primario. Seleccione un NIC primario. La configuración del NIC primario determina la puerta de enlace predeterminada y única de la máquina virtual. La máquina virtual puede usar cualquier NIC para conectarse a máquinas virtuales y físicas que estén conectadas directamente a la misma red que el NIC, pero solo puede usar el NIC primario para conectarse a máquinas de redes que requieran una conexión de puerta de enlace.
NIC	Número de la NIC.
Conectado	Active la casilla de verificación para conectar una NIC.
Red	Seleccione una red en el menú desplegable.
Modo de IP	<p>Seleccione un modo de IP.</p> <p>Precaución No establezca el modo de IP en Ninguno si seleccionó una red a la que conectar la NIC.</p> <ul style="list-style-type: none"> ■ Estática - Grupo de direcciones IP Extrae una dirección IP estática del grupo de direcciones IP de red. ■ Estática - Manual Le permite especificar una dirección IP concreta de forma manual. Si selecciona esta opción, debe introducir una dirección IP en la columna Dirección IP. ■ DHCP Extrae una dirección IP de un servidor DHCP.
Dirección MAC	En el menú desplegable, seleccione si desea conservar o restablecer la dirección MAC.

7 Haga clic en **Guardar**.

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


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

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

Requisitos previos

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

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **Máquinas virtuales**.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, si lo desea, organizar la lista de máquinas virtuales desde el menú desplegable **Ordenar por**.
- 3 En la tarjeta de la máquina virtual que desea editar, haga clic en **Detalles**.

- 4 Haga clic en **Propiedades y personalización de SO invitado** para expandir la lista de ajustes del sistema operativo invitado.

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

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

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

Entender la personalización de invitado

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

Casilla Habilitar personalización de invitado

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

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

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

Comportamiento de personalización de invitado para vApp y máquinas virtuales

Las casillas están desactivadas.

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

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

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

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

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

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

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

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

Encender y forzar volver a personalizar una máquina virtual

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


Si la configuración de una máquina virtual no está sincronizada con VMware Cloud Director o se ha producido un error al intentar realizar una personalización de invitado, puede forzar una nueva personalización de la máquina virtual.

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

Requisitos previos

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

Procedimiento

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

Resultados

La máquina virtual se volverá a personalizar y se encenderá.

Cambiar las propiedades avanzadas de una máquina virtual

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

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

Cuotas de asignación de recursos

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

Reserva de asignación de recursos

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

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

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

Límite de asignación de recursos

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


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

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

Requisitos previos

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

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **Máquinas virtuales**.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, si lo desea, organizar la lista de máquinas virtuales desde el menú desplegable **Ordenar por**.

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

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

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

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

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

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

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

Opción	Descripción
Sin límite	La opción de recursos de memoria predeterminada.
Máxima	Especifique un máximo de reserva de memoria que se puede asignar a una máquina virtual.

- 9 Haga clic en **Guardar**.


Insertar medios

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

Requisitos previos

Debe tener acceso a un catálogo con archivos de medios.

Procedimiento

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


Expulsar medio

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

Requisitos previos

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

Procedimiento

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

Resultados

Se expulsará el archivo de medios.

Copiar una máquina virtual en otra vApp


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

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

Requisitos previos

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

Procedimiento

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

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

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

Mover una máquina virtual a otra vApp

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

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

El movimiento de máquinas virtuales entre diferentes vApps depende de VMware vSphere[®] vMotion[®] y Enhanced vMotion Compatibility (EVC). Es posible mover una máquina virtual a una vApp diferente que pertenece al mismo VDC de organización o a uno distinto dentro de la misma organización. El VDC de organización puede estar dentro del mismo VDC de proveedor o de otro diferente.

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


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

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

Requisitos previos

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

Procedimiento

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

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

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

Afinidad y antiafinidad de máquinas virtuales

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


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

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

Ver reglas de afinidad y antiafinidad

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

Procedimiento

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

Resultados

Verá la lista de reglas de afinidad y antiafinidad existentes, las máquinas virtuales y el estado habilitado de cada regla.

Crear una regla de afinidad

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

Procedimiento

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

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

- 3 Introduzca un nombre de regla.

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

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

- 5 Deje activada la casilla de verificación **Obligatorio**.

De forma predeterminada, cada regla de afinidad es obligatoria. Esto significa que, si no se puede cumplir la regla, las máquinas virtuales agregadas a la regla no se encenderán.

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

- 7 Haga clic en **Guardar**.

Resultados

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

Crear una regla de antiafinidad

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

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **Reglas de afinidad**.
- 2 En **Reglas de antiafinidad**, haga clic en **Nuevo**.
- 3 Introduzca un nombre de regla.
- 4 Anule la selección de **Habilitado** para crear la regla sin habilitarla.
De forma predeterminada, la casilla se encuentra seleccionada y las reglas se habilitan una vez creadas.
- 5 Deje activada la casilla de verificación **Obligatorio**.
De forma predeterminada, cada regla de antiafinidad es obligatoria. Esto significa que, si no se puede cumplir la regla, las máquinas virtuales agregadas a la regla no se encenderán.
- 6 Seleccione las máquinas virtuales que desea agregar a la regla de antiafinidad.
- 7 Haga clic en **Guardar**.

Resultados

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

Editar una regla de afinidad o de antiafinidad

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

Requisitos previos

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

Procedimiento

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

- 2 Haga clic en el botón de radio junto al nombre de la regla que desea editar y haga clic en **Editar**.
- 3 Edite las propiedades de la regla.
 - a Cambie el nombre de la regla según sea necesario.
 - b Seleccione si desea activar o desactivar la regla.
 - c Deje activada la casilla de verificación **Obligatorio**.
 - d Agregue o elimine máquinas virtuales.
- 4 Haga clic en **Guardar**.

Eliminar una regla de afinidad o de antiafinidad

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

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **Reglas de afinidad**.
- 2 Haga clic en el botón de radio junto al nombre de la regla que desea eliminar y haga clic en **Eliminar**.
- 3 Para confirmar que desea eliminar la regla, haga clic en **Aceptar**.

Resultados

VMware Cloud Director elimina la regla de afinidad o antiafinidad.

Supervisar máquinas virtuales


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

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

Requisitos previos

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

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **Máquinas virtuales**.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, si lo desea, organizar la lista de máquinas virtuales desde el menú desplegable **Ordenar por**.
- 3 Seleccione la máquina virtual que desea supervisar y haga clic en **Detalles**.

- 4 Haga clic en **Gráfico de supervisión** para expandir la vista de supervisión.

Se muestra el gráfico de supervisión.

5

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

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

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

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

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

Trabajar con instantáneas

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

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

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

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

Tomar una instantánea de una máquina virtual


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

Requisitos previos

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

Nota Las instantáneas no capturan configuraciones NIC.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **Máquinas virtuales**.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, si lo desea, organizar la lista de máquinas virtuales desde el menú desplegable **Ordenar por**.
- 3 En el menú **Acciones** de la máquina virtual de la que desea tomar una instantánea, seleccione **Crear instantánea**.

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

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

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

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

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

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

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

- 6 Haga clic en **Aceptar**.

Resultados

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


Revertir una máquina virtual a una instantánea

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

Requisitos previos

La máquina virtual tiene una instantánea.

Procedimiento

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

Resultados

La máquina virtual se revertirá a la instantánea guardada.

Quitar una instantánea de una máquina virtual


Puede quitar una instantánea de una máquina virtual.

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

Requisitos previos

Una máquina virtual con una instantánea almacenada.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **Máquinas virtuales**.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, si lo desea, organizar la lista de máquinas virtuales desde el menú desplegable **Ordenar por**.
- 3 En el menú **Acciones** de la máquina virtual de la cual desea eliminar una instantánea, seleccione **Quitar instantánea**.
- 4 Haga clic en **Aceptar**.


Renovar una concesión de máquina virtual

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

Requisitos previos

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

Procedimiento

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

Resultados

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


Eliminar una máquina virtual

Puede eliminar una máquina virtual de una organización.

Requisitos previos

La máquina virtual debe estar apagada.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **Máquinas virtuales**.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, si lo desea, organizar la lista de máquinas virtuales desde el menú desplegable **Ordenar por**.
- 3 En el menú **Acciones** de la máquina virtual que desea eliminar, seleccione **Eliminar**.
- 4 Confirme la eliminación.

Resultados

Se eliminará la máquina virtual.

Grupos de escalado automático

A partir de VMware Cloud Director 10.2.2, puede escalar automáticamente las aplicaciones en función del uso actual de CPU y memoria.

Para obtener información sobre la configuración de la solución de escalado automático, consulte [Grupos de escalado automático](#) en la *Guía de instalación, configuración y actualización de VMware Cloud Director*.

Según los criterios predefinidos de uso de CPU y memoria, VMware Cloud Director puede ampliar o reducir automáticamente el número de máquinas virtuales en un grupo de escalado seleccionado. Para equilibrar la carga de los servidores que configure para ejecutar la misma aplicación, puede utilizar VMware NSX Advanced Load Balancer (Avi Networks).

Las funciones de **administrador del sistema** y **administrador de organización** tienen control total de las máquinas virtuales de los grupos de escalado. Las otras funciones globales de tenant pueden ver las máquinas virtuales y acceder a la consola web de la máquina virtual, pero no pueden eliminar, editar ni realizar operaciones de energía, entre otras tareas.

Si elimina un grupo de escalado, VMware Cloud Director no elimina ninguna de las máquinas virtuales que este incluye.

Crear un grupo de escalado

A partir de VMware Cloud Director 10.2.2, su proveedor de servicios puede concederle derechos para crear grupos de escalado. La cantidad de máquinas virtuales en un grupo de escalado cambia automáticamente según las condiciones que defina.

También puede acceder a grupos de escalado desde un centro de datos virtual (Virtual Data Center, VDC) de organización seleccionado.

Procedimiento

- 1 En la barra de navegación superior, seleccione **Aplicaciones** y haga clic en la pestaña **Grupos de escalado**.
- 2 Haga clic en **Nuevo grupo de escalado**.
- 3 Seleccione el VDC de organización en el que se creará el grupo de escalado.
- 4 Escriba un nombre y, opcionalmente, una descripción para el nuevo grupo de escalado.
- 5 Seleccione la cantidad mínima y máxima de máquinas virtuales para escalar el grupo y haga clic en **Siguiente**.
- 6 Seleccione una plantilla de máquina virtual para las máquinas virtuales del grupo de escalado y una directiva de almacenamiento. Haga clic en **Siguiente**.
- 7 Seleccione una red para el grupo de escalado.
 - Si el VDC está respaldado por NSX-T Data Center, seleccione un equilibrador de carga.
 - Si desea administrar el equilibrador de carga por su cuenta o si no hay necesidad de un equilibrador de carga, seleccione **Tengo una red completamente configurada**.
- 8 Haga clic en **Crear grupo y agregar reglas**.

Resultados

VMware Cloud Director inicia la expansión inicial del grupo de escalado para alcanzar el número mínimo de máquinas virtuales.

Pasos siguientes

- [Agregar una regla de escalado automático](#)
- En la vista de detalles de un grupo de escalado, al seleccionar **Supervisar**, puede ver todas las tareas relacionadas con este grupo de escalado. Por ejemplo, puede ver la hora de creación del grupo de escalado, todas las tareas de ampliación o reducción del grupo, las reglas que iniciaron las tareas, etcétera.
- Eliminar un grupo de escalado Cuando elimina un grupo de escalado, VMware Cloud Director no elimina ninguna de las máquinas virtuales que este incluye. Si desea reducir el número de máquinas virtuales, debe eliminarlas manualmente.

Agregar una regla de escalado automático

A partir de VMware Cloud Director 10.2.2, su proveedor de servicios puede concederle derechos para crear y administrar grupos de escalado. Puede agregar reglas que desencadenen la ampliación o la reducción de los grupos de escalado.

Requisitos previos

Crear un grupo de escalado

Procedimiento

- 1 En la barra de navegación superior, seleccione **Aplicaciones** y haga clic en la pestaña **Grupos de escalado**.
- 2 Seleccione un grupo de escalado y **Reglas**.
- 3 Haga clic en **Agregar regla**.
- 4 Escriba un nombre para la regla.
- 5 Seleccione si el grupo de escalado debe ampliarse o reducirse cuando se aplique la regla.
- 6 Seleccione el número de máquinas virtuales para que el grupo se amplíe o reduzca cuando la regla surta efecto.
- 7 Introduzca un período de recuperación en minutos después de cada escalado automático del grupo.

Las condiciones no pueden activar otro escalado hasta que caduque el período de recuperación. Este período se restablece cuando surte efecto cualquiera de las reglas del grupo de escalado.

- 8 Agregue una condición que active la regla.
El período de duración es el tiempo durante el cual la condición debe ser válida para activar la regla. Para activar la regla, se deben cumplir todas las condiciones.
- 9 (opcional) Para agregar otra condición, haga clic en **Agregar condición**.
- 10 Haga clic en **Agregar**.

Trabajar con vApp

3

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

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

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

Este capítulo incluye los siguientes temas:



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

- [Agregar una máquina virtual a una vApp](#)
- [Guardar una vApp como plantilla de vApp en un catálogo](#)
- [Descargar una vApp como un paquete OVF](#)
- [Renovar una concesión de vApp](#)
- [Eliminar una vApp](#)
- [Eliminar varias vApps](#)


Ver vApps

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


Procedimiento

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

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

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

Los detalles seleccionados aparecen como columnas para cada vApp.

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

Por ejemplo, puede apagar una vApp.

Generar una nueva vApp

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

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

Requisitos previos

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

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **vApps**.
- 2 Seleccione **Nueva vApp**.
- 3 Introduzca un nombre y, si lo desea, una descripción de la vApp.
- 4 (opcional) Si desea que la vApp se encienda inmediatamente tras implementarla, active la casilla de verificación **Encender**.

Nota La vApp solo puede encenderse si hay máquinas virtuales en ella.

- 5 (opcional) Busque máquinas virtuales en el catálogo para agregarlas a esta vApp o haga clic en **Agregar máquina virtual** para agregar una máquina virtual vacía nueva.

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

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

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

- b (opcional) Introduzca una descripción significativa.

c Seleccione cómo desea implementar la máquina virtual.

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

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

Puede ver la máquina virtual agregada en el catálogo.

6 (opcional) Repita el [Paso 5](#) para cada máquina virtual adicional que desee crear dentro de la vApp.

7 Para completar la creación de la vApp, haga clic en **Crear**.

Resultados

Se creará la vApp. Al encenderse la vApp, también se crean y se encienden las máquinas virtuales dentro de ella.

Crear una vApp a partir de un paquete OVF

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

VMware Cloud Director tiene sus propias restricciones para las implementaciones de OVF que difieren de las restricciones de vCenter Server. Como resultado, una implementación de OVF correcta en vCenter Server puede no serlo en VMware Cloud Director.

VMware Cloud Director admite OVF 1.1, pero no todas las secciones del esquema OVF 1.1. Por ejemplo, no se admite la sección `DeploymentOptions` de OVF.

Una implementación de OVF en VMware Cloud Director implica muchos componentes, como `TransferService`, área de cola en el montaje de NFS, conexión NFC a vCenter Server, validación de suma de comprobación, etc. Si se produce un error en alguno de estos componentes, se produce un error en la carga de OVF.

Si carga un paquete OVF con un archivo de manifiesto, VMware Cloud Director valida el hash SHA-1 del archivo descriptor OVF y todos los archivos VMDK con los valores del archivo `manifest.mf`. Si algún hash no coincide, se produce un error en la carga. Un **administrador del sistema** puede desactivar esta comprobación si establece la propiedad `CONFIG ovf.manifest.check.disabled`.

Requisitos previos

- Compruebe que tiene un paquete OVF para cargarlo y que dispone de permiso para cargar paquetes OVF e implementar vApps.
- Compruebe que la versión de OVF en el archivo descriptor de OVF no sea 0.9.
- El tamaño máximo admitido predeterminado de un archivo descriptor de OVF en VMware Cloud Director es 12 MB. Para anularlo, edite la propiedad `CONFIG ovf.descriptor.size.max`.
- Compruebe que el tamaño máximo permitido predeterminado del archivo de manifiesto (extensión `.mf`) sea 1 MB.
- Compruebe que el paquete de OVF cumpla con el esquema XSD de OVF.
- Si se proporciona una versión de hardware en el elemento `VirtualSystemType` del archivo descriptor de OVF, compruebe que sea inferior a la versión de hardware más alta admitida por el VDC donde se carga el OVF.
- Si el archivo descriptor de OVF contiene elementos `ExtraConfig`, compruebe que el **administrador del sistema** incluya estos elementos en la `AllowedList` de elementos `extraConfigs`. Los elementos que no se incluyen en la `AllowedList` provocan un error de validación en la carga de OVF.

Procedimiento

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

2 Haga clic en **Agregar vApp desde OVF**.

3 Haga clic en el botón **Cargar** y desplácese hasta una ubicación a la que se pueda acceder desde el equipo y seleccione el archivo de plantilla OVF/OVA.

La ubicación puede ser el disco duro local, un recurso compartido de red o una unidad de CD/DVD. Las extensiones de archivo admitidas incluyen `.ova`, `.ovf`, `.vmdk`, `.mf`, `.cert` y `.strings`. Si opta por cargar un archivo OVF, que hace referencia a más archivos de los que intenta cargar, por ejemplo, un archivo VMDK, debe examinar y seleccionar todos los archivos.

4 Haga clic en **Siguiente**.

5 Verifique los detalles de la plantilla OVF/OVA que va a implementar y haga clic en **Siguiente**.

6 Introduzca un nombre y, de manera opcional, una descripción para la vApp, y haga clic en **Siguiente**.

7 (opcional) Cambie el nombre del equipo de la vApp para que contenga únicamente caracteres alfanuméricos.

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

8 En el menú desplegable **Política de almacenamiento**, seleccione una política de almacenamiento para cada una de las máquinas virtuales de la vApp y haga clic en **Siguiente**.

9 Seleccione las redes a las que desea conectar cada máquina virtual.

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

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

10 Haga clic en **Siguiente**.

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

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

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

La nueva vApp aparecerá en la vista de tarjetas.

Agregar una vApp desde un catálogo

Si tiene acceso a un catálogo, puede utilizar las plantillas de vApp del catálogo para crear vApps.

Una plantilla de vApp se puede basar en un archivo OVF con propiedades para personalizar las máquinas virtuales de la vApp. La vApp hereda estas propiedades. Si el usuario puede configurar algunas de estas propiedades, especifique los valores.

Requisitos previos

- Para acceder a las plantillas de vApp de catálogos públicos, compruebe que sea **administrador de la organización** o **autor de vApps**.
- Para acceder a las plantillas de vApp de los catálogos de la organización que tenga como recursos compartidos, compruebe que tenga al menos un **usuario de vApp**.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **vApps**.
- 2 Haga clic en **Nueva** y seleccione **Agregar vApp desde catálogo**.
- 3 Seleccione la plantilla que desea importar y haga clic en **Siguiente**.
- 4 Introduzca un nombre y, si lo desea, una descripción de la vApp.
- 5 Introduzca una concesión de tiempo de ejecución y otra de almacenamiento para la vApp, y haga clic en **Siguiente**.
- 6 En el menú desplegable **Política de almacenamiento**, seleccione una política de almacenamiento para cada una de las máquinas virtuales de la vApp y haga clic en **Siguiente**.
- 7 Si se pueden configurar las políticas de colocación y tamaño de las máquinas virtuales de la vApp, seleccione una política para cada máquina virtual en el menú desplegable.
- 8 Si se pueden configurar las propiedades informáticas de las máquinas virtuales de la vApp, personalícelas y haga clic en **Siguiente**.

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

- 9 Si se pueden configurar las propiedades de hardware de las máquinas virtuales de la vApp, personalice el tamaño de los discos duros de las máquinas virtuales y haga clic en **Siguiente**.

- 10 Si se pueden configurar las propiedades de redes de las máquinas virtuales de la vApp, personalícelas y haga clic en **Siguiente**.
 - a En la página **Configurar redes**, seleccione las redes a las que desea conectar cada máquina virtual.
 - b (opcional) Seleccione la casilla de verificación para cambiar al flujo de trabajo de redes avanzadas y configure otras opciones de red para las máquinas virtuales de la vApp.
- 11 Revise la configuración de la vApp y haga clic en **Finalizar**.

Crear una vApp a partir de una plantilla de vApp

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

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

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en el panel izquierdo, seleccione **Plantillas de vApp**.

La lista de plantillas aparece en una vista de cuadrícula.
- 2 Haga clic en el botón de radio junto a la plantilla de vApp que desea usar y haga clic en **Crear vApp**.
- 3 Introduzca un nombre y, si lo desea, una descripción de la vApp.
- 4 Especifique la cantidad de horas o días durante los cuales se puede ejecutar la vApp antes de detenerse automáticamente.
- 5 Especifique la cantidad de horas o días durante los cuales permanece disponible la vApp detenida antes de limpiarse de manera automática.
- 6 Haga clic en **Siguiente**.
- 7 Seleccione el centro de datos virtual en el que desea crear la vApp.
- 8 Seleccione una política de almacenamiento.
- 9 Haga clic en **Siguiente**.

- 10 Para VMware Cloud Director 10.2.2 y versiones posteriores, configure las directivas de colocación y tamaño de máquinas virtuales.

A partir de la versión 10.2.2, las directivas de colocación son globales y puede publicirlas en varios VDC de proveedor. Además, las plantillas de vApp incluyen información de directivas de colocación y de tamaño.

- 11 Seleccione las redes a las que desea conectar cada máquina virtual.

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

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

- 12 Haga clic en **Siguiente**.

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

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

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

Resultados

La nueva vApp aparecerá en la vista de tarjetas.

Importar una máquina virtual desde vCenter Server como vApp

Si tiene derechos de **administrador del sistema**, puede importar máquinas virtuales de vCenter Server como vApps a VMware Cloud Director.

La importación de una máquina virtual no conserva la configuración de reserva, límite y recursos compartidos de la máquina virtual que se establece en vCenter Server. Las máquinas virtuales importadas obtienen la configuración de asignación de recursos del centro de datos virtual de organización en el que residen.

Requisitos previos

Para ver e importar máquinas virtuales desde vCenter Server, compruebe que tenga derechos de **administrador del sistema**.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **vApps**.
- 2 Haga clic en **Nueva** y seleccione **Importar desde vCenter**.
- 3 En el menú desplegable, seleccione la instancia de vCenter Server desde la que desea importar una máquina virtual.
- 4 Seleccione la máquina virtual que se debe importar.
- 5 Introduzca un nombre y, si lo desea, una descripción de la vApp.
- 6 En el menú desplegable, seleccione el centro de datos virtual en el que desea almacenar y ejecutar la vApp.
- 7 (opcional) En el menú desplegable, seleccione una política de almacenamiento para la vApp.
- 8 (opcional) Para eliminar la máquina virtual de origen, active la opción **Mover máquina virtual**.
- 9 Haga clic en **Importar**.

Realizar operaciones de encendido y apagado en vApps

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


Encender una vApp

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

Requisitos previos

Debe ser al menos autor de vApps.

Procedimiento

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

Resultados

La vApp se encenderá.


Apagar una vApp

Al desconectar una vApp, se apagan todas las máquinas virtuales de dicha vApp. Para realizar determinadas acciones, como agregar una vApp a un catálogo, copiarla o moverla a otro VDC, primero debe apagar la vApp.

Requisitos previos

La vApp debe estar iniciada.

Procedimiento

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

Resultados

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


Restablecer una vApp

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

Requisitos previos

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

Procedimiento

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

Resultados

Se borrará el estado y la vApp seguirá ejecutándose.


Suspender una vApp

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

Requisitos previos

La vApp debe estar en ejecución.

Procedimiento

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

Resultados

Se suspende la vApp y se conserva su estado.


Descartar el estado de suspensión de una vApp

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

Requisitos previos

La vApp debe estar en estado de suspensión.

Procedimiento

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

Resultados

El estado se descarta y la vApp se apaga.

Encender varias vApps

Puede encender varias vApps al mismo tiempo. Con esta acción se encienden todas las máquinas virtuales de las distintas vApps que aún no lo han hecho.

Requisitos previos

Compruebe que sea al menos un **autor de vApps**.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **vApps**.
- 2 Alterne la opción de **selección múltiple**.
- 3 Seleccione las vApps que desee encender.
- 4 En el menú **Acciones**, seleccione **Encender**.
- 5 Haga clic en **Aceptar** para confirmar.

Apagar varias vApps

Puede apagar varias vApps al mismo tiempo. Con esta acción se desconectan todas las máquinas virtuales de las vApps. Para realizar determinadas acciones, como agregar una vApp a un catálogo, copiarla o moverla a otro centro de datos virtual, primero debe apagar la vApp.

Requisitos previos

- Compruebe que se hayan iniciado las vApps.
- Compruebe que sea al menos un **autor de vApps**.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **vApps**.
- 2 Alterne la opción de **selección múltiple**.
- 3 Seleccione las vApps que desea apagar.
- 4 En el menú **Acciones**, seleccione **Apagar**.
- 5 Haga clic en **Aceptar** para confirmar.

Descartar el estado de suspensión de varias vApps

Si varias vApps se encuentran en estado de suspensión y ya no es necesario reanudar su uso, puede descartar este estado en todas ellas al mismo tiempo. Al hacerlo, se elimina la memoria guardada y las vApps vuelven a apagarse.

Requisitos previos

- Compruebe que las vApps se encuentren en estado suspendido.
- Compruebe que sea al menos un **autor de vApps**.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **vApps**.
- 2 Alterne la opción de **selección múltiple**.
- 3 Seleccione las vApps en suspensión que desea apagar.
- 4 En el menú **Acciones**, seleccione **Descartar estado de suspensión**.

Resultados

Las vApps se apagan.

Restablecer varias vApps

Cuando se restablecen varias vApps al mismo tiempo, se borran sus estados (lo que incluye memoria, memoria caché, etc.), pero se mantienen en ejecución.

Requisitos previos

- Compruebe que las vApps estén iniciadas y las máquinas virtuales que contienen estén encendidas.
- Compruebe que sea al menos un **autor de vApps**.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **vApps**.
- 2 Alterne la opción de **selección múltiple**.
- 3 Seleccione las vApps que desee restablecer.
- 4 En el menú **Acciones**, seleccione **Restablecer** y haga clic en **Aceptar** para confirmar.

Resultados

Al realizar esta acción, se borran los estados de las distintas vApps y estas se mantienen en ejecución.

Suspender varias vApps

Cuando se suspenden varias vApps al mismo tiempo, se conserva el estado que tienen en ese momento escribiendo la memoria en el disco.

Requisitos previos

Compruebe que las vApps se estén ejecutando.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **vApps**.
- 2 Alterne la opción de **selección múltiple**.
- 3 Seleccione las vApps que desee suspender.
- 4 En el menú **Acciones** de la vApp que desea suspender, seleccione **Suspender** y haga clic en **Aceptar** para confirmar.


Resultados

Al realizar esta acción, se suspenden las vApps y se conserva su estado.

Abrir una vApp

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

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **vApps**.
- 2 Haga clic en  para ver las instancias de vApp en una vista de tarjetas.
En la vista de tarjetas, puede ver información general de cada vApp, como: nombre, estado de encendido, información de concesión, fecha de creación, propietario, número de máquinas virtuales asociadas con la vApp, número total de CPU, almacenamiento y memoria totales, así como redes asociadas.
- 3 Para ver la configuración detallada de una vApp seleccionada, haga clic en **Detalles** en la tarjeta de la vApp.

Editar propiedades de una vApp

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


Editar las propiedades generales de la vApp

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

Requisitos previos

Compruebe que la vApp está apagada.

Procedimiento

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

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

Resultados

La configuración general se guardará.

Editar el orden de inicio y detención de las máquinas virtuales en una vApp

Puede configurar el orden de inicio y detención de las máquinas virtuales dentro de la vApp.


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

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

Requisitos previos

Compruebe que la vApp está apagada.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **vApps**.
- 2 Haga clic en  para ver las instancias de vApp en una vista de tarjetas.
- 3 En la tarjeta de la vApp seleccionada, haga clic en **Detalles**.
- 4 Haga clic en la pestaña **Orden de inicio y detención** y en **Editar**.
- 5 Edite las propiedades de orden de inicio y detención de cada máquina virtual y haga clic en **Aceptar**.

Opción	Acción
Orden de inicio	Especifique el orden en el que desea que se inicie la máquina virtual. Debe escribir un valor para cada máquina en la secuencia.
Acción de inicio	<p>Seleccione una acción de inicio.</p> <p>La acción de inicio determina lo que le sucede a una máquina virtual cuando se inicia la vApp que la contiene. Esta opción está establecida en Encender de manera predeterminada.</p>
Espera de inicio	<p>Especifique el tiempo de espera de inicio.</p> <p>El tiempo de espera de inicio es la cantidad de tiempo (en segundos) que desea esperar antes de que VMware Cloud Director inicie la siguiente máquina en la secuencia.</p>
Acción de detención	<p>Seleccione la acción de detención.</p> <p>La acción de detención es la acción que realiza la máquina virtual cuando se detiene la vApp que la contiene. Si selecciona Apagar, la máquina virtual se apaga sin realizar acciones de desconexión que garanticen la estabilidad (lo que equivaldría a desconectar un cable de un enchufe). Seleccione esta acción si no ha instalado VMware Tools. De lo contrario, seleccione Desconectar para garantizar la estabilidad durante la desconexión.</p>
Espera de detención	<p>Especifique el tiempo de espera de detención.</p> <p>El tiempo de espera de detención es la cantidad de tiempo (en segundos) que desea esperar antes de que VMware Cloud Director desconecte la siguiente máquina virtual en la secuencia.</p>

Editar las propiedades de invitado de una vApp


Si una vApp contiene propiedades de OVF que el usuario puede configurar, puede revisarlas y modificarlas.

Si una máquina virtual de la vApp contiene un valor para la propiedad configurable por el usuario con el mismo nombre, el valor de la máquina virtual tomará prioridad.

Requisitos previos

Compruebe que la vApp esté detenida y que el usuario pueda configurar sus propiedades de invitado.


Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **Máquinas virtuales**.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, si lo desea, organizar la lista de máquinas virtuales desde el menú desplegable **Ordenar por**.
- 3 En la tarjeta de la máquina virtual que desea editar, haga clic en **Detalles**.
- 4 Haga clic en **Propiedades de invitado** y en **Editar**.
- 5 Modifique las propiedades de invitado de la vApp y haga clic en **Aceptar**.

Compartir una vApp

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

Procedimiento

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

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

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

Resultados

La vApp se compartirá con los usuarios o grupos especificados.


Mostrar un diagrama de red de vApp

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

Requisitos previos

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

Procedimiento

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

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

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

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

Se resaltarán los objetos conectados y las conexiones entre ellos.

Pasos siguientes

Puede agregar máquinas virtuales o redes desde esta página.

Trabajar con redes en una vApp

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

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

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

Nota Los VDC de organización respaldados por NSX Data Center for vSphere admiten redes de vApp aisladas, directas y enrutadas.

Los VDC de organización respaldados por NSX-T Data Center admiten redes de vApp aisladas y directas.

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



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

Ver las redes de una vApp

Puede obtener acceso y ver las redes de una vApp.

Requisitos previos

Procedimiento

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

Colocar una barrera de red de vApp


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

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

Requisitos previos

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

Procedimiento

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

- 5 Si la vApp no tiene barreras, haga clic en el botón **Editar**.
- 6 Active la opción **Crear barrera en vApp** y haga clic en **Aceptar**.

Resultados

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

Agregar una red a una vApp

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


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

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

Requisitos previos

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

Procedimiento

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

4 Seleccione el tipo de red que desea agregar.

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

5 Haga clic en **Agregar**.

Resultados

La red se agregará a la vApp.

Pasos siguientes

Conecte una máquina virtual en la vApp a la red.

Configuración de servicios de redes para una red de vApp

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

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

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

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


Nota Los VDC de organización respaldados por NSX Data Center for vSphere admiten redes de vApp aisladas, directas y enrutadas.

Los VDC de organización respaldados por NSX-T Data Center admiten redes de vApp aisladas y directas.

Ver y editar los detalles generales de la red

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


Procedimiento

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

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

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


Procedimiento

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

Editar la configuración de DNS de una red de vApp

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

Procedimiento

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

Configurar DHCP para una red de vApp


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

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

Requisitos previos

- Compruebe que la red de vApp esté enrutada o aislada.
- Compruebe que la instancia de vApp se encuentre en un centro de datos virtual de organización respaldado por NSX Data Center for vSphere.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **vApps**.
- 2 Haga clic en  para ver las instancias de vApp en una vista de tarjetas.
- 3 En la tarjeta de la vApp seleccionada, haga clic en **Detalles**.
- 4 En la pestaña **Redes**, haga clic en una red para ver los detalles de la red.
- 5 En la pestaña **Administración de direcciones IP**, haga clic en **DHCP**.
Se muestra el estado de DHCP.
- 6 Haga clic en **Editar**.
- 7 Haga clic en **Habilitado**.

- 8 En el cuadro de texto **Grupo de direcciones IP**, introduzca un rango de direcciones IP.

VMware Cloud Director utiliza estas direcciones para responder a las solicitudes DHCP. El rango de las direcciones IP de DHCP no puede superponerse con el grupo de direcciones IP estáticas para la red de vApp.


- 9 Establezca el tiempo de concesión predeterminado y máximo en segundos.

- 10 Haga clic en **Guardar**.

Mostrar las asignaciones de IP de una red de vApp

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

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **vApps**.
- 2 Haga clic en  para ver las instancias de vApp en una vista de tarjetas.
- 3 En la tarjeta de la vApp seleccionada, haga clic en **Detalles**.
- 4 En la pestaña **Redes**, haga clic en una red para ver los detalles de la red.
- 5 En la pestaña **Administración de direcciones IP**, haga clic en **Asignaciones de IP**.

Se mostrarán las direcciones IP asignadas.

Configurar el enrutamiento estático para una red de vApp


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

Cualquier ruta estática que cree se activará automáticamente.

Requisitos previos

Debe existir una red de vApp con enrutamiento.

Procedimiento

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

Puede activar o desactivar el enrutamiento estático para la red.

Agregar enrutamiento estático para una red de vApp

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


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

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

Requisitos previos

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

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **vApps**.
- 2 Haga clic en  para ver las instancias de vApp en una vista de tarjetas.
- 3 En la tarjeta de la vApp seleccionada, haga clic en **Detalles**.
- 4 En la pestaña **Redes**, haga clic en una red para ver los detalles de la red.
- 5 En la pestaña **Enrutamiento**, haga clic en **Agregar** bajo Enrutamiento estático.
Se mostrarán las direcciones IP asignadas.
- 6 Introduzca el nombre de la ruta estática.
- 7 Introduzca la dirección de red con el formato CIDR.
La dirección de red es para la red de vApp a la que se agrega una ruta estática.
- 8 Introduzca la dirección IP del próximo salto.
La dirección IP del próximo salto es la dirección IP externa de ese enrutador de la red de vApp.
- 9 Haga clic en **Guardar**.
- 10 Repita el mismo procedimiento para la segunda red de vApp.

Ejemplo: Ejemplo de enrutamiento estático

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

Tabla 3-2. Información de red

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

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

Tabla 3-3. Configuración de enrutamiento estático

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

Agregar una regla de enrutamiento de puertos a una red de vApp

Es posible configurar ciertas redes de vApp para proporcionar enrutamiento de puertos al agregar una regla de asignación de NAT.

El enrutamiento de puertos proporciona acceso externo a servicios que se ejecutan en máquinas virtuales en la red de vApp.

Cuando configura el enrutamiento de puertos, VMware Cloud Director asigna un puerto externo a un servicio que se ejecuta en una máquina virtual dedicada al tráfico entrante.


Al agregar una regla de enrutamiento de puertos a una red de vApp, aparecerá al final de la lista de reglas de asignación de NAT. Para obtener información acerca de cómo establecer el orden de aplicación de las reglas de enrutamiento de puertos, consulte

Requisitos previos

- Compruebe que la red de vApp esté enrutada.
- Compruebe que el firewall de la red de vApp esté activado. Si desactiva el firewall, las reglas de asignación de NAT ya no se aplican a la red de vApp.

Procedimiento

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

- 2 Haga clic en  para ver las instancias de vApp en una vista de tarjetas.
- 3 En la tarjeta de la vApp seleccionada, haga clic en **Detalles**.
- 4 En la pestaña **Redes**, haga clic en una red para ver los detalles de la red.
- 5 Haga clic en **Servicios** y en **Editar**.
- 6 Para activar NAT, active la opción correspondiente.
- 7 En el menú desplegable **Tipo de NAT**, seleccione **Enrutamiento de puerto** y haga clic en **Agregar**.
- 8 (opcional) Para habilitar el enmascaramiento de IP, seleccione la casilla de verificación.
- 9 Configure la regla del enrutamiento de puertos.
 - a Seleccione un puerto externo.
 - b Seleccione un puerto al que desee reenviarlo.
 - c Seleccione una interfaz de máquina virtual.
 - d Seleccione un protocolo para el tipo de tráfico que se va a enrutar.
- 10 Haga clic en **Guardar**.

Pasos siguientes

Si es necesario, reorganice las reglas de enrutamiento de puertos con los botones **Subir** o **Bajar**.

Agregar una regla de conversión de IP a una red de vApp


Es posible configurar ciertas redes de vApp para proporcionar la conversión de una IP agregando una regla de asignación de NAT.

Al crear una regla de conversión de IP para una red, vCloud Director agrega una regla DNAT y SNAT a la puerta de enlace Edge asociada al grupo de puertos de la red. La regla DNAT convierte la dirección IP externa en una interna para el tráfico entrante. La regla SNAT convierte una dirección IP interna en una externa para el tráfico saliente.

Requisitos previos

- Compruebe que la red de vApp esté enrutada.
- Compruebe que el firewall de la red de vApp esté activado. Si desactiva el firewall, las reglas de asignación de NAT ya no se aplican a la red de vApp.

Procedimiento

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

- 4 En la pestaña **Redes**, haga clic en una red para ver los detalles de la red.
- 5 Haga clic en **Servicios** y en **Editar**.
- 6 Para activar NAT, active la opción correspondiente.
- 7 En el menú desplegable **Tipo de NAT**, seleccione **Conversión de IP** y haga clic en **Agregar**.
- 8 Seleccione una interfaz de máquina virtual y haga clic en **Conservar**.
- 9 Seleccione un modo de asignación.
- 10 Si seleccionó el modo de asignación **Manual**, introduzca una dirección IP externa.
- 11 Haga clic en **Guardar**.

Pasos siguientes

Si es necesario, reorganice las reglas de conversión de IP con los botones **Subir** o **Bajar**.


Eliminar una red de vApp

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

Requisitos previos

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

Procedimiento

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

Trabajar con instantáneas

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

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


Tomar una instantánea de una vApp

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

Las instantáneas de vApps tienen algunas limitaciones.

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

Procedimiento

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

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

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

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

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

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

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

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

6 Haga clic en **Aceptar**.

Resultados

Se crea una instantánea de la vApp.

Pasos siguientes

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


Revertir una vApp a una instantánea

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

Requisitos previos

Compruebe que la vApp tenga una instantánea.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **vApps**.
- 2 Haga clic en  para ver las instancias de vApp en una vista de tarjetas.
- 3 En el menú **Acciones** de la vApp que desea revertir, seleccione **Revertir a instantánea**.
- 4 Haga clic en **Aceptar**.

Resultados

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

Quitar una instantánea de una vApp


Puede quitar una instantánea de una vApp.

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

Requisitos previos

Ha tomado una instantánea de la vApp.

Procedimiento

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

- 3 En el menú **Acciones** de la vApp de la cual desea eliminar una instantánea, seleccione **Quitar instantánea**.
- 4 Haga clic en **Aceptar**.

Resultados

Se quitará la instantánea.

Crear instantáneas de varias vApps

Al crear instantáneas de varias vApps, se crean instantáneas de todas las máquinas virtuales de las vApps. Tras crearlas, puede revertir todas las máquinas virtuales de las vApps a las instantáneas, o bien eliminar las instantáneas si no las necesita.

Las instantáneas de vApps tienen algunas limitaciones.

- Las instantáneas de vApps no capturan configuraciones de NIC.
- Si una máquina virtual de una vApp está conectada a un disco con nombre, no se puede realizar una instantánea de esa vApp.
- Al realizar instantáneas de varias vApps, no se crean instantáneas de la memoria de dichas vApps y los sistemas de archivos invitados de estas no se ponen en modo inactivo. Si desea realizar una instantánea de la memoria de las vApps o poner los sistemas de archivos invitados en modo inactivo, debe crear instantáneas individuales para cada vApp. Consulte la [Tomar una instantánea de una vApp](#).

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **vApps**.
- 2 Alterne la opción de **selección múltiple**.
- 3 Seleccione las vApps de las que desea realizar instantáneas.
- 4 En el menú **Acciones**, seleccione **Crear instantánea** y haga clic en **Aceptar** para confirmar.

Pasos siguientes

- Puede revertir todas las máquinas virtuales de las vApps a las instantáneas más recientes. Consulte la [Revertir varias vApps a instantáneas](#).
- Puede eliminar las instantáneas de la vApps. Consulte la [Eliminar las instantáneas de varias vApps](#).

Eliminar las instantáneas de varias vApps

Si no necesita las instantáneas de varias vApps, puede eliminarlas al mismo tiempo.

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

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **vApps**.
- 2 Alterne la opción de **selección múltiple**.
- 3 Seleccione las vApps cuyas instantáneas desea eliminar.
- 4 En el menú **Acciones**, seleccione **Quitar instantánea**.

Revertir varias vApps a instantáneas

Puede revertir todas las máquinas virtuales de varias vApps al estado en el que se encontraban cuando se crearon las instantáneas de vApps.

Requisitos previos

Compruebe que las vApps que desea revertir cuentan con instantáneas existentes.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **vApps**.
- 2 Alterne la opción de **selección múltiple**.
- 3 Seleccione la vApps que desea revertir a sus instantáneas más recientes.
- 4 En el menú **Acciones**, seleccione **Revertir a instantánea**.
- 5 Haga clic en **Aceptar** para confirmar.


Cambiar el propietario de una vApp

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

Requisitos previos

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

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **vApps**.
- 2 Haga clic en  para ver las instancias de vApp en una vista de tarjetas.
- 3 En el menú **Acciones** de la vApp cuyo propietario desea cambiar, seleccione **Cambiar propietario**.
- 4 Seleccione un usuario de la lista.

5 Haga clic en **Aceptar**.

Resultados

Se cambia el propietario de la vApp.


Mover una vApp a otro centro de datos virtual

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

Requisitos previos

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

Procedimiento

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

Resultados

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


Copiar una vApp detenida en otro centro de datos virtual

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

Requisitos previos

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

Procedimiento

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

- 3 En el menú **Acciones** de la vApp que desea copiar, seleccione **Copiar a**.
- 4 Escriba un nombre y descripción.
- 5 Seleccione el centro de datos virtual en el que desea crear una copia de la vApp.
- 6 (opcional) Seleccione una política de almacenamiento.
- 7 Haga clic en **Aceptar**.

Resultados

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

Copiar una vApp encendida


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

Requisitos previos

Verifique que se cumplan las siguientes condiciones.

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

Procedimiento

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

Resultados

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

Pasos siguientes

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

Agregar una máquina virtual a una vApp

Puede agregar una máquina virtual a una vApp.

Requisitos previos

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

Procedimiento

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

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

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

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

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

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

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

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

8 Seleccione cómo desea implementar la máquina virtual.

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

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

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

Guardar una vApp como plantilla de vApp en un catálogo


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

A partir de VMware Cloud Director 10.2.2, al agregar una vApp a un catálogo, la plantilla de vApp incluye las políticas de colocación y tamaño de la vApp de origen como etiquetas no modificables.

Requisitos previos

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

Procedimiento

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

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

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

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

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

- 7 Especifique cómo se debe utilizar la plantilla.

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

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

- 8 Para completar la creación de la plantilla de vApp, haga clic en **Aceptar**.

Resultados

La plantilla de vApp aparece en el catálogo especificado.


Descargar una vApp como un paquete OVF

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

Requisitos previos

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

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **vApps**.
- 2 Haga clic en  para ver las instancias de vApp en una vista de tarjetas.
- 3 En el menú **Acciones** de la vApp que desea descargar, seleccione **Descargar**.
- 4 Seleccione el formato en que desea descargar la vApp.
- 5 (opcional) Seleccione **Proteger información de identidad** para incluir los UUID y las direcciones MAC de las máquinas virtuales que residen en la vApp en el paquete OVF descargado.

Esto limita la portabilidad del paquete y debe utilizarse solo cuando sea necesario.
- 6 Haga clic en **Aceptar** para confirmar la selección e iniciar la descarga.

Resultados

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

Renovar una concesión de vApp

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

Requisitos previos

Compruebe que tiene asignada la función predefinida **Usuario de vApp** o un conjunto equivalente de derechos.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **vApps**.
- 2 Seleccione la vApp que desea renovar.
- 3 En el menú **Acciones**, seleccione **Renovar concesión**.
- 4 Renueve la concesión de tiempo de ejecución de la vApp.
 - a Seleccione la casilla de verificación **Concesión de tiempo de ejecución**.
 - b En el menú desplegable, seleccione un valor para la concesión de tiempo de ejecución.

Puede seleccionar un valor en horas o días, o establecer la concesión en **Nunca caduca**. Los **administradores del sistema** pueden limitar la longitud máxima que puede elegir.

5 Renueve la concesión de almacenamiento de la vApp.

- a Seleccione la casilla de verificación **Concesión de almacenamiento**.
- b En el menú desplegable, seleccione un valor para la concesión de almacenamiento.

Puede seleccionar un valor en horas o días, o establecer la concesión en **Nunca caduca**.

Los **administradores del sistema** pueden limitar la longitud máxima que puede elegir.

Eliminar una vApp

Al eliminar una vApp, desaparece de la organización.

Requisitos previos

Debe detener la vApp.

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

Procedimiento

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

Resultados

Se eliminará la vApp.

Eliminar varias vApps

Si desea eliminar varias vApps de la organización, puede hacerlo al mismo tiempo.

Requisitos previos

- Compruebe que las vApps estén detenidas.
- Compruebe que es al menos un **autor de vApps**.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en el panel izquierdo, seleccione **vApps**.
- 2 Alterne la opción de **selección múltiple**.
- 3 Seleccione las vApps que desee eliminar.
- 4 En el menú **Acciones**, seleccione **Eliminar**.
- 5 Para confirmar, haga clic en **Eliminar**.

Trabajar con clústeres de Kubernetes

4

Puede crear clústeres de Kubernetes de diferentes tamaños de nodo a partir de las directivas de VDC de organización existentes.

Kubernetes Container Clusters es el complemento de Container Service Extension para VMware Cloud Director. Puede utilizar el complemento Kubernetes Container Clusters en el VMware Cloud Director Tenant Portal para implementar clústeres con clústeres nativos y de VMware Tanzu Kubernetes Grid Integrated Edition (TKGI). Puede crear clústeres de Tanzu Kubernetes sin el complemento Kubernetes Container Clusters.

Cuando se habilita en un clúster de vSphere, VMware vSphere® with VMware Tanzu™ proporciona la capacidad de crear clústeres de Kubernetes ascendentes en grupos de recursos dedicados. Para obtener más información, consulte la guía de *administración y configuración de vSphere with Kubernetes* en la documentación de vSphere.

Cuando un proveedor de servicios crea una directiva de Kubernetes de VDC de proveedor y la publica en un VDC de organización, se crea una directiva de Kubernetes de VDC de organización. Puede utilizar el complemento Kubernetes Container Clusters para crear clústeres de Tanzu Kubernetes aplicando una de las directivas de Kubernetes de VDC de organización.

Opciones de tiempo de ejecución de Kubernetes

- Clústeres de Tanzu Kubernetes: puede utilizar la opción de tiempo de ejecución vSphere Kubernetes para crear clústeres de Tanzu Kubernetes administrados por vSphere with VMware Tanzu. Esta opción ofrece más funciones, pero es posible que sea más costosa. Para obtener más información, consulte la guía de *administración y configuración de vSphere with Kubernetes* en la documentación de vSphere.
- Clústeres nativos: el complemento Kubernetes Container Clusters administra los clústeres con tiempo de ejecución nativo de Kubernetes. Estos clústeres tienen una función de alta disponibilidad reducida con un nodo de plano de control único, ofrecen menos opciones de volúmenes persistentes y ninguna automatización de redes. Sin embargo, pueden tener un costo más bajo.
- Clústeres de TKGI: VMware Tanzu Kubernetes Grid Integrated Edition es una solución de contenedor diseñada para operativizar Kubernetes para proveedores de servicios y empresas

de varias nubes. Algunas de sus capacidades son alta disponibilidad, escalado automático, comprobaciones de estado, corrección automática y actualizaciones graduales para clústeres de Kubernetes. Para obtener más información sobre los clústeres de TKGI, consulte la documentación de *VMware Tanzu Kubernetes Grid Integrated Edition*.

Este capítulo incluye los siguientes temas:

- [Agregar una política de Kubernetes de VDC de organización](#)
- [Editar una política de Kubernetes de VDC de organización](#)
- [Crear un clúster de Tanzu Kubernetes](#)
- [Crear un clúster de Kubernetes nativo](#)
- [Crear un clúster de VMware Tanzu Kubernetes Grid Integrated Edition](#)
- [Configurar el acceso externo a un servicio en un clúster de Tanzu Kubernetes](#)

Agregar una política de Kubernetes de VDC de organización

Si tiene derechos de **administrador del sistema**, puede agregar una política de Kubernetes de VDC de organización mediante una política de Kubernetes de VDC de proveedor. Puede usar la política de Kubernetes de VDC de organización para crear clústeres de Tanzu Kubernetes.

Al agregar o publicar una política de Kubernetes de VDC de proveedor en un VDC de organización, la política se pone a disposición de los tenants mediante la creación de una política de VDC de organización. Los tenants pueden utilizar las políticas de Kubernetes de VDC de organización disponibles para aprovechar la capacidad de Kubernetes al crear clústeres de Tanzu Kubernetes. Una política de Kubernetes encapsula las clases de colocación, calidad de infraestructura y almacenamiento de volúmenes persistentes. Las políticas de Kubernetes pueden tener distintos límites de recursos informáticos.

Puede agregar varias políticas de Kubernetes de VDC de organización a un solo VDC de organización. Puede utilizar una sola política de Kubernetes de VDC de proveedor para crear varias políticas de Kubernetes de VDC de organización. Puede utilizar las políticas de Kubernetes de VDC de organización como indicador de la calidad del servicio. Por ejemplo, puede publicar una política de Kubernetes Gold que permite una selección de las clases de máquinas garantizadas y una clase de almacenamiento rápido, o una política de Kubernetes Silver que permite una selección de las clases de máquinas de mejor esfuerzo y una clase de almacenamiento lento.

Requisitos previos

- Compruebe que tenga una función de **administrador del sistema** o una función que incluya un conjunto equivalente de derechos. Todas las demás funciones solo pueden ver las políticas de Kubernetes de VDC de organización.
- Compruebe que el entorno tenga al menos un VDC de proveedor respaldado por un clúster de supervisor. Los VDC de proveedor respaldados por un clúster de supervisor se marcan con

un icono de Kubernetes en la pestaña **VDC de proveedor** del Service Provider Admin Portal. Para obtener más información sobre vSphere with VMware Tanzu en VMware Cloud Director, consulte [Usar vSphere with Kubernetes en VMware Cloud Director](#) en *Guía del portal para administradores de proveedores de servicios de VMware Cloud Director*.

- Compruebe que ha iniciado sesión en un VDC de organización flexible.
- Familiarícese con los tipos de clases de máquinas virtuales para los clústeres de Tanzu Kubernetes. Consulte la guía de *administración y configuración de vSphere with Kubernetes* en la documentación de vSphere.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Centros de datos** y, a continuación, en **Centro de datos virtual**.
- 2 Seleccione un centro de datos virtual de organización.
- 3 En el panel izquierdo, en **Configuración**, seleccione **Políticas de Kubernetes** y haga clic en **Agregar**.

Aparece el asistente **Publicar en VDC de organización**.

- 4 Introduzca un nombre y una descripción visibles para los tenants para la política de Kubernetes de VDC de organización y haga clic en **Siguiente**.
- 5 Seleccione la política de Kubernetes de VDC de proveedor que desee utilizar y haga clic en **Siguiente**.
- 6 Seleccione los límites de CPU y memoria para los clústeres de Tanzu Kubernetes creados en esta política.

Los límites máximos dependen de las asignaciones de memoria y CPU del VDC de organización. Cuando se agrega la política, los límites seleccionados actúan como valores máximos para los tenants.

- 7 Elija si desea reservar CPU y memoria para los nodos del clúster de Tanzu Kubernetes creados en esta política, y haga clic en **Siguiente**.

Existen dos ediciones para cada tipo de clase: garantizada y de mejor esfuerzo. Una edición de clase garantizada reserva por completo sus recursos configurados, mientras que una edición de mejor esfuerzo permite que los recursos se sobreasignen. En función de la selección, en la siguiente página del asistente, puede elegir entre los tipos de clase de máquina virtual de edición garantizada o de mejor esfuerzo.

- Seleccione **Sí** para los tipos de clase de máquina virtual de edición garantizada para reservar totalmente la CPU y la memoria.
- Seleccione **No** para los tipos de clase de máquina virtual de edición de mejor esfuerzo sin reservas de CPU y memoria.

- En la página **Clases de máquina** del asistente, seleccione uno o varios de los tipos de clase de máquina virtual disponibles para esta política.

Las clases de máquinas seleccionadas son los únicos tipos de clase disponibles para los tenants cuando se agrega la política al VDC de organización.

- Seleccione una o varias políticas de almacenamiento.
- Revise las opciones y haga clic en **Publicar**.

Resultados

La información sobre la política publicada aparece en la lista de políticas de Kubernetes. La política publicada crea un espacio de nombres de supervisor en el clúster de supervisor con los límites de recursos especificados de la política.

Los tenants pueden empezar a utilizar la política de Kubernetes para crear clústeres de Tanzu Kubernetes. VMware Cloud Director coloca cada clúster de Tanzu Kubernetes creado bajo esta política de Kubernetes en el mismo espacio de nombres de supervisor. Los límites de recursos de políticas se convierten en límites de recursos para el espacio de nombres de supervisor. Todos los clústeres de Tanzu Kubernetes creados por el tenant en el espacio de nombres de supervisor compiten por los recursos dentro de estos límites.

Pasos siguientes

- Elimine una política de Kubernetes de VDC de organización.
- Mediante el Service Provider Admin Portal, puede administrar las cuotas de recursos de la organización. Consulte [Administrar cuotas para el uso de recursos de una organización](#) en *Guía del portal para administradores de proveedores de servicios de VMware Cloud Director*.
- [Administrar las cuotas de recursos de un grupo](#) o [Administrar las cuotas de recursos de un usuario](#)

Editar una política de Kubernetes de VDC de organización

Si tiene derechos de **administrador del sistema**, puede modificar una política de Kubernetes de VDC de organización para cambiar su descripción, así como sus límites de memoria y CPU.

Requisitos previos

Compruebe que tenga una función de **administrador del sistema** o una función que incluya un conjunto equivalente de derechos. Todas las demás funciones solo pueden ver las políticas de Kubernetes de VDC de organización.

Procedimiento

- En la barra de navegación superior, haga clic en **Centros de datos** y, a continuación, en **Centro de datos virtual**.
- Seleccione un centro de datos virtual de organización.

- 3 En el panel izquierdo, en **Configuración**, haga clic en **Políticas de Kubernetes**.
- 4 Seleccione la política de Kubernetes de VDC de organización que desee editar y haga clic en **Editar**.
Aparece el asistente **Editar política de Kubernetes de VDC**.
- 5 Edite la descripción de la política de Kubernetes de VDC de organización y haga clic en **Siguiente**.
El nombre de la política está vinculado al espacio de nombres de supervisor creado durante la publicación de la política y no se puede cambiar.
- 6 Edite el límite de CPU y memoria para la política de Kubernetes de VDC de organización y haga clic en **Siguiente**.
No se puede editar la reserva de CPU y memoria.
- 7 Revise los detalles de la nueva política y haga clic en **Guardar**.

Pasos siguientes

- Elimine una política de Kubernetes de VDC de organización.
- Mediante el Service Provider Admin Portal, puede cambiar las cuotas de recursos de la organización. Consulte [Administrar cuotas para el uso de recursos de una organización](#) en *Guía del portal para administradores de proveedores de servicios de VMware Cloud Director*.
- Cambie las cuotas de grupos y de usuarios. Consulte [Administrar las cuotas de recursos de un grupo](#) o [Administrar las cuotas de recursos de un usuario](#).

Crear un clúster de Tanzu Kubernetes

Puede crear clústeres de Tanzu Kubernetes mediante el complemento Kubernetes Container Clusters.

Para obtener más información sobre las diferentes opciones de tiempo de ejecución de Kubernetes para la creación de clústeres, consulte [Capítulo 4 Trabajar con clústeres de Kubernetes](#).

También puede administrar los clústeres de Kubernetes mediante la CLI de Container Service Extension. Consulte la documentación de [Container Service Extension](#).

VMware Cloud Director aprovisiona clústeres de Tanzu Kubernetes con el controlador de admisión de políticas de seguridad de pods habilitado. Debe crear una política de seguridad de pods para implementar cargas de trabajo. Para obtener información sobre cómo implementar el uso de las políticas de seguridad de pods en Kubernetes, consulte el tema *Usar políticas de seguridad de pods con clústeres de Tanzu Kubernetes* en la guía *Configuración y administración de vSphere with Kubernetes*.

Requisitos previos

- Compruebe que el proveedor de servicios haya publicado el complemento Kubernetes Container Clusters en su organización. Puede encontrar el complemento en la barra de navegación superior, en **Más > Kubernetes Container Clusters**.
- Compruebe que tiene al menos una política de Kubernetes de VDC de organización en el VDC de organización. Para agregar una política de Kubernetes de VDC de organización, consulte [Agregar una política de Kubernetes de VDC de organización](#).
- Compruebe que el proveedor de servicios haya publicado el paquete de derechos **Autorización de vmware:tkgcluster** en su organización y le haya otorgado a usted el derecho **Editar: Clúster invitado de Tanzu Kubernetes** para crear y modificar clústeres de Tanzu Kubernetes. Para poder eliminar clústeres, debe tener el derecho **Control total: Clúster invitado de Tanzu Kubernetes**.
- Compruebe que el proveedor de servicios haya creado una entrada de lista de control de acceso (ACL) para usted con información sobre su nivel de acceso.

Procedimiento

- 1 En la barra de navegación superior, seleccione **Más > Kubernetes Container Clusters**.
- 2 (opcional) Si el VDC de organización está habilitado para la creación de clústeres de TKGI, en la página **Kubernetes Container Clusters**, seleccione la pestaña **vSphere with Tanzu y nativo**.
- 3 Haga clic en **Nuevo**.
- 4 Seleccione la opción de tiempo de ejecución de **vSphere with Tanzu** y haga clic en **Siguiente**.
- 5 Escriba un nombre para el clúster de Kubernetes y haga clic en **Siguiente**.
- 6 Seleccione el VDC de organización en el que desea implementar un clúster de Tanzu Kubernetes y haga clic en **Siguiente**.
- 7 Seleccione una política de Kubernetes de VDC de organización y una versión de Kubernetes y, a continuación, haga clic en **Siguiente**.

VMware Cloud Director muestra un conjunto predeterminado de versiones de Kubernetes que no están ligadas a ninguna política de Kubernetes o de VDC de organización. Estas versiones son un ajuste global. Para cambiar la lista de versiones disponibles, utilice la herramienta de administración de celdas para ejecutar el comando `./cell-management-tool manage-config --name wcp.supported.kubernetes.versions -v version_number` con los números de versión separados por comas.

- 8 Seleccione la cantidad de nodos de trabajo y plano de control en el nuevo clúster.
- 9 Seleccione las clases de máquina para los nodos de trabajo y plano de control, y haga clic en **Siguiente**.
- 10 Seleccione una clase de almacenamiento de directivas de Kubernetes para los nodos de trabajo y haga clic en **Siguiente**.

- 11 (opcional) Para VMware Cloud Director 10.2.2 y versiones posteriores, especifique un rango de direcciones IP para los servicios de Kubernetes y un rango para los pods de Kubernetes, y haga clic en **Siguiente**.

El enrutamiento entre dominios sin clases (Classless Inter-Domain Routing, CIDR) es un método para el enrutamiento y la asignación de direcciones IP.

Opción	Descripción
Pods CIDR	Especifica un rango de direcciones IP que se puede usar para los pods de Kubernetes. El valor predeterminado es 192.168.0.0/16. El tamaño de subred de los pods debe ser igual o mayor que /24. Este valor no debe superponerse con la configuración del clúster de supervisor. Puede introducir un solo rango de direcciones IP.
Services CIDR	Especifica un rango de direcciones IP que se puede usar para los servicios de Kubernetes. El valor predeterminado es 10.96.0.0/12. Este valor no debe superponerse con la configuración del clúster de supervisor. Puede introducir un solo rango de direcciones IP.

- 12 Revise la configuración del clúster y haga clic en **Finalizar**.

Pasos siguientes

- Cambie el tamaño del clúster de Kubernetes si desea cambiar la cantidad de nodos de trabajo.
- Descargue el archivo kubeconfig. La herramienta de línea de comandos kubectl utiliza archivos kubeconfig para obtener información sobre los clústeres, los usuarios, los espacios de nombres y los mecanismos de autenticación.
- Elimine un clúster de Kubernetes.

Crear un clúster de Kubernetes nativo

Puede crear clústeres de Kubernetes administrados por Container Service Extension 3.0 mediante el complemento Kubernetes Container Clusters.

Para obtener más información sobre las diferentes opciones de tiempo de ejecución de Kubernetes para la creación de clústeres, consulte [Capítulo 4 Trabajar con clústeres de Kubernetes](#).

También puede administrar los clústeres de Kubernetes mediante la CLI de Container Service Extension. Consulte la documentación de [Container Service Extension](#).

Requisitos previos

- Compruebe que el proveedor de servicios haya publicado el complemento Kubernetes Container Clusters en su organización. Kubernetes Container Clusters es el complemento de Container Service Extension para VMware Cloud Director. Puede encontrar el complemento en la barra de navegación superior, en **Más > Kubernetes Container Clusters**.
- Compruebe que el proveedor de servicios haya completado la configuración del servidor de Container Service Extension 3.0 y haya publicado una política de colocación nativa de Container Service Extension en el VDC de organización.
- Compruebe que el proveedor de servicios haya publicado el paquete de derechos **Autorización de cse:nativeCluster** en su organización y le haya otorgado a usted el derecho **Editar CSE:NATIVECLUSTER** para crear y modificar los clústeres de Kubernetes nativos. Para poder eliminar clústeres, debe tener el derecho **Control total de CSE:NATIVECLUSTER**.
- Compruebe que el proveedor de servicios haya creado una entrada de lista de control de acceso (ACL) para usted con información sobre su nivel de acceso.

Procedimiento

- 1 En la barra de navegación superior, seleccione **Más > Kubernetes Container Clusters**.
- 2 (opcional) Si el VDC de organización está habilitado para la creación de clústeres de TKGI, en la página **Kubernetes Container Clusters**, seleccione la pestaña **vSphere with Tanzu y nativo**.
- 3 Haga clic en **Nuevo**.
- 4 Seleccione la opción **Nativo** para el tiempo de ejecución de Kubernetes.
- 5 Introduzca un nombre y seleccione una plantilla de Kubernetes en la lista.
- 6 (opcional) Introduzca una descripción para el nuevo clúster de Kubernetes y una clave pública SSH.
- 7 Haga clic en **Siguiente**.
- 8 Seleccione el VDC de organización en el que desea implementar un clúster nativo y haga clic en **Siguiente**.
- 9 Seleccione la cantidad de nodos de trabajo y plano de control y, si lo desea, políticas de tamaño para los nodos.
- 10 Haga clic en **Siguiente**.
- 11 Si desea implementar una máquina virtual adicional con el software de NFS, active el botón de alternancia **Habilitar NFS**.
- 12 (opcional) Seleccione las políticas de almacenamiento para los nodos de trabajo y plano de control.
- 13 Haga clic en **Siguiente**.
- 14 Seleccione una red para el clúster de Kubernetes y haga clic en **Siguiente**.
- 15 Revise la configuración del clúster y haga clic en **Finalizar**.

Pasos siguientes

- Cambie el tamaño del clúster de Kubernetes si desea cambiar la cantidad de nodos de trabajo.
- Descargue el archivo kubeconfig. La herramienta de línea de comandos kubectl utiliza archivos kubeconfig para obtener información sobre los clústeres, los usuarios, los espacios de nombres y los mecanismos de autenticación.
- Elimine un clúster de Kubernetes.

Crear un clúster de VMware Tanzu Kubernetes Grid Integrated Edition

Puede crear clústeres de VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) mediante Container Service Extension.

Para obtener más información sobre las diferentes opciones de tiempo de ejecución de Kubernetes para la creación de clústeres, consulte [Capítulo 4 Trabajar con clústeres de Kubernetes](#).

También puede administrar los clústeres de Kubernetes mediante la CLI de Container Service Extension. Consulte la documentación de [Container Service Extension](#).

Requisitos previos

- Compruebe que el proveedor de servicios haya publicado el complemento Kubernetes Container Clusters en su organización. Kubernetes Container Clusters es el complemento de Container Service Extension para VMware Cloud Director. Puede encontrar el complemento en la barra de navegación superior, en **Más > Kubernetes Container Clusters**.
- Compruebe que el proveedor de servicios haya completado la configuración del servidor de Container Service Extension 3.0 y haya publicado metadatos de habilitación de TKGI de Container Service Extension en el VDC de organización.
- Compruebe que tiene el derecho **Derecho de implementación de {cse}:PKS**.

Procedimiento

- 1 En la barra de navegación superior, seleccione **Más > Kubernetes Container Clusters**.
- 2 En la página **Kubernetes Container Clusters**, seleccione la pestaña **TKGI** y, a continuación, haga clic en **Nuevo**.

Se abrirá el asistente **Crear nuevo clúster de TKGI**.
- 3 Seleccione el VDC de organización en el que desea implementar un clúster de TKGI y haga clic en **Siguiente**.

La lista puede tardar más en cargarse porque VMware Cloud Director solicita la información del servidor de CSE.

- 4 Introduzca un nombre para el nuevo clúster de TKGI y seleccione la cantidad de nodos de trabajo.

Los clústeres de TKGI deben tener al menos un nodo de trabajo.

- 5 Haga clic en **Siguiente**.
- 6 Revise la configuración del clúster y haga clic en **Finalizar**.
- 7 (opcional) Haga clic en el botón **Actualizar** a la derecha de la página para que el nuevo clúster de TKGI aparezca en la lista de clústeres.

Pasos siguientes

- Cambie el tamaño del clúster de Kubernetes si desea cambiar la cantidad de nodos de trabajo.
- Descargue el archivo kubeconfig. La herramienta de línea de comandos kubectl utiliza archivos kubeconfig para obtener información sobre los clústeres, los usuarios, los espacios de nombres y los mecanismos de autenticación.
- Elimine un clúster de Kubernetes.

Configurar el acceso externo a un servicio en un clúster de Tanzu Kubernetes

A partir de VMware Cloud Director 10.2.2, de forma predeterminada, solo se puede acceder a los clústeres de Tanzu Kubernetes desde subredes IP de redes dentro del mismo centro de datos virtual de organización en el que se crea el clúster. Si es necesario, puede configurar manualmente el acceso externo a servicios específicos en un clúster de Tanzu Kubernetes.

Cuando se publica una política de Kubernetes de VDC en un VDC de organización, se aprovisiona automáticamente una política de firewall en la puerta de enlace Edge del clúster para permitir el acceso al clúster desde orígenes autorizados dentro del VDC. Además, se agrega automáticamente una regla SNAT del sistema a las puertas de enlace Edge de NSX-T Data Center dentro del VDC de organización para garantizar que las cargas de trabajo dentro del VDC de organización puedan acceder a la puerta de enlace Edge del clúster.

Nota Si el centro de datos virtual de organización forma parte de un grupo de NSX-T Data Center, los otros VDC del grupo de centros de datos no pueden acceder a la puerta de enlace Edge del clúster.

No es posible eliminar la directiva de firewall que se aprovisiona en la puerta de enlace Edge del clúster ni la regla SNAT en la puerta de enlace Edge de NSX-T Data Center, a menos que un **administrador del sistema** elimine la política de Kubernetes del VDC.

Si es necesario, puede configurar manualmente el acceso desde una red externa a un servicio específico de un clúster de Tanzu Kubernetes. Para ello, debe crear una regla DNAT en la puerta de enlace Edge de NSX-T Data Center que garantice que el tráfico proveniente de ubicaciones externas se reenvía a la puerta de enlace Edge del clúster.

Requisitos previos

- Compruebe que la infraestructura de nube esté respaldada por vSphere 7.0 Update 1C, 7.0 Update 2 o una versión posterior. Comuníquese con el **administrador del sistema**.
- Compruebe que es un **administrador de organización**.
- Compruebe que el **administrador del sistema** haya creado una puerta de enlace Edge de NSX-T Data Center dentro del centro de datos virtual de organización en el que se encuentra el clúster de Tanzu Kubernetes.
- Compruebe que la dirección IP pública que desea utilizar para el servicio se haya asignado a la interfaz de puerta de enlace Edge en la que desea agregar una regla DNAT.
- Utilice el comando `get services my-service` de la herramienta de línea de comandos `kubectl` para recuperar la dirección IP externa del servicio que desea exponer.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, en la pestaña **Puertas de enlace Edge**.
- 2 Haga clic en la puerta de enlace Edge y, en **Servicios**, haga clic en **NAT**.
- 3 Para agregar una regla, haga clic en **Nueva**.
- 4 Configure una regla DNAT para el servicio que desea conectar a una red externa.

Opción	Descripción
Nombre	Introduzca un nombre significativo para la regla.
Descripción	(Opcional) Introduzca una descripción para la regla.
Estado	Para habilitar la regla tras la creación, desactive el botón de alternancia Estado .
Tipo de interfaz	En el menú desplegable, seleccione DNAT.
IP externa	Introduzca la dirección IP pública del servicio. Las direcciones IP que introduzca deben pertenecer al rango de direcciones IP subasignadas de la puerta de enlace Edge de NSX-T Data Center.
Aplicación	Deje el cuadro en blanco.
IP interna	Introduzca la dirección IP del servicio que se asignó desde el grupo de entrada de Kubernetes.
Puerto interno	(Opcional) Introduzca un número de puerto al que se dirigirá el tráfico entrante.
Registro	(Opcional) Para que se registre la traducción de direcciones realizada por esta regla, active la opción Registro .

- 5 Haga clic en **Guardar**.

Pasos siguientes

Si desea proporcionar acceso a otras aplicaciones publicadas como servicios de Kubernetes desde redes externas, debe configurar reglas DNAT adicionales para cada una de ellas.

Trabajar con redes

5

Para proporcionar una infraestructura de red altamente flexible y segura en un entorno de nube multipropósito, VMware Cloud Director utiliza una arquitectura de red en capas con cuatro categorías de redes. Las categorías de redes son redes externas, redes de centros de datos virtuales de organización (VDC), redes de grupo de centros de datos y redes de vApp. La mayoría de los tipos de redes de VMware Cloud Director requieren objetos de infraestructura adicionales, como puertas de enlace Edge y grupos de redes.

Redes externas

Una red externa proporciona una interfaz de vínculo superior que conecta las redes y las máquinas virtuales del entorno de VMware Cloud Director con redes externas, como una VPN, una intranet corporativa o Internet público.

Una red externa cuenta con el respaldo de una sola red de vSphere, de varias redes de vSphere o de un enrutador lógico de nivel 0 de NSX-T Data Center.

Solo un **administrador del sistema** puede crear una red externa. Para obtener información acerca de las redes externas, consulte *Guía del portal para administradores de proveedores de servicios de VMware Cloud Director*.

Grupos de redes

Un grupo de redes es una colección de segmentos de red aislados de capa 2 que puede utilizar para crear redes de vApp y ciertos tipos de redes de VDC de organización a petición.

Los grupos de redes deben crearse antes que las redes de VDC de organización y las de vApp. Si no existen, la única opción de red disponible para una organización es la conexión directa con una red externa.

Solo un **administrador del sistema** puede crear un grupo de redes.

Para obtener información acerca de los grupos de redes, consulte la *Guía del portal para administradores de proveedores de servicios de VMware Cloud Director*.

Redes de VDC de organización

Las redes de centros de datos virtuales (VDC) de organización permiten que las vApps se comuniquen entre sí o con redes externas a la organización.

Existen varios tipos diferentes de redes de VDC de organización, que varían en función de la conexión existente entre estas redes y las redes externas.

Las redes de VDC de organización proporcionan conexiones directas o enrutadas a redes externas, o se pueden aislar de redes externas y otras redes de VDC de organización. Las conexiones enrutadas requieren un grupo de redes y una puerta de enlace Edge en el VDC de organización.

Un **administrador del sistema** o un **administrador de la organización** crea redes de VDC de organización y las asigna a la organización.

Los VDC de organización creados recientemente no tienen redes disponibles. Una vez que un **administrador del sistema** crea la infraestructura de red necesaria, un **administrador de la organización** puede crear y administrar la mayoría de los tipos de redes de VDC de organización.

Redes de grupo de centros de datos respaldadas por NSX Data Center for vSphere

Una red respaldada por NSX Data Center for vSphere que abarca un grupo de centros de datos. Un grupo de centros de datos puede incluir entre 1 y 16 VDC de organización en una implementación de VMware Cloud Director de un sitio o multisitio.

Redes de grupo de centros de datos respaldadas por NSX-T Data Center

Las redes de grupo de centros de datos son un tipo de redes de VDC de organización que se comparten entre uno o varios VDC y a las que las vApps se pueden conectar.

Un **administrador del sistema** o un **administrador de la organización** crea redes de grupo de centros de datos y las asigna a un único grupo de VDC.

VMware Cloud Director admite redes de grupo de centros de datos aisladas, importadas, directas y enrutadas respaldadas por NSX-T Data Center.

Redes de vApp

Las redes de vApp permiten que las máquinas virtuales se comuniquen entre sí o con las máquinas virtuales de otras vApps (en este último caso, conectándose a una red de VDC de organización).

Una red de vApp está dentro de una vApp y puede estar aislada de otras redes o conectada con una red de VDC de organización.

Cada vApp contiene una red de vApp. La red se crea cuando se implementa la vApp y se elimina cuando se anula la implementación de esta.

Un **administrador de organización** configura y controla las redes de vApp.

Tipos de redes en una vApp

Las máquinas virtuales de una vApp se pueden conectar a redes de vApp, que pueden ser directas o estar aisladas o enrutadas, y con redes de VDC de organización.

Nota Los VDC de organización respaldados por NSX Data Center for vSphere admiten redes de vApp aisladas, directas y enrutadas.

Los VDC de organización respaldados por NSX-T Data Center admiten redes de vApp aisladas y directas.

Puede agregar redes de distintos tipos a una vApp para resolver varios escenarios de redes.

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

Una vApp puede incluir redes de vApp y redes de VDC de organización. Una red de vApp aislada está dentro de la vApp.

También puede enrutar una red de vApp en una red de VDC de organización para proporcionar conectividad con máquinas virtuales fuera de la vApp. Para redes de vApp enrutadas, puede configurar servicios de redes, tal como un firewall y enrutamiento estático.

Puede conectar una vApp directamente a una red de VDC de organización.

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

Para obtener información, consulte [Trabajar con redes en una vApp](#).

Puertas de enlace Edge

Las puertas de enlace Edge proporcionan una red de VDC 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. VMware Cloud Director es compatible con puertas de enlace Edge IPv4 e IPv6.

Las puertas de enlace Edge requieren NSX Data Center for vSphere o NSX-T Data Center.

Este capítulo incluye los siguientes temas:

- [Administrar redes de centros de datos virtuales de organización](#)
- [Administrar redes de grupo de centros de datos con NSX-T Data Center](#)

- Administrar redes de grupo de centros de datos con NSX Data Center for vSphere
- Administrar servicios de puerta de enlace Edge de NSX Data Center for vSphere
- Administrar puertas de enlace Edge de NSX-T Data Center

Administrar redes de centros de datos virtuales de organización

Un **administrador del sistema** o un **administrador de la organización** crea redes de VDC de organización y las asigna al VDC de organización o a un grupo de VDC de organización.

Los **administradores de organización** pueden visualizar la información acerca de las redes o configurar servicios de red, entre otras cosas.

Puede utilizar redes de VDC de organización directas, enrutadas, aisladas o de centros de datos respaldadas por NSX Data Center for vSphere.

Puede utilizar redes de VDC de organización enrutadas, aisladas, importadas y directas respaldadas por NSX-T Data Center. También puede utilizar redes de grupo de centros de datos enrutadas, aisladas e importadas respaldadas por NSX-T Data Center.

Tabla 5-1. Tipos de redes de VDC de organización

Red de tipo de centro de datos	Descripción
Directa	<p>Una red de VDC de organización con una conexión directa a una de las redes externas aprovisionadas por el administrador del sistema y respaldadas con recursos de vSphere.</p> <p>Las redes directas son compatibles con VDC de organización respaldados por NSX Data Center for vSphere y, a partir de VMware Cloud Director 10.2.2, con los VDC de organización respaldados por NSX-T Data Center.</p> <p>Varios VDC de organización pueden acceder a las redes directas.</p> <p>Las máquinas virtuales que pertenecen a VDC de organización distintos pueden conectarse y ver el tráfico de esta red.</p> <p>Una red directa proporciona conectividad de capa 2 directa a las máquinas virtuales fuera del VDC de organización. Dichas máquinas pueden conectarse directamente a las máquinas virtuales en el VDC de organización.</p> <p>Nota Solo el administrador del sistema puede agregar una red de VDC de organización directa.</p> <p>Puede ser IPv4 o IPv6.</p>
Aislada (interna)	<p>Solo el mismo VDC de organización puede acceder a las redes aisladas. Las máquinas virtuales en este VDC de organización son las únicas que pueden conectarse a la red de VDC de organización interna y ver el tráfico de esta.</p> <p>Las redes aisladas son compatibles con los VDC de organización respaldados por NSX-T Data Center y los VDC de organización de NSX Data Center for vSphere.</p> <p>La red de VDC de organización aislada proporciona a un VDC de organización una red privada y aislada a la que se pueden conectar varias máquinas virtuales y vApps. La red no proporciona conectividad con máquinas virtuales fuera del VDC de organización. Dichas máquinas no tienen conectividad con las máquinas del VDC de organización.</p>

Tabla 5-1. Tipos de redes de VDC de organización (continuación)

Red de tipo de centro de datos	Descripción
Con enrutamiento	<p>Solo el mismo VDC de organización puede acceder a las redes enrutadas. Las máquinas virtuales de este VDC de organización son las únicas que pueden conectarse a la red.</p> <p>Además, esta red proporciona un acceso controlado a una red externa. Como administrador del sistema o administrador de la organización, puede configurar los ajustes de traducción de direcciones de red (Network Address Translation, NAT), firewall y VPN para que sea posible acceder a máquinas virtuales específicas desde la red externa.</p> <p>Puede ser IPv4 o IPv6.</p>
Conmutador lógico de NSX-T Data Center importado	<p>Las redes importadas de NSX-T Data Center son segmentos lógicos que se crean en NSX-T Data Center y utilizan un conmutador lógico de NSX-T Data Center existente. Se importan en una organización específica como una red de VDC de organización.</p> <p>Nota Solo un administrador del sistema puede importar una red de NSX-T Data Center.</p>
Redes de grupo de centros de datos respaldadas por NSX Data Center for vSphere	<p>Esta red forma parte de una red de grupo de centros de datos que abarca un grupo de centros de datos. Un grupo de centros de datos puede incluir entre 1 y 16 VDC de organización en una implementación de VMware Cloud Director de un sitio o multisitio.</p> <p>Las máquinas virtuales conectadas a esta red se conectan a la red expandida subyacente.</p>
Redes de grupo de centros de datos respaldadas por NSX-T Data Center	<p>Las redes de grupo de centros de datos son un tipo de redes de VDC de organización respaldadas por NSX-T Data Center que se comparten entre uno o varios VDC y a los que las vApps se pueden conectar.</p> <p>Las redes de grupo de centros de datos se pueden aislar, importar o enrutar, y requieren NSX-T Data Center.</p>

Todos los pasos para administrar las redes de VDC de la organización se documentan suponiendo que tiene más de un VDC en su entorno.

Ver las redes de VDC de organización disponibles

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

Requisitos previos

Compruebe que es **administrador de la organización**, **administrador del sistema** o que tiene asignada una función con un conjunto de derechos equivalente.

Procedimiento

- ◆ En la barra de navegación superior, haga clic en **Redes**.

Resultados

En la pestaña **Redes**, verá una lista de las redes disponibles que puede filtrar por varios criterios.

Pasos siguientes

Puede agregar una red de VDC de organización. También puede editar, aumentar el alcance, eliminar o restablecer una red de VDC de organización existente.

Agregar una red de centros de datos virtuales de organización aislada

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

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

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

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

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 En la pestaña **Redes**, haga clic en **Nueva**.
- 3 En la página **Alcance**, seleccione **Centro de datos virtual de organización**, elija un VDC en el que se creará la red y haga clic en **Siguiente**.
- 4 En la página **Seleccionar tipo de red**, seleccione **Aislada** y haga clic en **Siguiente**.
- 5 Introduzca un nombre significativo para la red.
- 6 Introduzca la configuración de enrutamiento de entre dominios sin clases (Classless Inter-Domain Routing, CIDR) para la red.

Utilice el formato *dirección_IP_de_puerta_de_enlace_de_red/longitud_de_prefijo_de_subred* (por ejemplo, **192.167.1.1/24**).
- 7 Introduzca una descripción de la red de VDC de organización.

- 8 (opcional) Si el VDC en el que se crea la red está respaldado por NSX Data Center for vSphere, active la opción **Compartido** para que la red de VDC de organización esté disponible para otros VDC de organización dentro de la misma organización.

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

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

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

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

- 13 Haga clic en **Siguiente**.
- 14 En la página **Listo para completar**, revise su configuración y haga clic en **Finalizar**.

Agregar una red de centros de datos virtuales de organización enrutada

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

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

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

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 En la pestaña **Redes**, haga clic en **Nueva**.
- 3 En la página **Alcance**, seleccione **Centro de datos virtual de organización**, elija un VDC en el que se creará la red y haga clic en **Siguiente**.
- 4 En la página **Seleccionar tipo de red**, seleccione **Enrutada** y haga clic en **Siguiente**.
- 5 Introduzca un nombre significativo para la red.
- 6 Introduzca la configuración de enrutamiento de entre dominios sin clases (Classless Inter-Domain Routing, CIDR) para la red.

Utilice el formato *dirección_IP_de_puerta_de_enlace_de_red/longitud_de_prefijo_de_subred* (por ejemplo, **192.167.1.1/24**).
- 7 Introduzca una descripción de la red de VDC de organización.
- 8 (opcional) Si el VDC en el que se crea la red está respaldado por NSX Data Center for vSphere, active la opción **Compartido** para que la red de VDC de organización esté disponible para otros VDC de organización dentro de la misma organización.

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

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

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

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

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

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

- 12 (opcional) Para habilitar el etiquetado de VLAN invitadas en esta red, active la opción **Admite VLAN invitada**.

- 13 Haga clic en **Siguiente**.

- 14 (opcional) Si desea reservar una o más direcciones IP para la asignación a máquinas virtuales que requieren direcciones IP estáticas, configure los **Grupos de IP estáticas** para la red.

- a Introduzca la dirección IP o el rango de direcciones IP y haga clic en **Agregar**.

Para agregar varias direcciones IP estáticas o rangos, repita este paso.

- b (opcional) Para modificar o eliminar direcciones IP y rangos de direcciones IP, haga clic en **Modificar** o **Eliminar**.

- 15 Haga clic en **Siguiente**.

- 16 (opcional) Establezca la configuración de DNS.

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

- 17 Haga clic en **Siguiente**.

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

Agregar una red de centros de datos virtuales de organización directa

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

A partir de VMware Cloud Director 10.2.2, se admite la creación de redes directas en VDC de organización respaldados por NSX-T Data Center y NSX Data Center for vSphere.

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

Requisitos previos

Compruebe que dispone de derechos de **administrador del sistema**.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 En la pestaña **Redes**, haga clic en **Nueva**.
- 3 En la página **Alcance**, seleccione **Centro de datos virtual de organización**, elija un VDC en el que se creará la red y haga clic en **Siguiente**.
- 4 En la página **Tipo de red**, seleccione **Directa** y haga clic en **Siguiente**.
- 5 Introduzca un nombre significativo para la red.
- 6 Introduzca una descripción de la red de VDC de organización.
- 7 (opcional) Con el fin de que la red de VDC de organización esté disponible para otros VDC de organización en la misma organización, active la opción **Compartida**.
- 8 En la página **Conexión de red externa**, seleccione la red externa a la que desea que se conecte directamente la nueva red de centros de datos virtuales de organización y haga clic en **Siguiente**.
- 9 En la página **Listo para completar**, revise su configuración y haga clic en **Finalizar**.

Agregar una red de VDC de organización con un conmutador lógico de NSX-T Data Center importado

Los **administradores del sistema** pueden crear una red de VDC de organización mediante la importación de un conmutador lógico desde una instancia de NSX-T Manager asociada.

Requisitos previos

- Compruebe que dispone de derechos de **administrador del sistema**.
- Compruebe que el centro de datos virtual del proveedor que respalda el centro de datos virtual de organización de destino esté asociado con una instancia de NSX-T Manager.
- Debe crear al menos un conmutador lógico de NSX-T que otras redes de centros de datos virtuales de organización no utilicen.

Para obtener información sobre la creación y la configuración de conmutadores lógicos de NSX-T, consulte la *Guía de administración de NSX-T Data Center*.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 En la pestaña **Redes**, haga clic en **Nueva**.
- 3 En la página **Alcance**, seleccione **Centro de datos virtual de organización**, elija un VDC en el que se creará la red y haga clic en **Siguiente**.
- 4 En la página **Tipo de red**, seleccione **Importada**. A continuación, seleccione un **conmutador lógico de NSX-T** y haga clic en **Siguiente**.
- 5 En la lista de conmutadores lógicos NSX-T disponibles, seleccione el conmutador de destino y haga clic en **Siguiente**.
- 6 Introduzca un nombre significativo para la red.
- 7 Introduzca la configuración de enrutamiento de entre dominios sin clases (Classless Inter-Domain Routing, CIDR) para la 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 Introduzca una descripción de la red de VDC de organización.
- 9 Haga clic en **Siguiente**.
- 10 (opcional) Ajuste la configuración de DNS y el grupo de direcciones IP estáticas.

Puede agregar varias direcciones IP y rangos de direcciones IP.
- 11 Haga clic en **Siguiente**.
- 12 En la página **Listo para completar**, revise su configuración y haga clic en **Finalizar**.

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

Puede modificar las propiedades de redes de VDC de organización.

Requisitos previos

Compruebe que es **administrador de la organización**, **administrador del sistema** o que tiene asignada una función con un conjunto de derechos equivalente.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 En la pestaña **Redes**, haga clic en el nombre de la red de VDC de organización que desea editar.

- 3 En la pestaña **General**, haga clic en **Editar**.
 - a Edite el nombre y la descripción de la red.
 - b Si el VDC en el que creó la red está respaldado por NSX Data Center for vSphere, active o desactive la opción **Compartido** para que la red de VDC de organización esté disponible para otros VDC de organización dentro de la misma organización.
- 4 Haga clic en **Guardar**.

Conectar una red de centros de datos virtuales de organización a una puerta de enlace Edge

Después de crear una red de VDC de organización, puede conectarla a una puerta de enlace Edge.

A partir de la versión 10.1, VMware Cloud Director admite que las redes de VDC de organización con respaldo de NSX Data Center for vSphere o NSX-T Data Center se conecten a una puerta de enlace Edge.

Requisitos previos

Para realizar esta operación, se requiere una de las funciones predefinidas **administrador de organización** o **administrador del sistema**, o bien cualquier otra que incluya los derechos **Red de organización VDC: Editar propiedades** y **Grupo de VDC: Ver** publicados en la organización.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 Haga clic en el nombre de la red de VDC de organización que desea conectar a una puerta de enlace Edge.
- 3 En la pestaña **General**, haga clic en **Editar**.
- 4 Haga clic en **Conexión**.
- 5 Conecte la red a una puerta de enlace Edge.
 - a Alterne la opción **Conectarse a una puerta de enlace Edge**.
 - b Seleccione la puerta de enlace Edge a la que se conectará en la lista de puertas de enlace Edge disponibles.
 - c Seleccione el tipo de interfaz.
 - d Para permitir una VLAN invitada, active la opción **Admite VLAN invitada**.
- 6 Haga clic en **Guardar**.

Resultados

La red de VDC de organización se conecta a una puerta de enlace Edge y pasa de aislada a enrutada.

Desconectar una red de VDC de organización de una puerta de enlace Edge

Si desconecta una red de VDC de organización de una puerta de enlace Edge puede cambiarla de enrutada a aislada.

A partir de la versión 10.1, las redes de VDC de organización con respaldo de NSX Data Center for vSphere o NSX-T Data Center pueden conectarse a una puerta de enlace Edge y desconectarse de ella.

Requisitos previos

Para realizar esta operación, se requiere una de las funciones predefinidas **administrador de organización** o **administrador del sistema**, o bien cualquier otra que incluya el derecho **Red de organización VDC: Editar propiedades**.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 Haga clic en el nombre de la red de VDC de organización que desea desconectar.
- 3 En la pestaña **General**, haga clic en **Editar**.
- 4 Haga clic en **Conexión**.
- 5 Para desconectar la red de la puerta de enlace Edge, desactive la opción **Conéctese a una puerta de enlace Edge**.
- 6 Haga clic en **Guardar**.

Resultados

Al realizar esta acción, se desconecta la red de VDC de organización de una puerta de enlace Edge. La red de VDC de organización cambia de enrutada a aislada.

Convertir la interfaz de una red de VDC de organización enrutada

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

Nota No se pueden convertir instancias de Cross VDC Networking.

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 Haga clic en el nombre de la red de VDC de organización que desea editar.

- 3 En la pestaña **General**, haga clic en **Editar**.
- 4 Haga clic en **Conexión**.
- 5 En el menú desplegable **Tipo de interfaz**, seleccione el tipo de interfaz.

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

- 6 Haga clic en **Guardar**.

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

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

Requisitos previos

- Compruebe que es **administrador de la organización**, **administrador del sistema** o que tiene asignada una función con un conjunto de derechos equivalente.
- Compruebe que la red sea una red de centros de datos virtuales de organización aislada o enrutada.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 Haga clic en el nombre de la red cuyas direcciones IP utilizadas desea ver.
- 3 En la sección **Administración de direcciones IP**, haga clic en **Uso de IP** para ver las direcciones IP que están en uso actualmente.

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

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

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

Requisitos previos

- Compruebe que es **administrador de la organización, administrador del sistema** o que tiene asignada una función con un conjunto de derechos equivalente.
- Compruebe que la red sea una red de centros de datos virtuales de organización aislada o enrutada.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 Haga clic en el nombre de la red que desea editar.
- 3 En la sección **Administración de direcciones IP**, haga clic en la pestaña **Grupos de direcciones IP estáticas**.
- 4 Haga clic en el botón **Editar** situado a la derecha.

En la ventana **Editar red**, puede ver el CIDR de la puerta de enlace y los rangos de direcciones IP, si los hubiera.
- 5 En el cuadro de texto **Grupos de IP estáticas**, introduzca la dirección IP o el rango de direcciones IP, y haga clic en **Agregar**.

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

- 6 Haga clic en **Guardar**.

Resultados

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

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

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

Requisitos previos

- Compruebe que es **administrador de la organización, administrador del sistema** o que tiene asignada una función con un conjunto de derechos equivalente.
- Compruebe que la red sea una red de centros de datos virtuales de organización aislada o enrutada.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 Haga clic en el nombre de la red que desea editar.

- 3 En la sección **Administración de direcciones IP**, haga clic en **Grupos de direcciones IP estáticas**.
- 4 Haga clic en el botón **Editar** en la derecha.
 - Para modificar un rango de IP, seleccione el rango, haga los cambios necesarios y haga clic en **Modificar**.
 - Para eliminar un rango de IP, seleccione el rango y haga clic en **Eliminar**.
- 5 Haga clic en **Guardar**.

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

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

Requisitos previos

- Compruebe que es **administrador de la organización**, **administrador del sistema** o que tiene asignada una función con un conjunto de derechos equivalente.
- Compruebe que la red sea una red de centros de datos virtuales de organización aislada o enrutada.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 Haga clic en el nombre de la red que desea editar.
- 3 En la sección **Administración de direcciones IP**, haga clic en **DNS**.
- 4 Haga clic en el botón **Editar** en la derecha.
- 5 Edite el DNS principal, el DNS secundario y la información del sufijo DNS según corresponda.
- 6 Haga clic en **Guardar**.

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

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

A partir de la versión 10.2, VMware Cloud Director admite la configuración de DHCP para IPv4 e IPv6. Puede configurar los ajustes de IPv6 mediante la API de VMware Cloud Director.

Requisitos previos

- Compruebe que es **administrador de la organización**, **administrador del sistema** o que tiene asignada una función con un conjunto de derechos equivalente.
- Compruebe que la red sea una red de centros de datos virtuales de organización aislada.
- Compruebe si la red está respaldada por NSX Data Center for vSphere.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 Haga clic en el nombre de la red que desea editar.
- 3 En la sección **Administración de direcciones IP**, haga clic en **DHCP**.
- 4 Para habilitar DHCP, haga clic en **Editar** a la derecha de **Servicio de grupos DHCP**.
- 5 Alterne la opción **Servicio de grupos DHCP** y haga clic en **Guardar**.

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

- 6 Cree un grupo DHCP para la red.
 - a Haga clic en **Nuevo**.
 - b Introduzca un rango de direcciones IP para el grupo.

El rango de direcciones IP que especifique no puede superponerse con el grupo de direcciones IP estáticas para el centro de datos virtual de organización.
 - c Especifique el tiempo de concesión predeterminado para las direcciones DHCP en segundos.

El valor predeterminado es de 3.600 segundos.
 - d Especifique el tiempo de concesión máximo para las direcciones DHCP en segundos.

Esta es la cantidad máxima de tiempo que las direcciones IP asignadas por DHCP se concesionan a las máquinas virtuales. El valor predeterminado es de 7.200 segundos.
- 7 Haga clic en **Guardar**.

Agregar un grupo DHCP a una red enrutada de centros de datos virtuales de organización respaldada por NSX-T Data Center

Puede agregar grupos DHCP a una red enrutada de VDC de organización respaldada por NSX-T Data Center.

Nota No se permite eliminar ni actualizar grupos DHCP para las redes de VDC de organización respaldadas por NSX-T Data Center.

Requisitos previos

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

- Comprobar si la red es una red enrutada de centros de datos virtuales de organización.
- Compruebe si la red está respaldada por NSX-T Data Center.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 Haga clic en el nombre de la red que desea editar.
- 3 En la sección **Administración de direcciones IP**, haga clic en DHCP.
- 4 Para agregar un grupo DHCP, haga clic en **Nuevo**.
- 5 Introduzca un rango de direcciones IPv4 para el grupo.
- 6 Haga clic en **Guardar**.

Editar o eliminar un grupo DHCP existente para una red de centros de datos virtuales de organización aislada respaldada por NSX Data Center for vSphere

Si ya no necesita un grupo DHCP dentro de la red de centros de datos virtuales de organización aislada, puede eliminar o editar el grupo respaldado por NSX Data Center for vSphere.

Requisitos previos

- Compruebe que es **administrador de la organización**, **administrador del sistema** o que tiene asignada una función con un conjunto de derechos equivalente.
- Compruebe que la red sea una red de centros de datos virtuales de organización aislada.
- Compruebe que la red de centros de datos virtuales de organización esté respaldada por NSX Data Center for vSphere.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 Haga clic en el nombre de la red que desea editar.
- 3 Haga clic en la sección **Administración de direcciones IP** y en **DHCP**.
- 4 Edite o elimine un grupo DHCP existente.

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

Restablecer una red de centros de datos virtuales de organización

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

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

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 Seleccione una red de VDC de organización.
- 3 Haga clic en **Restablecer** y confirme la operación de restablecimiento.

Eliminar una red de centros de datos virtuales de organización

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

Requisitos previos

- Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.
- La red no está conectada a máquinas virtuales, vApps u otras redes.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 Haga clic en el botón de radio junto al nombre de la red de destino y haga clic en **Eliminar**.
- 3 Para confirmar, haga clic en **Aceptar**.

Administrar redes de grupo de centros de datos con NSX-T Data Center

A partir de la versión 10.2, VMware Cloud Director admite redes de grupo de centros de datos respaldadas por NSX-T Data Center.

Para crear una red entre varios VDC de organización, primero deberá agrupar los VDC y, a continuación, crear una red de grupo de centros de datos compartida con ellos.

Las redes de grupo de centros de datos respaldadas por NSX-T Data Center proporcionan uso compartido de redes de nivel 2, configuración de un solo punto de salida activo y reglas de firewall distribuido (DFW) que se aplican a todo un grupo de centros de datos.

Grupo de centros de datos

Un grupo de centros de datos actúa como un enrutador entre VDC que proporciona administración centralizada de redes, configuración de un punto de salida y tráfico de este a oeste entre todas las redes del grupo. Un grupo de centros de datos puede tener entre 1 y 16 VDC configurados para compartir un punto de salida activo.

Zona de disponibilidad

Una zona de disponibilidad representa los clústeres informáticos, o los dominios de errores informáticos, que están disponibles para la red. De forma predeterminada, la zona de disponibilidad es el VDC de proveedor.

Importante El **administrador del sistema** debe configurar las zonas de disponibilidad para las redes de grupo con NSX-T Data Center estableciendo un **Alcance del proveedor de recursos informáticos** para la instancia de vCenter Server y, de manera opcional, para el VDC de proveedor respaldado por la instancia de vCenter Server. De forma predeterminada, el alcance del proveedor de recursos informáticos de un VDC de proveedor se copia desde la instancia de vCenter Server que respalda a este VDC. Un **administrador del sistema** puede diferenciar el alcance del proveedor de recursos informáticos de los distintos VDC de proveedor que están respaldados por una sola instancia de vCenter Server. Por ejemplo, puede tener una instancia de vCenter Server con el alcance **Alemania** y un VDC de proveedor con el alcance **Múnich**.

El **administrador del sistema** también puede volver a configurar la zona de disponibilidad para que sea el alcance del proveedor de red, que suele representar la instancia de vCenter Server subyacente con la instancia de NSX-T Manager asociada.

Punto de salida

Una puerta de enlace Edge de NSX-T Data Center existente que se configura para conectar un grupo de centros de datos a una red externa.

Red de grupo de centros de datos

Una red de capa 2 compartida entre todos los VDC de un grupo de centros de datos.

Administrar grupos de centros de datos con el tipo de proveedor de red NSX-T Data Center

Después de crear un grupo de centros de datos con el tipo de proveedor de red NSX-T Data Center, puede agregar centros de datos al grupo, eliminarlos, o editar la configuración del grupo.

Un grupo de centros de datos puede incluir hasta 16 centros de datos virtuales.

Los VDC que elimina del grupo de centros de datos no deben tener cargas de trabajo asociadas a ninguna de las redes que participan en el grupo de centros de datos.

Crear un grupo de centros de datos con el tipo de proveedor de red NSX-T Data Center

Puede agrupar entre 1 y 16 VDC en un grupo de centros de datos con el tipo de proveedor de red NSX-T Data Center.

Requisitos previos

Compruebe que es **administrador de la organización**, **administrador del sistema** o que tiene asignada una función con un conjunto de derechos equivalente.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.
- 2 Haga clic en **Nuevo**.
- 3 En la página **VDC inicial**, seleccione un centro de datos virtual respaldado por NSX-T Data Center para iniciar el grupo.
- 4 Introduzca un nombre y, si lo desea, una descripción para el nuevo grupo de centros de datos.
- 5 En la página **VDC participante**, seleccione centros de datos adicionales para el nuevo grupo de centros de datos y haga clic en **Siguiente**.
- 6 Revise los detalles del grupo de centros de datos y haga clic en **Finalizar**.

Resultados

El grupo recién creado aparece en la lista de grupos de centros de datos.

Pasos siguientes

Cree una red que abarque el grupo de centros de datos con el tipo de proveedor de red NSX-T Data Center.

Ver y editar la configuración general de un grupo de centros de datos con el tipo de proveedor de red NSX-T Data Center

Puede ver y editar los grupos de centros de datos con el tipo de proveedor de red NSX-T Data Center en su organización.

Requisitos previos

Compruebe que es **administrador de la organización** o que tiene una función con un conjunto de derechos equivalente.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.
Aparece la lista de grupos de centros de datos.
- 2 Haga clic en el grupo de centros de datos de destino.
- 3 En el panel **Configuración general**, haga clic en **Editar**.
- 4 Edite el nombre y, opcionalmente, la descripción del grupo de centros de datos. Haga clic en **Guardar** para confirmar.

Administrar los VDC participantes en un grupo de centro de datos

Puede seleccionar algunos VDC para que sean parte de un grupo de VDC y se comuniquen entre sí.

Requisitos previos

Compruebe que es **administrador de la organización** o que tiene una función con un conjunto de derechos equivalente.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.
Aparece la lista de grupos de centros de datos.
- 2 Haga clic en el grupo de centros de datos de destino.
- 3 Haga clic en **VDC participantes** y, a continuación, haga clic en **Administrar**.
- 4 Seleccione los VDC que desea incluir en el grupo y haga clic en **Guardar** para confirmar.

Sincronizar un grupo de centros de datos con el tipo de proveedor de red NSX-T Data Center

Para comprobar si todos los VDC que participan en un grupo de centros de datos aún existen y están configurados correctamente, puede sincronizar el grupo de centros de datos.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.
Aparece la lista de grupos de centros de datos.
- 2 Haga clic en el grupo de centros de datos de destino.
- 3 Haga clic en **Sincronizar** y confirme.

Usar el firewall distribuido en un grupo de centros de datos con el tipo de proveedor de red NSX-T Data Center

A partir de la versión 10.2, VMware Cloud Director admite un servicio de firewall distribuido para los grupos de centros de datos con el tipo de proveedor de red NSX-T Data Center.

Cuando se habilita un firewall distribuido para un grupo de centros de datos con el tipo de proveedor de red NSX-T Data Center, se crea una única política de seguridad predeterminada que se aplica al grupo de centros de datos.

Como **administrador de organización**, puede crear y modificar otras reglas de firewall distribuido que estén asociadas a la directiva de seguridad predeterminada del grupo de centros de datos.

De forma predeterminada, el servicio de firewall distribuido no está habilitado. Después de habilitar el firewall distribuido, puede crear conjuntos de direcciones IP y grupos de seguridad para facilitar la creación de reglas de firewall distribuido.

Nota Las reglas de firewall distribuido que se crean solo se aplican a las cargas de trabajo que están asociadas a las redes del grupo de centros de datos.

Activar el firewall distribuido para un grupo de centros de datos con el tipo de proveedor de red NSX-T Data Center

Al usar el firewall distribuido, puede aplicar un conjunto de reglas de firewall de nivel 3 en un único grupo de centros de datos.

El firewall distribuido no está habilitado de forma predeterminada. Cuando se habilita, se crea una única política de seguridad predeterminada.

Requisitos previos

Compruebe que es un **administrador del sistema**.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.
Aparece la lista de grupos de centros de datos.
- 2 Haga clic en el grupo de centros de datos de destino.
- 3 En la sección **Firewall distribuido**, haga clic en **Activar** y confirme que desea activar el firewall distribuido.

Pasos siguientes

Cree reglas de firewall distribuido.

Agregar un conjunto de direcciones IP a un grupo de centros de datos

Para crear reglas de firewall distribuido y agregarlas a un grupo de centros de datos, primero debe crear conjuntos de direcciones IP. Los conjuntos de direcciones IP son grupos de

direcciones IP y redes a los que se aplican las reglas de firewall. La combinación de varios objetos en conjuntos de direcciones IP le ayuda a reducir la cantidad total de reglas de firewall distribuido que deben crearse.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.
Aparece la lista de grupos de centros de datos.
- 2 Haga clic en el grupo de centros de datos de destino.
- 3 En Seguridad, haga clic en **Conjuntos de direcciones IP**.
- 4 Haga clic en **Nuevo**.
- 5 Escriba un nombre significativo y, opcionalmente, una descripción para el nuevo conjunto de direcciones IP.
- 6 Introduzca una dirección IPv4, una dirección IPv6 o un rango de direcciones en formato CIDR, y haga clic en **Agregar**.
- 7 Para modificar una dirección IP o un rango existentes, haga clic en **Modificar** y edite el valor.
- 8 Para confirmar, haga clic en **Guardar**.

Crear un grupo de seguridad de centros de datos con el tipo de proveedor de red NSX-T Data Center

Antes de crear reglas de firewall distribuido para un grupo de centros de datos, puede agrupar las redes de grupo de centros de datos en grupos de seguridad a los que se aplican las reglas.

Los grupos de seguridad son grupos de redes de grupo de centros de datos a los que se aplican las reglas de firewall distribuido. La agrupación de redes ayuda a reducir la cantidad total de reglas de firewall distribuido que deben crearse.

Requisitos previos

Compruebe que tiene al menos una red de grupo de centros de datos respaldada por NSX-T Data Center.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.
Aparece la lista de grupos de centros de datos.
- 2 Haga clic en el grupo de centros de datos de destino.
- 3 En Seguridad, haga clic en **Grupos de seguridad** y haga clic en **Nuevo**.

- 4 Escriba un nombre y, opcionalmente, una descripción para el grupo de seguridad. Luego, haga clic en **Guardar**.
El nuevo grupo de seguridad se muestra en la lista.
- 5 Seleccione el grupo de seguridad que acaba de crear y haga clic en **Gestionar miembros**.
- 6 Seleccione las redes de grupo de centros de datos que desee agregar al grupo de seguridad.
- 7 Haga clic en **Guardar**.

Pasos siguientes

[Agregar una regla de firewall distribuido a un grupo de centros de datos con el tipo de proveedor de red NSX-T Data Center](#)

Agregar un perfil de puerto de aplicación a un grupo de centros de datos

Para crear reglas de firewall distribuido, puede usar perfiles de puerto de aplicación preconfigurados y perfiles de puerto de aplicación personalizados.

Los perfiles de puerto de aplicación incluyen una combinación de un protocolo y un puerto (o un grupo de puertos) que se utiliza para los servicios de firewall. Además de los perfiles de puerto predeterminados que están preconfigurados, puede crear perfiles de puerto de aplicación personalizados.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.
Aparece la lista de grupos de centros de datos.
- 2 Haga clic en el grupo de centros de datos de destino.
- 3 En Seguridad, haga clic en **Perfiles de puerto de aplicación**.
- 4 En el panel **Aplicaciones personalizadas**, haga clic en **Nueva**.
- 5 Introduzca un nombre y, si lo desea, una descripción para el perfil de puerto de aplicación.
- 6 En el menú desplegable **Protocolo**, seleccione el protocolo que desea utilizar.
- 7 Introduzca un puerto o un rango de puertos separados por comas y haga clic en **Guardar**.
- 8 Para configurar perfiles de puerto adicionales, repita los pasos.

Pasos siguientes

Utilice los perfiles de puerto de aplicación para crear reglas de firewall distribuido.

Agregar una regla de firewall distribuido a un grupo de centros de datos con el tipo de proveedor de red NSX-T Data Center

Las reglas de firewall distribuido que se crean solo se aplican a las cargas de trabajo que están asociadas a las redes del grupo de centros de datos.

Requisitos previos

Compruebe que el servicio de firewall distribuido para el grupo de centros de datos esté habilitado.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.
Aparece la lista de grupos de centros de datos.
- 2 Haga clic en el grupo de centros de datos de destino.
- 3 Haga clic en la pestaña **Firewall distribuido** que se encuentra a la izquierda.
- 4 Haga clic en **Editar reglas**.
- 5 Para agregar una regla de firewall, haga clic en **Nuevo en la parte superior**.
- 6 Configure la regla.

Opción	Descripción
Nombre	Escriba un nombre para la regla.
Estado	Para habilitar la regla tras crearla, active la opción Estado .
Aplicaciones	(Opcional) Para seleccionar un perfil de puerto específico al que se aplica la regla, active el botón de alternancia Aplicaciones y haga clic en Guardar .
Contexto	(Opcional) Seleccione un perfil contextual de NSX-T Data Center predeterminado para la regla.
Origen	<p>Seleccione el tráfico de origen y haga clic en Conservar.</p> <ul style="list-style-type: none"> ■ Para permitir o denegar el tráfico desde cualquier dirección de origen, active Cualquier origen. ■ Para permitir o denegar el tráfico proveniente de conjuntos de direcciones IP o grupos de seguridad específicos, seleccione los conjuntos de direcciones IP y los grupos de seguridad de la lista.
Destino	<p>Seleccione el tráfico de destino y haga clic en Conservar.</p> <ul style="list-style-type: none"> ■ Para permitir o denegar el tráfico a cualquier dirección de destino, active Cualquier destino. ■ Para permitir o denegar el tráfico que se dirige hacia conjuntos de direcciones IP o grupos de seguridad específicos, seleccione los conjuntos de direcciones IP y los grupos de seguridad de la lista.
Acción	<p>En el menú desplegable Acción, seleccione si desea permitir o denegar el tráfico desde o hacia orígenes específicos.</p> <ul style="list-style-type: none"> ■ Para permitir el tráfico desde o hacia los orígenes, los destinos y los servicios especificados, seleccione Aceptar. ■ Para bloquear el tráfico desde o hacia los orígenes, los destinos y los servicios especificados, seleccione Denegar.
Protocolo IP	Seleccione si desea aplicar la regla al tráfico de IPv4 o IPv6.
Habilite el registro.	Para que se registre la traducción de direcciones realizada por esta regla, active el botón de alternancia Habilitar registro .

7 Haga clic en **Guardar**.

8 Para configurar reglas adicionales, repita los pasos.

Resultados

Una vez creadas las reglas de firewall, estas aparecen en la lista de reglas de firewall distribuido. Puede mover las reglas hacia arriba o abajo, editarlas o eliminarlas según sea necesario.

Desactivar la directiva de firewall distribuido predeterminada

Si desea desactivar el servicio de firewall distribuido, primero debe desactivar la directiva de firewall distribuido predeterminada.

Cuando se desactiva la directiva predeterminada, se pueden editar las reglas de firewall distribuido, pero estas ya no se aplican.

Procedimiento

1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.

Aparece la lista de grupos de centros de datos.

2 Haga clic en el grupo de centros de datos de destino.

3 Haga clic en la pestaña **Firewall distribuido** que se encuentra a la izquierda.

4 En la tarjeta **Política predeterminada** situada encima de la lista de reglas de firewall distribuido, haga clic en **Deshabilitar** y confirme la acción.

Resultados

Se desactiva la directiva predeterminada. El resto de las reglas de firewall distribuido se pueden editar, pero no se aplican.

Desactivar el servicio de firewall distribuido

Si no desea utilizar el servicio de firewall distribuido, puede desactivarlo.

Cuando se desactiva el servicio de firewall distribuido para un grupo de centros de datos, la configuración de las reglas de seguridad de ese grupo se elimina de forma permanente y no se puede recuperar.

Requisitos previos

[Desactivar la directiva de firewall distribuido predeterminada](#)

Procedimiento

1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.

Aparece la lista de grupos de centros de datos.

2 Haga clic en el grupo de centros de datos de destino.

3 Haga clic en **General**.

4 En el panel **Firewall distribuido** a la derecha, haga clic en **Desactivar** y confirme la acción.

Resultados

El servicio de firewall distribuido se desactivará y la configuración de las reglas de seguridad se eliminará.

Administrar redes de grupo de centros de datos con el tipo de proveedor de red NSX-T Data Center

Después de crear y configurar un grupo de centros de datos, puede crear y administrar redes de grupo de centros de datos que abarquen los VDC participantes.

Puede utilizar redes de grupo de centros de datos de organización enrutadas, aisladas e importadas respaldadas por NSX-T Data Center.

Una red de grupo de centros de datos solo puede estar dentro del ámbito de un único grupo de centros de datos.

Puede aumentar el ámbito de una red existente de un VDC de organización a un grupo de centros de datos.

Puede agregar todos los tipos de redes a un grupo de centros de datos.

Importante Las direcciones IP de las redes que participan en un grupo de centros de datos no deben superponerse, aunque las redes estén aisladas.

Tabla 5-2. Tipos de redes de grupo de centros de datos

Tipo de red de grupo de centros de datos	Descripción
Aislada	Solo los VDC pueden acceder a una red de grupo de centros de datos aislada en el mismo grupo de centros de datos. Las máquinas virtuales en este grupo de centros de datos son las únicas que pueden conectarse a la red de grupo de centros de datos aislada y ver el tráfico de esta.
Con enrutamiento	Una red de grupo de centros de datos enrutada proporciona un acceso controlado a una red externa a través de una puerta de enlace Edge de NSX-T Data Center que forma parte del grupo de centros de datos.
Importada	Una red de grupo de centros de datos importada utiliza un conmutador lógico de NSX-T Data Center existente. Solo un administrador del sistema puede importar una red.

Crear una red de grupo de centros de datos aislada respaldada por una instancia de NSX-T Data Center

Puede agregar una red de grupo de centros de datos aislada a la que solo puedan acceder las máquinas virtuales del grupo de centros de datos. Las máquinas virtuales que se encuentran fuera de esta red no tienen conectividad con ella, independientemente de si están conectadas a otras redes en el mismo grupo de centros de datos.

Requisitos previos

- Compruebe que es un **administrador de organización**.
- Compruebe que ha creado un grupo de centros de datos con el tipo de proveedor de red NSX-T Data Center.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 En la pestaña **Redes**, haga clic en **Nueva**.
- 3 En la página **Ámbito**, seleccione **Grupo de centros de datos** y, a continuación, seleccione el grupo con un proveedor de red de NSX-T Data Center en el que se creará la red.
- 4 En la página **Tipo de red**, seleccione **Aislada** y haga clic en **Siguiente**.

- 5 Introduzca un nombre significativo para la red.

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

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

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

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

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

Crear una red de grupo de centros de datos enrutada respaldada por NSX-T Data Center

Para controlar el acceso a una red externa, puede agregar una red de grupo de centros de datos enrutada.

Requisitos previos

- Compruebe que es **administrador de la organización** o que tiene una función con un conjunto de derechos equivalente.
- Compruebe que ha creado un grupo de centros de datos con el tipo de proveedor de red NSX-T Data Center.
- Compruebe que haya colocado dentro del ámbito una puerta de enlace Edge de NSX-T Data Center existente para el grupo de centros de datos en el que desea crear una red enrutada.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 En la pestaña **Redes**, haga clic en **Nueva**.
- 3 En la página **Ámbito**, seleccione **Grupo de centros de datos** y, a continuación, seleccione el grupo con un proveedor de red de NSX-T Data Center en el que se creará la red.
- 4 En la página **Tipo de red**, seleccione **Enrutada** y haga clic en **Siguiente**.

Si solo hay una puerta de enlace Edge disponible en el ámbito del grupo de centros de datos, esta se asigna automáticamente a la red.

- 5 Si hay más de una instancia de NSX-T Data Center disponible para el grupo de centros de datos, seleccione una puerta de enlace Edge de la lista y haga clic en **Siguiente**.
- 6 Introduzca un nombre significativo para la red.
- 7 Introduzca la configuración de enrutamiento de entre dominios sin clases (Classless Inter-Domain Routing, CIDR) para la red.

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

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

11 (opcional) Establezca la configuración de DNS.

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

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

Crear una red de grupo de centros de datos con un conmutador lógico de NSX-T importado

Los **administradores del sistema** pueden crear una red de VDC de organización mediante la importación de un segmento desde una instancia de NSX-T Manager asociada.

Requisitos previos

- Compruebe que es un **administrador del sistema**.
- Compruebe que ha creado un grupo de centros de datos con el tipo de proveedor de red NSX-T Data Center.
- Compruebe que el centro de datos virtual de proveedor que respalda el grupo de centros de datos virtuales de destino esté asociado con una instancia de NSX-T Manager.
- Compruebe que se haya creado al menos un conmutador lógico de NSX-T que otras redes no utilicen. Para obtener información sobre la creación y la configuración de conmutadores lógicos de NSX-T, consulte la *Guía de administración de NSX-T Data Center*.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 En la pestaña **Redes**, haga clic en **Nueva**.
- 3 En la página **Ámbito**, seleccione **Grupo de centros de datos** y, a continuación, seleccione el grupo con un proveedor de red de NSX-T Data Center en el que se creará la red.
- 4 En la página **Tipo de red**, seleccione **Importada** y haga clic en **Siguiente**.
- 5 En la lista de conmutadores lógicos NSX-T disponibles, seleccione el conmutador de destino y haga clic en **Siguiente**.
- 6 Introduzca un nombre significativo para la red.
- 7 Introduzca la configuración de enrutamiento de entre dominios sin clases (Classless Inter-Domain Routing, CIDR) para la red.

Utilice el formato *dirección_IP_de_puerta_de_enlace_de_red/longitud_de_prefijo_de_subred* (por ejemplo, **192.167.1.1/24**).
- 8 Introduzca una descripción de la red de VDC de organización.

9 Haga clic en **Siguiente**.

10 (opcional) Si desea reservar una o más direcciones IP para la asignación a máquinas virtuales que requieren direcciones IP estáticas, configure los **Grupos de IP estáticas** para la red.

a Introduzca la dirección IP o el rango de direcciones IP y haga clic en **Agregar**.

Para agregar varias direcciones IP estáticas o rangos, repita este paso.

b (opcional) Para modificar o eliminar direcciones IP y rangos de direcciones IP, haga clic en **Modificar** o **Eliminar**.

11 (opcional) Establezca la configuración de DNS.

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

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

Incrementar el ámbito de una red de VDC de organización respaldada por NSX-T Data Center

Después de incrementar el ámbito de una red de VDC de organización a una red de grupo de centros de datos, puede conectar las cargas de trabajo de todos los centros de datos que participan en el grupo de centros de datos.

Requisitos previos

- Compruebe que es **administrador de la organización** o que tiene una función con un conjunto de derechos equivalente.
- Compruebe que ha creado un grupo de centros de datos con el tipo de proveedor de red NSX-T Data Center.
- Compruebe que ha creado una red de VDC de organización respaldada por NSX-T Data Center.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 Haga clic en el botón de radio situado junto a la red de VDC de organización de la que desea incrementar el ámbito y haga clic en **Aumentar alcance**.
- 3 Seleccione un grupo de centros de datos de la lista de grupos de centros de datos y haga clic en **Aceptar** para confirmar.

Resultados

El ámbito de la red se incrementa a una red de grupo de centros de datos. En la lista de redes, aparece como dentro del ámbito del grupo de centros de datos que seleccionó.

Disminuir el ámbito de una red de grupo de centros de datos respaldada por NSX-T Data Center

Puede disminuir el ámbito de una red de grupo de centros de datos respaldada por NSX-T Data Center a una red de VDC de organización.

Si disminuye el ámbito de una red de grupo de centros de datos a una sola red de VDC de organización, debe proporcionar conectividad de red para las cargas de trabajo que pertenezcan solo al VDC de organización.

Requisitos previos

- Compruebe que es **administrador de la organización** o que tiene una función con un conjunto de derechos equivalente.
- Compruebe que ha creado una red de VDC que se encuentra en el ámbito de un grupo de centros de datos con el tipo de proveedor de red NSX-T Data Center.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 Haga clic en el botón de radio situado junto a la red de grupo de centros de datos de la que desea disminuir el ámbito y haga clic en **Reducir alcance**.
- 3 En la lista de VDC que son miembros de la red de grupos, seleccione el VDC que desea colocar dentro del ámbito de la red y haga clic en **Aceptar**.

Resultados

El ámbito de la red disminuye a una sola red de VDC de organización.

Administrar puntos de salida para grupos de centros de datos con el tipo de proveedor de red NSX-T Data Center

Para enrutar el tráfico entrante y saliente de una red de grupo de centros de datos a una red externa, puede configurar una puerta de enlace Edge de NSX-T Data Center para que sea el punto de salida de un grupo de centros de datos.

Cuando configure una puerta de enlace Edge para que sea el punto de salida de un grupo de centros de datos, aumente su ámbito al grupo de centros de datos. La puerta de enlace Edge se comparte entre todos los centros de datos que participan en el grupo. Todas las redes enrutadas que están conectadas a la puerta de enlace Edge se asocian al grupo de centros de datos y se colocan dentro de su ámbito.

Todos los servicios de la puerta de enlace Edge siguen formando parte de las funciones de la puerta de enlace Edge. Para obtener más información, consulte [Administrar puertas de enlace Edge de NSX-T Data Center](#).

Si un VDC es miembro del grupo de centros de datos, y no hay ninguna carga de trabajo asociada a ninguna de las redes enrutadas que no forman parte del ámbito de destino, puede eliminar una puerta de enlace Edge de un grupo de centros de datos y colocarla en el ámbito de un solo VDC.

Puede agregar una puerta de enlace Edge a una red de grupo de centros de datos aislada y convertirla en una red de centros de datos enrutada. También puede eliminar la conexión a una puerta de enlace Edge desde una red de grupo de centros de datos y convertir la red enrutada en una red de grupo de centros de datos aislada.

Agregar una puerta de enlace Edge de NSX-T Data Center a un grupo de centros de datos

Para configurar una puerta de enlace Edge de NSX-T Data Center para que sea el punto de salida de un grupo de centros de datos, aumente el ámbito de la puerta de enlace Edge. La puerta de enlace se comparte entre todos los centros de datos que participan en el grupo.

Cuando el ámbito de una puerta de enlace Edge es un grupo de centros de datos, todas las redes enrutadas que están conectadas a la puerta de enlace Edge se adjuntan al grupo de centros de datos y se colocan dentro de su ámbito.

Todas las redes enrutadas nuevas que se conectan a la puerta de enlace Edge pertenecen al grupo de centros de datos.

Una red enrutada que está conectada a una puerta de enlace Edge que se encuentra en el ámbito de un VDC puede participar en un grupo de centros de datos solo si el ámbito de la instancia de Edge aumenta a este grupo de centros de datos.

Requisitos previos

Compruebe que haya asociado una puerta de enlace Edge de NSX-T Data Center existente con uno de los VDC que participan en el grupo de centros de datos.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.
Aparece la lista de grupos de centros de datos.
- 2 Haga clic en el grupo de centros de datos de destino.
- 3 Haga clic en **Puerta de enlace Edge** y, a continuación, en **Agregar instancia de Edge**.
- 4 Seleccione una de las puertas de enlace Edge disponibles y haga clic en **Guardar**.

Resultados

El ámbito de la puerta de enlace Edge se incrementa al grupo de centros de datos. El cambio de ámbito no afecta a ninguna de las redes ni a los servicios subyacentes existentes.

Reducir el ámbito de una puerta de enlace Edge de NSX-T Data Center a un VDC

Puede reducir el ámbito de una puerta de enlace Edge de NSX-T Data Center a un VDC específico eliminando la puerta de enlace Edge del grupo de centros de datos del ámbito.

Cuando se reduce el ámbito de una puerta de enlace Edge a un VDC específico, todos los objetos del grupo de seguridad que utiliza la puerta de enlace Edge permanecen en él. Los grupos de seguridad que el firewall distribuido utiliza de manera exclusiva siguen formando parte del grupo de VDC.

Requisitos previos

- Compruebe que el VDC al que desea reducir el ámbito de la puerta de enlace Edge sea miembro del grupo de centros de datos.
- Compruebe que no haya cargas de trabajo asociadas a una red enrutada que no forme parte del ámbito de la puerta de enlace Edge de destino.
- Compruebe que la puerta de enlace Edge y el firewall distribuido no estén usando grupos de seguridad ni conjuntos de direcciones IP del grupo de centros de datos.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.
Aparece la lista de grupos de centros de datos.
- 2 Haga clic en el grupo de centros de datos de destino.
- 3 Haga clic en **Puerta de enlace Edge** y, a continuación, en **Eliminar instancia de Edge**.
- 4 Seleccione un VDC al cual reducir el ámbito de la puerta de enlace Edge y haga clic en **Guardar**.

Administrar redes de grupo de centros de datos con NSX Data Center for vSphere

Para crear una red entre varios centros de datos virtuales de organización, primero deberá agrupar los centros de datos virtuales y, a continuación, crear una red de VDC cuyo ámbito sea el grupo de centros de datos.

VMware Cloud Director admite redes de grupo de centros de datos para centros de datos virtuales de organización respaldados por NSX Data Center for vSphere con un punto de salida activo y en espera para un solo dominio de errores de red.

Un grupo de centros de datos respaldado por NSX Data Center for vSphere puede tener una configuración de punto de salida común, de punto de salida para cada dominio de error de red o de grupo local.

Grupo de centros de datos

Un grupo de centros de datos actúa como un enrutador de grupo de centros de datos virtuales que proporciona administración centralizada de redes, configuración para varios puntos de salida en múltiples centros de datos virtuales y tráfico de este a oeste entre todas las redes del grupo. Un grupo de centros de datos puede tener entre uno y dieciséis centros de datos virtuales configurados para compartir varios puntos de salida. Un grupo de centros de datos puede tener una de las siguientes configuraciones de puntos de salida:

Tabla 5-3. Tipo de configuración de puntos de salida para los grupos de centros de datos respaldados por NSX Data Center for vSphere

Tipo de configuración de puntos de salida	Descripción
Configuración común de puntos de salida	<p>Puede configurar el grupo de centros de datos con un punto de salida activo y otro en espera. Los dos puntos de salida son comunes a todos los centros de datos virtuales participantes entre todos los dominios de errores de red del grupo de centros de datos.</p> <p>Un grupo de centros de datos con esta configuración puede incluir centros de datos de hasta cuatro dominios de error de red.</p>
Configuración de puntos de salida por dominio de error	<p>Puede configurar el grupo de centros de datos con un punto de salida activo y otro en espera para cada dominio de error de red que contenga.</p> <p>Un grupo de centros de datos con esta configuración puede incluir centros de datos de hasta cuatro dominios de error de red.</p>
Configuración de grupo local	<p>Los centros de datos virtuales de organización de un grupo local de centros de datos están respaldados mediante una sola instancia de vCenter Server. Puede configurar el grupo local de centros de datos con un punto de salida activo y otro en espera para un único dominio de error de red.</p>

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

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

Dominio de error de red

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

Punto de salida

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

Red extendida

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

Administrar grupos de centros de datos con tipo de proveedor de red NSX Data Center for vSphere

Después de crear un grupo de centros de datos que está respaldado por NSX Data Center for vSphere, puede editar la topología de la red de un grupo de centros de datos. Puede agregar y eliminar los centros de datos virtuales del grupo. Puede intercambiar, reemplazar y eliminar los puntos de salida. Puede realizar distintas tareas de sincronización para corregir errores de configuración.

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

Crear y configurar un grupo de centros de datos respaldados por NSX Data Center for vSphere con una configuración de salida común

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

Requisitos previos

- Esta operación requiere la función **Administrador del sistema** o una función con el derecho **Grupo de VDC: Configurar grupo de VDC** publicado en la organización.
- El **administrador del sistema** debe habilitar los centros de datos virtuales de destino para Cross VDC Networking.

Procedimiento

- 1 [Crear un grupo de centros de datos respaldado por NSX Data Center for vSphere con una configuración de salida común](#)

Puede agrupar entre 1 y 16 centros de datos virtuales en un grupo de centros de datos con una configuración de salida común.

2 [Agregar un punto de salida activo a un grupo de centros de datos con tipo de proveedor de red NSX Data Center for vSphere](#)

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

3 [Agregar un punto de salida en espera a un grupo de centros de datos con tipo de proveedor de red NSX Data Center for vSphere](#)

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

Crear un grupo de centros de datos respaldado por NSX Data Center for vSphere con una configuración de salida común

Puede agrupar entre 1 y 16 centros de datos virtuales en un grupo de centros de datos con una configuración de salida común.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.
Aparece la lista de grupos de centros de datos.
- 2 Haga clic en **Nuevo**.
- 3 En la página **VDC inicial**, seleccione un VDC para iniciar el grupo de VDC.
- 4 Introduzca un nombre y, si lo desea, una descripción para el nuevo grupo de centros de datos.
- 5 Seleccione **Puntos de salida comunes** y haga clic en **Siguiente**.
- 6 En la página **VDC participante**, seleccione centros de datos adicionales para el nuevo grupo de centros de datos y haga clic en **Siguiente**.
La página **Centros de datos** contiene una lista de los VDC que el **administrador del sistema** ha habilitado para las redes entre centros de datos virtuales.
- 7 Revise los detalles del grupo de centros de datos y haga clic en **Finalizar**.

Resultados

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

Agregar un punto de salida activo a un grupo de centros de datos con tipo de proveedor de red NSX Data Center for vSphere

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

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.

Aparece la lista de grupos de centros de datos.

- 2 Haga clic en el grupo de centros de datos de destino.

Se abre la vista de **topología de red** de este grupo de centros de datos. El diagrama de la topología de la red actual muestra los VDC participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.

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

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

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

Resultados

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

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

Agregar un punto de salida en espera a un grupo de centros de datos con tipo de proveedor de red NSX Data Center for vSphere

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

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.

Aparece la lista de grupos de centros de datos.

- 2 Haga clic en el grupo de centros de datos de destino.

Se abre la vista de **topología de red** de este grupo de centros de datos. El diagrama de la topología de la red actual muestra los VDC participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.

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

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

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

Resultados

Las rutas de BGP se configuran en la puerta de enlace Edge que representa el punto de salida y el enrutador universal del dominio de error de red. La configuración no afecta a las rutas existentes en la puerta de enlace Edge.

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

Crear y configurar un grupo de centros de datos respaldado por NSX Data Center for vSphere con una configuración de salida de dominio de errores

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

Requisitos previos

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

Procedimiento

- 1 [Crear un grupo de centros de datos respaldado por NSX Data Center for vSphere con una configuración de salida de dominio de errores](#)

Puede agrupar entre 1 y 16 centros de datos virtuales en un grupo de centros de datos respaldado por NSX Data Center for vSphere con una configuración de salida de dominio de errores.

- 2 [Agregar un punto de salida para un dominio de error](#)

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

Crear un grupo de centros de datos respaldado por NSX Data Center for vSphere con una configuración de salida de dominio de errores

Puede agrupar entre 1 y 16 centros de datos virtuales en un grupo de centros de datos respaldado por NSX Data Center for vSphere con una configuración de salida de dominio de errores.

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.
Aparece la lista de grupos de centros de datos.
- 2 Haga clic en **Nuevo**.
- 3 Introduzca un nombre y, si lo desea, una descripción para el nuevo grupo de centros de datos.
- 4 Seleccione **Puntos de salida por dominio de error** y haga clic en **Siguiente**.
- 5 En la página **VDC participante**, seleccione centros de datos adicionales para el nuevo grupo de centros de datos y haga clic en **Siguiente**.
La página **Centros de datos** contiene una lista de los VDC que el **administrador del sistema** ha habilitado para las redes entre centros de datos virtuales.
- 6 Revise los detalles del grupo de centros de datos y haga clic en **Finalizar**.

Resultados

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

Agregar un punto de salida para un dominio de error

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

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.

Aparece la lista de grupos de centros de datos.

- 2 Haga clic en el grupo de centros de datos de destino.

Se abre la vista de **topología de red** de este grupo de centros de datos. El diagrama de la topología de la red actual muestra los VDC participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.

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

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

Los dominios de error seleccionados se marcan con color azul.

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

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

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

Resultados

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

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

Crear y configurar un grupo local de centros de datos virtuales con tipo de proveedor de red NSX Data Center for vSphere

A partir de la versión 10.1, VMware Cloud Director admite grupos de centros de datos respaldados por NSX Data Center for vSphere que tienen un punto de salida activo y otro en espera para un único dominio de errores de red.

Una única instancia de vCenter Server respalda los centros de datos virtuales de organización de un grupo local.

En un grupo local de centros de datos, puede establecer un par de puertas de enlace Edge (un punto de salida activo y otro en espera) para admitir escenarios de alta disponibilidad y recuperación ante desastres en un mismo dominio de error de red.

Requisitos previos

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

Procedimiento

- 1 [Crear un grupo local de centros de datos con tipo de proveedor de red NSX Data Center for vSphere](#)

Puede agrupar entre 1 y 16 centros de datos virtuales (virtual data centers, VDC) en un grupo de centros de datos respaldado por NSX Data Center for vSphere con una configuración de salida de dominio de errores.

- 2 [Agregar un punto de salida activo para un grupo local de centros de datos con tipo de proveedor de red NSX Data Center for vSphere](#)

Para conectar a Internet los centros de datos del grupo local de centros de datos respaldados por NSX Data Center for vSphere, debe agregar un punto de salida activo al dominio de errores de red.

- 3 [Agregar un punto de salida en espera para un grupo local de centros de datos con tipo de proveedor de red NSX Data Center for vSphere](#)

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

Crear un grupo local de centros de datos con tipo de proveedor de red NSX Data Center for vSphere

Puede agrupar entre 1 y 16 centros de datos virtuales (virtual data centers, VDC) en un grupo de centros de datos respaldado por NSX Data Center for vSphere con una configuración de salida de dominio de errores.

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.
Aparece la lista de grupos de centros de datos.
- 2 Haga clic en **Nuevo**.
- 3 En la página **VDC inicial**, seleccione un VDC para iniciar el grupo de VDC.
- 4 Introduzca un nombre y, si lo desea, una descripción para el nuevo grupo de centros de datos.
- 5 Para crear un grupo que contenga únicamente centros de datos virtuales de un único dominio de error de red, active la opción **Crear grupo local**.
- 6 Haga clic en **Siguiente**.
- 7 En la página **VDC participante**, seleccione centros de datos adicionales para el nuevo grupo de centros de datos y haga clic en **Siguiente**.
La página **Centros de datos** contiene una lista de los VDC que el **administrador del sistema** ha habilitado para las redes entre centros de datos virtuales.
- 8 Revise los detalles del grupo de centros de datos y haga clic en **Finalizar**.

Resultados

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

Agregar un punto de salida activo para un grupo local de centros de datos con tipo de proveedor de red NSX Data Center for vSphere

Para conectar a Internet los centros de datos del grupo local de centros de datos respaldados por NSX Data Center for vSphere, debe agregar un punto de salida activo al dominio de errores de red.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.
Aparece la lista de grupos de centros de datos.
- 2 Haga clic en el grupo de centros de datos de destino.
Se abre la vista de **topología de red** de este grupo de centros de datos. El diagrama de la topología de la red actual muestra los VDC participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.

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

4 En la lista de puertas de enlace Edge que pertenecen a los centros de datos virtuales participantes, seleccione una puerta de enlace Edge para que actúe como punto de salida activo del grupo de centros de datos y haga clic en **Agregar**.

Resultados

Las rutas de BGP se configuran en la puerta de enlace Edge que representa el punto de salida y el enrutador universal del dominio de error de red. La configuración no afecta a las rutas existentes en la puerta de enlace Edge.

El punto de salida activo recién agregado se muestra en el diagrama de la topología de la red. Una línea continua azul representa el tráfico que va desde los centros de datos virtuales en el dominio de errores de red a Internet.

Pasos siguientes

Si desea permitir la tolerancia a errores de puntos de salida, agregue un punto de salida en espera para el grupo local de centros de datos.

Agregar un punto de salida en espera para un grupo local de centros de datos con tipo de proveedor de red NSX Data Center for vSphere

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

Requisitos previos

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

Procedimiento

1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.

Aparece la lista de grupos de centros de datos.

2 Haga clic en el grupo de centros de datos de destino.

Se abre la vista de **topología de red** de este grupo de centros de datos. El diagrama de la topología de la red actual muestra los VDC participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.

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

Se abrirá la página **Agregar punto de salida en espera**, la cual proporciona una lista de las puertas de enlace Edge sin utilizar que pertenecen a los centros de datos virtuales participantes. La puerta de enlace Edge que emplea el punto de salida activo en este grupo de centros de datos virtuales se muestra atenuada.

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

Resultados

Las rutas de BGP se configuran en la puerta de enlace Edge que representa el punto de salida y el enrutador universal del dominio de error de red. La configuración no afecta a las rutas existentes en la puerta de enlace Edge.

El punto de salida recién agregado aparece en el diagrama de topología de la red. Una línea discontinua azul representa el tráfico de los centros de datos virtuales participantes hacia Internet en escenarios de tolerancia a errores.

Ver un grupo de centros de datos con el tipo de proveedor de red NSX Data Center for vSphere

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

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.

Aparece la lista de grupos de centros de datos.

- 2 Haga clic en el grupo de centros de datos de destino.

Se abre la vista de **topología de red** de este grupo de centros de datos. El diagrama de la topología de la red actual muestra los VDC participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.

Agregar un centro de datos virtual a un grupo de centros de datos con tipo de proveedor de red NSX Data Center for vSphere

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

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.

Aparece la lista de grupos de centros de datos.

- 2 Haga clic en el grupo de centros de datos de destino.

Se abre la vista de **topología de red** de este grupo de centros de datos. El diagrama de la topología de la red actual muestra los VDC participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.

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

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

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

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

Eliminar un centro de datos virtual de un grupo de centros de datos con tipo de proveedor de red NSX Data Center for vSphere

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

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.

Aparece la lista de grupos de centros de datos.

- 2 Haga clic en el grupo de centros de datos de destino.

Se abre la vista de **topología de red** de este grupo de centros de datos. El diagrama de la topología de la red actual muestra los VDC participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.

- 3 En la esquina superior derecha de la tarjeta del centro de datos virtual de destino, haga clic en los tres puntos y haga clic en **Quitar**.

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

Resultados

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

Sincronizar un grupo de centros de datos con tipo de proveedor de red NSX Data Center for vSphere

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

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

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.
Aparece la lista de grupos de centros de datos.
- 2 Haga clic en el grupo de centros de datos de destino.
Se abre la vista de **topología de red** de este grupo de centros de datos. El diagrama de la topología de la red actual muestra los VDC participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.
- 3 Haga clic en **Sincronizar grupo de centros de datos**.
- 4 Para confirmar, haga clic en **Aceptar**.

Intercambiar los puntos de salida en un grupo de centros de datos con tipo de proveedor de red NSX Data Center for vSphere y una configuración de salida común

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

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.
Aparece la lista de grupos de centros de datos.
- 2 Haga clic en el grupo de centros de datos de destino.
Se abre la vista de **topología de red** de este grupo de centros de datos. El diagrama de la topología de la red actual muestra los VDC participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.
- 3 Haga clic en **Intercambiar puntos de salida**.
- 4 Para confirmar, haga clic en **Aceptar**.

Resultados

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

Reemplazar la puerta de enlace Edge de un punto de salida de un grupo de centros de datos con tipo de proveedor de red NSX Data Center for vSphere

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

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.
Aparece la lista de grupos de centros de datos.
- 2 Haga clic en el grupo de centros de datos de destino.
Se abre la vista de **topología de red** de este grupo de centros de datos. El diagrama de la topología de la red actual muestra los VDC participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.

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

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

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

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

Se abrirá la página **Reemplazar punto de salida**, que muestra la lista de las puertas de enlace Edge que pertenecen a los centros de datos virtuales participantes.

- 5 Seleccione la nueva puerta de enlace Edge y haga clic en **Reemplazar**.

Resultados

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

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

Quitar un punto de salida de un grupo de centros de datos con tipo de proveedor de red NSX Data Center for vSphere

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

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.

Aparece la lista de grupos de centros de datos.

- 2 Haga clic en el grupo de centros de datos de destino.

Se abre la vista de **topología de red** de este grupo de centros de datos. El diagrama de la topología de la red actual muestra los VDC participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.

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

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

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

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

Resultados

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

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

Sincronizar las rutas y los puntos de salida de un grupo de centros de datos con tipo de proveedor de red NSX Data Center for vSphere

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

Requisitos previos

- Esta operación requiere la función **Administrador del sistema** o una función con el derecho **Grupo de VDC: Configurar grupo de VDC** publicado en la organización.
- Ha configurado un punto de salida para el dominio de errores de red o para el grupo de centros de datos de destino.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en la pestaña **Grupos de centros de datos**.

Aparece la lista de grupos de centros de datos.

- 2 Haga clic en el grupo de centros de datos de destino.

Se abre la vista de **topología de red** de este grupo de centros de datos. El diagrama de la topología de la red actual muestra los VDC participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.

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

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

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

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

Administrar redes de grupo de centros de datos respaldadas por NSX Data Center for vSphere

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

Agregar una red de grupos de VDC respaldada por NSX Data Center for vSphere

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

Solo se puede agregar una red de grupo de centros de datos IPv4 respaldada por NSX Data Center for vSphere.

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 En la pestaña **Redes**, haga clic en **Nueva**.
- 3 En la página **Alcance**, seleccione **Grupo de centros de datos** y, a continuación, elija un grupo de centros de datos respaldado por NSX Data Center for vSphere en el que se creará la red y haga clic en **Siguiente**.
- 4 Introduzca un nombre significativo para la red.

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

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

- 6 Introduzca una descripción de la red de VDC de organización.
- 7 Haga clic en **Siguiente**.
- 8 Revise la configuración y haga clic en **Finalizar**.

Resultados

Puede ver la red de grupos de centros de datos recién creada en la lista de redes de la organización.

Su tipo de red se muestra como Cross VDC.

Se crea una red de centros de datos virtuales de organización del tipo de enrutamiento Cross VDC para cada centro de datos virtual participante. Para ver las redes de grupos de VDC de los centros de datos virtuales participantes, haga clic en la tarjeta de un centro de datos virtual participante y, a continuación, haga clic en **Redes**. Si una máquina virtual o una vApp se conectan a tal red de centros de datos virtuales de organización, la máquina virtual o la vApp se conectan a la red de grupos de VDC.

Pasos siguientes

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

Para las configuraciones DNS y DHCP de máquinas virtuales conectadas a una red de grupos de VDC , puede usar VMware Cloud Director OpenAPI. Para consultar la documentación de VMware Cloud Director OpenAPI, desplácese hasta https://Cloud_Director_IP_address_or_host_name/docs. Para ver muestras de código y probar llamadas de VMware Cloud Director OpenAPI, desplácese hasta https://Cloud_Director_IP_address_or_host_name/api-explorer?scope=organization_name.

Ver o editar una red de grupo de centros de datos respaldada por NSX Data Center for vSphere

Puede ver el nombre, la descripción y la configuración de CIDR de una red de grupo de centros de datos respaldada por NSX Data Center for vSphere. Solo puede editar el nombre y la descripción de una red de grupo de centros de datos respaldada por NSX Data Center for vSphere.

Para obtener información sobre cómo editar la asignación del grupo de direcciones IP estáticas para una red de grupo de centros de datos a nivel del centro de datos virtual, consulte [Agregar direcciones IP a un grupo de direcciones IP de red de centros virtuales de organización](#).

Requisitos previos

Compruebe que tenga asignada la función predefinida **Administrador de organización** o una función que incluya el derecho **Red de VDC de organización: Ver propiedades** y **Red de VDC de organización: Editar propiedades**.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 Haga clic en la red de destino para ver sus detalles.
- 3 Para editar el nombre y la descripción de las redes, haga clic en **Editar**.
- 4 Edite los detalles de la red y haga clic en **Guardar**.

Sincronizar una red de grupo de centros de datos respaldada por NSX Data Center for vSphere

Para asegurarse de que todos los centros de datos virtuales participantes puedan acceder a su red de grupo de centros de datos respaldada por NSX Data Center for vSphere, puede sincronizar la red del grupo de centros de datos.

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes**.
- 2 En la pestaña Redes, seleccione el botón de radio junto al nombre de la red de destino y haga clic en **Sincronizar**.
- 3 Para confirmar, haga clic en **Aceptar**.

Administrar servicios de puerta de enlace Edge de NSX Data Center for vSphere

VMware Cloud Director proporciona capacidades de red avanzadas con la tecnología del software de virtualización de red NSX Data Center for vSphere, que ofrece capacidades de escalado de red, enrutamiento y controles de seguridad mejorados en un entorno en la nube.

Con estas capacidades de red, puede alcanzar un nivel de seguridad y aislamiento sin precedentes en el centro de datos virtual de organización. Estas capacidades ofrecen las siguientes ventajas:

- **Enrutamiento dinámico.** Las capacidades de NSX Data Center for vSphere en el entorno de VMware Cloud Director admiten protocolos de enrutamiento, como Border Gateway Protocol (BGP) y Open Shortest Path First (OSPF), para simplificar la integración de red entre sistemas con el fin de proporcionar redundancia y continuidad en la implementación de aplicaciones alojadas en la nube.
- **Seguridad y aislamiento de red específicos.** Las capacidades de NSX Data Center for vSphere en el entorno de VMware Cloud Director admiten el uso de las definiciones de regla basadas en objetos para proporcionar un aislamiento del tráfico de red con estado sin necesidad de contar con varias redes virtuales. Este modelo de seguridad sin confianza impide que los intrusos obtengan acceso a la red completa si una aplicación o una máquina virtual están en riesgo. Se simplifica la configuración de red utilizando las mismas políticas de seguridad de red para proteger las aplicaciones sin importar si están ubicadas físicamente en el entorno de VMware Cloud Director, y para ampliar el modelo de seguridad sin confianza a la seguridad portátil independientemente de dónde se implemente una aplicación.
- **Otras capacidades que ofrece NSX Data Center for vSphere** incluyen la compatibilidad mejorada con VPN para la conectividad de punto a sitio (VPN de IPsec) y de usuario (VPN-Plus de SSL), equilibrio de carga mejorado para HTTPS y mayor escalabilidad de red.

Puede configurar dos tipos de firewall: el firewall de puerta de enlace Edge y el distribuido. Para obtener más información sobre las diferencias entre estos firewall, consulte [Configuración del firewall de tenant con NSX Data Center for vSphere](#).

Puede acceder a estas capacidades de red avanzadas a través del portal para tenants de VMware Cloud Director o del VMware Cloud Director Service Provider Admin Portal. La puerta de enlace Edge primero debe convertirse en una puerta de enlace Edge avanzada. Consulte la [Convertir una puerta de enlace Edge de NSX Data Center for vSphere en una puerta de enlace Edge avanzada](#).

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

Introducción a las redes avanzadas de VMware Cloud Director con NSX Data Center for vSphere

Se utilizan las redes avanzadas de VMware Cloud Director para realizar tareas de administración en una organización de un sistema de VMware Cloud Director. Puede administrar los firewalls distribuidos y otras capacidades de redes avanzadas proporcionadas por NSX Data Center for vSphere y que un administrador del sistema de VMware Cloud Director pone a disposición de una organización.

Los usuarios típicos de las redes avanzadas proporcionadas por NSX Data Center for vSphere son:

- **Administradores del sistema** de VMware Cloud Director que pueden usar el portal para tenants para configurar el firewall distribuido y otras capacidades de redes avanzadas de una organización.
- **Administradores de organización** que usan el portal para tenants para administrar el firewall distribuido y otras capacidades de redes avanzadas que el **administrador del sistema** ha puesto a disposición de esa organización.

Configuración del firewall de tenant con NSX Data Center for vSphere

En el portal para tenants, puede configurar las capacidades de firewall que ofrece NSX Data Center for vSphere en el centro de datos virtual de la organización de VMware Cloud Director. Puede crear reglas de firewall para firewalls distribuidos a fin de proporcionar seguridad entre las máquinas virtuales de un centro de datos virtual de organización y reglas de firewall que se apliquen a un firewall de puerta de enlace Edge a fin de proteger las máquinas virtuales de un centro de datos virtual de organización contra el tráfico de red externo.

Nota El portal para tenants proporciona la capacidad para configurar firewalls de puerta de enlace Edge y firewalls distribuidos.

La tecnología de firewall lógico de NSX Data Center for vSphere consta de dos componentes para abordar escenarios de uso de implementación diferentes. El firewall de puerta de enlace Edge se centra en la aplicación de tráfico de norte a sur mientras que el firewall distribuido se centra en los controles de acceso de este a oeste.

Diferencias clave entre los firewalls de puerta de enlace Edge y los firewalls distribuidos

Un firewall de puerta de enlace Edge supervisa el tráfico de norte a sur para proporcionar la funcionalidad de seguridad del perímetro, incluidos el firewall y la traducción de direcciones de red (Network Address Translation, NAT), así como la funcionalidad VPN de SSL y de IPsec de sitio a sitio.

Un firewall distribuido proporciona la capacidad para aislar y proteger cada máquina virtual y aplicación hacia abajo hasta el nivel de capa 2 (L2). La configuración de firewalls distribuidos coloca en cuarentena con eficacia todo riesgo de seguridad de red externo o interno, ya que aísla el tráfico de este a oeste entre las máquinas virtuales en el mismo segmento de red. Las políticas de seguridad se pueden administrar centralmente, así como heredar y anidar, para que los administradores de redes y seguridad puedan administrarlas a gran escala. Además, una vez implementadas, las políticas de seguridad definidas siguen a las máquinas virtuales o las aplicaciones cuando se mueven de un centro de datos virtual a otro.

Acerca de las reglas de firewall

Como se describe en la documentación del producto correspondiente, en NSX Data Center for vSphere, las reglas de firewall definidas en el nivel centralizado se conocen como reglas previas. También es posible agregar reglas en un nivel de puerta de enlace Edge individual. Estas reglas se denominan reglas locales.

Cada sesión de tráfico se compara con la regla principal de la tabla de firewall antes de bajar a las reglas subsiguientes de la tabla. Se aplica la primera regla de la tabla que coincide con los parámetros de tráfico. Las reglas se muestran en el siguiente orden:

- 1 Las reglas previas definidas por el usuario tienen la prioridad más alta y se aplican en orden de arriba a abajo con prioridad por nivel de NIC virtual.
- 2 Las reglas asociadas automáticamente (las reglas que permiten que el tráfico de control fluya en los servicios de puerta de enlace Edge).
- 3 Las reglas locales definidas en el nivel de puerta de enlace Edge.
- 4 La regla de firewall distribuido predeterminada.

Para obtener más información sobre cómo el software NSX Data Center for vSphere hace cumplir las reglas de firewall, consulte *Cambiar el orden de una regla de firewall* en la documentación de NSX Data Center for vSphere.

Firewall de puerta de enlace Edge de NSX Data Center for vSphere

El firewall de la puerta de enlace Edge ayuda a satisfacer los requisitos clave de seguridad del perímetro, como la creación de DMZ con base en construcciones IP/VLAN, el aislamiento de tenant a tenant en centros de datos virtuales de varios tenants, la traducción de direcciones de red (Network Address Translation, NAT), las VPN de socios (extranet) y las VPN de SSL basadas en usuarios.

NSX Data Center for vSphere proporciona la capacidad de firewall de puerta de enlace Edge en el entorno de VMware Cloud Director. En NSX Data Center for vSphere, esta capacidad de firewall también se conoce como firewall de Edge. El firewall de puerta de enlace Edge supervisa el tráfico de norte a sur para proporcionar la funcionalidad de seguridad del perímetro, incluidos el firewall y la traducción de direcciones de red (Network Address Translation, NAT), así como la funcionalidad VPN de SSL y de IPSec de sitio a sitio.

Para obtener información más detallada sobre las capacidades que ofrece el firewall de puerta de enlace Edge de NSX Data Center for vSphere, consulte la documentación de NSX Data Center for vSphere.

Administrar un firewall de puerta de enlace Edge de NSX Data Center for vSphere

Para proteger el tráfico hacia y desde una puerta de enlace Edge, es posible crear y administrar reglas de firewall en esa puerta de enlace Edge.

Para obtener información sobre cómo proteger el tráfico que se transmite entre máquinas virtuales de un centro de datos virtual de organización, consulte [Administrar reglas de firewall distribuido de NSX Data Center for vSphere mediante el portal para tenants](#).

Las reglas creadas en la pantalla de firewall distribuido en las que se ha especificado una puerta de enlace Edge avanzada en la columna Aplicado a no se muestran en la pantalla Firewall de dicha puerta de enlace Edge avanzada.

Las reglas de firewall de puerta de enlace Edge para una puerta de enlace Edge se muestran en la pantalla **Firewall** y se aplican en el siguiente orden:

- 1 Reglas internas (también conocidas como reglas asociadas automáticamente). Estas reglas internas permiten que el tráfico de control fluya en los servicios de puerta de enlace Edge.
- 2 Reglas definidas por el usuario.
- 3 Regla predeterminada.

La configuración de la regla predeterminada se aplica al tráfico que no coincide con ninguna de las reglas de firewall definidas por el usuario. La regla predeterminada se muestra en la parte inferior de las reglas en la pantalla Firewall.

En el portal para tenants, utilice el botón de alternancia **Habilitar** en la pantalla Reglas de firewall de la puerta de enlace Edge para activar o desactivar el firewall de una puerta de enlace Edge.

Convertir una puerta de enlace Edge de NSX Data Center for vSphere en una puerta de enlace Edge avanzada

Para trabajar con una puerta de enlace Edge de NSX Data Center for vSphere en el portal para tenants, debe convertirla en una puerta de enlace Edge avanzada. Después de convertirla en una puerta de enlace Edge avanzada, puede utilizar el portal para tenants para configurar las capacidades de enrutamiento estático y dinámico que proporciona NSX Data Center for vSphere para las puertas de enlace Edge avanzadas.

Requisitos previos

Debe tener una puerta de enlace Edge.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, en la pestaña **Puertas de enlace Edge**.
- 2 Seleccione la puerta de enlace Edge que se editará.
- 3 Haga clic en **Convertir en avanzada**.

Resultados

La puerta de enlace Edge se convierte en una puerta de enlace Edge avanzada.

Pasos siguientes

Después de convertirla en una puerta de enlace Edge avanzada, puede seleccionar la puerta de enlace y hacer clic en **Servicios** para modificar la configuración.

Agregar una regla de firewall de puerta de enlace Edge de NSX Data Center for vSphere

Las reglas de firewall de la puerta de enlace Edge se agregan en la pestaña **Firewall** de la puerta de enlace Edge en cuestión. Es posible 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.

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 la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Servicios**.
- 2 Si aún no está visible la pantalla **Reglas de firewall**, 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 de NSX Data Center for vSphere

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 de NSX Data Center for vSphere](#).

Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
 - a En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Servicios**.
- 2 Haga clic en la pestaña **Firewall**.
- 3 Administre las reglas de firewall.
 - Para desactivar 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 desactivada. Si la regla está desactivada y desea activarla, haga clic en el icono de color rojo que indica que está desactivada.

- Para editar el nombre de una regla, haga doble clic en la celda **Nombre** y escriba el nuevo nombre.
- Para modificar la configuración de una regla, como la configuración de origen o acción, seleccione la celda adecuada y utilice los controles que se muestran.
- Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar** situado encima de la tabla de reglas.
- Oculte las reglas generadas por el sistema mediante el botón de alternancia **Mostrar solo reglas definidas por el usuario**.
- Para subir o bajar una regla en la tabla de reglas, seleccione la regla y haga clic en los botones de flecha arriba y abajo situados encima de la tabla de reglas.

4 Haga clic en **Guardar cambios**.

Firewall distribuido de NSX Data Center for vSphere

El firewall distribuido permite segmentar las entidades de centros de datos virtuales de la organización (como las máquinas virtuales) en función de los atributos y los nombres de las máquinas virtuales.

VMware Cloud Director admite servicios de firewall distribuido en centros de datos virtuales de organización respaldados por NSX Data Center for vSphere. Como se describe en la documentación de NSX Data Center for vSphere, el firewall distribuido es un firewall integrado en el kernel del hipervisor que proporciona visibilidad y control sobre las redes y las cargas de trabajo virtualizadas. Puede crear políticas de control de acceso basadas en objetos, como nombres de máquinas virtuales, y en construcciones de red, como direcciones IP o conjuntos de direcciones IP. Las reglas de firewall se aplican en el nivel de vNIC de cada máquina virtual para proporcionar control de acceso consistente incluso cuando vSphere vMotion mueve la máquina virtual a un nuevo host ESXi. Este firewall distribuido es compatible con un modelo de seguridad de microsegmentación en el que se puede inspeccionar el tráfico de este a oeste en un procesamiento casi a velocidad de línea.

Como se describe en la documentación de NSX Data Center for vSphere, para los paquetes de capa 2 (L2), el firewall distribuido crea una memoria caché para aumentar el rendimiento. Los paquetes de capa 3 (L3) se procesan en la siguiente secuencia:

- 1 Se comprueba el estado existente de todos los paquetes.
 - 2 Cuando se encuentra una coincidencia de estado, se procesan los paquetes.
 - 3 Cuando no se encuentra una coincidencia de estado, se procesan los paquetes mediante las reglas hasta que se encuentra una coincidencia.
- Para los paquetes TCP, solo se establece un estado para los paquetes con la marca SYN. Sin embargo, las reglas que no especifican un protocolo (servicio ANY), pueden hacer coincidir paquetes TCP con cualquier combinación de marcas.

- Para los paquetes UDP, se extraen los detalles de 5-tupla de los paquetes. Cuando no existe un estado en la tabla de estado, se crea un nuevo estado mediante los detalles de 5-tupla extraídos. Los paquetes recibidos posteriormente se comparan con el estado que se acaba de crear.
- Para los paquetes ICMP, la dirección de paquete, el código y el tipo de ICMP se utilizan para crear un estado.

El firewall distribuido también puede ayudar a crear reglas basadas en identidades. Los administradores pueden aplicar el control de acceso según la pertenencia a grupos del usuario definida en la instancia de Active Directory (AD) de la empresa. Algunos escenarios de uso cuando es posible utilizar reglas de firewall basadas en identidades son:

- Los usuarios acceden a aplicaciones virtuales con un equipo portátil o un dispositivo móvil en los que se utiliza AD para la autenticación de usuario
- Los usuarios acceden a aplicaciones virtuales mediante la infraestructura de VDI en la que las máquinas virtuales se basan en Microsoft Windows

Para obtener información más detallada sobre las capacidades que ofrece el firewall distribuido, consulte la documentación de NSX Data Center for vSphere.

Habilitar el firewall distribuido en un centro de datos virtual de organización respaldado por NSX Data Center for vSphere

Antes de utilizar el portal para tenants para trabajar con las capacidades de firewall distribuido que ofrece NSX Data Center for vSphere en un centro de datos virtual de organización, se debe habilitar el firewall distribuido para ese centro de datos virtual de organización. Un administrador del sistema de VMware Cloud Director o un usuario al que se haya concedido el derecho **org_vdc_distributed_firewall_enable** puede habilitar el firewall distribuido en un centro de datos virtual de organización.

Se utiliza la pantalla Firewall distribuido del portal para tenants a fin de habilitar el firewall distribuido de un centro de datos virtual de organización.

Requisitos previos

Compruebe que se hayan asignado los siguientes derechos a la organización a la que pertenece el centro de datos virtual de organización:

- Firewall distribuido de VDC de organización: habilitar o deshabilitar
- Firewall distribuido de VDC de organización: configurar reglas
- Firewall distribuido de VDC de organización: ver reglas

El **administrador del sistema** de VMware Cloud Director asigna derechos a una organización. El derecho Firewall distribuido de VDC de organización: habilitar o deshabilitar es necesario para activar el firewall distribuido mediante la interfaz de usuario en el portal para tenants. El derecho Firewall distribuido de VDC de organización: ver reglas es necesario para ver las reglas de firewall en el portal para tenants, mientras que el derecho Firewall distribuido de VDC de organización: configurar reglas es necesario para la configuración de las reglas de firewall mediante el portal para tenants.

Compruebe que se le haya asignado una función que le otorga el derecho llamado Firewall distribuido de VDC de organización: habilitar o deshabilitar. De las funciones predefinidas en un sistema de VMware Cloud Director, solo la función de administrador del sistema tiene ese derecho de forma predeterminada.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en **Redes**, seleccione **Seguridad**.
- 2 Seleccione el centro de datos virtual de organización para el que desea configurar reglas de firewall distribuido.
- 3 Haga clic en **Configurar servicios**.
- 4 Habilite el firewall distribuido en la pestaña **Firewall distribuido**.

Pasos siguientes

Para obtener una descripción de la regla de firewall distribuido predeterminada, consulte [Administrar reglas de firewall distribuido de NSX Data Center for vSphere mediante el portal para tenants](#).

Administrar reglas de firewall distribuido de NSX Data Center for vSphere mediante el portal para tenants

Tal como se describe en la documentación de NSX Data Center for vSphere, la configuración de firewall predeterminada se aplica al tráfico que no coincide con ninguna de las reglas de firewall definidas por el usuario. En el VMware Cloud Director Tenant Portal, la regla de firewall distribuido predeterminada tiene la etiqueta Regla para permitir predeterminada.

Para poder administrar la configuración del firewall distribuido mediante el VMware Cloud Director Tenant Portal, es necesario habilitar la funcionalidad del firewall distribuido en un centro de datos virtual de organización.

Se configura la regla de firewall distribuido predeterminada para permitir que todo el tráfico de capa 3 y de capa 2 pase por el centro de datos virtual de organización. Esta configuración se indica mediante la opción Permitir establecida en la columna Acción de la interfaz de usuario. La regla predeterminada siempre se ubica en la parte inferior de la tabla de reglas.

Importante No puede eliminar ni modificar las reglas predeterminadas del firewall distribuido.

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 respaldado por NSX Data Center for vSphere](#)
- Si desea utilizar un conjunto de direcciones IP como origen o destino en una regla, [Crear un conjunto de direcciones IP para usarlas en las reglas de firewall y la configuración de retransmisión de DHCP](#).
- Si desea utilizar un conjunto de direcciones MAC como origen o destino en una regla, [Crear un conjunto de direcciones MAC para utilizarlas en las reglas de firewall](#).
- Si desea utilizar un grupo de seguridad como origen o destino en una regla, [Crear un grupo de seguridad](#).


Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en **Redes**, seleccione **Seguridad**.
- 2 Seleccione la red de VDC de servicios de seguridad para la que desea modificar las reglas de firewall y haga clic en **Configurar servicios**.

Aparecerá la pantalla Servicios de seguridad.

- 3 Seleccione el tipo de regla que desea crear. Puede crear una regla general o una regla de Ethernet.

Las reglas de capa 3 (Layer 3, L3) se configuran en la pestaña **General**. Las reglas de capa 2 (Layer 2, L2) se configuran en la pestaña **Ethernet**.

- 4 Para agregar una regla debajo de una regla existente en la tabla de firewall, haga clic en la fila existente y, a continuación, haga clic en el botón **Crear** ().

Se agrega una fila para la nueva regla debajo de la regla seleccionada y se le asigna un destino cualquiera, un servicio cualquiera y la acción **Permitir** de forma predeterminada. Cuando la regla definida por el sistema Permitir de manera predeterminada es la única regla en la tabla de firewall, la nueva regla se agrega arriba de la regla predeterminada.

- 5 Haga clic en la celda **Nombre** y escriba un nombre.

- 6 Haga clic en la celda **Origen** y utilice los iconos que ahora pueden verse para seleccionar un origen y agregarlo a la regla:

Acción	Descripción
Hacer clic en el icono IP	Se aplica a las reglas definidas en la pestaña 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>

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

Acción	Descripción
Hacer clic en el icono IP	Se aplica a las reglas definidas en la pestaña 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>

- 8 Haga clic en la celda **Servicio** de la nueva regla y realice una de las siguientes acciones:

Acción	Descripción
Hacer clic en el icono IP	Para especificar el servicio como una combinación de puerto y protocolo, realice lo siguiente: <ul style="list-style-type: none"> 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.

- 9 En la celda **Acción** de la nueva regla, configure la acción de la regla.

Opción	Descripción
Permitir	Permite el tráfico desde los orígenes, los destinos y los servicios especificados, o bien hacia los mismos.
Denegar	Bloquea el tráfico desde los orígenes, los destinos y los servicios especificados, o bien hacia los mismos.

- 10 En la celda **Dirección** de la nueva regla, determine si la regla se aplica al tráfico entrante, al tráfico saliente o a ambos.
- 11 Si se trata de una regla en la pestaña **General**, en la celda **Tipo de paquete** de la nueva regla, seleccione el tipo de paquete **Cualquiera**, **IPV4** o **IPV6**.
- 12 Seleccione la celda **Aplicado a** y use el icono + para definir el alcance de objetos al que se aplica esta regla.

Cuando la regla contiene máquinas virtuales en las celdas **Origen** y **Destino**, debe agregar las máquinas virtuales de origen y destino a la sección **Aplicado a** de la regla para que esta funcione correctamente.

Importante Los grupos de direcciones IP (conjuntos de direcciones IP), los grupos de direcciones MAC (conjuntos de direcciones MAC) y los grupos de seguridad que contienen conjuntos de direcciones IP o MAC no son parámetros de entrada válidos.

- 13 Haga clic en **Guardar cambios**.

Editar una regla de firewall distribuido

En un entorno de VMware Cloud Director, para modificar una regla de firewall distribuido existente de un centro de datos virtual de organización, utilice la pantalla **Firewall distribuido**.

Para obtener más información sobre la configuración disponible para las diversas celdas de una regla, consulte [Agregar una regla de firewall distribuido](#).

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en **Redes**, seleccione **Seguridad**.
- 2 Seleccione la red de VDC de servicios de seguridad para la que desea modificar las reglas de firewall y haga clic en **Configurar servicios**.
Aparecerá la pantalla Servicios de seguridad.
- 3 Realice cualquiera de las siguientes acciones para administrar las reglas de firewall distribuido:
 - Para desactivar 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 desactivada. Si la regla está desactivada y desea activarla, haga clic en el icono de color rojo que indica que está desactivada.
 - Para editar el nombre de una regla, haga doble clic en la celda **Nombre** y escriba el nuevo nombre.
 - Para modificar la configuración de una regla, como la configuración de origen o acción, seleccione la celda adecuada y utilice los controles que se muestran.
 - Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar** situado encima de la tabla de reglas.
 - Para subir o bajar una regla en la tabla de reglas, seleccione la regla y haga clic en los botones de flecha arriba y abajo situados encima de la tabla de reglas.
- 4 Haga clic en **Guardar cambios**.

Administrar DHCP de puerta de enlace Edge de NSX Data Center for vSphere

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 que tiene DHCP activado, es posible que dicha puerta 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 desactivar y después volver a activar 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 de NSX Data Center for vSphere. 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 la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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

VMware Cloud 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 la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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 de NSX Data Center for vSphere

La capacidad de retransmisión de DHCP que ofrece NSX en el entorno de VMware Cloud Director permite aprovechar la infraestructura de DHCP existente dentro del entorno de VMware Cloud 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 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 de NSX Data Center for vSphere

El software NSX en el entorno de VMware Cloud 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 VMware Cloud 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 la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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**.

Administrar la traducción de direcciones de red en una puerta de enlace Edge de NSX Data Center for vSphere

El software NSX Data Center for vSphere en el entorno de VMware Cloud Director permite que las puertas de enlace Edge proporcionen un servicio de traducción de direcciones de red (Network Address Translation, NAT). Con esta capacidad, se reduce la cantidad de direcciones IP públicas que debe usar una organización para fines de seguridad y economía.

El servicio NAT de la puerta de enlace Edge proporciona la capacidad de asignar una dirección pública a una máquina virtual o un grupo de máquinas virtuales en una red privada. Para permitir que las puertas de enlace Edge proporcionen acceso a los servicios que se ejecutan en máquinas virtuales con direcciones privadas del centro de datos virtual de organización, debe configurar reglas NAT en las puertas de enlace Edge. En el caso más común, se asocia un servicio NAT con una interfaz de vínculo superior en una puerta de enlace Edge del entorno de VMware Cloud Director para que las direcciones en las redes de centros de datos virtuales de organización no queden expuestas en la red externa.

La configuración del servicio NAT se separa en reglas NAT de origen (Source NAT, SNAT) y reglas NAT de destino (Destination NAT, DNAT). Cuando se configura una regla SNAT o DNAT en una puerta de enlace Edge en el entorno de VMware Cloud Director, siempre se configura la regla desde la perspectiva del centro de datos virtual de organización. En concreto, eso significa que se deben configurar las reglas de las siguientes maneras:

- SNAT: el tráfico se transmite desde una máquina virtual en una red interna del centro de datos virtual de organización (origen) a través de Internet hasta la red externa (el destino). Una regla SNAT traduce la dirección IP de origen de los paquetes salientes de una red de centros de datos virtuales de organización que se envían a una red externa o a otra red de centros de datos virtuales de organización.
- DNAT: el tráfico se transmite desde Internet (origen) hasta una máquina virtual dentro del centro de datos virtual de organización (destino). Una regla DNAT traduce la dirección IP (y opcionalmente, el puerto) de los paquetes que recibe una red de centros de datos virtuales de organización de una red externa o de otra red de centros de datos virtuales de organización.

Puede configurar reglas NAT para crear un espacio de direcciones IP privadas dentro del centro de datos virtual de organización. Esta configuración ofrece la capacidad de mover un espacio de direcciones IP privadas de un centro de datos virtual de organización a otro. La configuración de reglas NAT permite utilizar las mismas direcciones IP privadas para máquinas virtuales de un centro de datos virtual de organización que se utilizaron en otro.

La capacidad de reglas NAT en el entorno de VMware Cloud Director admite lo siguiente:

- Crear subredes dentro de un espacio de direcciones IP privadas
- Crear varios espacios de direcciones IP privadas para una puerta de enlace Edge

- Configurar varias reglas NAT en varias interfaces de puerta de enlace Edge

Importante Debe configurar reglas NAT y de firewall en la puerta de enlace Edge para que sea posible acceder a las máquinas virtuales en una red de la puerta de enlace Edge. De forma predeterminada, las puertas de enlace Edge se implementan con reglas de firewall configuradas para denegar todo el tráfico de red desde y hacia las máquinas virtuales en las redes de puerta de enlace Edge. Además, la opción NAT está desactivada de forma predeterminada en las puertas de enlace Edge de modo que dichas puertas no pueden traducir las direcciones IP del tráfico entrante y saliente, a menos que se configure NAT en las puertas de enlace Edge. Se producirá un error al intentar hacer ping en una máquina virtual de una red después de configurar una regla NAT a menos que se agregue una regla de firewall para permitir el tráfico correspondiente.

Agregar una regla SNAT o DNAT

Puede crear una regla NAT (Source NAT, SNAT) de origen para cambiar la dirección IP de origen de pública a privada, o viceversa. Puede crear una regla NAT (Destination NAT, DNAT) de destino para cambiar la dirección IP de destino de pública a privada, o viceversa.

Al crear reglas NAT, puede especificar las direcciones IP originales y traducidas mediante los siguientes formatos:

- Dirección IP (por ejemplo, 192.0.2.0)
- Rango de direcciones IP (por ejemplo, 192.0.2.0-192.0.2.24)
- Dirección IP/máscara de subred (por ejemplo, 192.0.2.0/24)
- any

Cuando se configura una regla SNAT o DNAT en una puerta de enlace Edge en el entorno de VMware Cloud 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

Se deben haber agregado direcciones IP públicas a la interfaz de puerta de enlace Edge de NSX Data Center for vSphere en la que se 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 la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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 que se requiere o seleccione la dirección IP asignada en la lista.</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.
Dirección IP de origen	Si desea que la regla se aplique solo para el tráfico a un dominio específico, introduzca una dirección IP para este dominio o un rango de direcciones IP con formato CIDR. Si deja en blanco este cuadro de texto, la regla DNAT se aplicará a todas las direcciones IP que estén fuera de la subred local.
Puerto de origen	(Opcional) Introduzca un número de puerto para el origen.
Descripción	(Opcional) Introduzca una descripción significativa para la regla DNAT.

Opción	Descripción
Habilitado	Active el botón de alternancia para activar 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 original o el rango de direcciones IP que se aplicarán a esta regla, o bien seleccione la dirección IP asignada en la lista.</p> <p>Estas direcciones son las direcciones IP de una o varias máquinas virtuales para las que se configura la regla SNAT, de modo que puedan enviar tráfico a la red externa.</p>
IP/rango de origen traducido	<p>Escriba la dirección IP requerida.</p> <p>Esta dirección es siempre la dirección IP pública de la puerta de enlace para la que se va a configurar la regla SNAT. Especifica la dirección IP a la que se traducen las direcciones de origen (las máquinas virtuales) en paquetes salientes cuando envían tráfico a la red externa.</p>
Dirección IP de destino	(Opcional) Si desea que la regla se aplique solo para el tráfico a un dominio específico, introduzca una dirección IP para este dominio o un rango de direcciones IP con formato CIDR. Si deja en blanco este cuadro de texto, la regla SNAT se aplicará a todos los destinos fuera de la subred local.
Puerto de destino	(Opcional) Introduzca un número de puerto para el destino.
Descripción	(Opcional) Introduzca una descripción significativa para la regla SNAT.
Habilitado	Active el botón de alternancia para activar 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 de NSX Data Center for vSphere](#).

Configuración avanzada de enrutamiento para puertas de enlace Edge de NSX Data Center for vSphere

Puede configurar el enrutamiento estático y dinámico en las puertas de enlace Edge de NSX Data Center for vSphere.

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 Data Center for vSphere, consulte la documentación de NSX Data Center for vSphere.

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 Data Center for vSphere 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 de NSX Data Center for vSphere

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 la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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 de NSX Data Center for vSphere](#) 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 NSX Data Center for vSphere. 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 la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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 de NSX Data Center for vSphere](#).

Configurar OSPF

Es posible 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 de NSX Data Center for vSphere. Una aplicación habitual de OSPF en una puerta de enlace Edge en un entorno de VMware Cloud Director consiste en intercambiar información de enrutamiento entre puertas de enlace Edge en VMware Cloud 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 de NSX Data Center for vSphere.](#)

Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
 - a En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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.

- a 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.
- b Seleccione el identificador del área que se asignará a la interfaz seleccionada.
- c (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.

- d 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 de NSX Data Center for vSphere](#).

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

Es posible 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 de NSX Data Center for vSphere.

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 la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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 le 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 de NSX Data Center for vSphere](#).

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 de NSX Data Center for vSphere.

Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
 - a En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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 aprendiz	Seleccione el protocolo que va a aprender rutas de otros protocolos en este criterio de redistribución.

Opción	Descripción
Permitir el aprendizaje desde	Seleccione los tipos de redes desde los que se pueden aprender rutas para el protocolo seleccionado en la lista 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 con NSX Data Center for vSphere

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 proporciona alta disponibilidad de aplicaciones y 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 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 evita sobrecargas.

El equilibrador de carga de NSX admite 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 de NSX Data Center for vSphere 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.

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 capa

7 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

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 se ajuste a 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 la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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. 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> <hr/>
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**.

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 la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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	<p>Seleccione el tipo de protocolo usado para enviar solicitudes al servidor. La lista de parámetros obligatorios depende del protocolo seleccionado. No se pueden introducir parámetros que no sean aplicables para el protocolo seleccionado. Todos los demás parámetros son obligatorios.</p>
Habilitar acceso directo SSL	<p>Haga clic aquí para habilitar la autenticación SSL que se transferirá al servidor virtual.</p> <p>De lo contrario, la autenticación SSL se realizará en la dirección de destino.</p>
URL de redirección HTTP	<p>(HTTP y HTTPS) Introduzca la dirección URL a la que debe redirigirse el tráfico que llega a la dirección de destino.</p>

Opción	Descripción
Persistencia	<p>Especifique un mecanismo de persistencia para el perfil.</p> <p>La persistencia realiza el seguimiento de los datos de sesión y los almacena. Estos datos pueden ser, por ejemplo, el miembro de grupo específico que ha procesado una solicitud de cliente. Esto garantiza que las solicitudes de cliente se dirijan al mismo miembro de grupo durante toda una sesión o las sesiones posteriores. Las opciones son las siguientes:</p> <ul style="list-style-type: none"> ■ 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> ■ 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> ■ ID de sesión SSL <p>La persistencia del ID de sesión SSL está disponible cuando se habilita el acceso directo a SSL. La persistencia del ID de sesión SSL garantiza que las conexiones repetidas del mismo cliente se envíen al mismo servidor. La persistencia del ID de sesión permite el uso de la reanudación de la sesión SSL, lo que ahorra tiempo de procesamiento tanto para el cliente como para el servidor.</p>
Nombre de cookie	<p>(HTTP y HTTPS) Si ha especificado Cookie como el mecanismo de persistencia, introduzca el nombre de la cookie. La persistencia de cookie usa una cookie para identificar de manera exclusiva la sesión la primera vez que un cliente accede al sitio. El equilibrador de carga hace referencia a esta cookie cuando conecta solicitudes posteriores en la sesión, de modo que todas van al mismo servidor virtual.</p>

Opción	Descripción
Modo	<p>Seleccione el modo mediante el cual debe insertarse la cookie. Se admiten los siguientes modos:</p> <ul style="list-style-type: none"> ■ 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 app Para esta opción, el servidor no envía una cookie. En su lugar, envía la información de la sesión del usuario como una URL. Por ejemplo, <code>http://example.com/admin/UpdateUserServlet;jsessionid=0I24B9ASD7BSSD</code>, donde <code>jsessionid</code> es la información de sesión del usuario y se utiliza para la persistencia. No es posible ver la tabla de persistencia de Sesión de aplicación para solucionar problemas.
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> <p>Nota No se admite el uso de este encabezado si se habilitó el acceso directo a SSL.</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 Para mantener los cambios, haga clic en **Conservar**.

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

- Abra los servicios de puerta de enlace Edge.
 - En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - Seleccione la puerta de enlace Edge que desea editar y haga clic en **Servicios**.
- Desplácese hasta **Equilibrador de carga > Supervisión del servicio**.
- Haga clic en el botón **Crear** ().
- 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 activadas o desactivadas.</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 Para mantener los cambios, haga clic en **Conservar**.

Ejemplo: Extensiones admitidas para cada protocolo

Tabla 5-4. 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 <i>SECONDS</i> . El número puede tener el formato 10m para minutos, 10h para horas o 10d para días.
content-type= <i>STRING</i>	Especifica un tipo de medios para el encabezado Content-Type en las llamadas POST.
linespan	Permite que la expresión regular abarque líneas nuevas (debe preceder a -r o -R).
regex= <i>STRING</i> o ereg= <i>STRING</i>	Busca en la página una expresión regular que reemplaza a <i>STRING</i> en el ejemplo.
eregi= <i>STRING</i>	Busca en la página una expresión regular que no distingue mayúsculas de minúsculas que reemplaza a <i>STRING</i> en el ejemplo.
invert-regex	Devuelve CRITICAL cuando lo encuentra y OK cuando no lo encuentra.
proxy-authorization= <i>AUTH_PAIR</i>	Especifica el par nombre de usuario:contraseña en servidores proxy con autenticación básica.
useragent= <i>STRING</i>	Envía la cadena en el encabezado HTTP como User Agent.
header= <i>STRING</i>	Envía cualquier otra etiqueta en el encabezado HTTP. Utilícelo varias veces para encabezados adicionales.
onredirect=ok warning critical follow sticky stickyport	Indica cómo controlar páginas redirigidas. <i>sticky</i> es similar a <i>follow</i> , pero se queda con la dirección IP especificada. <i>stickyport</i> garantiza que el puerto permanezca igual.
pagesize= <i>INTEGER:INTEGER</i>	Especifica los tamaños de página máximo y mínimo necesarios en bytes.
warning=DOUBLE	Especifica el tiempo de respuesta en segundos que produce un estado de advertencia.
critical=DOUBLE	Especifica el tiempo de respuesta en segundos que produce un estado crítico.

Tabla 5-5. 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 5-6. Extensiones para protocolo TCP

Extensión de supervisión	Descripción
escape	Permite el uso de <code>\n</code> , <code>\r</code> , <code>\t</code> o <code>\</code> 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 <code>\r\n</code> 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 <code>any</code> .
quit=STRING	Envía una cadena al servidor para cerrar la conexión correctamente.
refuse=ok warn crit	Acepta rechazos de TCP con los estados <code>ok</code> , <code>warn</code> o <code>crit</code> . De forma predeterminada, utiliza el estado <code>crit</code> .
mismatch=ok warn crit	Acepta faltas de coincidencia de la cadena esperada con los estados <code>ok</code> , <code>warn</code> o <code>crit</code> . De forma predeterminada, utiliza el estado <code>warn</code> .
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 <code>#days</code> para la advertencia y el segundo valor es <code>critical</code> (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 la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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 <code>host</code> como el parámetro del algoritmo HTTP HEADER.
URL	El parámetro de URL especificado en el argumento se busca en la cadena de consulta de cada solicitud HTTP GET. Si al parámetro le sigue un signo igual (=) y un valor, al valor se le aplica hash y se divide por el peso total de los servidores en ejecución. El resultado determina el servidor que recibe la solicitud. Este proceso se utiliza para realizar un seguimiento de los identificadores de usuario de las solicitudes y asegurarse de que el mismo identificador de usuario se envíe siempre al mismo servidor, siempre que ningún servidor se active o desactive. Si no se encuentra ningún parámetro ni ningún valor, se aplica un algoritmo por turnos. El parámetro del algoritmo URL tiene una opción <code>urlParam=<url></code> .

6 Agregue miembros al grupo.

- a Haga clic en el botón **Agregar** (.
 - b Introduzca el nombre del miembro de grupo.
 - c Introduzca la dirección IP del miembro de grupo.
 - d Introduzca el puerto en el que el miembro recibirá el tráfico desde el equilibrador de carga.
 - e Introduzca el puerto de supervisión en el que el miembro recibirá las solicitudes de supervisión de estado.
 - f En el cuadro de texto **Ponderación**, escriba la proporción de tráfico que gestionará este miembro. Debe ser un número entero entre 1 y 256.
 - g (opcional) En el cuadro de texto **Conexiones máximas**, escriba el número máximo de conexiones simultáneas que el miembro podrá gestionar.

Cuando el número de solicitudes entrantes supera el valor máximo, las solicitudes se colocan en cola y el equilibrador de carga espera hasta que se libere una conexión.
 - h (opcional) En el cuadro de texto **Conexiones mínimas**, escriba el número mínimo de conexiones simultáneas que un miembro siempre debe aceptar.
 - i Haga clic en **Conservar** para agregar el nuevo miembro al grupo.
- La operación puede tardar un minuto en completarse.

- 7 (opcional) A fin de lograr que las direcciones IP de cliente sean visibles para los servidores back-end, seleccione **Transparente**.

Si no se selecciona **Transparente** (el valor predeterminado), los servidores back-end ven la dirección IP del origen del tráfico como la dirección IP interna del equilibrador de carga.

Cuando **Transparente** está seleccionado, la dirección IP de origen es la dirección IP real del cliente y la puerta de enlace Edge se debe establecer como la puerta de enlace predeterminada para garantizar que los paquetes devueltos pasen por la puerta de enlace Edge.

- 8 Para mantener los cambios, haga clic en **Conservar**.


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 la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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/2.2/configuration.html>.
- 6 Para mantener los cambios, haga clic en **Conservar**.

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 interfaz de vínculo superior o una puerta de enlace Edge interna de NSX Data Center for vSphere como 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 la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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 Para mantener los cambios, haga clic en **Conservar**.

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 de NSX Data Center for vSphere](#).

Configurar el acceso seguro mediante VPN en una puerta de enlace Edge de NSX Data Center for vSphere

Es posible configurar las capacidades de VPN que proporciona el software NSX Data Center for vSphere para las puertas de enlace Edge de NSX Data Center for vSphere. 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 VMware Cloud 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 VMware Cloud 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 de NSX Data Center for vSphere en un entorno de VMware Cloud Director permiten a los usuarios remotos conectarse 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 VMware Cloud 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 en una puerta de enlace Edge de NSX Data Center for vSphere](#).

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 de NSX Data Center for vSphere.

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 de NSX Data Center for vSphere, 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 de NSX Data Center for vSphere](#)

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 de NSX Data Center for vSphere](#)

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 activadas se instalarán 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 de NSX Data Center for vSphere](#)

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 de NSX Data Center for vSphere.

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 NSX Data Center for vSphere](#)

De forma predeterminada, el sistema establece algunos ajustes de VPN-Plus de SSL para una puerta de enlace Edge en el entorno de VMware Cloud Director. Puede utilizar la pantalla **Configuración general** en la pestaña **VPN-Plus de SSL** en el portal para tenants de VMware Cloud 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 de NSX Data Center for vSphere.

Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
 - a En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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 de NSX Data Center for vSphere](#).

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 de NSX Data Center for vSphere, 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 activado de forma predeterminada. Puede cambiar el nivel de los mensajes que se registran o desactivar 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 de NSX Data Center for vSphere](#).

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 de NSX Data Center for vSphere](#).

Crear un grupo de direcciones IP para usarlo con VPN-Plus de SSL en una puerta de enlace Edge de NSX Data Center for vSphere

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	Introduzca la máscara de red del grupo de direcciones IP (por ejemplo, 255.255.255.0).
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 activar o desactivar 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 de NSX Data Center for vSphere](#).

Agregar una red privada para usarla con VPN-Plus de SSL en una puerta de enlace Edge de NSX Data Center for vSphere

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 activadas se instalarán 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 activar 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 desactivar la optimización de TCP para esa red privada. Además, la red privada para dicho servidor FTP debe estar activada 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 de NSX Data Center for vSphere.

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 activada 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 activa 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	Active o desactive 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 de NSX Data Center for vSphere](#).

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 de NSX Data Center for vSphere](#).

Configurar un servicio de autenticación para VPN-Plus de SSL en una puerta de enlace Edge de NSX Data Center for vSphere

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 de NSX Data Center for vSphere](#).
- 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 de NSX Data Center for vSphere.

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 de NSX Data Center for vSphere](#).

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 activado o desactivado.
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 de NSX Data Center for vSphere. 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 activado o desactivado.

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) Desactive la reconexión automática.

La opción **Habilitar reconexión automática** está activada de forma predeterminada. Si la reconexión automática está activada, 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 desactivada de forma predeterminada. Si activa 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 NSX Data Center for vSphere

De forma predeterminada, el sistema establece algunos ajustes de VPN-Plus de SSL para una puerta de enlace Edge en el entorno de VMware Cloud Director. Puede utilizar la pantalla **Configuración general** en la pestaña **VPN-Plus de SSL** en el portal para tenants de VMware Cloud 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 de NSX Data Center for vSphere en un entorno de VMware Cloud Director son compatibles con el protocolo de seguridad de Internet (Internet Protocol Security, IPsec) de sitio a sitio para proteger los túneles VPN entre las redes de centros de datos virtuales de organización o 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 (AES256-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 la configuración del tamaño de la puerta de enlace Edge, desplácese hasta la puerta de enlace Edge y haga clic en el nombre de la puerta de enlace Edge.

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 de IPsec para una puerta de enlace Edge de NSX Data Center for vSphere.

2 Configurar conexiones de sitio de VPN de IPsec para la puerta de enlace Edge de NSX Data Center for vSphere

Utilice la pantalla **Sitios de VPN de IPsec** del portal para tenants de VMware Cloud 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 de NSX Data Center for vSphere

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 de IPsec para una puerta de enlace Edge de NSX Data Center for vSphere.

Procedimiento

1 Abra los servicios de puerta de enlace Edge.

- a En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
- b Seleccione la puerta de enlace Edge que desea editar 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 de NSX Data Center for vSphere](#).

Configurar conexiones de sitio de VPN de IPsec para la puerta de enlace Edge de NSX Data Center for vSphere

Utilice la pantalla **Sitios de VPN de IPsec** del portal para tenants de VMware Cloud 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 VMware Cloud Director.

- Las subredes locales y del mismo nivel especifican las redes a las que se conecta la VPN. Cuando se especifican dichas subredes en las configuraciones de sitios de VPN de IPsec, indique un rango de redes en lugar de una dirección IP específica. Utilice el formato CIDR (por ejemplo, **192.168.99.0/24**).
- El identificador del mismo nivel es un identificador que identifica de manera exclusiva el dispositivo remoto que finaliza la conexión de VPN (por lo general, su dirección IP pública). Para elementos del mismo nivel con autenticación de certificados, este identificador debe ser el nombre distintivo que se ha definido en el certificado del elemento del mismo nivel. Para elementos del mismo nivel de PSK, este identificador puede ser cualquier cadena. Una práctica recomendada en NSX es utilizar la dirección IP pública del dispositivo remoto o el FQDN como el identificador del mismo nivel. Si la dirección IP del mismo nivel es de otra red de centros de datos virtuales de organización, introduzca la dirección IP nativa del mismo nivel. Si NAT está configurada para el elemento del mismo nivel, debe escribir la dirección IP privada del elemento del mismo nivel.
- El endpoint del mismo nivel especifica la dirección IP pública del dispositivo remoto al que se va a conectar. El endpoint del mismo nivel puede ser una dirección diferente del identificador del mismo nivel si no se puede acceder directamente a la puerta de enlace del elemento del mismo nivel desde Internet, sino que se conecta a través de otro dispositivo. Si NAT está configurada para el elemento del mismo nivel, debe escribir la dirección IP pública que utilizan los dispositivos para NAT.
- El identificador local especifica la dirección IP pública de la puerta de enlace Edge del centro de datos virtual de organización. Puede introducir una dirección IP o un nombre de host junto con el firewall de la puerta de enlace Edge.
- El endpoint local especifica la red en el centro de datos virtual de organización en la que transmite la puerta de enlace Edge. Por lo general, la red externa de la puerta de enlace Edge es el endpoint local.

Requisitos previos

- [Desplazarse a la pantalla VPN de IPsec.](#)
- [Configurar VPN de IPsec.](#)
- Si decide utilizar un certificado global como el método de autenticación, compruebe que la autenticación de certificados esté habilitada en la pantalla **Configuración global**. Consulte [Especificar la configuración de VPN de IPsec global](#).

Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
 - a En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Servicios**.
- 2 En la pestaña **VPN de IPsec**, haga clic en **Sitios de VPN de IPsec**.
- 3 Haga clic en el botón **Agregar** ().
- 4 Configure los ajustes de la conexión de VPN de IPsec.

Opción	Acción
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.
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>

Opción	Acción
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>
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	<p>(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.</p>

Opción	Acción
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.

5 Haga clic en **Conservar**.

6 Haga clic en **Guardar cambios**.

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 de NSX Data Center for vSphere](#).

Habilitar el servicio VPN de IPsec en una puerta de enlace Edge de NSX Data Center for vSphere

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 de NSX Data Center for vSphere](#).

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 la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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 de una puerta de enlace Edge de NSX Data Center for vSphere](#).

Configurar VPN de capa 2

Las puertas de enlace Edge de NSX Data Center for vSphere en un entorno de VMware Cloud Director admiten VPN de capa 2. Con la VPN de capa 2, es posible 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.

NSX Data Center for vSphere proporciona las capacidades de VPN de capa 2 para una puerta de enlace Edge. Con la VPN de capa 2, es posible 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.

Desplazarse a la pantalla VPN de capa 2

Para comenzar a configurar el servicio VPN de capa 2 de una puerta de enlace Edge de NSX Data Center for vSphere, debe desplazarse a la pantalla **VPN de capa 2**.

Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
 - a En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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 de NSX Data Center for vSphere como un servidor VPN de capa 2](#).

Configurar la puerta de enlace Edge de NSX Data Center for vSphere 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.
- [Desplazarse a la pantalla VPN de capa 2](#).
- Si desea enlazar un certificado de servicio a la conexión de VPN de capa 2, compruebe que el certificado de servidor ya se ha cargado en la puerta de enlace Edge. Consulte [Agregar un certificado de servicio a la puerta de enlace Edge](#).
- Debe configurar la dirección IP de escucha del servidor, el puerto de escucha, el algoritmo de cifrado y al menos un sitio del mismo nivel para habilitar el servicio VPN de capa 2.

Procedimiento

- 1 En la pestaña **VPN de capa 2**, seleccione **Servidor** para el modo de VPN de capa 2.
- 2 En la pestaña **Servidor global**, ajuste los detalles de configuración global del servidor VPN de capa 2.

Opción	Acción
IP de escucha	Seleccione la dirección IP principal o secundaria de una interfaz externa de la puerta de enlace Edge.
Puerto de escucha	Edite el valor que se muestra según las necesidades de su organización. El puerto predeterminado para el servicio VPN de capa 2 es 443.
Algoritmo de cifrado	Seleccione el algoritmo de cifrado para la comunicación entre el servidor y el cliente.
Detalles del certificado de servicio	Haga clic en Cambiar certificado del servidor para seleccionar el certificado que se enlazará 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 .

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

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

5 Configure los ajustes para un sitio del mismo nivel de VPN de capa 2.

Opción	Acción
Habilitado	Habilite este sitio del mismo nivel.
Nombre	Introduzca un nombre único para el sitio del mismo nivel.
Descripción	(Opcional) Escriba una descripción.
ID de usuario	Introduzca el nombre de usuario y la contraseña con los que se autenticará el sitio del mismo nivel.
Contraseña	
Confirmar contraseña	
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.

6 Haga clic en **Conservar**.

7 Haga clic en **Guardar cambios**.

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 de NSX Data Center for vSphere](#).

Configurar la puerta de enlace Edge de NSX Data Center for vSphere 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**.
- 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**.

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 de NSX Data Center for vSphere](#).

Habilitar el servicio VPN de capa 2 en una puerta de enlace Edge de NSX Data Center for vSphere

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 de NSX Data Center for vSphere 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 de NSX Data Center for vSphere 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 de NSX Data Center for vSphere

Es posible quitar la configuración existente del servicio VPN de capa 2 de la puerta de enlace Edge. Esta acción también desactiva 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 desactivará el servicio VPN de capa 2 y se quitarán los detalles de configuración de la puerta de enlace Edge.

Administración de certificados SSL en una puerta de enlace Edge de NSX Data Center for vSphere

El software NSX Data Center for vSphere en el entorno de VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 Data Center for vSphere.
- 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 la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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 VMware Cloud 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>

Opción	Descripción
Nombre del estado o de la provincia	Escriba el nombre completo (no utilice abreviaturas) del estado, de la provincia, de la región o del territorio donde se registró legalmente la empresa.
Código de país	Escriba el nombre del país donde se registró legalmente la empresa.
Algoritmo de clave privada	Escriba el tipo de clave, RSA o DSA, para el certificado. Por lo general, se utiliza RSA. El tipo de clave define el algoritmo de cifrado para la comunicación entre los hosts. Nota VPN-Plus de SSL admite solamente certificados RSA.
Tamaño de clave	Escriba el tamaño de la clave en bits. El valor mínimo es de 2048 bits.
Descripción	(Opcional) Escriba una descripción para el certificado.

5 Haga clic en **Conservar**.

El sistema generará la solicitud CSR y agregará una nueva entrada con el tipo CSR a la lista en pantalla.

Resultados

En la lista en pantalla, al seleccionar una entrada con el tipo CSR, se mostrarán los detalles de la CSR en la pantalla. Puede copiar los datos de la CSR con formato PEM que se muestran y enviarlos a una entidad de certificación (Certificate Authority, CA) para obtener un certificado firmado por CA.

Pasos siguientes

Utilice la solicitud CSR para crear un certificado de servicio mediante una de estas dos opciones:

- Transmita la solicitud CSR a una entidad de certificación para obtener un certificado firmado por una CA. Cuando la entidad de certificación le envíe el certificado firmado, importe el certificado al sistema. Consulte [Importar el certificado firmado por CA correspondiente a la solicitud CSR generada para una puerta de enlace Edge](#).
- Utilice la solicitud CSR para crear un certificado autofirmado. Consulte [Configurar un certificado de servicio autofirmado](#).

Importar el certificado firmado por CA correspondiente a la solicitud CSR generada para una puerta de enlace Edge

Después de generar una solicitud de firma del certificado (Certificate Signing Request, CSR) y obtener el certificado firmado por una entidad de certificación en función de esa CSR, puede importar el certificado firmado por CA para que lo utilice la puerta de enlace Edge.

Requisitos previos

Compruebe que ha obtenido el certificado firmado por CA correspondiente a la solicitud CSR. Si la clave privada en el certificado firmado por CA no coincide con la de la CSR seleccionada, se producirá un error en el proceso de importación.

Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
 - a En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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 la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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 la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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 la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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 la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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.

Cuando el modo FIPS está activado, el tamaño de la clave de RSA debe ser mayor o igual que 2048 bits.

- 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) Introduzca 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 para puertas de enlace Edge de NSX Data Center for vSphere

El software NSX Data Center for vSphere del entorno de VMware Cloud Director proporciona la capacidad de definir conjuntos y grupos de determinadas entidades, que puede utilizar más adelante cuando especifique otras configuraciones relacionadas con la red, como en las reglas de firewall.

Crear un conjunto de direcciones IP para usarlas en las reglas de firewall y la configuración de retransmisión de DHCP

Un conjunto de direcciones IP es un grupo de direcciones IP que se puede crear en el nivel de un centro de datos virtual de organización. Es posible utilizar un conjunto de direcciones IP como origen o destino en una regla de firewall o en una configuración de retransmisión de DHCP.

Para crear un conjunto de direcciones IP, utilice la página **Objetos de agrupamiento** del portal para tenants de VMware Cloud Director. La página **Objetos de agrupamiento** está disponible en las pantallas Servicios y Puerta de enlace Edge.

Procedimiento

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

Opción	Acción
Abrir a través de servicios de puerta de enlace Edge	<ul style="list-style-type: none"> a Desplácese hasta Redes > Instancias de Edge. b Seleccione la puerta de enlace Edge que desea editar y haga clic en Configurar servicios. c Haga clic en Objetos de agrupamiento.
Abrir a través de servicios de seguridad	<ul style="list-style-type: none"> a Desplácese hasta Redes > Seguridad. b Seleccione el servicio de seguridad que desea editar y haga clic en Configurar servicios. c Haga clic en 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 (opcional) Si desea especificar el conjunto de direcciones IP mediante la página **Objetos de agrupamiento** en la pantalla Servicios, utilice el botón de alternancia **Herencia** para habilitar la herencia y permitir la visibilidad en los alcances subyacentes.

Herencia está habilitada de forma predeterminada.

6 Para guardar este conjunto de direcciones IP, haga clic en **Conservar**.

Resultados

El nuevo conjunto de direcciones IP puede seleccionarse como el origen o el destino en las reglas de firewall o en las configuraciones de retransmisión de DHCP.

Crear un conjunto de direcciones MAC para utilizarlas en las reglas de firewall

Un conjunto de direcciones MAC es un grupo de direcciones MAC que se puede crear en un nivel de centro de datos virtual de una organización. Los conjuntos de direcciones MAC se pueden usar como origen o como destino en una regla de firewall.

Para crear un conjunto de direcciones MAC, utilice la página **Objetos de agrupamiento** del portal para tenants de VMware Cloud Director. La página Objetos de agrupamiento está disponible en las pantallas **Servicios** y **Puerta de enlace Edge**.

Procedimiento

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

Opción	Acción
Abrir a través de servicios de puerta de enlace Edge	<ul style="list-style-type: none"> a Desplácese hasta Redes > Instancias de Edge. b Seleccione la puerta de enlace Edge que desea editar y haga clic en Configurar servicios. c Haga clic en Objetos de agrupamiento.
Abrir a través de servicios de seguridad	<ul style="list-style-type: none"> a Desplácese hasta Redes > Seguridad. b Seleccione el servicio de seguridad que desea editar y haga clic en Configurar servicios. c Haga clic en 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 (opcional) Si va a especificar el conjunto de direcciones MAC mediante la página **Objetos de agrupamiento** en la pantalla **Servicios**, utilice el botón de alternancia **Herencia** para habilitar la herencia y permitir la visibilidad en alcances subyacentes.

Herencia está habilitada de forma predeterminada.

6 Para guardar el conjunto de direcciones MAC, haga clic en **Conservar**.

Resultados

El nuevo conjunto de direcciones MAC puede seleccionarse como el origen o el destino en las reglas de firewall.

Ver los servicios disponibles para reglas de firewall

Puede ver la lista de servicios disponibles para su uso en reglas de firewall. En este contexto, un servicio es una combinación de un protocolo y un puerto.

Puede ver los servicios disponibles en la página **Objetos de agrupamiento** del portal para tenants de VMware Cloud Director. La página **Objetos de agrupamiento** está disponible en las pantallas **Servicios** y **Puerta de enlace Edge**.

No se pueden agregar nuevos servicios a la lista mediante el portal para tenants. El conjunto de servicios disponibles para su uso lo gestiona el administrador del sistema de VMware Cloud Director.

Procedimiento

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

Opción	Acción
Abbr a través de servicios de puerta de enlace Edge	<ul style="list-style-type: none"> a Desplácese hasta Redes > Instancias de Edge. b Seleccione la puerta de enlace Edge que desea editar y haga clic en Configurar servicios. c Haga clic en Objetos de agrupamiento.
Abbr a través de servicios de seguridad	<ul style="list-style-type: none"> a Desplácese hasta Redes > Seguridad. b Seleccione el servicio de seguridad que desea editar y haga clic en Configurar servicios. c Haga clic en 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 en la página **Objetos de agrupamiento** del portal para tenants de VMware Cloud Director. La página **Objetos de agrupamiento** está disponible en las pantallas **Servicios** y **Puerta de enlace Edge**.

No se pueden crear grupos de servicios mediante el portal para tenants. El conjunto de grupos de servicios disponibles para su uso lo gestiona el administrador del sistema de VMware Cloud Director.

Procedimiento

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

Opción	Acción
Abbr a través de servicios de puerta de enlace Edge	<ul style="list-style-type: none"> a Desplácese hasta Redes > Instancias de Edge. b Seleccione la puerta de enlace Edge que desea editar y haga clic en Configurar servicios. c Haga clic en Objetos de agrupamiento.
Abbr a través de servicios de seguridad	<ul style="list-style-type: none"> a Desplácese hasta Redes > Seguridad. b Seleccione el servicio de seguridad que desea editar y haga clic en Configurar servicios. c Haga clic en 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.

Estadísticas y logs de una puerta de enlace Edge de NSX Data Center for vSphere

Es posible ver las estadísticas y los logs de una puerta de enlace Edge de NSX Data Center for vSphere.

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 la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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 del tráfico que fluye a través de las interfaces de la puerta de enlace Edge seleccionada y gráficos del firewall. 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

- Compruebe que es **administrador de la organización** o que tiene asignada una función con un conjunto de derechos equivalente.
- Compruebe que su función incluya el derecho **Configurar el registro del sistema**.

Procedimiento

1 Abra los servicios de puerta de enlace Edge.

- a En la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
- b Seleccione la puerta de enlace Edge que desea editar 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 VMware Cloud Director ya configuró un servidor syslog para el entorno de VMware Cloud 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 de NSX Data Center for vSphere

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 la barra de navegación superior, haga clic en **Redes** y, a continuación, haga clic en **Puertas de enlace Edge**.
 - b Seleccione la puerta de enlace Edge que desea editar 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	De forma predeterminada, el nombre de usuario de SSH es admin .
Vuelva a escribir la contraseña	Introduzca el período de caducidad de la contraseña (en días).
Caducidad de contraseña	Introduzca el texto que se mostrará a los usuarios cuando inicien una conexión de SSH a la puerta de enlace Edge.
Titular de inicio de sesión	

- 4 Active el botón de alternancia **Habilitado**.

Pasos siguientes

Configure las reglas de firewall o NAT correspondientes para permitir un acceso SSH a esta puerta de enlace Edge.

Trabajar con etiquetas de seguridad para puertas de enlace Edge de NSX Data Center for vSphere

Las etiquetas de seguridad son etiquetas que se pueden asociar a una máquina virtual o a un grupo de máquinas virtuales. Las etiquetas de seguridad están diseñadas para usarse con grupos de seguridad. Una vez que se crean las etiquetas de seguridad, estas se asocian a un grupo de seguridad que se puede utilizar en reglas de firewall. Puede crear, editar o asignar una etiqueta de seguridad definida por el usuario. También puede ver las máquinas virtuales o los grupos de seguridad a los que se ha aplicado una etiqueta de seguridad determinada.


Un caso de uso común para las etiquetas de seguridad consiste en agrupar objetos de forma dinámica para simplificar las reglas de firewall. Por ejemplo, puede crear varias etiquetas de seguridad diferentes en función del tipo de actividad que espera que se produzca en una máquina virtual determinada. Crea una etiqueta de seguridad para los servidores de base de datos y otra para los servidores de correo electrónico. A continuación, aplica la etiqueta adecuada a las máquinas virtuales que alojan servidores de base de datos o servidores de correo electrónico. Posteriormente, puede asignar la etiqueta a un grupo de seguridad y escribir una regla de firewall correspondiente a ella, en la que aplica una configuración de seguridad diferente dependiendo de si la máquina virtual ejecuta un servidor de base de datos o un servidor de correo electrónico. Más adelante, si cambia la funcionalidad de la máquina virtual, puede quitarla de la etiqueta de seguridad en lugar de modificar la regla de firewall.

Crear y asignar etiquetas de seguridad

Puede crear una etiqueta de seguridad y asignarla a una máquina virtual o a un grupo de máquinas virtuales.

Cree una etiqueta de seguridad y asígnela a una máquina virtual o a un grupo de máquinas virtuales.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en **Redes**, seleccione **Seguridad**.
- 2 Seleccione un servicio de seguridad y haga clic en **Configurar servicios**.
- 3 Haga clic en la pestaña **Etiquetas de seguridad**.
- 4 Haga clic en el botón **Crear** () e introduzca un nombre para la etiqueta de seguridad.
- 5 (opcional) Escriba una descripción para la etiqueta de seguridad.
- 6 (opcional) Asigne la etiqueta de seguridad a una máquina virtual o a un grupo de máquinas virtuales.

En el menú desplegable **Examinar objetos del tipo**, la opción **Máquinas virtuales** está seleccionada de forma predeterminada.

- a Seleccione una máquina virtual del panel de la izquierda.
- b Para asignar la etiqueta de seguridad a la máquina virtual seleccionada, haga clic en la flecha derecha.

La máquina virtual se mueve al panel de la derecha se le asigna la etiqueta de seguridad.

- 7 Cuando termine de asignar la etiqueta a las máquinas virtuales seleccionadas, haga clic en **Conservar**.

Resultados

Se crea la etiqueta de seguridad y, si se ha elegido esta opción, se asigna a las máquinas virtuales seleccionadas.

Pasos siguientes

Las etiquetas de seguridad están diseñadas para funcionar con un grupo de seguridad. Para obtener más información sobre cómo crear grupos de seguridad, consulte [Crear un grupo de seguridad](#).

Cambiar la asignación de etiquetas de seguridad

Después de crear una etiqueta de seguridad, puede asignarla manualmente a las máquinas virtuales. También puede editar una etiqueta de seguridad para quitarla de las máquinas virtuales a las que ya se ha asignado.

Si ha creado las etiquetas de seguridad, puede asignarlas a las máquinas virtuales. Puede utilizar etiquetas de seguridad con el fin de agrupar máquinas virtuales para escribir reglas de firewall. Por ejemplo, puede asignar una etiqueta de seguridad a un grupo de máquinas virtuales con datos altamente confidenciales.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en **Redes**, seleccione **Seguridad**.
- 2 Seleccione un servicio de seguridad y haga clic en **Configurar servicios**.
- 3 Haga clic en la pestaña **Etiquetas de seguridad**.
- 4 En la lista de etiquetas de seguridad, seleccione la etiqueta de seguridad que desea editar y haga clic en el botón **Editar**.
- 5 Seleccione máquinas virtuales del panel de la izquierda y asígneles la etiqueta de seguridad haciendo clic en la flecha derecha.

Las máquinas virtuales del panel de la derecha se asignan a la etiqueta de seguridad.
- 6 Seleccione máquinas virtuales del panel de la derecha y quíteles la etiqueta haciendo clic en la flecha izquierda.

Las máquinas virtuales en el panel de la izquierda no tienen la etiqueta de seguridad asignada.
- 7 Cuando haya terminado de agregar los cambios, haga clic en **Conservar**.

Resultados

La etiqueta de seguridad se asigna a las máquinas virtuales seleccionadas.

Pasos siguientes

Las etiquetas de seguridad están diseñadas para funcionar con un grupo de seguridad. Para obtener más información sobre cómo crear grupos de seguridad, consulte [Crear un grupo de seguridad](#).

Ver las etiquetas de seguridad aplicadas

Puede ver las etiquetas de seguridad aplicadas a máquinas virtuales del entorno. También puede ver las etiquetas de seguridad aplicadas a grupos de seguridad en el entorno.

Requisitos previos

Se debe haber creado una etiqueta de seguridad y debe haberse aplicado a una máquina virtual o a un grupo de seguridad.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en **Redes**, seleccione **Seguridad**.
- 2 Seleccione un servicio de seguridad y haga clic en **Configurar servicios**.
- 3 Vea las etiquetas asignadas en la pestaña **Etiquetas de seguridad**.
 - a En la pestaña **Etiquetas de seguridad**, elija la etiqueta de seguridad para la que desea ver asignaciones y haga clic en el icono **Editar**.
 - b En **Asignar/desasignar MV** puede ver la lista de máquinas virtuales asignadas a la etiqueta de seguridad.
 - c Haga clic en **Descartar**.
- 4 Vea las etiquetas asignadas en la pestaña **Grupos de seguridad**.
 - a Haga clic en la pestaña **Objetos de agrupamiento** y haga clic en **Grupos de seguridad**.
 - b Seleccione un grupo de seguridad.
 - c En la lista bajo **Incluir miembros**, puede ver la etiqueta de seguridad asignada a un grupo de seguridad.

Resultados

Puede ver las etiquetas de seguridad existentes, así como las máquinas virtuales y los grupos de seguridad asociados. De este modo, puede determinar una estrategia de creación de reglas de firewall basadas en etiquetas y grupos de seguridad.

Editar una etiqueta de seguridad

Puede editar una etiqueta de seguridad definida por el usuario.

Si cambia el entorno o la función de una máquina virtual, es aconsejable que utilice una etiqueta de seguridad diferente para que las reglas de firewall sean correctas en la nueva configuración de máquina. Por ejemplo, si tiene una máquina virtual en la que ya no almacena datos confidenciales, se aconseja asignar una etiqueta de seguridad diferente para que las reglas de firewall que se aplican a datos confidenciales ya no se ejecuten en la máquina virtual.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en **Redes**, seleccione **Seguridad**.
- 2 Seleccione un servicio de seguridad y haga clic en **Configurar servicios**.
- 3 Haga clic en la pestaña **Etiquetas de seguridad**.
- 4 En la lista de etiquetas de seguridad, seleccione la etiqueta de seguridad que desea editar.
- 5 Haga clic en el botón **Editar**.
- 6 Edite el nombre y la descripción de la etiqueta de seguridad.
- 7 Asigne la etiqueta a las máquinas virtuales que seleccione o elimine la asignación de estas.
- 8 Para guardar los cambios, haga clic en **Conservar**.

Pasos siguientes

Si edita una etiqueta de seguridad, es posible que también deba editar reglas de firewall o un grupo de seguridad asociado. Para obtener más información acerca de los grupos de seguridad, consulte [Trabajar con grupos de seguridad para puertas de enlace Edge de NSX Data Center for vSphere](#).

Eliminar una etiqueta de seguridad

Puede eliminar una etiqueta de seguridad definida por el usuario.

Es aconsejable eliminar una etiqueta de seguridad si cambia la función o el entorno de la máquina virtual. Por ejemplo, si tiene una etiqueta de seguridad para bases de datos de Oracle, pero decide utilizar un servidor de base de datos diferente, puede quitar la etiqueta de seguridad para que las reglas de firewall que se aplican a las bases de datos de Oracle ya no se ejecuten en la máquina virtual.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en **Redes**, seleccione **Seguridad**.
- 2 Seleccione un servicio de seguridad y haga clic en **Configurar servicios**.
- 3 Haga clic en la pestaña **Etiquetas de seguridad**.
- 4 En la lista de etiquetas de seguridad, seleccione la etiqueta de seguridad que desea eliminar.
- 5 Haga clic en el botón **Eliminar**.
- 6 Para confirmar la eliminación, haga clic en **Aceptar**.

Resultados

Se eliminará la etiqueta de seguridad.

Pasos siguientes

Si elimina una etiqueta de seguridad, es posible que también deba editar las reglas de firewall o un grupo de seguridad asociado. Para obtener más información acerca de los grupos de seguridad, consulte [Trabajar con grupos de seguridad para puertas de enlace Edge de NSX Data Center for vSphere](#).

Trabajar con grupos de seguridad para puertas de enlace Edge de NSX Data Center for vSphere

Un grupo de seguridad es una colección de activos u objetos de agrupamiento, como máquinas virtuales, redes de centros de datos virtuales de organización o etiquetas de seguridad.

Los grupos de seguridad pueden tener criterios de pertenencia dinámica basados en etiquetas de seguridad, nombre de máquina virtual, nombre de sistema operativo invitado de máquina virtual o nombre de host invitado de máquina virtual. Por ejemplo, todas las máquinas virtuales que tengan la etiqueta de seguridad “web” se agregarán automáticamente a un grupo de seguridad específico destinado a servidores web. Después de crear un grupo de seguridad, se aplica una política de seguridad a dicho grupo.

Crear un grupo de seguridad

Puede crear grupos de seguridad definidos por el usuario.

Requisitos previos

Si desea utilizar etiquetas de seguridad con los grupos de seguridad, [Crear y asignar etiquetas de seguridad](#).

Procedimiento

- 1 Abra los servicios de seguridad.
 - a Desplácese hasta **Redes > Seguridad**.
 - b Seleccione el VDC de organización en el que desea aplicar la configuración de seguridad y haga clic en **Configurar servicios**.

El portal para tenants abrirá Servicios de seguridad.

- 2 Desplácese hasta **Objetos de agrupamiento > Grupos de seguridad**


Se abrirá la página **Grupos de seguridad**.

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

- 4 Escriba un nombre y, si lo desea, una descripción para el grupo de seguridad.

La descripción se muestra en la lista de grupos de seguridad, por lo que agregar una descripción significativa puede facilitar la rápida identificación del grupo de seguridad.

5 (opcional) Agregue un conjunto de miembros dinámicos.

- a Haga clic en el botón **Agregar** () que aparece en Conjuntos de miembros dinámicos.
- b Seleccione **Cualquiera** o **Todo** para buscar coincidencias con cualquiera de los criterios de la instrucción o con todos ellos, respectivamente.
- c Introduzca el primer objeto para el que se buscarán coincidencias.
Las opciones son **Etiqueta de seguridad**, **Nombre de SO invitado de MV**, **Nombre de MV** y **Nombre de host invitado de MV**.
- d Seleccione un operador, por ejemplo, **Contiene**, **Comienza con** o **Termina con**.
- e Introduzca un valor.
- f (opcional) Para agregar otra instrucción, use un operador booleano **And** u **Or**.

6 (opcional) Incluya miembros.

- a En el menú desplegable **Examinar objetos del tipo**, seleccione el tipo de objetos, como **Máquinas virtuales**, **Redes de VDC de organización**, **Conjuntos de direcciones IP**, **Conjuntos de direcciones MAC** o **Etiquetas de seguridad**.
- b Para incluir un objeto en la lista Incluir miembros, seleccione el objeto del panel izquierdo y muévelo al panel derecho haciendo clic en la flecha derecha.

7 (opcional) Excluya miembros.

- a En el menú desplegable **Examinar objetos del tipo**, seleccione el tipo de objetos, como **Máquinas virtuales**, **Redes de VDC de organización**, **Conjuntos de direcciones IP**, **Conjuntos de direcciones MAC** o **Etiquetas de seguridad**.
- b Para incluir un objeto en la lista Excluir miembros, seleccione el objeto del panel izquierdo y muévelo al panel derecho haciendo clic en la flecha derecha.

8 Para mantener los cambios, haga clic en **Conservar**.

Resultados

Ahora es posible utilizar el grupo de seguridad en reglas (por ejemplo, reglas de firewall).

Editar un grupo de seguridad

Puede editar los grupos de seguridad definidos por el usuario.

Procedimiento

- 1 Abra los servicios de seguridad.
 - a Desplácese hasta **Redes > Seguridad**.
 - b Seleccione el VDC de organización en el que desea aplicar la configuración de seguridad y haga clic en **Configurar servicios**.

El portal para tenants abrirá Servicios de seguridad.
- 2 Desplácese hasta **Objetos de agrupamiento > Grupos de seguridad**

Se abrirá la página **Grupos de seguridad**.
- 3 Seleccione el grupo de seguridad que desea editar.

Debajo de la lista de grupos de seguridad se muestran los detalles del grupo de seguridad.
- 4 (opcional) Edite el nombre y la descripción del grupo de seguridad.
- 5 (opcional) Agregue un conjunto de miembros dinámicos.
 - a Haga clic en el botón **Agregar** que aparece en **Conjuntos de miembros dinámicos**.
 - b Seleccione **Cualquiera** o **Todo** para buscar coincidencias con cualquiera de los criterios de la instrucción o con todos ellos, respectivamente.
 - c Introduzca el primer objeto para el que se buscarán coincidencias.

Las opciones son **Etiqueta de seguridad**, **Nombre de SO invitado de MV**, **Nombre de MV** y **Nombre de host invitado de MV**.
 - d Seleccione un operador, por ejemplo, **Contiene**, **Comienza con** o **Termina con**.
 - e Introduzca un valor.
 - f (opcional) Para agregar otra instrucción, use un operador booleano **And** u **Or**.
- 6 (opcional) Para editar un conjunto de miembros dinámicos, haga clic en el icono **Editar** que aparece junto al conjunto de miembros que desee modificar.
 - a Aplique los cambios necesarios al conjunto de miembros dinámicos.
 - b Haga clic en **Aceptar**.
- 7 (opcional) Para eliminar un conjunto de miembros dinámicos, haga clic en el icono **Eliminar** que aparece junto al conjunto de miembros que desee borrar.

- 8 (opcional) Para editar la lista de miembros incluidos, haga clic en el icono **Editar** que aparece junto a la lista Incluir miembros.
 - a En el menú desplegable **Examinar objetos del tipo**, seleccione el tipo de objetos, como **Máquinas virtuales**, **Redes de VDC de organización**, **Conjuntos de direcciones IP**, **Conjuntos de direcciones MAC** o **Etiquetas de seguridad**.
 - b Para incluir un objeto en la lista Incluir miembros, seleccione el objeto del panel izquierdo y muévelo al panel derecho haciendo clic en la flecha derecha.
 - c Para excluir un objeto de la lista Incluir miembros, seleccione el objeto del panel derecho y muévelo al panel izquierdo haciendo clic en la flecha izquierda.
- 9 (opcional) Para editar la lista de miembros excluidos, haga clic en el icono **Editar** que aparece junto a la lista Excluir miembros.
 - a En el menú desplegable **Examinar objetos del tipo**, seleccione el tipo de objetos, como **Máquinas virtuales**, **Redes de VDC de organización**, **Conjuntos de direcciones IP**, **Conjuntos de direcciones MAC** o **Etiquetas de seguridad**.
 - b Para incluir un objeto en la lista Excluir miembros, seleccione el objeto del panel izquierdo y muévelo al panel derecho haciendo clic en la flecha derecha.
 - c Para excluir un objeto de la lista Excluir miembros, seleccione el objeto del panel derecho y muévelo al panel izquierdo haciendo clic en la flecha izquierda.
- 10 Haga clic en **Guardar cambios**.

Se guardarán los cambios realizados en el grupo de seguridad.

Eliminar un grupo de seguridad

Puede eliminar un grupo de seguridad definido por el usuario.

Procedimiento

- 1 Abra los servicios de seguridad.
 - a Desplácese hasta **Redes > Seguridad**.
 - b Seleccione el VDC de organización en el que desea aplicar la configuración de seguridad y haga clic en **Configurar servicios**.

El portal para tenants abrirá Servicios de seguridad.
- 2 Desplácese hasta **Objetos de agrupamiento > Grupos de seguridad**

Se abrirá la página **Grupos de seguridad**.
- 3 Seleccione el grupo de seguridad que desea eliminar.
- 4 Haga clic en el botón **Eliminar**.
- 5 Para confirmar la eliminación, haga clic en **Aceptar**.

Resultados

Se eliminará el grupo de seguridad.

Administrar puertas de enlace Edge de NSX-T Data Center

Una puerta de enlace Edge de NSX-T Data Center proporciona una red de VDC de organización enrutada o una red de grupo de centros de datos con conectividad a las redes externas y las propiedades de administración de IP. También puede proporcionar servicios como firewall, NAT, VPN de IPSec, reenvío de DNS y DHCP, que está habilitado de forma predeterminada.

Redes externas dedicadas

Para proporcionar una topología de red completamente enrutada en un centro de datos virtual, el **administrador del sistema** puede dedicar una red externa a una puerta de enlace Edge de NSX-T Data Center específica.

En esta configuración existe una relación de uno a uno entre la red externa y la puerta de enlace Edge de NSX-T Data Center. Ninguna otra puerta de enlace Edge puede conectarse a la red externa.

Un enrutador lógico de nivel 0 o una puerta de enlace VRF de NSX-T Data Center asociados con una red externa dedicada forman parte de la pila de redes de tenant. La red externa se considera parte del dominio de enrutamiento de redes de VMware Cloud Director.

Una red externa dedicada proporciona servicios de enrutamiento de puerta de enlace Edge adicionales, como la administración de anuncios de rutas y la configuración de Border Gateway Protocol (BGP).

Puede decidir cuál de las redes asociadas a la puerta de enlace Edge deben anunciarse en la red externa. Esto permite combinar redes de centros de datos virtuales de organización completamente enrutadas y con enrutamiento NAT.

Agregar un conjunto de direcciones IP a una puerta de enlace Edge de NSX-T Data Center

Para crear reglas de firewall y agregarlas a una puerta de enlace Edge de NSX-T Data Center, primero debe crear conjuntos de direcciones IP. Los conjuntos de direcciones IP son grupos de objetos en los que se aplican las reglas de firewall. La combinación de varios objetos en conjuntos de direcciones IP ayuda a reducir la cantidad total de reglas de firewall que deben crearse.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, en la pestaña **Puertas de enlace Edge**.
- 2 Haga clic en la puerta de enlace NSX-T Edge.
- 3 En **Seguridad**, haga clic en la pestaña **Conjuntos de direcciones IP** y, a continuación, en **Nuevo**.

- 4 Introduzca un nombre y, si lo desea, una descripción del conjunto de direcciones IP.
- 5 Introduzca una dirección IP o un rango de direcciones IP para las máquinas virtuales que incluye el conjunto de direcciones IP, y haga clic en **Agregar**.
- 6 Para guardar el grupo de firewall, haga clic en **Guardar**.

Resultados

Ha creado un conjunto de direcciones IP y lo ha añadido a la puerta de enlace NSX-T Edge.

Pasos siguientes

[Agregar una regla de firewall de puerta de enlace Edge de NSX-T Data Center](#)

Agregar una regla de firewall de puerta de enlace Edge de NSX-T Data Center

Para controlar el tráfico de red entrante y saliente hacia y desde una puerta de enlace Edge de NSX-T Data Center, debe crear reglas de firewall.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, en la pestaña **Puertas de enlace Edge**.
- 2 Haga clic en la puerta de enlace Edge.
- 3 Si la pantalla **Firewall** no se puede ver en la sección Servicios, haga clic en la pestaña **Firewall**.
- 4 Haga clic en **Editar reglas**.
- 5 Haga clic en el botón **Nuevo en la parte superior**.

Se agregará una fila para la nueva regla encima de la regla seleccionada.

- 6 Configure la regla de firewall.

Opción	Descripción
Nombre	Escriba un nombre para la regla.
Estado	Para habilitar la regla tras la creación, desactive el botón de alternancia Estado .
Aplicaciones	(Opcional) Para seleccionar un perfil de puerto específico al que se aplica la regla, active el botón de alternancia Aplicaciones y haga clic en Guardar .
Origen	<p>Seleccione una opción y haga clic en Conservar.</p> <ul style="list-style-type: none"> ■ Para permitir o denegar el tráfico desde cualquier dirección de origen, active Cualquier origen. ■ Para permitir o denegar el tráfico desde grupos de firewall específicos, seleccione los grupos de firewall de la lista.

Opción	Descripción
Destino	<p>Seleccione una opción y haga clic en Conservar.</p> <ul style="list-style-type: none"> ■ Para permitir o denegar el tráfico a cualquier dirección de destino, active Cualquier destino. ■ Para permitir o denegar el tráfico hacia grupos de firewall específicos, seleccione los grupos de firewall de la lista.
Acción	<p>En el menú desplegable Acción, seleccione una opción.</p> <ul style="list-style-type: none"> ■ Para permitir el tráfico desde o hacia los orígenes, los destinos y los servicios especificados, seleccione Aceptar. ■ Para bloquear el tráfico desde o hacia los orígenes, los destinos y los servicios especificados, sin notificar al cliente bloqueado, seleccione Descartar. ■ Para bloquear el tráfico desde o hacia los orígenes, los destinos y los servicios especificados, y para notificar al cliente bloqueado que se rechazó el tráfico, seleccione Rechazar.
Protocolo IP	Seleccione si desea aplicar la regla al tráfico de IPv4 o IPv6.
Dirección	<p>Seleccione la dirección de tráfico en la que se va a aplicar la regla.</p> <p>Nota En VMware Cloud Director 10.2.1 y versiones posteriores, esta opción ya no está disponible.</p>
Habilite el registro.	Para que se registre la traducción de direcciones realizada por esta regla, active el botón de alternancia Habilitar registro .

7 Haga clic en **Guardar**.

8 Para configurar reglas adicionales, repita estos pasos.

Resultados

Una vez creadas las reglas de firewall, estas aparecen en la lista de reglas de firewall de la puerta de enlace Edge. Puede subir, bajar, editar o eliminar las reglas como sea necesario.

Agregar una regla SNAT o una regla DNAT a una puerta de enlace NSX-T Edge

Para cambiar la dirección IP de origen de una dirección IP privada a una pública, cree una regla NAT (SNAT) de origen. Para cambiar la dirección IP de destino de una dirección IP pública a una privada, cree una regla NAT de destino (Destination NAT, DNAT).

Cuando se configura una regla SNAT o una regla DNAT en una puerta de enlace Edge en el entorno de VMware Cloud Director, siempre se configura la regla desde la perspectiva del VDC de la organización.

Una regla SNAT traduce la dirección IP de origen de los paquetes enviados a partir de una red de VDC de organización a una red externa o a otra red de VDC de organización.

Una regla SIN SNAT impide la traducción de la dirección IP interna de los paquetes enviados desde un VDC de organización a una red externa o a otra red de VDC de organización.

Una regla DNAT traduce la dirección IP (y, opcionalmente, el puerto) de los paquetes recibidos por una red de VDC de organización que provienen de una red externa o de otra red de VDC de organización.

Una regla SIN DNAT impide la traducción de la dirección IP externa de los paquetes que recibe un VDC de organización desde una red externa u otra red de VDC de organización.

VMware Cloud Director admite la redistribución automática de rutas cuando se utilizan los servicios NAT en una puerta de enlace Edge de NSX-T Data Center.

Importante Si utiliza clústeres de Tanzu Kubernetes, anote la regla SNAT del sistema creada en la puerta de enlace Edge para evitar crear una regla conflictiva.

Requisitos previos

Las direcciones IP públicas deben haberse agregado a la interfaz de puerta de enlace Edge en la que desea agregar la regla.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, en la pestaña **Puertas de enlace Edge**.
- 2 Haga clic en la puerta de enlace Edge y, en **Servicios**, haga clic en **NAT**.
- 3 Para agregar una regla, haga clic en **Nueva**.
- 4 Configure una regla SNAT o SIN SNAT (del interior al exterior).

Opción	Descripción
Nombre	Introduzca un nombre significativo para la regla.
Descripción	(Opcional) Introduzca una descripción para la regla.
Tipo de interfaz	En el menú desplegable, seleccione SNAT o SIN SNAT.
IP externa	Según el tipo de regla que esté creando, elija una de las siguientes opciones. <ul style="list-style-type: none"> ■ Si va a crear una regla SNAT, introduzca la dirección IP pública de la puerta de enlace Edge para la que configurará la regla SNAT. ■ Si va a crear una regla SIN SNAT, deje vacío el cuadro de texto.
IP interna	Introduzca la dirección IP o una lista de direcciones IP de las máquinas virtuales para las que va a configurar SNAT, de modo que puedan enviar tráfico a la red externa.

Opción	Descripción
IP de destino	(Opcional) Si desea que la regla se aplique solo para el tráfico a un dominio específico, introduzca una dirección IP para este dominio o una lista de direcciones IP. Si deja en blanco este cuadro de texto, la regla SNAT se aplicará a todos los destinos fuera de la subred local.
Configuración avanzada (opcional)	<p>Haga clic en la pestaña Configuración avanzada para ver ajustes adicionales.</p> <p>Estado</p> <p>Para activar la regla tras crearla, active la opción Estado.</p> <p>Registro</p> <p>Para que se registre la traducción de direcciones realizada por esta regla, active la opción Registro.</p> <p>Prioridad</p> <p>Si una dirección tiene varias reglas NAT, puede asignar diferentes prioridades a estas reglas para determinar el orden en el que se aplican. Un valor inferior significa una prioridad más alta para esta regla.</p> <p>Coincidencia de firewall</p> <p>Puede establecer una regla de coincidencia de firewall para determinar cómo se aplica el firewall durante NAT. En el menú desplegable, seleccione una de las siguientes opciones.</p> <ul style="list-style-type: none"> ■ Para aplicar reglas de firewall a la dirección interna de una regla NAT, seleccione Coincidir con dirección interna. ■ Para aplicar reglas de firewall a la dirección externa de una regla NAT, seleccione Coincidir con dirección externa. ■ Para omitir la aplicación de reglas de firewall, seleccione Omitir.

5 Configure una regla DNAT o SIN DNAT (del exterior al interior).

Opción	Descripción
Nombre	Introduzca un nombre significativo para la regla.
Descripción	(Opcional) Introduzca una descripción para la regla.
Tipo de interfaz	En el menú desplegable, seleccione DNAT o SIN DNAT.
IP externa	<p>Introduzca la dirección IP pública de la puerta de enlace Edge para la que se va a configurar la regla DNAT.</p> <p>Las direcciones IP que introduzca deben estar subasignadas a la puerta de enlace Edge.</p>
Puerto externo	(Opcional) Introduzca el puerto al que se traduce la regla DNAT para los paquetes entrantes a las máquinas virtuales.
IP interna	<p>Según el tipo de regla que esté creando, elija una de las siguientes opciones.</p> <ul style="list-style-type: none"> ■ Si va a crear una regla DNAT, introduzca la dirección IP o una lista de direcciones IP de las máquinas virtuales para las que configurará DNAT, de modo que puedan recibir tráfico de la red externa. ■ Si va a crear una regla SIN DNAT, deje vacío el cuadro de texto.

Opción	Descripción
Aplicación	<p>(Opcional) Seleccione un perfil de puerto de aplicación específico al cual se va a aplicar la regla.</p> <p>El perfil de puerto de aplicación incluye un puerto y un protocolo que el tráfico entrante utiliza en la puerta de enlace Edge para conectarse a la red interna.</p>
Configuración avanzada (opcional)	<p>Haga clic en la pestaña Configuración avanzada para ver ajustes adicionales.</p> <p>Estado</p> <p>Para activar la regla tras crearla, active la opción Estado.</p> <p>Registro</p> <p>Para que se registre la traducción de direcciones realizada por esta regla, active la opción Registro.</p> <p>Prioridad</p> <p>Si una dirección tiene varias reglas NAT, puede asignar diferentes prioridades a estas reglas para determinar el orden en el que se aplican. Un valor inferior significa una prioridad más alta para esta regla.</p> <p>Coincidencia de firewall</p> <p>Puede establecer una regla de coincidencia de firewall para determinar cómo se aplica el firewall durante NAT. En el menú desplegable, seleccione una de las siguientes opciones.</p> <ul style="list-style-type: none"> ■ Para aplicar reglas de firewall a la dirección interna de una regla NAT, seleccione Coincidir con dirección interna. ■ Para aplicar reglas de firewall a la dirección externa de una regla NAT, seleccione Coincidir con dirección externa. ■ Para omitir la aplicación de reglas de firewall, seleccione Omitir.

6 Haga clic en **Guardar**.

7 Para configurar reglas adicionales, repita estos pasos.

Configurar un servicio de reenviador de DNS en una puerta de enlace NSX-T Edge

Para reenviar consultas DNS a servidores DNS externos, configure un reenviador DNS.

Como parte de la configuración del servicio de reenviador DNS, también puede agregar zonas de reenviador condicional. Una zona de reenviador condicional se configura como una lista que contiene hasta cinco zonas de DNS de FQDN. Si una consulta de DNS coincide con un nombre de dominio de esa lista, la consulta se reenvía a los servidores de la zona de reenviador correspondiente.

Procedimiento

1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, en la pestaña **Puertas de enlace Edge**.

- 2 Haga clic en la puerta de enlace Edge y, en **Administración de direcciones IP**, haga clic en **DNS**.
- 3 En la sección **Reenviador DNS**, haga clic en **Editar**.
- 4 Para habilitar el servicio de reenviador DNS, active el botón de alternancia **Estado**.
- 5 Introduzca un nombre y, si lo desea, una descripción para la zona de DNS predeterminada.
- 6 Introduzca una o varias direcciones IP de servidor ascendente, separadas por comas.
- 7 Haga clic en **Guardar**.
- 8 (opcional) Agregue una zona de reenviador condicional.
 - a En la sección **Zona de reenviador condicional**, haga clic en **Agregar**.
 - b Introduzca un nombre para la zona de reenviador.
 - c Introduzca una o varias direcciones IP de servidor ascendente, separadas por comas.
 - d Introduzca uno o varios nombres de dominio separados por comas y haga clic en **Guardar**.

Crear perfiles de puerto de aplicación personalizados

Para crear reglas de firewall y NAT, puede usar perfiles de puerto de aplicación preconfigurados y perfiles de puerto de aplicación personalizados.

Los perfiles de puerto de aplicación incluyen una combinación de un protocolo y un puerto (o un grupo de puertos) que se utiliza para los servicios de firewall y NAT en la puerta de enlace Edge. Además de los perfiles de puerto predeterminados que están preconfigurados para NSX-T Data Center, puede crear perfiles de puerto de aplicación personalizados.

Cuando se crea un perfil de puerto de aplicación personalizado en una puerta de enlace Edge, este se vuelve visible para todas las otras puertas de enlace Edge de NSX-T Data Center que se encuentran en el mismo VDC de organización.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, en la pestaña **Puertas de enlace Edge**.
- 2 Haga clic en la puerta de enlace Edge.
- 3 En **Seguridad**, haga clic en **Perfiles de puerto de aplicación**.
- 4 En la sección **Aplicaciones personalizadas**, haga clic en **Nueva**.
- 5 Introduzca un nombre y, si lo desea, una descripción para el perfil de puerto de aplicación.
- 6 Seleccione un protocolo del menú desplegable.
- 7 Introduzca un puerto o un rango de puertos separados por comas y haga clic en **Guardar**.

Pasos siguientes

Utilice los perfiles de puerto de aplicación para crear reglas de firewall y NAT. Consulte [Agregar una regla de firewall de puerta de enlace Edge de NSX-T Data Center](#) y [Agregar una regla SNAT o una regla DNAT a una puerta de enlace NSX-T Edge](#).

VPN de IPSec basada en políticas para puertas de enlace Edge de NSX-T Data Center

A partir de la versión 10.1, VMware Cloud Director admite la VPN de IPSec basada en políticas de sitio a sitio entre una instancia de puerta de enlace Edge de NSX-T Data Center y un sitio remoto.

La VPN de IPSec ofrece conectividad de sitio a sitio entre una puerta de enlace Edge y sitios remotos que también utilizan NSX-T Data Center o tienen enrutadores de hardware o puertas de enlace VPN de terceros compatibles con IPSec.

La VPN de IPSec basada en políticas requiere la aplicación de una política de VPN a los paquetes para determinar qué tráfico debe protegerse mediante IPSec antes de pasar a través de un túnel VPN. Este tipo de VPN se considera estática debido a que, cuando se cambian la configuración y la topología de una red local, la configuración de política VPN también debe actualizarse para reflejar los cambios.

Las puertas de enlace Edge de NSX-T Data Center admiten la configuración de túnel dividida, con prioridad de enrutamiento para el tráfico IPSec.

VMware Cloud Director admite la redistribución automática de rutas cuando se utiliza la VPN de IPSec en una puerta de enlace NSX-T Edge.

Configurar la VPN de IPSec basada en políticas de NSX-T

Si lo considera conveniente, puede configurar la conectividad de sitio a sitio entre los sitios remotos y una puerta de enlace Edge de NSX-T Data Center. Los sitios remotos deben utilizar NSX-T Data Center y tener enrutadores de hardware de terceros o puertas de enlace VPN compatibles con IPSec.

VMware Cloud Director admite la redistribución automática de rutas cuando se configura VPN de IPSec en una puerta de enlace Edge de NSX-T Data Center.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, en la pestaña **Puertas de enlace Edge**.
- 2 Haga clic en la puerta de enlace Edge.
- 3 En **Servicios**, haga clic en **VPN de IPSec**.
- 4 Para configurar un túnel VPN de IPSec, haga clic en **Nuevo**.
- 5 Introduzca un nombre y, si lo desea, una descripción del túnel VPN de IPSec.
- 6 Para habilitar el túnel tras su creación, active la opción **Habilitado**.

- 7 Elija una clave compartida previamente que se debe introducir.

Nota Debe utilizarse la misma clave compartida previamente en el otro extremo del túnel VPN de IPSec.

- 8 Introduzca una de las direcciones IP disponibles para la puerta de enlace Edge del endpoint local.

Nota La dirección IP debe ser la dirección IP principal de la puerta de enlace Edge o una dirección IP asignada de forma independiente a la puerta de enlace Edge desde la red externa.

- 9 Introduzca al menos una dirección de subred IP local con la notación de CIDR para utilizarla en el túnel VPN de IPSec.
- 10 Introduzca la dirección IP del sitio remoto.
- 11 Introduzca al menos una dirección de subred IP remota con la notación de CIDR para utilizarla en el túnel VPN de IPSec.
- 12 (opcional) Active la opción **Registro** para habilitar esta función.
- 13 Haga clic en **Guardar**.
- 14 Para comprobar que el túnel funciona, selecciónelo y haga clic en **Ver estadísticas**.

Si un túnel funciona, en **Estado del túnel** y **Estado del servicio IKE** aparece **Accesible**.

Resultados

El túnel VPN de IPSec recién creado aparece en la vista **VPN de IPSec** y se genera con un perfil de seguridad predeterminado.

Pasos siguientes

Puede editar la configuración del túnel VPN de IPSec y personalizar su perfil de seguridad como guste.

Personalizar el perfil de seguridad de un túnel VPN de IPSec

Si decide no utilizar el perfil de seguridad que genera el sistema y se asignó al túnel VPN de IPSec cuando se creó, puede personalizarlo.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, en la pestaña **Puertas de enlace Edge**.
- 2 Haga clic en la puerta de enlace Edge.
- 3 En **Servicios**, haga clic en **VPN de IPSec**.
- 4 Seleccione el túnel VPN de IPSec y haga clic en **Personalización del perfil de seguridad**.

5 Configure los perfiles IKE.

Los perfiles de intercambio de claves por red (Internet Key Exchange, IKE) ofrecen información sobre los algoritmos que se utilizan para autenticar, cifrar y establecer un secreto compartido entre los sitios de red cuando se establece un túnel IKE.

- a Seleccione una versión del protocolo IKE para configurar una asociación de seguridad (Security Association, SA) en el conjunto de protocolos IPSec.

Opción	Descripción
IKEv1	Cuando se selecciona esta opción, se inicia VPN de IPSec y responde únicamente al protocolo IKEv1.
IKEv2	La opción predeterminada. Cuando se selecciona esta versión, se inicia VPN de IPSec y responde únicamente al protocolo IKEv2.
IKE-Flex	Cuando se selecciona esta opción, si se produce un error al establecer el túnel con el protocolo IKEv2, el sitio de origen no retrocede e inicia una conexión con el protocolo IKEv1. Si el sitio remoto inicia una conexión con el protocolo IKEv1, se acepta la conexión.

- b Seleccione un algoritmo de cifrado compatible para utilizarlo durante la negociación de intercambio de claves por red (Internet Key Exchange, IKE).
- c En el menú desplegable **Resumen**, seleccione un algoritmo de hash seguro para utilizarlo durante la negociación de IKE.
- d En el menú desplegable **Grupo Diffie-Hellman**, seleccione un esquema de criptografía que permita establecer un secreto compartido al sitio de mismo nivel y a la puerta de enlace Edge a través de un canal de comunicaciones no seguro.
- e (opcional) En el cuadro de texto **Duración de la asociación**, modifique el número predeterminado de segundos que deben transcurrir antes de que se restablezca el túnel de IPSec.

6 Configure el túnel VPN de IPSec.

- a Para habilitar la confidencialidad directa total, active la opción correspondiente.
- b Seleccione una política de desfragmentación.

La política de desfragmentación ayuda a procesar los bits de desfragmentación presentes en el paquete interno.

Opción	Descripción
Copiar	Copia el bit de desfragmentación del paquete IP interno en el paquete externo.
Borrar	Ignora el bit de desfragmentación presente en el paquete interno.

- c Seleccione un algoritmo de cifrado compatible para utilizarlo durante la negociación de intercambio de claves por red (Internet Key Exchange, IKE).

- d En el menú desplegable **Resumen**, seleccione un algoritmo de hash seguro para utilizarlo durante la negociación de IKE.
 - e En el menú desplegable **Grupo Diffie-Hellman**, seleccione un esquema de criptografía que permita establecer un secreto compartido al sitio de mismo nivel y a la puerta de enlace Edge a través de un canal de comunicaciones no seguro.
 - f (opcional) En el cuadro de texto **Duración de la asociación**, modifique el número predeterminado de segundos que deben transcurrir antes de que se restablezca el túnel de IPSec.
- 7 (opcional) En el cuadro de texto **Intervalo de sondeo**, modifique el número predeterminado de segundos dedicados a la detección de elementos del mismo nivel desactivados.
- 8 Haga clic en **Guardar**.

Resultados

En la vista VPN de IPSec, el perfil de seguridad del túnel VPN de IPSec se muestra como **Definido por el usuario**.

Configurar servicios de red externa dedicada

Para proporcionar una topología de red completamente enrutada en un centro de datos virtual, el **administrador del sistema** puede dedicar una red externa a una puerta de enlace Edge de NSX-T Data Center específica.

Si utiliza una red externa dedicada, puede configurar servicios de enrutamiento adicionales, como la administración de anuncios de rutas y la configuración de Border Gateway Protocol (BGP).

Procedimiento

1 Administrar el anuncio de rutas

Con el anuncio de rutas es posible crear un entorno de red completamente enrutado en un centro de datos virtual (Virtual Data Center, VDC) de organización.

2 Configurar los ajustes generales de BGP

Puede configurar una conexión interna o externa de Border Gateway Protocol (iBGP y eBGP, respectivamente) entre una puerta de enlace Edge de NSX-T Data Center que tenga una red externa dedicada y un enrutador en la infraestructura física.

3 Crear una lista de prefijos de IP

Puede crear listas de prefijos de IP que contengan una o varias direcciones IP. Utilice estas listas para asignar vecinos de BGP con permisos de acceso para el anuncio de rutas.

4 Agregar un vecino de BGP

Puede configurar ajustes individuales de los vecinos de enrutamiento de BGP al agregarlos.

Administrar el anuncio de rutas

Con el anuncio de rutas es posible crear un entorno de red completamente enrutado en un centro de datos virtual (Virtual Data Center, VDC) de organización.

Puede decidir cuál de las subredes de red asociadas a la puerta de enlace Edge de NSX-T Data Center debe anunciarse en la red externa dedicada.

Si no se agrega ninguna subred al filtro de anuncio, tampoco se anuncia la ruta correspondiente a la red externa, de modo que la subred permanece privada.

Nota VMware Cloud Director anuncia todas las redes de VDC de organización de la ruta anunciada. Por ello, no es necesario crear un filtro para cada subred de una red anunciada.

El anuncio de rutas se configura automáticamente en la puerta de enlace Edge de NSX-T Data Center.

VMware Cloud Director admite la redistribución automática de rutas cuando se utiliza el anuncio de estas en una puerta de enlace NSX-T Edge. La redistribución de rutas se configura automáticamente en el enrutador lógico de nivel 0, que representa la red externa dedicada.

Requisitos previos

- Compruebe que el **administrador del sistema** ha dedicado una red externa a una puerta de enlace Edge de NSX-T Data Center en la organización.
- Compruebe que es **administrador de la organización** o que tiene asignada una función con un conjunto de derechos equivalente.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, en la pestaña **Puertas de enlace Edge**.
- 2 Haga clic en la puerta de enlace Edge.
- 3 En **Enrutamiento**, haga clic en **Anuncio de rutas** y en **Editar**.
- 4 Para agregar una subred que debe anunciarse, haga clic en **Agregar**.
- 5 Agregue una subred IPv4 o IPv6.

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

Configurar los ajustes generales de BGP

Puede configurar una conexión interna o externa de Border Gateway Protocol (iBGP y eBGP, respectivamente) entre una puerta de enlace Edge de NSX-T Data Center que tenga una red externa dedicada y un enrutador en la infraestructura física.

BGP toma decisiones de enrutamiento central mediante una tabla de redes IP, o prefijos, que designan varias rutas entre sistemas autónomos (Autonomous System, AS).

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.

Nota En una puerta de enlace Edge que está conectada a una red externa respaldada por una puerta de enlace VRF, el número de AS local y la configuración de reinicio correcto son de solo lectura. El **administrador del sistema** puede editar esta configuración en la puerta de enlace de nivel 0 principal en NSX-T Data Center.

Requisitos previos

- Compruebe que el **administrador del sistema** ha dedicado una red externa a una puerta de enlace Edge de NSX-T Data Center en la organización.
- Compruebe que es **administrador de la organización** o que tiene asignada una función con un conjunto de derechos equivalente.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, en la pestaña **Puertas de enlace Edge**.
- 2 Haga clic en la puerta de enlace Edge.
- 3 En **Enrutamiento**, haga clic en **BGP** y, en **Configuración**, haga clic en **Editar**.
- 4 Active la opción **Estado** para activar BGP.
- 5 Introduzca el número de identificador de sistema autónomo (Autonomous System, AS) que se utilizará en la función de AS local del protocolo.

VMware Cloud Director asigna el número de AS local a la puerta de enlace Edge. La puerta de enlace Edge anuncia este identificador cuando se conecta con los vecinos de BGP en otros sistemas autónomos.

- 6 En el menú desplegable, seleccione una opción **Modo de reinicio correcto**.

Opción	Descripción
Auxiliar y reinicio correcto	<p>No se recomienda activar la capacidad de reinicio correcto en la puerta de enlace Edge, ya que los elementos del mismo nivel de BGP de todas las puertas de enlace siempre están activos.</p> <p>En caso de producirse una conmutación por error, la capacidad de reinicio correcto aumenta el tiempo que tarda un vecino remoto en seleccionar una puerta de enlace de nivel 0 alternativa. Esto retrasa la convergencia basada en BFD.</p> <p>Nota La configuración de puerta de enlace Edge se aplica a todos los vecinos de BGP (si la configuración específica de vecino no la reemplaza).</p>
Solo auxiliar	<p>Resulta útil para reducir o eliminar la interrupción del tráfico asociado a rutas que se han aprendido de un vecino capaz de reiniciarse correctamente. El vecino debe ser capaz de conservar su tabla de reenvío mientras se reinicia.</p>
Deshabilitar	<p>Desactive el modo de reinicio correcto en la puerta de enlace Edge.</p>

- 7 (opcional) Cambie el valor predeterminado del temporizador de reinicio correcto.
- 8 (opcional) Cambie el valor predeterminado del temporizador de ruta obsoleta.
- 9 Active la opción **ECMP** para activar este tipo de enrutamiento.
- 10 Haga clic en **Guardar**.

Pasos siguientes

- [Crear una lista de prefijos de IP](#)
- [Agregar un vecino de BGP](#)

Crear una lista de prefijos de IP

Puede crear listas de prefijos de IP que contengan una o varias direcciones IP. Utilice estas listas para asignar vecinos de BGP con permisos de acceso para el anuncio de rutas.

Se hace referencia a las listas de prefijos de IP con a través de filtros de vecinos de BGP para limitar el número de actualizaciones de BGP que se intercambian los elementos del mismo nivel de BGP. Mediante el filtrado de rutas, puede reducir la cantidad de recursos del sistema necesarios para las actualizaciones de BGP.

Por ejemplo, puede agregar la dirección IP 192.168.100.3/27 a la lista de prefijos de IP y denegar la redistribución de la ruta a la puerta de enlace Edge.

También puede anexas una dirección IP con los modificadores `less than or equal to (le)` y `greater than or equal to (ge)` para conceder o limitar la redistribución de rutas. Por ejemplo, los modificadores 192.168.100.3/27 ge 26 le 32 coinciden con máscaras de subred que tienen una longitud mayor o igual que 26 bits y menor o igual que 32 bits.

Requisitos previos

- Compruebe que el **administrador del sistema** ha dedicado una red externa a una puerta de enlace Edge de NSX-T Data Center en la organización.
- Compruebe que es **administrador de la organización** o que tiene asignada una función con un conjunto de derechos equivalente.
- [Configurar los ajustes generales de BGP.](#)

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, en la pestaña **Puertas de enlace Edge**.
- 2 Haga clic en la puerta de enlace Edge.
- 3 En **Enrutamiento**, haga clic en **BGP** y en **Listas de prefijos de IP**.
- 4 Para agregar una lista de prefijos de IP, haga clic en **Nueva**.
- 5 Introduzca un nombre y, si lo desea, una descripción para la lista de prefijos.
- 6 Haga clic en **Nueva** y agregue una notación de CIDR para el prefijo.
- 7 En el menú desplegable, seleccione la acción que desea aplicar al prefijo.
- 8 (opcional) Introduzca los modificadores `greater than or equal to` y `less than or equal to` para conceder o limitar la redistribución de rutas.

Pasos siguientes

- Puede editar o eliminar la lista de prefijos de IP como sea necesario.
- Configure el filtrado de rutas. Consulte la [Agregar un vecino de BGP](#).

Agregar un vecino de BGP

Puede configurar ajustes individuales de los vecinos de enrutamiento de BGP al agregarlos.

Requisitos previos

- Compruebe que el **administrador del sistema** ha dedicado una red externa a una puerta de enlace Edge de NSX-T Data Center en la organización.
- Compruebe que es **administrador de la organización** o que tiene asignada una función con un conjunto de derechos equivalente.
- Compruebe que ha configurado los ajustes globales de BGP para la puerta de enlace Edge. Consulte la [Configurar los ajustes generales de BGP](#).
- Si utiliza el filtrado de rutas, compruebe que ha creado las listas de prefijos de IP. Consulte la [Crear una lista de prefijos de IP](#).

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, en la pestaña **Puertas de enlace Edge**.
- 2 Haga clic en la puerta de enlace Edge.
- 3 En **Enrutamiento**, haga clic en **BGP** y en **Vecinos**.
- 4 Para agregar un nuevo vecino de BGP, haga clic en **Nuevo**.
- 5 Introduzca la configuración general del nuevo vecino de BGP.
 - a Introduzca una dirección IPv4 o IPv6 para el nuevo vecino de BGP.
 - b Introduzca un número de sistema autónomo (Autonomous System, AS) remoto en formato ASPLAIN.
 - c Introduzca el intervalo de tiempo que debe transcurrir entre el envío de cada mensaje de conexión persistente a un elemento del mismo nivel de BGP.
 - d Introduzca un intervalo de tiempo antes de declarar que un elemento del mismo nivel de BGP está desactivado.
 - e En el menú desplegable, seleccione una opción **Modo de reinicio correcto** para este vecino.

Opción	Descripción
Deshabilitar	Reemplaza la configuración global de puerta de enlace Edge y desactiva el modo de reinicio correcto para este vecino.
Solo auxiliar	Reemplaza la configuración global de puerta de enlace Edge y configura el modo de reinicio correcto como Solo auxiliar para este vecino.
Auxiliar y reinicio correcto	Reemplaza la configuración global de puerta de enlace Edge y configura el modo de reinicio correcto como Auxiliar y reinicio correcto para este vecino.

- f Active el botón de alternancia **AllowAS-in** para habilitar las rutas de recepción con el mismo AS.
 - g Introduzca la contraseña del vecino de BGP si este requiere autenticación.
- 6 Ajuste la configuración de detección de reenvío bidireccional (Bidirectional Forwarding Detection, BFD) para el nuevo vecino de BGP.
 - a (opcional) Active la opción **BFD** con el fin de habilitar el BFD para la detección de errores.
 - b En el cuadro de texto de intervalo de BFD, defina el intervalo de tiempo para enviar paquetes de latidos.
 - c En el cuadro de texto **Varias declaraciones de inactividad**, introduzca el número de errores de envío de paquetes de latidos que puede generar el vecino de BGP antes de que BFD lo declare inactivo.

7 (opcional) Configure el filtrado de rutas.

- a Seleccione una familia de direcciones IP en el menú desplegable **Familia de direcciones IP**.
- b Para configurar un filtro de entrada, seleccione una lista de prefijos de IP.
- c Para configurar un filtro de salida, seleccione una lista de prefijos de IP.

8 Haga clic en **Guardar**.

Pasos siguientes

Puede ver el estado de los distintos vecinos de BGP, así como editarlos o eliminarlos según sea necesario.

Trabajar con equilibrio de carga avanzado de NSX

Como **administrador de la organización**, al configurar servicios virtuales que distribuyen el tráfico a través de varios grupos de servidores, puede equilibrar las cargas de trabajo en los centros de datos respaldados por NSX-T Data Center.

A partir de la versión 10.2, VMware Cloud Director proporciona servicios de equilibrio de carga utilizando las capacidades de VMware NSX Advanced Load Balancer (Avi Networks).

VMware Cloud Director admite el equilibrio de carga de capa 4 y capa 7 que se puede configurar en una puerta de enlace Edge de NSX-T Data Center.

El equilibrio de carga de nivel 4 (capa 4) dirige el tráfico en función de los datos de los protocolos de red y de capa de transporte, como la dirección IP y el puerto TCP.

El equilibrio de carga de nivel 7 (capa 7) distribuye el tráfico en función de atributos, como el encabezado HTTP, el identificador uniforme de recursos, el identificador de sesión SSL y los datos de formularios HTML.

Habilitar un equilibrador de carga en la puerta de enlace Edge de NSX-T Data Center

Para que un **administrador de la organización** pueda configurar los servicios de equilibrio de carga, primero un **administrador del sistema** debe habilitar el equilibrador de carga en la puerta de enlace Edge de NSX-T Data Center.

Requisitos previos

- Compruebe que es un **administrador del sistema**.
- Compruebe que ha integrado VMware NSX Advanced Load Balancer en la infraestructura de nube. Para obtener más información sobre la administración de NSX Advanced Load Balancer, consulte *Guía del portal para administradores de proveedores de servicios de VMware Cloud Director*.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, en la pestaña **Puertas de enlace Edge**.
- 2 Haga clic en la puerta de enlace Edge de NSX-T Data Center en la que desea habilitar el equilibrio de carga.
- 3 En Equilibrador de carga, haga clic en **Configuración general**.
- 4 Haga clic en **Editar** y active la opción **Estado de equilibrador de carga**.
- 5 Introduzca un CIDR de red para una subred de red de servicio desde la que se usarán direcciones IP para la creación de servicios virtuales.

Para utilizar la subred de red de servicio predeterminada, seleccione la casilla de verificación **Usar valor predeterminado**.

- 6 Haga clic en **Guardar**.

Pasos siguientes

[Asignar un grupo de motores de servicio a una puerta de enlace Edge de NSX-T Data Center.](#)

Asignar un grupo de motores de servicio a una puerta de enlace Edge de NSX-T Data Center

Para que un **administrador de la organización** pueda configurar los servicios de equilibrio de carga en una puerta de enlace Edge de NSX-T Data Center, un **administrador del sistema** primero debe asignar un grupo de motores de servicio a la puerta de enlace Edge.

La infraestructura informática de equilibrio de carga proporcionada por NSX Advanced Load Balancer se organiza en grupos de motores de servicio. Un **administrador del sistema** puede asignar uno o varios grupos de motores de servicio a una puerta de enlace Edge de NSX-T Data Center.

Todos los grupos de motores de servicio que están asignados a una única puerta de enlace Edge usan la misma red de servicio.

Requisitos previos

- Compruebe que es un **administrador del sistema**.
- [Habilitar un equilibrador de carga en la puerta de enlace Edge de NSX-T Data Center.](#)

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, en la pestaña **Puertas de enlace Edge**.
- 2 Haga clic en la puerta de enlace Edge de NSX-T Data Center a la que desea asignar un grupo de motores de servicio.
- 3 En Equilibrador de carga, haga clic en **Grupos de motores de servicios**.

- 4 Haga clic en **Agregar**.
- 5 Seleccione un grupo de motores de servicio disponible en la lista.
- 6 Introduzca un número para la cantidad máxima de servicios virtuales que se pueden colocar en la puerta de enlace Edge.
- 7 Introduzca un número para la cantidad de servicios virtuales garantizados disponibles para la puerta de enlace Edge.
- 8 Para confirmar la configuración, haga clic en **Guardar**.

Editar la configuración de un grupo de motores de servicio

Un **administrador del sistema** puede editar la cantidad máxima de servicios virtuales admitidos y la cantidad de servicios virtuales reservados para un grupo de motores de servicio.

Después de sincronizar un grupo de motores de servicio, si la nueva cantidad máxima de servicios virtuales admitidos es inferior a la cantidad de servicios virtuales reservados, el grupo de motores de servicio se marca como sobreasignado.

Si se sobreasigna un motor de servicio, se puede producir un error en la creación de un nuevo servicio virtual, incluso si la puerta de enlace Edge en la que se crea el servicio virtual tiene suficiente capacidad reservada.

Para evitar errores en la creación de un servicio virtual, cuando edite la configuración de un grupo de motores de servicio, no reduzca la cantidad máxima de servicios virtuales admitidos por debajo de la cantidad de servicios virtuales reservados inicialmente.

Requisitos previos

- Compruebe que es un **administrador del sistema**.
- [Habilitar un equilibrador de carga en la puerta de enlace Edge de NSX-T Data Center.](#)
- [Asignar un grupo de motores de servicio a una puerta de enlace Edge de NSX-T Data Center.](#)

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, en la pestaña **Puertas de enlace Edge**.
- 2 Haga clic en la puerta de enlace Edge de NSX-T Data Center a la que se asigna el grupo de motores de servicio.
- 3 En Equilibrador de carga, haga clic en **Grupos de motores de servicios**.
- 4 Haga clic en **Editar**.
- 5 Edite la cantidad máxima de servicios virtuales permitidos que puede usar la puerta de enlace Edge.

No reduzca la cantidad a menos que sea obligatorio. De lo contrario, es posible que se produzcan errores al crear servicios virtuales.
- 6 Edite la cantidad de servicios virtuales garantizados disponibles para la puerta de enlace Edge.

7 Haga clic en **Guardar**.

Agregar un grupo de servidores de equilibrador de carga

Un grupo de servidores es un grupo de uno o varios servidores que se configuran para ejecutar la misma aplicación y para proporcionar alta disponibilidad.

Requisitos previos

- Compruebe que es un **administrador de organización**.
- Compruebe que el **administrador del sistema** haya habilitado el equilibrio de carga en la puerta de enlace Edge de NSX-T.
- Compruebe que el **administrador del sistema** haya asignado al menos un grupo de motores de servicio a la puerta de enlace Edge.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, en la pestaña **Puertas de enlace Edge**.
- 2 Haga clic en la puerta de enlace Edge de NSX-T Data Center para la que desea configurar un grupo de equilibradores de carga.
- 3 En Equilibrador de carga, haga clic en **Grupos** y, a continuación, haga clic en **Agregar**.

4 Establezca la configuración general del grupo de equilibradores de carga.

- a Escriba un nombre significativo y, opcionalmente, una descripción para el grupo de servidores.
- b Seleccione un método de equilibrio de algoritmos.

El algoritmo de equilibrio de carga define cómo se distribuyen las conexiones entrantes entre los miembros del grupo de servidores.

Opción	Descripción
Menos conexiones	Las nuevas conexiones se envían al servidor que, en el momento, tiene el menor número de conexiones.
Por turnos	Las nuevas conexiones se envían al siguiente servidor apto en el grupo en orden secuencial.
Respuesta más rápida	Las nuevas conexiones se envían al servidor que proporciona la respuesta más rápida a las nuevas conexiones o solicitudes.
Hash coherente	Las nuevas conexiones se distribuyen entre los servidores utilizando la dirección IP del cliente para generar una clave de hash de IP.
Menor carga	Las nuevas conexiones se envían al servidor con la carga más baja, independientemente de la cantidad de conexiones que tenga el servidor.
Menos servidores	En lugar de intentar distribuir todas las conexiones o solicitudes entre todos los servidores, el equilibrador de carga determina la cantidad mínima de servidores necesarios para satisfacer la carga actual del cliente.
Aleatorio	El equilibrador de carga selecciona los servidores de forma aleatoria.
Menos tareas	La carga se equilibra de forma adaptada según la información del servidor.
Afinidad del núcleo	Cada núcleo de CPU utiliza un subconjunto de servidores, y cada servidor es utilizado por un subconjunto de núcleos. Esencialmente, proporciona una asignación de muchos a muchos entre servidores y núcleos.

- c Para habilitar el grupo de servidores tras su creación, active la opción **Estado**.
- d Introduzca un puerto de servidor de destino predeterminado que se utilizará para el tráfico hacia el miembro del grupo.
- e (opcional) En el cuadro de texto **Tiempo de espera de deshabilitación correcto**, introduzca el tiempo máximo en minutos para desactivar de manera correcta un miembro de grupo.

El servicio virtual espera el tiempo especificado antes de cerrar las conexiones existentes con los miembros desactivados.

- f (opcional) Para activar una supervisión de estado pasivo, active la opción **Supervisión de estado pasivo**.
- g (opcional) Seleccione un supervisor de estado activo.

Opción	Descripción
HTTP	Se utiliza una solicitud y una respuesta HTTP para validar el estado.
HTTPS	Se utiliza con servidores web HTTPS cifrados para validar el estado.
TCP	Se utiliza una conexión TCP para validar el estado.
UDP	Se utiliza un datagrama UDP para validar el estado.
PING	Se utiliza un ping ICMP para validar el estado.

- 5 Agregue un miembro al grupo de servidores.
 - a Haga clic en la pestaña **Miembros** y haga clic en **Agregar**.
 - b Introduzca una dirección IP para el miembro del grupo.
 - c Active la opción **Estado** para habilitar el miembro del grupo.
 - d (opcional) Agregue un puerto personalizado para el miembro del grupo de servidores.
De manera predeterminada, el número de puerto es el puerto de destino que introdujo para el grupo.
 - e Introduzca una proporción para el miembro del grupo.
La proporción de cada miembro del grupo indica el tráfico que se dirige a cada miembro del grupo de servidores. Un servidor con una proporción de 2 obtiene el doble de tráfico que un servidor con una proporción de 1. El valor predeterminado es 1.
- 6 En la pestaña **Configuración de SSL**, configure los ajustes de SSL para validar los certificados presentados por los miembros del grupo de equilibradores de carga.
 - a Para activar SSL, active la opción **Habilitar SSL**.
 - b Para ocultar certificados con claves privadas y ver una lista de certificados de CA únicamente, seleccione la casilla de verificación **Ocultar certificados de servicio**.
- 7 Para activar la comprobación de nombres comunes para certificados de servidor, active la opción **Comprobación de nombre común** y escriba un máximo de 10 nombres de dominio para el grupo.
- 8 Haga clic en **Guardar**.

Pasos siguientes

[Crear un servicio virtual.](#)

Crear un servicio virtual

Un servicio virtual escucha para detectar el tráfico hacia una dirección IP, procesa las solicitudes de los clientes y dirige las solicitudes válidas a un miembro del grupo de servidores de equilibrador de carga.

Un servicio virtual es una combinación de una dirección IP y un puerto que utiliza un solo protocolo de red. El servicio virtual se anuncia a las redes externas y escucha para detectar las solicitudes de los clientes. Cuando un cliente se conecta al servicio virtual, el equilibrador de carga dirige la solicitud a un miembro del grupo de servidores de equilibrador de carga que configuró.

Para proteger la finalización SSL de un servicio virtual, puede utilizar un certificado de la biblioteca de certificados. Para obtener más información, consulte [Importar certificados en la biblioteca de certificados](#).

Requisitos previos

- Compruebe que es un **administrador de organización**.
- Compruebe que el **administrador del sistema** haya habilitado el equilibrio de carga en la puerta de enlace Edge de NSX-T.
- Compruebe que el **administrador del sistema** haya asignado al menos un grupo de motores de servicio a la puerta de enlace Edge.
- [Agregar un grupo de servidores de equilibrador de carga](#).

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Redes** y, a continuación, en la pestaña **Puertas de enlace Edge**.
- 2 Haga clic en la puerta de enlace Edge de NSX-T Data Center en la que desea crear un servicio virtual.
- 3 En Equilibrador de carga, haga clic en **Servicios virtuales** y, a continuación, haga clic en **Agregar**.
- 4 Escriba un nombre significativo y, si lo desea, una descripción para el servicio virtual.
- 5 Para activar el servicio virtual tras su creación, active la opción **Habilitado**.
- 6 Seleccione un grupo de motores de servicio para el servicio virtual.
- 7 Seleccione un grupo de equilibradores de carga para el servicio virtual.
- 8 Introduzca una dirección IP para el servicio virtual.

9 Seleccione el tipo de servicio virtual.

Opción	Descripción
HTTP	<p>El servicio virtual escucha para detectar solicitudes HTTP de capa 7 no seguras.</p> <p>Al seleccionar este tipo de servicio, se rellena automáticamente el cuadro de texto de puerto de servicio con 80, valor que puede reemplazar por otro número de puerto válido.</p>
HTTPS	<p>El servicio virtual escucha para detectar solicitudes HTTPS de nivel 7 seguras.</p> <p>Al seleccionar este tipo de servicio, se rellena automáticamente el cuadro de texto de puerto de servicio con el puerto 443, valor que puede reemplazar por otro número de puerto válido. Seleccione un certificado SSL para utilizar para la terminación SSL.</p>
L4	<p>El servicio virtual escucha para detectar solicitudes de capa 4.</p> <p>Al seleccionar este tipo de servicio, se rellena automáticamente el cuadro de texto de puerto de servicio con 80, valor que puede reemplazar por otro número de puerto válido.</p>
TLS L4	<p>El servicio virtual escucha para detectar solicitudes TLS de capa 4 seguras.</p> <p>Al seleccionar este tipo de servicio, se rellena automáticamente el cuadro de texto de puerto de servicio con el puerto TCP 443, valor que puede reemplazar por otro número de puerto válido. Seleccione un certificado SSL para utilizar para la terminación SSL.</p>

10 Haga clic en **Guardar**.

Usar discos con nombre y revisar políticas de almacenamiento

6

Para crear y administrar discos con nombre y revisar las políticas de almacenamiento de centros de datos virtuales de organización, puede usar el portal para tenants de VMware Cloud Director.

Este capítulo incluye los siguientes temas:

- [Crear y usar discos con nombre](#)
- [Revisar las propiedades de la política de almacenamiento](#)

Crear y usar discos con nombre

Los discos con nombre son discos virtuales autónomos que se crean en los VDC de organización. Los **administradores de la organización** y los usuarios que tengan los derechos correspondientes pueden crear, eliminar y actualizar discos con nombre, así como conectarlos a máquinas virtuales.

Cuando crea un disco con nombre, este se asocia con un VDC de organización, pero no con una máquina virtual. Después de crear el disco en un VDC, el propietario del disco o un administrador pueden asociarlo a cualquier máquina virtual implementada en el VDC. Si tiene el derecho **Crear un disco compartido**, puede crear un disco con nombre compartido para asociar a varias máquinas virtuales. El propietario del disco también puede modificar las propiedades del disco, desasociarlo de una máquina virtual y quitarlo del VDC. Los **administradores del sistema** y los **administradores de la organización** tienen los mismos derechos que el propietario del disco para usarlo y modificarlo.

Nota Aunque vSphere admite configuraciones como clústeres de conmutación por error de Windows Server (Windows Server Failover Cluster, WSFC) y permite crear un disco compartido mediante el uso compartido de un bus SCSI físico, VMware Cloud Director 10.2 no admite esta función. Al crear un disco compartido en VMware Cloud Director, solo se crea un disco persistente independiente subyacente en vSphere con el modo multiescritura habilitado.

Si asocia un disco con nombre, no se pueden crear instantáneas de la máquina virtual. Si un disco compartido está asociado a una máquina virtual, no se puede editar su configuración de disco duro desde la vista de detalles de la máquina virtual.

Si el VDC de organización tiene una política de almacenamiento con cifrado de máquina virtual habilitado, puede cifrar estas máquinas y los discos asociándolos a las políticas de almacenamiento que tengan esta capacidad de cifrado. Consulte la [Cifrar máquinas virtuales](#).

Crear un disco con nombre

Puede crear un disco con nombre y asociarlo a una o varias máquinas virtuales en otro momento.

Para crear un disco con nombre, debe especificar el nombre y el tamaño de este. Si lo desea, puede incluir una descripción y seleccionar un perfil de almacenamiento para que lo use el disco. Puede crear un disco compartido que pueda asociar a varias máquinas virtuales.

Nota Aunque vSphere admite configuraciones como clústeres de conmutación por error de Windows Server (Windows Server Failover Cluster, WSFC) y permite crear un disco compartido mediante el uso compartido de un bus SCSI físico, VMware Cloud Director 10.2 no admite esta función. Al crear un disco compartido en VMware Cloud Director, solo se crea un disco persistente independiente subyacente en vSphere con el modo multiescritura habilitado.

Requisitos previos

- 1 Debe tener una función **Administrador de organización** o derechos de propietario de disco.
- 2 Si desea crear un disco compartido, debe tener el derecho **Crear un disco compartido**.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en **Almacenamiento**, en el panel izquierdo, seleccione **Discos con nombre**.
- 2 Haga clic en **Nuevo**.
- 3 Introduzca un nombre y, si lo desea, una descripción del disco.
- 4 Seleccione la política de almacenamiento del menú desplegable **Política de almacenamiento**.
- 5 Introduzca el tamaño del disco con nombre.
- 6 Seleccione el tipo y el subtipo de bus en los menús desplegables **Tipo de bus** y **Subtipo de bus**, respectivamente.
- 7 Si desea asociar el disco con nombre a varias máquinas virtuales, seleccione la casilla **Se puede compartir**.
No puede editar esta configuración más adelante.
- 8 Haga clic en **Guardar**.

Pasos siguientes

Utilice la API de VMware Cloud Director para asociar el disco independiente a una máquina virtual. Consulte *Guía de programación de API de VMware Cloud Director* en [VMware {code}](#).

Editar un disco con nombre

Después de crear el disco, puede modificar el nombre, la descripción, la política de almacenamiento y el tamaño de este.

No puede editar el ajuste de **Se puede compartir** de un disco con nombre.

Requisitos previos

- 1 Debe tener una función **Administrador de organización** o derechos de propietario de disco.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en **Almacenamiento**, en el panel izquierdo, seleccione **Discos con nombre**.
- 2 Seleccione el disco que desea modificar y haga clic en **Editar**.
- 3 Edite los ajustes como nombre, descripción, política de almacenamiento y tamaño.
- 4 Haga clic en **Guardar**.

Asociar un disco con nombre a una máquina virtual

Después de crear un disco con nombre en un VDC, puede asociarlo a cualquier máquina virtual implementada en el VDC. Puede asociar un disco con nombre compartido a varias máquinas virtuales.

Requisitos previos

Debe tener una función **Administrador de organización** o derechos de propietario de disco.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en **Almacenamiento**, en el panel izquierdo, seleccione **Discos con nombre**.
- 2 Haga clic en el botón de radio junto al nombre del disco con nombre que desea asociar a una máquina virtual y haga clic en **Conectar**.
- 3 En el menú desplegable, seleccione la máquina virtual a la que desea asociar el disco con nombre y haga clic en **Aplicar**.
- 4 Si desea asociar otra máquina virtual a un disco compartido, repita [Paso 2](#) y [Paso 3](#).

Pasos siguientes

Puede asociar más discos con nombre a la máquina virtual o desasociarlos según sea necesario.

Eliminar un disco con nombre

Si no necesita un disco con nombre, puede eliminarlo.

Requisitos previos

Debe tener una función **Administrador de organización** o derechos de propietario de disco.

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en **Almacenamiento**, en el panel izquierdo, seleccione **Discos con nombre**.
- 2 Seleccione el disco que desea eliminar y haga clic en **Eliminar**.
- 3 Haga clic en **Aceptar**.

Revisar las propiedades de la política de almacenamiento

Puede revisar las políticas de almacenamiento y sus detalles.

Requisitos previos

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

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar.
- 2 En **Almacenamiento**, haga clic en **Políticas de almacenamiento**.
Aparecerá la lista de las políticas de almacenamiento disponibles.
- 3 Para ver los detalles de una política de almacenamiento, haga clic en el nombre de esta.
- 4 Revise los detalles en las pestañas **General** y **Metadatos**, y haga clic en **Aceptar**.
Puede revisar el nombre, el límite, la configuración de IOPS y los detalles de metadatos de la política de almacenamiento.

Revisar y editar las propiedades del centro de datos virtual

7

Como **administrador de organización**, puede revisar las propiedades del centro de datos virtual. También puede controlar el acceso a los VDC de organización por parte usuarios y grupos de la organización.

Este capítulo incluye los siguientes temas:

- [Revisar las propiedades del centro de datos virtual](#)
- [Revisar los metadatos del centro de datos virtual](#)
- [Limitar el acceso a un VDC de organización a usuarios y grupos específicos de la organización](#)

Revisar las propiedades del centro de datos virtual

Puede revisar las propiedades de los centros de datos virtuales asignados a la organización.

Requisitos previos

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

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar.
- 2 En **Configuración**, haga clic en **General**.

Resultados

Puede revisar las propiedades del centro de datos virtual, como el nombre, la descripción y el estado. La información de métricas sobre el centro de datos incluye modelo de asignación, vCPU y uso de memoria y CPU.

Revisar los metadatos del centro de datos virtual

VMware Cloud Director ofrece un componente de uso general para asociar metadatos definidos por el usuario con un objeto. Si el administrador del sistema ha creado metadatos para el

centro de datos virtual de la organización, puede revisar los metadatos del centro de datos de la organización.

Requisitos previos

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

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual que desea explorar.
- 2 En **Configuración**, haga clic en **Metadatos**.

Aparecerá la lista de los metadatos disponibles.

Limitar el acceso a un VDC de organización a usuarios y grupos específicos de la organización

Como **administrador de organización** puede limitar el acceso a cada uno de los VDC de organización de la organización a usuarios y grupos específicos.

De forma predeterminada, los VDC de organización se comparten con todos los usuarios y los grupos que tienen una función que incluye el derecho **Permitir acceso a todos los VDC de organización**.

Si su organización tiene varios VDC de organización y desea que se administren por separado, puede crear una función personalizada que funcione como administrador de VDC de organización y asignarla a usuarios o grupos específicos dentro de la organización, proporcionándoles acceso solo a los recursos informáticos y de redes de un VDC específico.

Requisitos previos

- 1 Compruebe que es un **administrador de organización**.
- 2 Cree una función personalizada para los usuarios y grupos a los que desea proporcionar acceso a un VDC de organización específico. Esta función debe excluir el derecho **Permitir el acceso a todos los VDC de organización**. Consulte la [Capítulo 13 Administración de usuarios, grupos y funciones](#).

Procedimiento

- 1 En la pantalla del panel de control **Centro de datos virtual**, haga clic en la tarjeta del centro de datos virtual a la que desea limitar el acceso.
- 2 En **Ajustes**, haga clic en **Uso compartido**.
Aparece la lista de usuarios y grupos dentro de la organización que tienen acceso al VDC.
- 3 Para cambiar la configuración de acceso al VDC de organización, haga clic en **Editar**.
- 4 Seleccione **Usuarios y grupos específicos**.

- 5 En la lista **Usuarios**, seleccione los usuarios a los que desea proporcionar acceso al VDC.
- 6 En la lista **Grupos**, seleccione los grupos a los que desea proporcionar acceso al VDC.
- 7 Para compartir el VDC con los usuarios y grupos seleccionados, haga clic en **Compartir**.

Resultados

El acceso al VDC de organización se limita a los usuarios y grupos que seleccionó.

Trabajar con instancias de vCenter Server dedicadas, endpoints y servidores proxy



Puede acceder a un entorno de vCenter Server dedicado o a componentes de vCenter Server desde el VMware Cloud Director Tenant Portal.

Centros de datos de vSphere dedicados

En VMware Cloud Director, un centro de datos definido por software (Software-Defined Data Center, SDDC) encapsula un entorno de vCenter Server dedicado completo.

Las instancias de vCenter Server dedicadas en VMware Cloud Director hacen que ya no se requiera que una instancia de vCenter Server sea accesible de manera pública.

El **administrador del sistema** puede publicar una o varias instancias de vCenter Server dedicadas en su organización. Puede usar los endpoints para acceder a la interfaz de usuario o a la API de los componentes con o sin proxy.

Endpoints

Una instancia de vCenter Server dedicada puede incluir uno o varios endpoints que proporcionan acceso a diferentes componentes del entorno subyacente. Los endpoints pueden proporcionar un punto de acceso a un componente de centro de datos (por ejemplo, una instancia de vCenter Server, un host ESXi, una instancia de NSX Manager o una instancia de NSX-T Manager).

Los endpoints pueden o no estar conectados a un proxy.

Proxies

VMware Cloud Director puede actuar como un servidor proxy HTTPS y proporcionar acceso a una instancia de vCenter Server dedicada y a distintos componentes de instancias de vCenter Server compartidas o dedicadas que creen copias de seguridad del entorno.

Puede iniciar sesión en la interfaz de usuario o la API de los componentes con proxy mediante la cuenta de VMware Cloud Director.

Para acceder a componentes con proxy, debe utilizar Chrome Browser Extension for VMware Cloud Director o configurar manualmente el navegador con la configuración del proxy.

Este capítulo incluye los siguientes temas:

- [Usar Chrome Browser Extension for VMware Cloud Director](#)
- [Configurar el navegador con la configuración de proxy](#)
- [Iniciar sesión en la interfaz de usuario de un componente mediante un endpoint](#)

Usar Chrome Browser Extension for VMware Cloud Director

Puede utilizar Chrome Browser Extension for VMware Cloud Director para iniciar sesión en los componentes de vSphere con proxy del entorno.

Chrome Browser Extension for VMware Cloud Director proporciona autenticación y configuración del proxy.

Chrome Browser Extension for VMware Cloud Director admite entornos de varios sitios.

Puede agregar la extensión al navegador Chrome a través de la [Chrome Web Store](#).

Configurar el navegador con la configuración de proxy

Para poder acceder a la interfaz de usuario de un componente de vSphere con proxy, debe configurar los servidores proxy que están publicados en su organización.

Para configurar el explorador de modo que use los proxies publicados, copie la dirección URL del archivo de configuración automática de proxy (Proxy Auto-Config, PAC) en el explorador.

Nota Cuando el **administrador del sistema** publica un centro de datos de vSphere dedicado en su organización o agrega un proxy a uno de los centros de datos de vSphere dedicados, es posible que el explorador tarde unos minutos en volver a recuperar la PAC desde la URL proporcionada. Para forzar la actualización del explorador, puede repetir este procedimiento.

Requisitos previos

- Compruebe si el **administrador del sistema** publicó al menos una instancia de vCenter Server dedicada y habilitada en su organización.
- Compruebe si el **administrador del sistema** publicó **SDDC_VIEW** y los derechos **Token: administrar** en la organización, y si su función incluye estos derechos.
- Compruebe si el **administrador del sistema** publicó y habilitó el complemento de la **extensión CPOM** en su organización. Este complemento proporciona la función para ver y utilizar centros de datos de vSphere dedicados en VMware Cloud Director Tenant Portal.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Centros de datos** y, a continuación, en **Centro de datos virtual**.
- 2 En el panel **Centros de datos de vSphere dedicados**, haga clic en **Haga clic aquí para ver la guía de configuración de proxy**.
- 3 Copie la URL de PAC y haga clic en **Siguiente**.

- 4 Siga las instrucciones para configurar el explorador de modo que dirija a la URL de PAC.
- 5 Si un componente con proxy utiliza certificados autofirmados, impórtelos en el explorador.
 - a En la tarjeta del centro de datos de vSphere de destino, haga clic en **Acciones** y, a continuación, en **Importar certificado**.
 - b Descargue el certificado y la lista de revocación de certificados (Certificate Revocation List, CRL).
 - c Importe el certificado descargado en el explorador.Consulte las instrucciones de usuario del navegador.

Iniciar sesión en la interfaz de usuario de un componente mediante un endpoint

Los endpoints se pueden utilizar para acceder a la interfaz de usuario de los componentes con proxy o sin proxy con la cuenta de VMware Cloud Director.

Requisitos previos

Si desea acceder a un componente con proxy, [Configurar el navegador con la configuración de proxy](#) o [Usar Chrome Browser Extension for VMware Cloud Director](#) a Google Chrome.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Centros de datos** y, a continuación, en **Centro de datos virtual**.
- 2 Seleccione la pestaña **Centros de datos de vSphere dedicados**.
- 3 Abra el endpoint de la instancia de vCenter Server dedicada.
 - Para abrir el proxy predeterminado, haga clic en **Abrir vSphere**.
 - Para abrir un endpoint que no sea el predeterminado, siga estos pasos:
 - Haga clic en el menú **Acciones** y en **Ver endpoints**.
 - Haga clic en la URL del endpoint.

Si va a acceder a un componente con proxy, se abre una nueva tarjeta con sus credenciales de proxy.

- 4 Si va a iniciar sesión en un componente con proxy, acceda al componente mediante sus credenciales.
 - a Copie el nombre de usuario y la contraseña.
 - b Para activar el proxy, haga clic en **Abrir**.

Se abrirá una nueva tarjeta donde se solicitará la autenticación en el proxy.

- c En el cuadro de texto **Nombre de usuario**, pegue el nombre de usuario copiado.
- d En el cuadro de texto **Contraseña**, pegue la contraseña copiada y haga clic en **Aceptar**.

Trabajar con plantillas de vApp

9

Una plantilla de vApp es una imagen de máquina virtual cargada con un sistema operativo, aplicaciones y datos. Estas plantillas garantizan que las máquinas virtuales estén configuradas correctamente en toda la organización. Las plantillas de vApp se añaden a los catálogos.

Este capítulo incluye los siguientes temas:

- [Ver una plantilla de vApp](#)
- [Crear una plantilla de vApp desde un archivo OVF](#)
- [Importar una máquina virtual desde vCenter Server como plantilla de vApp](#)
- [Asignar una política de colocación de máquinas virtuales y una política de tamaño de máquina virtual a una plantilla de vApp](#)
- [Descargar una plantilla de vApp](#)
- [Eliminar una plantilla de vApp](#)

Ver una plantilla de vApp

Puede ver la lista de plantillas de vApp disponibles en los catálogos a los que tiene acceso. Puede ver una plantilla de vApp y explorar las máquinas virtuales que contiene.

Puede acceder solo a las plantillas de vApp que se incluyen en los elementos de catálogo que se han compartido con usted. Para obtener más información acerca del uso compartido de catálogos, consulte [Compartir un catálogo](#).


Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en el panel izquierdo, seleccione **Plantillas de vApp**.


La lista de plantillas aparece en una vista de cuadrícula.

- 2 (opcional) Configure la vista de cuadrícula para que contenga los elementos que desea ver.
 - a En la vista de cuadrícula, haga clic en el icono de editor de cuadrícula () que aparece debajo de la lista de plantillas de vApp.
 - b Seleccione los elementos que desea incluir en la vista de cuadrícula, como la versión, el estado, el catálogo, el propietario, etc.
 - c Haga clic en **Aceptar**.

La cuadrícula muestra los elementos seleccionados para cada plantilla de vApp en la lista.

- 3 Para ver las máquinas virtuales incluidas en una plantilla de vApp, haga clic en el nombre de la plantilla de vApp.

Las máquinas virtuales que se incluyen en la plantilla de vApp se muestran en una cuadrícula.

- 4 (opcional) Para seleccionar los elementos que desea ver en la vista de cuadrícula, haga clic en el icono de editor de cuadrícula () que aparece debajo de la lista de máquinas virtuales.
 - a Seleccione los elementos que desea incluir en la vista de cuadrícula.
 - b Haga clic en **Aceptar**.

Crear una plantilla de vApp desde un archivo OVF

Puede cargar un paquete OVF para crear una plantilla de vApp en un catálogo.

VMware Cloud Director admite las especificaciones de Open Virtualization Format (OVF) y Open Virtualization Appliance (OVA). Si carga un archivo OVF que incluya propiedades OVF para personalizar sus máquinas virtuales, dichas propiedades se conservarán en la plantilla de vApp. Para obtener más información acerca de la creación de paquetes OVF, consulte la *Guía del usuario de herramientas OVF* y la *Guía del usuario de VMware vCenter Converter*.

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en el panel izquierdo, seleccione **Plantillas de vApp**.
La lista de plantillas aparece en una vista de cuadrícula.
- 2 Haga clic en **Nuevo**.

- 3 Introduzca una dirección URL del archivo OVF o haga clic en el icono **Cargar** para ir hasta una ubicación accesible desde el equipo y después seleccione el archivo de plantilla OVF/OVA.

La ubicación puede ser el disco duro local, un recurso compartido de red o una unidad de CD/DVD. Las extensiones de archivo admitidas incluyen `.ova`, `.ovf`, `.vmdk`, `.mf`, `.cert` y `.strings`. Si opta por cargar un archivo OVF, que hace referencia a más archivos de los que intenta cargar, por ejemplo, un archivo VMDK, debe examinar y seleccionar todos los archivos.

- 4 Verifique los detalles de la plantilla OVF/OVA que va a implementar y haga clic en **Siguiente**.
- 5 Introduzca un nombre y, si lo desea, una descripción de la plantilla de vApp y haga clic en **Siguiente**.
- 6 En el menú desplegable **Catálogo**, seleccione el catálogo al que desea agregar la plantilla.
- 7 Revise la configuración de la plantilla de vApp y haga clic en **Finalizar**.

Resultados

La nueva plantilla de vApp aparecerá en la vista de cuadrícula de plantillas.

Importar una máquina virtual desde vCenter Server como plantilla de vApp

Si tiene derechos de **administrador del sistema**, puede importar máquinas virtuales de vCenter Server en VMware Cloud Director como plantillas de vApp en catálogos.

Requisitos previos

Para ver e importar máquinas virtuales desde vCenter Server como plantillas de vApp, compruebe que tenga derechos de **administrador del sistema**.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en el panel izquierdo, seleccione **Plantillas de vApp**.

La lista de plantillas aparece en una vista de cuadrícula.
- 2 Haga clic en **Importar desde vCenter**.
- 3 En el menú desplegable, seleccione la instancia de vCenter Server desde la que desea importar la plantilla de vApp.
- 4 Seleccione una plantilla de la lista de máquinas virtuales.
- 5 Escriba un nombre y, si lo desea, una descripción para la plantilla de vApp.
- 6 En el menú desplegable, seleccione el catálogo al que desea agregar la plantilla de vApp.
- 7 (opcional) Para eliminar la máquina virtual de origen, active la opción **Mover máquina virtual**.
- 8 (opcional) Marque la plantilla de vApp como plantilla preferida en el catálogo.

9 Haga clic en **Importar**.

Asignar una política de colocación de máquinas virtuales y una política de tamaño de máquina virtual a una plantilla de vApp

Para asociar las máquinas virtuales de una plantilla de vApp con políticas específicas de colocación de máquinas virtuales y tamaño de máquina virtual, puede etiquetar las máquinas virtuales individuales de una plantilla de vApp con las políticas que desea asignar.

A partir de VMware Cloud Director 10.0, puede permitir que los usuarios cambien las políticas predefinidas de dimensionamiento o colocación de máquinas virtuales al editar una máquina virtual.

Nota Tras actualizar a VMware Cloud Director 10.0 o una versión posterior, todas las etiquetas de plantilla preexistentes se pueden modificar. Si desea prohibir los cambios en las políticas predefinidas de dimensionamiento o colocación de máquinas virtuales, debe anular la activación de la casilla de verificación **Modificable** de las políticas que desea que sean inmodificables.

Requisitos previos

- Esta operación requiere el derecho a editar una plantilla de vApp.
- Compruebe que tiene al menos una plantilla de vApp en el entorno de VMware Cloud Director.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en el panel izquierdo, seleccione **Plantillas de vApp**.
La lista de plantillas aparece en una vista de cuadrícula.
- 2 Seleccione el botón de radio junto a la plantilla de vApp que desea etiquetar y haga clic en **Etiqueta con políticas de recursos informáticos**.
- 3 Si desea asignar una política de colocación de máquinas virtuales a una máquina virtual en la plantilla de vApp, seleccione una política en el menú desplegable **Política de colocación de máquinas virtuales** en la fila correspondiente a la máquina virtual.
- 4 Si desea asignar una política de tamaño de máquina virtual a una máquina virtual en la plantilla de vApp, seleccione una política en el menú desplegable **Política de tamaño de máquina virtual** en la fila correspondiente a la máquina virtual.
- 5 (opcional) Para permitir que los usuarios cambien las políticas predefinidas de colocación o tamaño de la máquina virtual al editar una máquina virtual, seleccione la casilla **Modificable** en el menú desplegable de la política.
- 6 Haga clic en **Etiquetar**.

Descargar una plantilla de vApp

Puede descargar una plantilla de vApp desde un catálogo como un archivo OVA en la máquina local.


Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en el panel izquierdo, seleccione **Plantillas de vApp**.

La lista de plantillas aparece en una vista de cuadrícula.

- 2 Haga clic en la barra de listas () que se encuentra a la izquierda de la plantilla de vApp que desea descargar y seleccione **Descargar**.

Nota Puede descargar plantillas de vApp de los catálogos de la organización. Si es administrador de la organización, puede descargar plantillas de vApp de un catálogo público. De lo contrario, el botón **Descargar** estará atenuado.

- 3 (opcional) Para preservar los UUID y las direcciones MAC de las máquinas virtuales en el paquete OVA descargado, active la casilla de verificación **Proteger información de identidad**.
- 4 Haga clic en **Aceptar** y espere hasta que finalice la descarga.

El archivo OVA se guarda en la ubicación de descarga predeterminada del navegador web.

Eliminar una plantilla de vApp

Puede eliminar una plantilla de vApp de un catálogo de organización. Si el catálogo está publicado, la plantilla de vApp también se eliminará de los catálogos públicos.


Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en el panel izquierdo, seleccione **Plantillas de vApp**.

La lista de plantillas aparece en una vista de cuadrícula.

- 2 Haga clic en la barra de listas () que se encuentra a la izquierda de la plantilla de vApp que desea eliminar y seleccione **Eliminar**.

3 Confirme la eliminación.

La plantilla de vApp eliminada se quitará de la vista de cuadrícula.

Trabajar con archivos de medios

10

Un catálogo permite cargar, copiar, mover o editar las propiedades de los archivos de medios.

Este capítulo incluye los siguientes temas:

- [Cargar archivos de medios](#)
- [Eliminar un archivo de medios](#)
- [Descargar un archivo de medios](#)

Cargar archivos de medios

Puede cargar en un catálogo nuevos archivos de medios o versiones nuevas de los archivos de medios existentes. Los usuarios con acceso al catálogo pueden abrir los archivos de medios con sus máquinas virtuales.

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en el panel izquierdo, seleccione **Medios y otros**.
La lista de archivos de medios aparece en una vista de cuadrícula.
- 2 Haga clic en **Agregar**.
- 3 En el menú desplegable **Catálogo**, seleccione el catálogo en el que desea cargar el archivo de medios.
- 4 Introduzca un nombre para el archivo de medios.
Si no introduce un nombre, el cuadro de texto de nombre se rellenará automáticamente con el nombre del archivo de medios.
- 5 Haga clic en el icono de carga para examinar y seleccionar el archivo de imagen de disco (por ejemplo, un archivo `.iso`).

6 Haga clic en **Aceptar**.

Cuando se inicie la carga, el archivo de medios aparecerá en la cuadrícula.

Pasos siguientes

En función del tamaño del archivo, la carga podría tardar en completarse. Puede supervisar el estado de la descarga en la vista **Tareas recientes**. Para obtener más información, consulte [Ver tareas](#).

Eliminar un archivo de medios

Puede eliminar del catálogo los archivos de medios que ya no desee utilizar.


Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en el panel izquierdo, seleccione **Medios y otros**.

La lista de archivos de medios aparece en una vista de cuadrícula.

- 2 Haga clic en la barra de listas () que se encuentra a la izquierda del archivo de medios que desea eliminar y seleccione **Eliminar**.
- 3 Confirme la eliminación.

El archivo de medios eliminado se quitará de la vista de cuadrícula.

Descargar un archivo de medios

Puede descargar un archivo de medios desde un catálogo.


Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en el panel izquierdo, seleccione **Medios y otros**.

La lista de archivos de medios aparece en una vista de cuadrícula.

- 2 Haga clic en la barra de listas () que se encuentra a la izquierda del archivo de medios que desea descargar y seleccione **Descargar**.

Se inicia la tarea de descarga y el archivo se guarda en la ubicación de descarga predeterminada del navegador web.

Pasos siguientes

En función de cuál sea el tamaño del archivo, esta descarga podría tardar algún tiempo en completarse. Puede supervisar el estado de la descarga en el panel **Tareas recientes**. Para obtener más información, consulte [Ver tareas](#).

Trabajar con catálogos

11

Un catálogo es el lugar donde se guardan plantillas de vApp y archivos de medios en una organización. Los administradores de organización y los autores de catálogos pueden crear catálogos en una organización. El contenido del catálogo se puede compartir con otros usuarios u organizaciones de la instalación de VMware Cloud Director, o bien se puede publicar de forma externa para que puedan acceder a él las organizaciones fuera de la instalación de VMware Cloud Director.

VMware Cloud Director contiene catálogos privados, compartidos y de acceso externo. Los catálogos privados incluyen plantillas de vApp y los archivos de medios que puede compartir con otros usuarios de la organización. Si un administrador del sistema habilita el uso compartido de catálogos para la organización, podrá compartir un catálogo de organización para crear un catálogo al que puedan acceder otras organizaciones de la instalación de VMware Cloud Director. Si un administrador del sistema habilita la publicación externa de catálogos para la organización, puede publicar un catálogo de organización para que puedan acceder a él organizaciones fuera de la instalación de VMware Cloud Director. Una organización fuera de la instalación de VMware Cloud Director debe suscribirse a un catálogo publicado de forma externa para poder acceder a su contenido.

Puede cargar un paquete OVF directamente a un catálogo, guardar una vApp como una plantilla de vApp o importar una plantilla de vApp desde vSphere. Consulte [Crear una plantilla de vApp desde un archivo OVF](#) y [Guardar una vApp como plantilla de vApp en un catálogo](#).

Los miembros de una organización pueden acceder a plantillas de vApp y a archivos de medios que son propios o que se han compartido con ellos. Los administradores de organización y administradores del sistema pueden compartir un catálogo con todos los socios de una organización o con usuarios y grupos específicos de una organización. Consulte [Compartir un catálogo](#).

Este capítulo incluye los siguientes temas:

- [Ver catálogos](#)
- [Crear un catálogo](#)
- [Compartir un catálogo](#)
- [Eliminar un catálogo](#)
- [Cambiar el propietario de un catálogo](#)

- [Administrar metadatos de un catálogo](#)
- [Publicar un catálogo](#)
- [Suscribirse a un catálogo externo](#)
- [Actualizar la dirección URL de ubicación y la contraseña de un catálogo suscrito](#)
- [Sincronizar un catálogo suscrito](#)



Ver catálogos

Puede acceder a catálogos compartidos con usted en la organización. Puede acceder a catálogos públicos si un administrador de la organización ha hecho que sean accesibles en la organización.

El acceso al catálogo se controla mediante el uso compartido de catálogos, no mediante los derechos de su función. Puede acceder únicamente a los catálogos o los elementos de catálogo que se han compartido con usted. Para obtener más información, consulte [Compartir un catálogo](#).

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en el panel izquierdo, seleccione **Catálogos**.

La lista de catálogos aparece en una vista de cuadrícula.
- 2 (Opcional) Configure la vista de cuadrícula para que contenga los elementos que desea ver.
 - a En la vista de cuadrícula, haga clic en el icono del editor de cuadrícula () que aparece debajo de la lista de catálogos.
 - b Seleccione los elementos que desea incluir en la vista de cuadrícula, como la versión, la descripción, el estado, etc.
 - c Haga clic en **Aceptar**.
La cuadrícula muestra los elementos seleccionados para cada catálogo.
- 3 (Opcional) En la vista de cuadrícula, use la barra de listas () para mostrar las acciones que puede realizar en cada catálogo.

Por ejemplo, puede compartir o eliminar un catálogo.

Crear un catálogo

Puede crear catálogos nuevos y asociarlos con una política de almacenamiento.

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en el panel izquierdo, seleccione **Catálogos**.
La lista de catálogos aparece en una vista de cuadrícula.
- 2 Haga clic en **Nuevo** para crear un catálogo nuevo.
- 3 Escriba el nombre y, si lo desea, una descripción del catálogo.
- 4 (opcional) Determine si desea asignar una política de almacenamiento al catálogo y elija una.
- 5 Haga clic en **Aceptar**.

Resultados

El catálogo nuevo aparecerá en la vista de cuadrícula en la pestaña **Catálogos**.


Compartir un catálogo

Puede compartir un catálogo con todos los miembros de la organización o con miembros específicos.

Requisitos previos

- Esta operación requiere los derechos incluidos en la función predefinida **Autor de catálogo** o un conjunto de derechos equivalente.
- Debe ser el propietario del catálogo.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en el panel izquierdo, seleccione **Catálogos**.
La lista de catálogos aparece en una vista de cuadrícula.
- 2 Haga clic en la barra de listas () que se encuentra a la izquierda del catálogo que desea compartir y seleccione **Compartir**.
La lista de usuarios que pueden acceder al catálogo se muestra en la vista de cuadrícula de la ventana **Compartir catálogo**.
- 3 Haga clic en **Agregar** para compartir el catálogo con otros usuarios.

Opción	Descripción
Compartir con todos en esta organización	Conceda acceso a todos los usuarios y los grupos de la organización.
Compartir con usuarios y grupos específicos	Seleccione los usuarios o los grupos a quienes desee conceder acceso al catálogo y haga clic en Agregar .

4 Seleccione el nivel de acceso.

Opción	Descripción
Solo lectura	Los usuarios que pueden acceder a este catálogo tienen acceso de lectura a las plantillas de vApp y los archivos ISO del catálogo.
Leer/escribir	Los usuarios que pueden acceder a este catálogo tienen acceso de lectura a las plantillas de vApp y los archivos ISO del catálogo, y pueden agregar al catálogo plantillas de vApp y archivos ISO.
Control total	Los usuarios con acceso a este catálogo tienen control total sobre el contenido y la configuración del catálogo.

5 Haga clic en **Aceptar**.

Los usuarios o los grupos que ahora pueden acceder al catálogo aparecen en la vista de cuadrícula del cuadro de diálogo **Compartir catálogo**.

6 (opcional) Elija compartir el acceso de solo lectura con los administradores de todas las demás organizaciones.

7 Haga clic en **Guardar**.

Resultados

En la pestaña **Catálogos**, cambiará el estado Compartido de este catálogo en la vista de cuadrícula.

Eliminar un catálogo

Puede eliminar un catálogo de una organización.

Requisitos previos

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

Nota El catálogo no debe contener plantillas de vApp ni archivos de medios. Puede mover estos elementos a otro catálogo o eliminarlos.

Procedimiento

1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en el panel izquierdo, seleccione **Catálogos**.

La lista de catálogos aparece en una vista de cuadrícula.

2 Haga clic en la barra de listas () que se encuentra a la izquierda del catálogo que desea eliminar y seleccione **Eliminar**.

3 Confirme la eliminación.

El elemento de catálogo eliminado se quitará de la vista de cuadrícula.

Cambiar el propietario de un catálogo

Los **administradores de organización** pueden cambiar el propietario de un catálogo.

Para eliminar el usuario propietario de un catálogo, debe cambiar el propietario o eliminar el catálogo.


Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en el panel izquierdo, seleccione **Catálogos**.

La lista de catálogos aparece en una vista de cuadrícula.

- 2 Haga clic en la barra de listas () situada a la izquierda de un catálogo y seleccione **Cambiar propietario**.

En la vista de cuadrícula de la ventana **Cambiar propietario** se muestra la lista de usuarios que pueden acceder al catálogo.

- 3 Seleccione el usuario que desea convertir en el nuevo propietario del catálogo y haga clic en **Aceptar**.

Resultados

Al realizar esta acción, cambia el nombre del propietario del catálogo en la vista de cuadrícula de la pestaña **Catálogos**.


Administrar metadatos de un catálogo

Como **administrador de organización** o **propietario de catálogo**, puede crear o actualizar los metadatos de los catálogos que posea.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en el panel izquierdo, seleccione **Catálogos**.

La lista de catálogos aparece en una vista de cuadrícula.

- 2 Haga clic en la barra de listas () que se encuentra a la izquierda de un catálogo y seleccione **Metadatos**.

Los metadatos del catálogo seleccionado se mostrarán en una vista de cuadrícula.

- 3 (opcional) Para agregar metadatos, haga clic en **Agregar**.
 - a Introduzca el nombre de los metadatos.

Este debe ser diferente de los nombres de los metadatos asociados a este objeto.
 - b Seleccione el tipo de metadatos, como **Texto**, **Número**, **Fecha y hora** o **Sí o No**.
 - c Introduzca el valor de los metadatos.
 - d Haga clic en **Guardar**.
- 4 (opcional) Actualice los metadatos existentes.

No se puede actualizar el nombre de los metadatos.

 - a Actualice el tipo de metadatos.
 - b Introduzca un nuevo valor de metadatos.
 - c Haga clic en **Guardar**.
- 5 (opcional) Elimine los metadatos existentes.
 - a Haga clic en el icono Eliminar.
 - b Haga clic en **Guardar**.

Publicar un catálogo


Si el **administrador del sistema** le ha otorgado acceso a catálogos, podrá publicar un catálogo de forma externa para hacer que sus plantillas de vApp y archivos de medios estén disponibles para que puedan suscribirse organizaciones fuera de la instalación de VMware Cloud Director.

Requisitos previos

Compruebe que el **administrador del sistema** ha habilitado la publicación de catálogos externos para la organización y le ha otorgado acceso a los catálogos.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en el panel izquierdo, seleccione **Catálogos**.

La lista de catálogos aparece en una vista de cuadrícula.
- 2 Haga clic en la barra de listas () que se encuentra a la izquierda del catálogo que desea publicar y seleccione **Publicar configuración**.
- 3 Seleccione **Habilitar publicación** y, si lo desea, escriba una contraseña para acceder al catálogo.

Únicamente se admiten caracteres ASCII.
- 4 Haga clic en **Guardar**.

Suscribirse a un catálogo externo

Puede suscribirse a un catálogo externo y, por tanto, crear una copia de solo lectura de un catálogo publicado de forma externa. No puede modificar los catálogos suscritos.

Requisitos previos

- Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.
- El **administrador del sistema** debe conceder a su organización permiso para poder suscribirse a catálogos externos.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en el panel izquierdo, seleccione **Catálogos**.

La lista de catálogos aparece en una vista de cuadrícula.

- 2 Haga clic en **Nuevo** para crear un catálogo nuevo.
- 3 Escriba el nombre y, si lo desea, una descripción del catálogo.
- 4 Elija suscribirse a un catálogo externo y proporcione la dirección URL de suscripción.
- 5 Escriba la contraseña opcional para acceder al catálogo.
- 6 Determine si desea descargar automáticamente el contenido del catálogo externo.
- 7 Haga clic en **Aceptar**.

Actualizar la dirección URL de ubicación y la contraseña de un catálogo suscrito

Después de crear un catálogo suscrito, puede actualizar la URL de ubicación y la contraseña del catálogo suscrito.


Requisitos previos

- Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.
- Debe haber creado un catálogo suscrito.
- El **administrador del sistema** debe conceder a su organización permiso para poder suscribirse a catálogos externos.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en el panel izquierdo, seleccione **Catálogos**.

La lista de catálogos aparece en una vista de cuadrícula.

- 2 Haga clic en la barra de listas () que se encuentra a la izquierda de un catálogo suscrito y seleccione **Configuración de suscripción**.

Si no se trata de un catálogo suscrito, la opción aparecerá atenuada.

- 3 Actualice la dirección URL de ubicación y la contraseña para este catálogo suscrito.
- 4 Determine si desea descargar automáticamente el contenido del catálogo externo.
- 5 Haga clic en **Guardar**.

Sincronizar un catálogo suscrito

Después de crear un catálogo suscrito, puede sincronizarlo con el catálogo original para determinar si hay cambios. Por ejemplo, si cambian los metadatos del catálogo original, cuando realiza la sincronización, se actualizan los metadatos del catálogo suscrito.


Requisitos previos

- Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.
- Debe haber creado un catálogo suscrito.
- El **administrador del sistema** debe conceder a su organización permiso para poder suscribirse a catálogos externos.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en el panel izquierdo, seleccione **Catálogos**.

La lista de catálogos aparece en una vista de cuadrícula.

- 2 Haga clic en la barra de listas () que se encuentra a la izquierda de un catálogo suscrito y seleccione **Sincronizar**.

Si no se trata de un catálogo suscrito, la opción aparecerá atenuada.

El catálogo suscrito se sincronizará con el original.

Trabajar con plantillas de centros de datos virtuales de organización

12

Como administrador de organización o si es titular de cualquier función que tiene derechos para ver y crear instancias de plantillas de centro de datos virtual de organización, puede crear centros de datos virtuales de organización adicionales.

Una plantilla de centro de datos virtual de organización especifica una configuración para un centro de datos virtual de organización y, de forma opcional, una puerta de enlace Edge y una red de centros de datos virtuales de organización. Los administradores del sistema pueden permitir a los administradores de organización crear estos recursos en sus organizaciones. Para ello crearán plantillas de centros de datos virtuales de organización y las compartirán con estas organizaciones.

Al crear y compartir plantillas de centros de datos virtuales, los administradores del sistema pueden habilitar el aprovisionamiento de autoservicio de centros de datos virtuales de organización a la vez que conservan el control administrativo sobre la asignación de recursos del sistema como, por ejemplo, centros de datos virtuales de proveedor y redes externas.

Los administradores del sistema crean plantillas de centro de datos virtual de organización y proporcionan a diferentes organizaciones acceso a las plantillas.

Si se ha proporcionado a su organización acceso a plantillas de centro de datos virtual, puede utilizar VMware Cloud Director Tenant Portal para crear centros de datos virtuales a partir de las plantillas disponibles.

Este capítulo incluye los siguientes temas:

- [Ver plantillas disponibles del centro de datos virtual](#)
- [Crear instancias de un centro de datos virtual desde una plantilla](#)

Ver plantillas disponibles del centro de datos virtual

Puede ver las plantillas de centro de datos virtual de organización que un administrador del sistema ha creado para usted.

Vea las plantillas de centro de datos virtual antes de crear un nuevo centro de datos virtual de organización a partir de una plantilla de centro de datos virtual.

Requisitos previos

Esta operación requiere los derechos incluidos en la función predefinida **Administrador de organización** o una función que tenga derechos para ver y crear instancias de plantillas de centros de datos virtuales de organización.

Procedimiento

- ◆ En la barra de navegación superior, haga clic en **Bibliotecas** y, en el panel izquierdo, seleccione **Plantillas de VDC de organización**.

La lista de plantillas de centros de datos virtuales se muestra en una vista de cuadrícula.

Pasos siguientes

Revise las descripciones de las plantillas de centro de datos virtual de organización y seleccione la plantilla desde la que desea crear un nuevo centro de datos virtual de organización.

Crear instancias de un centro de datos virtual desde una plantilla

Cuando un administrador del sistema crea una plantilla de centro de datos virtual (Virtual Data Center, VDC) de organización y publica la plantilla en su organización, usted puede crear un VDC de organización a partir de la plantilla.

Requisitos previos

Esta operación requiere los derechos incluidos en la función predefinida **Administrador de organización** o una función que tenga derechos para ver y crear instancias de plantillas de VDC de organización.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en el panel izquierdo, seleccione **Plantillas de VDC de organización**.

La lista de plantillas de centros de datos virtuales se muestra en una vista de cuadrícula.

- 2 Seleccione una plantilla y haga clic en **Nuevo VDC**.

A partir de VMware Cloud Director 10.2.2, después de seleccionar una plantilla, debe hacer clic en **Crear instancias de VDC**.

- 3 Escriba un nombre para el VDC y, opcionalmente, una descripción.
- 4 Haga clic en **Crear**.

Resultados

Se genera una instancia de creación del nuevo centro de datos virtual de organización, la que puede tardar unos minutos. Puede ver el progreso de la tarea en el panel **Tareas recientes**.

Pasos siguientes

Puede administrar el centro de datos virtual de organización recién creado mediante la creación de máquinas virtuales y vApps, la administración de la configuración de red y seguridad, entre otras acciones.

Administración de usuarios, grupos y funciones

13

Puede agregar administradores de organización a VMware Cloud Director de forma individual o como parte de un grupo LDAP. También puede agregar y modificar las funciones que determinan los derechos que tiene un usuario dentro de su organización.

Importante Debe ser un **administrador de organización** para administrar usuarios, grupos y funciones dentro de la organización. El **administrador del sistema** puede publicar una o varias funciones globales para el tenant y, como **administrador de organización**, puede verlas en la lista de roles. Esas funciones son, por ejemplo, **Autor de catálogo**, **Autor de vApp**, **Usuario de vApp**, **Administrador de organización**, etc. No puede modificar las funciones de tenant globales predefinidas, pero puede crear y actualizar funciones de tenant personalizadas similares, y asignarlas a los usuarios dentro de su tenant.

Este capítulo incluye los siguientes temas:

- [Administración de usuarios](#)
- [Administración de grupos](#)
- [Funciones y derechos](#)

Administración de usuarios

Desde el portal para tenants, es posible crear, editar, importar y eliminar usuarios. Además, también se pueden desbloquear las cuentas de usuario si un usuario intentó iniciar sesión con una contraseña incorrecta y, como resultado, bloqueó su propia cuenta de usuario.

Crear un usuario

Puede crear un usuario dentro de la organización de VMware Cloud Director.

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Administración**.

- En el panel izquierdo, en **Control de acceso**, haga clic en **Usuarios**.

Aparece la lista de usuarios.

- Haga clic en **Nuevo**.

- Introduzca un nombre de usuario y la configuración de contraseña del usuario.

La longitud mínima de contraseña es de seis caracteres.

- Seleccione si desea habilitar el usuario tras la creación.

- Si desea establecer una limitación específica de los recursos disponibles para el usuario, active el botón de alternancia **Configurar la cuota del usuario**.

Si activa el botón de alternancia, al finalizar este asistente, VMware Cloud Director le redirigirá a la página **Cuotas**. Puede agregar cuotas para la cantidad de clústeres de Tanzu Kubernetes, todas las máquinas virtuales administradas por el usuario o solo las que están en ejecución, la CPU usada, la memoria y el almacenamiento. Seleccione **ilimitado** si desea que el usuario tenga recursos ilimitados del tipo seleccionado.

- Seleccione la función que desea asignar al usuario.

El menú **Funciones disponibles** consta de una lista de funciones predefinidas y las funciones personalizadas que usted o el administrador del sistema pueden haber creado.

Función predefinida	Descripción
Autor de vApp	Los derechos asociados a la función predefinida Autor de vApp permiten a un usuario usar catálogos y crear vApps.
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.
Usuario de vApp	Los derechos asociados a la función predefinida Usuario de vApp permiten a un usuario utilizar vApps existentes.
Administrador de organización	Un usuario con la función predefinida Administrador de organización puede utilizar el portal para tenants de VMware Cloud Director o Cloud Director OpenAPI para administrar usuarios y grupos en la organización y asignarles funciones, incluida la función predefinida Administrador de organización . Un administrador de organización puede utilizar Cloud Director OpenAPI para crear o actualizar objetos de función que son locales para la organización. Otras organizaciones no pueden ver las funciones que un administrador de organización haya creado o modificado.
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 se asigna a un usuario la función Aplazar a proveedor de identidad , el nombre de función suministrado por el proveedor de identidad debe coincidir con una función o un nombre definidos en la organización de manera exacta, y con distinción de mayúsculas y minúsculas.
Autor de catálogo	Los derechos asociados con la función predefinida Autor de catálogo permiten a los usuarios crear y publicar catálogos.

- 8 (opcional) Introduzca la información de contacto, como el nombre, la dirección de correo electrónico, el número de teléfono y el identificador de mensajería instantánea.
- 9 Haga clic en **Guardar**.

Pasos siguientes

Si habilitó la configuración de cuotas para el usuario y VMware Cloud Director le redirige a la página **Cuotas**, consulte [Administrar las cuotas de recursos de un usuario](#).

Importar usuarios

Para agregar usuarios a las organizaciones, puede importar un usuario LDAP o un usuario SAML, y asignarles una función determinada.

Requisitos previos

- Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.
- Compruebe que cuenta con una conexión válida a un servidor LDAP o que [Habilitar el uso de un proveedor de identidad SAML en la organización](#).

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Administración**.
- 2 En el panel izquierdo, en **Control de acceso**, haga clic en **Usuarios**.
Aparece la lista de usuarios.
- 3 Haga clic en **Importar usuarios**.

4 Seleccione el origen desde el que desea importar los usuarios.

Solo verá el servidor SAML o el servidor LDAP de origen que configuró como proveedor de identidad.

Origen	Acción
LDAP	<p>Importe usuarios de un servidor LDAP.</p> <p>a Introduzca un nombre completo o parcial en el cuadro de texto y haga clic en Buscar.</p> <p>b Seleccione los usuarios que desea importar y haga clic en Agregar.</p>
SAML	<p>Importe usuarios de un servidor SAML. Introduzca los nombres de los usuarios que desea importar.</p> <p>Los nombres de usuario deben tener el formato de identificador de nombre que admita el proveedor de identidad SAML configurado para esta organización.</p> <p>Nota Si utiliza vCenter Single Sign-On como proveedor de identidad SAML, los nombres de usuario que importe de un dominio de vCenter Single Sign-On deben tener el formato de nombre principal de usuario (User Principal Name, UPN); por ejemplo, jdoe@mydomain.com.</p> <p>Utilice una línea nueva para cada nombre de usuario.</p>

5 Seleccione la función que desea asignar a los usuarios que va a importar.

6 Haga clic en **Guardar**.

Modificar un usuario

Como administrador de organización, puede modificar la contraseña, el contacto y los ajustes de cuota de la máquina virtual de un usuario existente. Además, también puede cambiar la función del usuario.

Requisitos previos

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

Procedimiento

- En la barra de navegación superior, haga clic en **Administración**.
- En el panel izquierdo, en **Control de acceso**, haga clic en **Usuarios**.
Aparece la lista de usuarios.
- Haga clic en el botón de radio junto al nombre del usuario que desea editar y haga clic en **Modificar**.
- Actualice la configuración que desee modificar.
 - Cambie la contraseña según sea necesario.
 - Seleccione si desea activar o desactivar el usuario.

- c Actualice la función de usuario.
- d Actualice la información de contacto, como el nombre, la dirección de correo electrónico, el número de teléfono y el identificador de mensajería instantánea.
- e Edite la cuota de máquina virtual para el usuario.

5 Haga clic en **Guardar**.

Desactivar o activar una cuenta de usuario

Puede desactivar una cuenta de usuario para evitar que el usuario inicie sesión en VMware Cloud Director. Para eliminar un usuario, primero debe desactivar su cuenta.

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Administración**.
- 2 En el panel izquierdo, en **Control de acceso**, haga clic en **Usuarios**.
Aparece la lista de usuarios.
- 3 Para desactivar una cuenta de usuario, haga clic en el botón de radio junto al nombre de usuario, haga clic en **Deshabilitar** y confirme.
- 4 Para activar una cuenta de usuario que ya ha desactivado, haga clic en el botón de radio junto al nombre de usuario y haga clic en **Habilitar**.

Eliminar un usuario

Puede eliminar un usuario de la organización de VMware Cloud Director si elimina la cuenta de usuario.

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Administración**.
- 2 En el panel izquierdo, en **Control de acceso**, haga clic en **Usuarios**.
Aparece la lista de usuarios.
- 3 Haga clic en el botón de radio junto al nombre del usuario que desea eliminar y haga clic en **Eliminar**.

- 4 Para confirmar que desea eliminar la cuenta de usuario, haga clic en **Aceptar**.

Desbloquear una cuenta de usuario bloqueada

Si se habilitó una política de bloqueo en la organización de VMware Cloud Director, se bloquea una cuenta de usuario tras un número determinado de intentos de inicio de sesión no válidos. Puede desbloquear la cuenta de usuario bloqueada. La práctica recomendada es cambiar la contraseña del usuario y desbloquear la cuenta.

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Administración**.
- 2 En el panel izquierdo, en **Control de acceso**, haga clic en **Usuarios**.
Aparece la lista de usuarios.
- 3 Haga clic en el botón de radio junto al nombre de usuario y seleccione **Desbloquear**.

Administrar las cuotas de recursos de un usuario

Puede administrar el límite general de uso de recursos de un usuario. Puede agregar, editar y eliminar cuotas de un usuario para máquinas virtuales, clústeres de Tanzu Kubernetes, CPU, memoria o almacenamiento.

Los usuarios pueden ver las cuotas relevantes solo para su tipo de usuario. Los usuarios heredan las cuotas del grupo al que pertenecen. Si un usuario hereda la cuota de un recurso de su grupo y tiene una cuota de nivel de usuario explícita definida para ese recurso, la cuota de nivel de usuario tiene prioridad sobre la cuota de nivel de grupo.

Para obtener información sobre cómo crear o importar usuarios, consulte [Crear un usuario](#) o [Importar usuarios](#).

Requisitos previos

Compruebe que tiene los derechos necesarios para agregar, editar y eliminar cuotas de recursos. De forma predeterminada, los **administradores de organización** pueden cambiar las cuotas de los usuarios.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Administración**.
- 2 En el panel izquierdo, debajo de **Control de acceso**, haga clic en **Usuarios**.

3 Seleccione el nombre de un usuario y elija la pestaña **Cuotas**.

De forma predeterminada, los usuarios no tienen ninguna cuota. Todos los usuarios que pertenecen a un grupo heredan las cuotas del grupo. Si el usuario pertenece a un grupo que tiene una cuota de recursos, la cuota aparece en la lista de cuotas del usuario como no editable.

4 Haga clic en **Editar**.

5 Modifique la cuota del usuario seleccionado.

Puede agregar, editar o eliminar cuotas para la cantidad de clústeres de Tanzu Kubernetes, todas las máquinas virtuales administradas por el usuario o solo las que están en ejecución, la CPU usada, la memoria y el almacenamiento. Seleccione **ilimitado** si desea que el usuario tenga recursos ilimitados del tipo seleccionado.

6 Haga clic en **Guardar**.

Administración de grupos

Si tiene una conexión válida a un servidor LDAP o ha habilitado la organización para que utilice un proveedor de identidad SAML, puede importar un grupo LDAP o un grupo SAML. También se puede editar o eliminar un grupo importado.

Importar un grupo

Para agregar un grupo de usuarios, puede importar un grupo LDAP o un grupo SAML.

Requisitos previos

- Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.
- Compruebe que cuenta con una conexión válida a un servidor LDAP o que [Habilitar el uso de un proveedor de identidad SAML en la organización](#).

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Administración**.
- 2 En el panel izquierdo, debajo de **Control de acceso**, haga clic en **Grupos**.
Aparece la lista de grupos de usuarios.
- 3 Haga clic en **Importar grupo**.

4 Seleccione el origen desde el que desea importar el grupo de usuarios.

Solo puede ver el servidor SAML o el servidor LDAP de origen que configuró como proveedor de identidad.

Origen	Acción
LDAP	<p>Importe un grupo de usuarios de un servidor LDAP.</p> <p>a Introduzca un nombre completo o parcial en el cuadro de texto y haga clic en Buscar.</p> <p>b Seleccione los grupos de usuarios que desea importar y haga clic en Agregar.</p>
SAML	<p>Importe grupos de usuarios de un servidor SAML. Introduzca los nombres de los grupos que desea importar.</p> <p>Utilice una línea nueva para cada nombre de grupo.</p>

5 Seleccione la función que desea asignar al grupo de usuarios que va a importar.

6 Haga clic en **Guardar**.

Pasos siguientes

Si habilitó la configuración de cuotas para el grupo y VMware Cloud Director le redirige a la página **Cuotas**, consulte [Administrar las cuotas de recursos de un grupo](#).

Eliminar un grupo

Puede eliminar un grupo de la organización de VMware Cloud Director si elimina su grupo LDAP.

Cuando se elimina un grupo LDAP, los usuarios que tienen una cuenta VMware Cloud Director basada solo en su pertenencia al grupo se deshabilitan y no pueden iniciar sesión.

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Administración**.
- 2 En el panel izquierdo, debajo de **Control de acceso**, haga clic en **Grupos**.
Aparece la lista de grupos de usuarios.
- 3 Haga clic en el botón de radio junto al nombre del grupo que desea eliminar y haga clic en **Eliminar**.
- 4 Para confirmar que desea eliminar el grupo, haga clic en **Aceptar**.

Editar un grupo

Puede editar un grupo desde el portal para tenants de VMware Cloud Director.

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Administración**.
- 2 En el panel izquierdo, debajo de **Control de acceso**, haga clic en **Grupos**.
Aparece la lista de grupos de usuarios.
- 3 Haga clic en el botón de radio junto al nombre del grupo que desea eliminar y, luego, haga clic en **Editar**.
- 4 Edite el grupo según sea necesario.
 - a Cambie la descripción.
 - b Cambie la función de los miembros del grupo según sea necesario.
- 5 Haga clic en **Guardar**.

Administrar las cuotas de recursos de un grupo

Al establecer la cuota directamente en un grupo, puede administrar el límite general de uso de recursos de cada usuario del grupo. Puede agregar, editar y eliminar cuotas de un grupo para máquinas virtuales, clústeres de Tanzu Kubernetes, CPU, memoria o almacenamiento. Las cuotas de un grupo se aplican a cada miembro del grupo.

Los usuarios heredan las cuotas del grupo al que pertenecen. Si un usuario hereda la cuota de un recurso de su grupo y tiene una cuota de nivel de usuario explícita definida para ese recurso, la cuota de nivel de usuario tiene prioridad sobre la cuota de nivel de grupo.

Para obtener más información sobre la importación de grupos, consulte [Importar un grupo](#).

Requisitos previos

Compruebe que tiene los derechos necesarios para agregar, editar y eliminar cuotas de recursos. De forma predeterminada, los **administradores de organización** pueden cambiar las cuotas de los grupos.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Administración**.
- 2 En el panel izquierdo, debajo de **Control de acceso**, haga clic en **Grupos**.
- 3 Seleccione el nombre de un grupo y elija la pestaña **Cuotas**.

De forma predeterminada, los grupos no tienen ninguna cuota. Todos los usuarios que pertenecen a un grupo heredan las cuotas del grupo. Si el usuario pertenece a un grupo que tiene una cuota de recursos, la cuota aparece en la lista de cuotas del usuario como no editable.

4 Haga clic en **Editar**.

5 Modifique la cuota del grupo seleccionado.

Puede agregar, editar o eliminar cuotas para la cantidad de clústeres de Tanzu Kubernetes, todas las máquinas virtuales administradas por el grupo o solo las que están en ejecución, la CPU usada, la memoria y el almacenamiento. Seleccione **Ilimitado** si desea que el grupo de usuarios tenga recursos ilimitados del tipo seleccionado.

6 Haga clic en **Guardar**.

Funciones y derechos

VMware Cloud Director utiliza funciones y derechos para determinar las acciones que un usuario puede realizar en una organización. VMware Cloud Director incluye una serie de funciones predefinidas con derechos específicos.

Los **administradores del sistema** y los **administradores de organización** deben asignar una función a cada usuario o grupo. El mismo usuario puede tener una función diferente en organizaciones diferentes. Los **administradores del sistema** pueden crear funciones y modificar las funciones existentes para todo el sistema, mientras que los **administradores de organización** solo pueden crear y modificar funciones para la organización que administran.

El portal para tenants de VMware Cloud Director permite a los **administradores de organización** administrar las funciones de su organización. Si un **Administrador del sistema** publica en su organización una o varias funciones de tenant predefinidas, como **administrador de organización**, podrá ver esas funciones pero no podrá modificarlas. Sin embargo, puede crear funciones de tenant personalizadas con derechos similares y asignarlas a los usuarios dentro de su organización.

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

Funciones predeterminadas y sus derechos

Cada función predefinida de VMware Cloud 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. Para obtener una lista

de los derechos que solo están disponibles para la función **Administrador del sistema**, consulte *Guía del portal para administradores de proveedores de servicios de VMware Cloud Director*. 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 Cloud Director OpenAPI 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 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` de su token OAuth.
- 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`, que se encuentra en el elemento `SamlAttributeMapping` del elemento `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**. Para obtener una lista de los derechos de las funciones de tenant predefinidas, consulte [Derechos en funciones globales de tenant predefinidas](#).

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**.

Derechos incluidos en las funciones de tenant globales de VMware Cloud Director

Novedad en esta versión	Nombre del derecho	Administrador de organización	Autor de catálogo	Autor de vApp	Usuario de vApp	Solo acceso a la consola
	Acceso a todos los VDC de organización	✓				
	Catálogo: Agregar una vApp desde Mi nube	✓	✓	✓		
	Catálogo: Cambiar propietario	✓				
	Catálogo: Suscripción a publicación de CLSP	✓	✓			
	Catálogo: Crear o eliminar un catálogo	✓	✓			
	Catálogo: Editar propiedades	✓	✓			
	Catálogo: Publicar	✓	✓			
	Catálogo: Uso compartido	✓	✓			
	Catálogo: Ver ACL	✓	✓			
	Catálogo: Ver catálogos privados y compartidos	✓	✓	✓		
	Catálogo: Ver catálogos publicados	✓				
	Entidad personalizada: Ver todas las instancias de entidad personalizada de la organización	✓				
	Entidad personalizada: Ver instancia de entidad personalizada	✓				
	Disco: Cambiar propietario	✓	✓			
	Disco: Crear	✓	✓	✓		
	Disco: Eliminar	✓	✓	✓		
	Disco: Editar propiedades	✓	✓	✓		
	Disco: Ver estado de cifrado	✓		✓		
	Disco: Ver propiedades	✓	✓	✓	✓	
	General: Control de administrador	✓				
	General: Vista de administrador	✓				
	General: Enviar notificación	✓				

Novedad en esta versión	Nombre del derecho	Administrador de organización	Autor de catálogo	Autor de vApp	Usuario de vApp	Solo acceso a la consola
	Grupo o usuario: Ver	✓				
	Operaciones de nube híbrida: Adquirir ticket de control	✓				
	Operaciones de nube híbrida: Adquirir ticket de túnel desde la nube	✓				
	Operaciones de nube híbrida: Adquirir ticket de túnel a la nube	✓				
	Operaciones de nube híbrida: Crear túnel desde la nube	✓				
	Operaciones de nube híbrida: Crear túnel a la nube	✓				
	Operaciones de nube híbrida: Eliminar túnel desde la nube	✓				
	Operaciones de nube híbrida: Eliminar túnel a la nube	✓				
	Operaciones de nube híbrida: Actualizar etiqueta de endpoint del túnel desde la nube	✓				
	Operaciones de nube híbrida: Ver túnel desde la nube	✓				
	Operaciones de nube híbrida: Ver túnel a la nube	✓				
	Red de organización: Editar propiedades	✓				
	Red de organización: Ver	✓				
	Política de recursos informáticos de vDC de organización: Ver	✓	✓	✓	✓	
	Firewall distribuido de vDC de organización: Configurar reglas	✓				
	Firewall distribuido de vDC de organización: Ver reglas	✓				
	Puerta de enlace de vDC de organización: Configurar DHCP	✓				
	Puerta de enlace de vDC de organización: DNS	✓				
	Puerta de enlace de vDC de organización: Configurar enrutamiento de ECMP	✓				

Novedad en esta versión	Nombre del derecho	Administrador de organización	Autor de catálogo	Autor de vApp	Usuario de vApp	Solo acceso a la consola
	Puerta de enlace de vDC de organización: Configurar firewall	✓				
	Puerta de enlace de vDC de organización: Configurar VPN de IPSec	✓				
	Puerta de enlace de vDC de organización: Configurar equilibrador de carga	✓				
	Puerta de enlace de vDC de organización: Configurar NAT	✓				
	Puerta de enlace de vDC de organización: Configurar enrutamiento estático	✓				
	Puerta de enlace de vDC de organización: Configurar Syslog	✓				
	Puerta de enlace de vDC de organización: Convertir a redes avanzadas	✓				
	Puerta de enlace de vDC de organización: Ver	✓				
	Puerta de enlace de vDC de organización: Ver DHCP	✓				
	Puerta de enlace de vDC de organización: Ver DNS	✓				
	Puerta de enlace de vDC de organización: Ver firewall	✓				
	Puerta de enlace de vDC de organización: Ver VPN de IPSec	✓				
	Puerta de enlace de vDC de organización: Ver equilibrador de carga	✓				
	Puerta de enlace de vDC de organización: Ver NAT	✓				
	Puerta de enlace de vDC de organización: Ver enrutamiento estático	✓				
	Red de vDC de organización: Editar propiedades	✓				
	Red de vDC de organización: Ver propiedades	✓		✓		

Noiedad en esta versión	Nombre del derecho	Administrador de organización	Autor de catálogo	Autor de vApp	Usuario de vApp	Solo acceso a la consola
	Política de almacenamiento de VDC de organización: Ver funcionalidades	✓				
	Perfil de almacenamiento de vDC de organización: Establecer como predeterminado	✓				
	vDC de organización: Editar	✓				
	vDC de organización: Editar ACL	✓				
	vDC de organización: Administrar firewall	✓				
	vDC de organización: Ver	✓	✓			
	vDC de organización: Ver ACL	✓				
	vDC de organización: Ver métricas	✓				
	vDC de organización: Editar afinidad de MV y MV	✓	✓	✓		
	Organización: Editar configuración de asociación	✓				
	Organización: Editar configuración de federación	✓				
	Organización: Editar configuración de LDAP	✓				
	Organización: Editar política de concesiones	✓				
	Organización: Editar configuración de OAuth	✓				
	Organización: Editar política de contraseña	✓				
	Organización: Editar propiedades	✓				
	Organización: Editar política de cuotas	✓				
	Organización: Editar configuración SMTP	✓				
	Organización: Importar usuario o grupo de IdP mientras se edita ACL de VDC	✓				
	Organización: Ver	✓	✓	✓		
	Organización: Ver métricas	✓				

Novedad en esta versión	Nombre del derecho	Administrador de organización	Autor de catálogo	Autor de vApp	Usuario de vApp	Solo acceso a la consola
✓	Capacidades de política de cuota: Ver	✓				
	Función: Crear, editar, eliminar o copiar	✓				
	Biblioteca de servicios: Ver bibliotecas de servicios	✓				
	Complementos de interfaz de usuario: Ver	✓	✓	✓	✓	
	Plantilla de vApp o medios: Copiar	✓	✓	✓		
	Plantilla de vApp o medios: Crear o cargar	✓	✓			
	Plantilla de vApp o medios: Editar	✓	✓	✓		
	Plantilla de vApp o medios: Ver	✓	✓	✓	✓	
	Plantilla de vApp: Cambiar propietario	✓	✓			
	Plantilla de vApp: Retirar	✓	✓	✓	✓	
	Plantilla de vApp: Descargar	✓	✓			
	vApp: Cambiar propietario	✓				
	vApp: Copiar	✓	✓	✓	✓	
	vApp: Crear o reconfigurar	✓	✓	✓		
	vApp: Eliminar	✓	✓	✓	✓	
	vApp: Descargar	✓	✓	✓		
	vApp: Editar propiedades	✓	✓	✓	✓	
	vApp: Editar política de recursos informáticos de la máquina virtual	✓	✓	✓		
	vApp: Editar CPU de MV	✓	✓	✓		
	vApp: Editar disco duro de MV	✓	✓	✓		
	vApp: Editar memoria de MV	✓	✓	✓		
	vApp: Editar red de MV	✓	✓	✓	✓	
	vApp: Editar propiedades de MV	✓	✓	✓	✓	
	vApp: Administrar configuración de contraseña de MV	✓	✓	✓	✓	✓

Novedad en esta versión	Nombre del derecho	Administrador de organización	Autor de catálogo	Autor de vApp	Usuario de vApp	Solo acceso a la consola
	vApp: Operaciones de energía	✓	✓	✓	✓	
	vApp: Uso compartido	✓	✓	✓	✓	
	vApp: Operaciones de instantánea	✓	✓	✓	✓	
	vApp: Cargar	✓	✓	✓		
	vApp: Usar consola	✓	✓	✓	✓	✓
	vApp: Ver ACL	✓	✓	✓	✓	
	vApp: Ver estado de cifrado de MV y sus discos	✓		✓		
	vApp: Ver métricas de MV	✓		✓	✓	
	vApp: Opciones de inicio de MV	✓	✓	✓		
	vApp: Metadatos de MV para vCenter	✓	✓	✓		
✓	Grupo de VDC: Configurar	✓				
✓	Grupo de VDC: Ver	✓				
✓	Grupo de VDC: Configurar registro	✓				
	Plantilla de VDC: Crear instancia	✓				
	Plantilla de VDC: Ver	✓				

Crear una función de tenant personalizada

Los administradores de organización pueden utilizar el portal para tenants para crear objetos de función de tenant personalizada en las organizaciones que administran.

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Administración**.
- 2 En el panel izquierdo, debajo de **Control de acceso**, haga clic en **Funciones**.
Aparece la lista de funciones.
- 3 Haga clic en **Agregar**.

- 4 Escriba un nombre y, si lo desea, una descripción de la función.
- 5 Expanda los derechos de la función y selecciónelos.

Los derechos se agrupan en categorías y subcategorías que permiten ver o administrar objetos.

Opción	Descripción
Control de acceso	Derechos que controlan el acceso para ver y administrar determinados objetos.
Administración	Derechos que controlan el acceso administrativo.
Proceso	Derechos que controlan el acceso y la administración de los centros de datos virtuales de organización y de proveedor, las vApps, las plantillas de centros de datos virtuales de organización, los grupos de máquinas virtuales y la supervisión de máquinas virtuales.
Extensiones	Derechos que controlan el acceso a complementos y extensiones de VMware Cloud Director adicionales.
Infraestructura	Derechos que controlan el acceso y la administración de los objetos de infraestructura, como los almacenes de datos, los discos, los hosts, etc.
Bibliotecas	Derechos que controlan el acceso y la administración de los catálogos y sus elementos.
Red	Derechos que controlan el acceso y la administración de la configuración de red.

- 6 Haga clic en **Guardar**.

Editar una función de tenant personalizada

Los administradores de organización pueden utilizar el portal para tenants con el fin de editar objetos de funciones de tenant personalizadas en las organizaciones que administran. Como administrador de organización, solo puede ver las funciones de tenant globales que un administrador del sistema ha publicado en su organización. No puede editar las funciones de tenant globales.

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Administración**.
- 2 En el panel izquierdo, debajo de **Control de acceso**, haga clic en **Funciones**.
Aparece la lista de funciones.
- 3 Haga clic en el botón de radio junto a la función que desea editar y haga clic en **Editar**.

- 4 Modifique la configuración de la función según sea necesario.
 - a Cambie el nombre y, si lo desea, la descripción de la función.
 - b Edite los derechos de la función.
- 5 Haga clic en **Guardar**.

Eliminar una función

Los administradores de organización pueden utilizar el portal para tenants para eliminar objetos de función en las organizaciones que administran.

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Administración**.
- 2 En el panel izquierdo, debajo de **Control de acceso**, haga clic en **Funciones**.

Aparece la lista de funciones.
- 3 Haga clic en el botón de radio junto a la función que desea eliminar y haga clic en **Eliminar**.
- 4 Haga clic en **Aceptar** para confirmar que desea eliminar la función.

Configurar proveedores de identidad

14

Puede integrar la nube con un proveedor de identidad externo e importar usuarios y grupos a su organización.

Asimismo, puede habilitar la organización para que utilice un proveedor de identidad SAML o configurar una conexión de servidor LDAP.

Este capítulo incluye los siguientes temas:

- [Habilitar el uso de un proveedor de identidad SAML en la organización](#)
- [Editar la configuración LDAP de una organización](#)
- [Configurar, probar y sincronizar una conexión LDAP](#)

Habilitar el uso de un proveedor de identidad SAML en la organización

Habilite en la organización el uso de un proveedor de identidad de Lenguaje de marcado de aserción de seguridad (SAML), también denominado inicio de sesión único, para importar de él usuarios y grupos y permitir a los usuarios importados iniciar sesión en la organización con las credenciales establecidas en dicho proveedor.

Cuando importa los usuarios y grupos, el sistema extrae una lista de atributos del token SAML, si está disponible, y los usa para interpretar la información correspondiente sobre el usuario que intenta iniciar sesión.

- `email address = "EmailAddress"`
- `user name = "UserName"`
- `full name = "FullName"`
- `user's groups = "Groups"`
- `user's roles = "Roles"`

El atributo funciones se puede configurar.

Se necesita información relacionada con el grupo si un usuario no se ha importado directamente, pero se espera que dicho usuario pueda iniciar sesión debido a que pertenece a grupos importados. Un usuario puede pertenecer a varios grupos y, por tanto, puede tener varias funciones durante una sesión.

Si se asigna la función **Aplazar a proveedor de identidad** a un grupo o un usuario importados, las funciones se asignan con base en la información recopilada a partir del atributo Funciones del token. Si se utiliza un atributo diferente, este nombre de atributo solo se puede configurar mediante el uso de la API, y únicamente el atributo Funciones es configurable. Si se utiliza la función **Aplazar a proveedor de identidad**, pero no se puede extraer información de funciones, el usuario puede iniciar sesión, pero no tiene derechos para realizar actividades.

Requisitos previos

- Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.
- Compruebe que tiene acceso a un proveedor de identidad compatible con SAML 2.0.
- Compruebe que recibe los metadatos necesarios del proveedor de identidad SAML. Debe importar los metadatos a VMware Cloud Director de forma manual o como un archivo XML. Los metadatos deben incluir la siguiente información:
 - La ubicación del servicio de inicio de sesión único
 - La ubicación del servicio de cierre de sesión único
 - La ubicación del certificado X.509 del servicio

Para obtener información sobre la configuración y la adquisición de metadatos de un proveedor de identidad SAML, consulte la documentación relativa a su proveedor de identidad SAML.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Administración**.
- 2 En **Proveedores de identidad**, haga clic en **SAML**.
- 3 Haga clic en **Editar**.
- 4 En la pestaña **Proveedor de servicios**, introduzca el ID de entidad.

El ID de entidad es el identificador único de su organización para el proveedor de identidades. Puede utilizar el nombre de la organización, o cualquier otra cadena que cumpla los requisitos del proveedor de identidad SAML.

Importante Una vez que se especifica un ID de entidad, no puede eliminarlo. Para cambiar el ID de entidad, debe realizar una reconfiguración completa de SAML para su organización. Para obtener más información sobre los ID de entidad, consulte el documento relacionado con [las aserciones y los protocolos del Lenguaje de marcado de aserción de seguridad \(SAML\) 2.0 de OASIS](#).

- 5 Haga clic en el vínculo **Metadatos** para descargar los metadatos de SAML de su organización.
Los metadatos descargados deben proporcionarse como están al proveedor de identidades.
- 6 Revise la fecha de caducidad del certificado y, si lo desea, haga clic en Volver a generar para volver a generar el certificado utilizado para firmar los mensajes de la federación.
El certificado se incluye en los metadatos de SAML y se utiliza para el cifrado y la firma. El cifrado o la firma pueden ser necesarios dependiendo de cómo se establezca la confianza entre su organización y el proveedor de identidad SAML.
- 7 En la pestaña **Proveedor de identidad**, habilite el botón de alternancia **Utilizar proveedor de identidad SAML**.
- 8 Copie y pegue los metadatos SAML que recibió del proveedor de identidad en el cuadro de texto o haga clic en **Cargar** para buscar y cargar los metadatos desde un archivo XML.
- 9 Haga clic en **Guardar**.

Pasos siguientes

- Configure el proveedor SAML con los metadatos de VMware Cloud Director. Consulte la documentación del proveedor de identidad SAML y la *Guía de instalación, configuración y actualización de VMware Cloud Director*.
- Importe usuarios y grupos de su proveedor de identidad SAML. Consulte [Capítulo 13 Administración de usuarios, grupos y funciones](#).

Editar la configuración LDAP de una organización

Puede configurar una organización para que utilice la conexión LDAP del sistema como origen compartido de usuarios y grupos. Si lo prefiere, también puede configurarla para que utilice una conexión LDAP independiente como origen privado de usuarios y grupos.

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Administración**.
- 2 En el panel izquierdo, en **Proveedores de identidad**, haga clic en **LDAP**.
Se mostrará la configuración de LDAP actual.
- 3 En la pestaña **Configuración LDAP**, haga clic en **Editar**.

- 4 Configure el origen de usuarios y grupos de LDAP para la 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 de VMware Cloud Director	La organización utiliza la conexión LDAP del sistema de VMware Cloud Director que configuró el proveedor de servicios. Introduzca el nombre distintivo de la unidad organizativa.
Servicio LDAP personalizado	La organización utiliza un servidor LDAP privado como un origen de usuarios y grupos de organización.

Pasos siguientes

Si seleccionó **Servicio LDAP personalizado**, haga clic en la pestaña **LDAP personalizado** para [Configurar, probar y sincronizar una conexión LDAP](#).

Configurar, probar y sincronizar una conexión LDAP

Para configurar una conexión LDAP, debe establecer 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 la conexión LDAP es correcta, se puede sincronizar la información de usuario y grupo con el servidor LDAP en cualquier momento.

Requisitos previos

Si ha pensado conectarse a un servidor LDAP a través de SSL (LDAP over SSL, LDAPS), compruebe que el certificado de dicho servidor es conforme con la identificación de endpoint introducida en Java 8 Update 181. El nombre común (Common Name, CN) o el nombre alternativo del firmante (Subject Alternative Name, SAN) del certificado deben coincidir con el FQDN del servidor LDAP. Para obtener más información, consulte los *Cambios de la versión Java 8* en <https://www.java.com>.

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

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	El nombre distintivo (Distinguished Name, DN) de la base es la ubicación en el directorio LDAP en el que se conecta VMware Cloud Director. Para conectarse en el nivel de raíz, introduzca solo los componentes de dominio (por ejemplo, DC=example,DC=com). Para conectarse a un nodo de la estructura de árbol de dominio, introduzca el nombre distintivo de dicho nodo (por ejemplo, OU=ServiceDirector,DC=example,DC=com). La conexión a un nodo limita el alcance del directorio disponible para VMware Cloud Director.
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 botón Cargar e importe un certificado SSL de LDAP, o bien seleccione Aceptar todos los certificados .
Método de autenticación	La autenticación simple consiste en enviar el DN y la contraseña del usuario al servidor LDAP. Si se utiliza LDAP, la contraseña LDAP se envía por la red en texto sin formato. Si desea usar Kerberos, debe configurar la conexión LDAP mediante la API de vCloud.
Nombre de usuario	Introduzca el nombre distintivo (DN) de LDAP completo de una cuenta de servicio con derechos de administrador de dominio. VMware Cloud Director usa esta cuenta para consultar el directorio LDAP y recuperar la información del usuario. Si en su servidor LDAP está habilitado el soporte para lectura anónima, puede dejar vacíos estos cuadros de texto.
Contraseña	La contraseña de la cuenta de servicio que se conecta al servidor LDAP. Si la compatibilidad de lectura anónima está habilitada en su servidor LDAP, puede dejar estos cuadros de texto en blanco.

- 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 Si seleccionó la casilla de verificación **Utilizar SSL** y el certificado del servidor LDAPS aún no es de confianza, en la ventana **Certificado de confianza**, confirme si confía en el certificado que ha presentado el endpoint de servidor.
- 6 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**.
- 7 Para sincronizar VMware Cloud Director con el servidor LDAP configurado, haga clic en **Sincronizar**.

VMware Cloud 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.

Administrar certificados

15

Puede importar, descargar, editar y eliminar certificados de VMware Cloud Director. Puede copiar los datos de PEM del certificado en el portapapeles.

Este capítulo incluye los siguientes temas:

- [Importar certificados de confianza](#)
- [Importar certificados en la biblioteca de certificados](#)

Importar certificados de confianza

Puede importar certificados de servidores con los que VMware Cloud Director se comunica, como vCenter Server, NSX Manager, etc.

Cuando usa VMware Cloud Director en modo FIPS, debe usar claves privadas compatibles con FIPS. Puede usar pyOpenSSL para generar claves privadas en formato PKCS#8 compatible con FIPS. Si genera claves privadas PKCS#8 mediante OpenSSL, las claves privadas no son compatibles con FIPS. Para obtener más información sobre el modo FIPS, consulte [Activar el modo FIPS en las celdas del grupo de servidores](#) o [Activar o desactivar el modo FIPS en el dispositivo de VMware Cloud Director](#).

Requisitos previos

Compruebe que ha iniciado sesión como **administrador del sistema** o **administrador de la organización**.

Procedimiento

- 1 En la barra de navegación superior, seleccione **Administración**.
- 2 En el panel izquierdo, en **Administración de certificados**, seleccione **Certificados de confianza** y haga clic en **Importar**.
- 3 Cargue un archivo PEM que contenga los certificados que desea importar y haga clic en **Importar**.
- 4 (opcional) Edite el nombre del certificado.
- 5 Haga clic en **Importar**.

Pasos siguientes

- Descargue un certificado.
- Edite el nombre de un certificado.
- Elimine un certificado.
- Copie los datos de PEM en el portapapeles.

Importar certificados en la biblioteca de certificados

En la biblioteca de certificados de VMware Cloud Director, puede importar los certificados utilizados al crear entidades que debe proteger, como servidores, puertas de enlace Edge, etc.

La biblioteca de certificados contiene información sobre certificados individuales, cadenas de certificados, claves privadas, fechas de caducidad de certificados, entidades a las cuales protegen los certificados, etc.

Cuando usa VMware Cloud Director en modo FIPS, debe usar claves privadas y certificados autofirmados compatibles con FIPS. Puede generar claves privadas y certificados autofirmados sin cifrar mediante pyOpenSSL. Si genera claves privadas y certificados autofirmados mediante OpenSSL, los certificados y las claves privadas no son compatibles con FIPS. Para obtener más información sobre el modo FIPS, consulte [Activar el modo FIPS en las celdas del grupo de servidores](#) o [Activar o desactivar el modo FIPS en el dispositivo de VMware Cloud Director](#).

Requisitos previos

Compruebe que ha iniciado sesión como **administrador del sistema** o **administrador de la organización**.

Procedimiento

- 1 En la barra de navegación superior, seleccione **Administración**.
- 2 En el panel izquierdo, en **Administración de certificados**, seleccione **Biblioteca de certificados** y haga clic en **Importar**.
- 3 Escriba un nombre y, si lo desea, una descripción para este certificado de la biblioteca de certificados y haga clic en **Siguiente**.
- 4 Cargue un archivo PEM que contenga la cadena de certificados que desea importar y haga clic en **Siguiente**.
- 5 (opcional) Cargue un archivo de clave privada.

Es posible que el archivo de clave privada no esté protegido con una frase de contraseña.

- 6 Haga clic en **Importar**.

Resultados

El certificado importado aparecerá en la lista de certificados disponibles durante la creación de las entidades que se deben proteger.

Pasos siguientes

- Descargue un certificado.
- Edite el nombre y la descripción de un certificado.
- Elimine un certificado. Solo se pueden eliminar los certificados que no protejan ninguna entidad.
- Copie los datos de PEM del certificado en el portapapeles.

Administrar la organización

16

Como **administrador de organización**, puede modificar varios ajustes de la organización, como el nombre, la configuración de correo electrónico y dominio, los metadatos, las políticas, etc.

Puede utilizar la API de VMware Cloud Director para suscribirse a mensajes sobre eventos y tareas de la organización a través del protocolo MQTT. Para obtener información sobre cómo suscribirse a eventos y tareas con un cliente de MQTT, consulte la *Guía de instalación, configuración y actualización de VMware Cloud Director*.

Este capítulo incluye los siguientes temas:

- Editar el nombre y la descripción de la organización
- Modificar la configuración de correo electrónico
- Probar la configuración SMTP
- Modificar la configuración de dominio para las máquinas virtuales de la organización
- Trabajar con varios sitios
- Configurar y administrar implementaciones multisitio
- Entender las concesiones
- Modificar las políticas de concesión de la vApp y la plantilla de vApp dentro de la organización
- Modificar las políticas de cuenta de usuario y contraseña en la organización
- Crear un panel de control de avisos

Editar el nombre y la descripción de la organización

Puede editar el nombre completo y la descripción de la organización.

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Administración**.

2 En **Configuración**, haga clic en **General**.

Se mostrará la lista de los ajustes generales, como el nombre de la organización, la URL predeterminada, el nombre completo y la descripción.

3 Para modificar el nombre completo y la descripción de la organización, haga clic en **Editar**.

4 Aplique los cambios necesarios y haga clic en **Guardar**.

Modificar la configuración de correo electrónico

Puede revisar y modificar la configuración de correo electrónico predeterminada que se estableció cuando el administrador del sistema creó la organización.

VMware Cloud Director envía alertas por correo electrónico cuando debe comunicar información importante (por ejemplo, cuando un almacén de datos se está quedando sin espacio). De forma predeterminada, una organización envía alertas de correo electrónico a los administradores del sistema o a una lista de direcciones de correo electrónico especificadas en el nivel del sistema mediante un servidor SMTP definido en dicho nivel. Puede modificar la configuración de correo electrónico en el nivel de organización si desea que VMware Cloud Director envíe alertas para esa organización a un conjunto de direcciones de correo electrónico distinto al especificado en el nivel del sistema o si desea que la organización utilice un servidor SMTP para enviar alertas diferente del especificado en el nivel del sistema.

Requisitos previos

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

Procedimiento

1 En la barra de navegación superior, haga clic en **Administración**.

2 En **Configuración**, haga clic en **Correo electrónico**.

Aparecerá la configuración de correo electrónico de la organización.

3 Haga clic en **Editar**.

4 Edite la configuración del servidor SMTP en la pestaña **Servidor SMTP**.

- a Seleccione si desea utilizar un servidor SMTP personalizado o el predeterminado.
- b Si decide utilizar un servidor SMTP personalizado, escriba la dirección IP o el nombre de host de DNS del servidor SMTP en el cuadro de texto **Nombre del servidor SMTP**.
- c (opcional) Introduzca el puerto del servidor SMTP.
- d (opcional) Seleccione si desea solicitar la autenticación y escriba un nombre de usuario y una contraseña.

- 5 Para editar la configuración de notificaciones, haga clic en la pestaña **Configuración de notificación**.
 - a Utilice la configuración de notificaciones personalizada.
 - b Introduzca la dirección de correo electrónico que aparece como remitente de los correos electrónicos de la organización.
 - c (opcional) Introduzca el texto que se usará como prefijo del asunto del correo electrónico.
 - d (opcional) Seleccione si desea enviar notificaciones a todos los administradores de la organización o a direcciones de correo electrónico específicas.
 - e (opcional) Si decide enviar notificaciones a direcciones de correo electrónico específicas, introduzca las direcciones separadas por comas.
- 6 Haga clic en **Guardar**.

Probar la configuración SMTP

Después de modificar la configuración de correo electrónico de la organización, puede probar la configuración de SMTP.

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Administración**.
- 2 En **Configuración**, haga clic en **Correo electrónico**.

Aparecerá la configuración de correo electrónico de la organización.
- 3 Haga clic en **Probar**.
- 4 Introduzca una dirección de correo electrónico de destino y la contraseña del servidor SMTP para probar la configuración de SMTP y haga clic en el botón **Probar**.

Modificar la configuración de dominio para las máquinas virtuales de la organización

Puede establecer un dominio predeterminado de Windows al que se puedan unir las máquinas virtuales creadas en su organización. Las máquinas virtuales podrán unirse siempre a aquellos dominios para los que tengan credenciales, independientemente de si especifica un dominio predeterminado.

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Administración**.
- 2 En **Configuración**, haga clic en **Personalización de invitado**.
- 3 Habilite la unión de dominio para las máquinas virtuales de la organización.
- 4 Introduzca el nombre de dominio, el nombre de usuario y la contraseña.

Las credenciales que introduzca se aplican a un usuario de dominio convencional, no a un administrador de dominio.

- 5 (opcional) Introduzca una unidad organizativa de cuenta.
- 6 Haga clic en **Guardar**.

Trabajar con varios sitios

La función multisitio de VMware Cloud Director permite a un proveedor de servicios o a un tenant de varias instalaciones (grupos de servidores) de VMware Cloud Director distribuidas geográficamente administrar y supervisar dichas instalaciones y sus organizaciones como entidades únicas.

El portal para tenants de VMware Cloud Director ofrece a los **administradores de organización** una manera de asociar organizaciones en sitios asociados.

Para obtener más información sobre las asociaciones de sitios, consulte la *Guía del portal para administradores de proveedores de servicios de VMware Cloud Director*.

Configurar y administrar implementaciones multisitio

Después de que un **administrador del sistema** haya asociado dos sitios, los **administradores de organización** de cualquier sitio miembro pueden empezar a asociar sus organizaciones.

Para crear una asociación entre dos organizaciones (denominadas Org-A y Org-B en este documento), debe ser un **administrador de organización** de ambas organizaciones, de modo que pueda iniciar sesión en cada organización, recuperar los datos de asociación local y enviar los datos recuperados a la otra organización.

Importante El proceso de asociación de dos organizaciones se puede desglosar lógicamente en dos operaciones de emparejamiento complementarias. La primera operación (en este ejemplo) empareja Org-A en el sitio A con Org-B en el sitio B. Posteriormente, debe emparejar Org-B en el sitio B con Org-A en el sitio A. La asociación estará incompleta si no se realizan ambos emparejamientos.

Requisitos previos

- Los sitios ocupados por las organizaciones deben estar asociados.
- Debe ser un **administrador del sistema** en ambos sitios o un **administrador de organización** en ambas organizaciones.

Procedimiento

- 1 Inicie sesión en el portal para tenants de VMware Cloud Director de Org-A en el sitio A para recuperar los datos de asociación local.
 - a Haga clic en **Administración**.
 - b En **Configuración**, haga clic en **Multisitio**.
 - c Para descargar los datos en formato XML, haga clic en **Exportar datos de asociación local**.

El navegador guarda los datos en un archivo en la carpeta Descargas.

- 2 Inicie sesión en el portal para tenants de VMware Cloud Director de Org-B en el sitio B para enviar los datos de asociación local de Org-A en el sitio A.

- a Haga clic en **Administración**.
- b En **Configuración**, haga clic en **Multisitio**.
- c Haga clic en **Crear nueva asociación de organización**.

Envíe los datos de asociación que ha descargado en el [paso 1](#) a Org-B haciendo clic en la flecha de carga situada debajo del cuadro de texto **XML de asociación nueva** y seleccione los datos de asociación local que ha descargado en el [paso 1](#).

- d Haga clic en **Siguiente** para comprobar y enviar los datos.

El sistema empareja Org-A en el sitio A con Org-B en el sitio B.

- e Haga clic en **Finalizar** para ver la organización asociada.
- f Para ver los detalles de la organización asociada o eliminar la asociación, haga clic en la tarjeta **Nombre de organización**.

- 3 Para completar la asociación, repita los pasos 1 y 2 para recuperar los datos de asociación local de Org-B y enviarlos a Org-A.

Entender las concesiones

La creación de una organización implica la especificación de concesiones. Las concesiones proporcionan un nivel de control sobre el almacenamiento y los recursos informáticos de la organización mediante la especificación de un límite máximo de tiempo de ejecución de las vApps, así como de almacenamiento de las vApps y las plantillas de vApp.

El objetivo de una concesión de tiempo de ejecución es evitar que las vApps inactivas consuman recursos informáticos. Por ejemplo, si un usuario inicia una vApp y se va de vacaciones sin detenerla, la vApp continuará consumiendo recursos.

Una concesión de tiempo de ejecución empieza cuando un usuario inicia una vApp. Cuando una concesión de tiempo de ejecución caduca, VMware Cloud 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, VMware Cloud Director marca la vApp o la plantilla de vApp como caducada, o elimina la vApp o la plantilla de vApp, en función de la política de organización que haya establecido.

Modificar las políticas de concesión de la vApp y la plantilla de vApp dentro de la organización

Puede revisar y modificar las directivas predeterminadas que el administrador del sistema estableció al crear la organización.

Requisitos previos

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

Procedimiento

1 En la barra de navegación superior, haga clic en **Administración**.

2 En **Configuración**, haga clic en **Políticas**.

Puede ver las políticas predeterminadas que configuró el **administrador del sistema**.

3 Haga clic en **Editar**.

4 Edite las concesiones de vApp.

Las concesiones de vApp proporcionan un nivel de control sobre el almacenamiento y los recursos informáticos de la organización mediante la especificación de un límite máximo de tiempo de ejecución y de almacenamiento de las vApps. De igual modo, puede especificar lo que sucede con las vApps cuando caduca la concesión de almacenamiento.

- a Para definir la cantidad de tiempo durante la que se pueden ejecutar las vApps antes de detenerse automáticamente, introduzca la concesión de tiempo de ejecución máxima.
- b Seleccione una acción de caducidad de tiempo de ejecución, como el apagado o la suspensión.

- c Para definir la cantidad de tiempo durante la que permanecen disponibles las vApps detenidas antes de limpiarse automáticamente, introduzca la concesión de almacenamiento máxima.
- d Seleccione una acción de limpieza de almacenamiento, como la eliminación permanente de las vApps o la transferencia de estas a los elementos caducados.

5 Edite la concesión de plantillas de vApp.

Las concesiones de plantillas de vApp proporcionan un nivel de control sobre el almacenamiento y los recursos informáticos de la organización mediante la especificación de la cantidad de tiempo máxima que se pueden almacenar las plantillas de vApp. De igual modo, puede especificar lo que sucede con las plantillas de vApp cuando caduca la concesión de almacenamiento.

- a Para definir la cantidad de tiempo durante la que permanecen disponibles las plantillas de vApp antes de limpiarse automáticamente, introduzca la concesión de almacenamiento máxima.
- b Seleccione una acción de limpieza de almacenamiento, como la eliminación permanente de las plantillas de vApp o la transferencia de estas a los elementos caducados.

6 Haga clic en **Aceptar**.

Modificar las políticas de cuenta de usuario y contraseña en la organización

Puede revisar y modificar las políticas de cuenta de usuario y contraseña predeterminadas que el administrador del sistema estableció al crear la organización.

Las políticas de cuenta de usuario y contraseña definen el comportamiento de VMware Cloud Director cuando un usuario introduce una contraseña no válida.

Requisitos previos

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

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Administración**.
- 2 En **Configuración**, haga clic en **Políticas**.
Puede ver las políticas predeterminadas que configuró el **administrador del sistema**.
- 3 Haga clic en **Editar**.
- 4 Habilitar el bloqueo de la cuenta de usuario después de una cantidad de intentos no válidos de inicio de sesión.
- 5 Introduzca el número de intentos de inicio de sesión no válidos antes de que se bloquee la cuenta de usuario.

- 6 Introduzca el intervalo de tiempo en minutos durante el cual el usuario con una cuenta bloqueada no puede volver a iniciar sesión.
- 7 Haga clic en **Aceptar**.

Crear un panel de control de avisos

Puede crear notificaciones que aparezcan en la parte superior de las páginas de la interfaz de usuario del Tenant Portal. Los mensajes pueden aparecer para los usuarios de una organización o para los usuarios de todas las organizaciones.

No puede editar los avisos una vez que los crea.

Requisitos previos

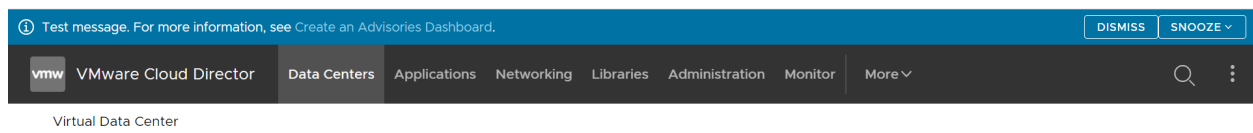
Compruebe que ha iniciado sesión como **administrador del sistema**.

Procedimiento

- 1 En la barra de navegación superior, seleccione **Administración**.
- 2 En el panel izquierdo, en **Configuración**, seleccione **Avisos** y haga clic en **Agregar**.
- 3 En el cuadro de descripción, escriba el texto de la notificación.
Puede usar Markdown básico para agregar vínculos a las notificaciones.
- 4 Seleccione la prioridad del mensaje.
Los mensajes con distintas prioridades aparecen con diferentes colores. Las notificaciones se ordenan según su prioridad. Los avisos obligatorios no se pueden ignorar ni posponer.
- 5 Seleccione el período para el cual desea que aparezca la notificación en la interfaz de usuario.
Puede ver todos los avisos en la pestaña **Avisos**, aunque solo aparecen para el grupo de usuarios seleccionado durante el período elegido.
- 6 Haga clic en **Aceptar**.

Resultados

La notificación aparece sobre la barra de navegación superior del portal seleccionado.



Pasos siguientes

Para eliminar la notificación, seleccione el botón de opción situado junto a ella y haga clic en **Eliminar**. Los avisos aparecen en la pestaña **Avisos** incluso después de que caduquen. Para quitarlos de la lista, debe eliminarlos.

Trabajar con Biblioteca de servicios

17

Los elementos de Biblioteca de servicios de VMware Cloud Director son flujos de trabajo de vRealize Orchestrator que amplían las capacidades de administración de la nube y permiten a los administradores de los proveedores o los tenants supervisar y manipular diferentes servicios.

Este capítulo incluye los siguientes temas:

- [Buscar un servicio](#)
- [Ejecutar un servicio](#)

Buscar un servicio

En la página **Biblioteca de servicios** del portal para tenants de VMware Cloud Director se muestra el conjunto de flujos de trabajo de vRealize Orchestrator que se han importado en VMware Cloud Director y se han publicado en la organización.

Requisitos previos

Esta operación requiere que los derechos de la biblioteca de servicios se incluyan en la función de usuario predefinida.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en **Servicios**, seleccione **Biblioteca de servicios**.

La lista de servicios aparece en una vista de tarjeta con 12 elementos por página, organizados por nombre en orden alfabético. Cada tarjeta muestra el nombre del servicio y una etiqueta que se corresponde con la categoría del servicio donde se importa vRealize Orchestrator.

- 2 En el cuadro de texto **Buscar** que se encuentra en la parte superior de la página, introduzca la primera palabra del nombre del servicio o el nombre de la categoría a la que pertenece el servicio.

a Determine si desea buscar en los nombres del servicio o en las categorías.

Los resultados de la búsqueda se muestran en una vista de tarjetas con doce elementos por página organizados por nombre y en orden alfabético.

Ejecutar un servicio

Los servicios se pueden ejecutar desde la página Biblioteca de servicios del portal para tenants de VMware Cloud Director.

Requisitos previos

Esta operación requiere que los derechos de la biblioteca de servicios se incluyan en la función de usuario predefinida.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en **Servicios**, seleccione **Biblioteca de servicios**.

La lista de servicios aparece en una vista de tarjeta con 12 elementos por página, organizados por nombre en orden alfabético. Cada tarjeta muestra el nombre del servicio y una etiqueta que se corresponde con la categoría del servicio donde se importa vRealize Orchestrator.

- 2 Busque el servicio que desea ejecutar.
- 3 Haga clic en **Ejecutar** en la tarjeta del servicio.

Se abrirá un cuadro de diálogo nuevo. Debe introducir valores para los parámetros de entrada necesarios del servicio.

- 4 Haga clic en **Finalizar** para confirmar la ejecución del servicio.

Pasos siguientes

Puede supervisar el estado de la ejecución en la vista **Tareas recientes**. Para obtener más información, consulte [Ver tareas](#).

A partir de VMware Cloud Director 10.2, los proveedores de servicios pueden utilizar la API de VMware Cloud Director para crear extensiones que proporcionen capacidades de VMware Cloud Director adicionales a los tenants. Si un proveedor de servicios le otorgó acceso, puede administrar las entidades definidas y compartirlas con otros tenants.

Los proveedores de servicios pueden crear entidades definidas en tiempo de ejecución (RDE), lo que permite que las extensiones almacenen y manipulen información específica de la extensión en VMware Cloud Director. Por ejemplo, una extensión de Kubernetes puede almacenar información sobre los clústeres de Kubernetes que administra en las RDE. A continuación, la extensión puede proporcionar API de extensión para administrar esos clústeres con la información de las RDE.

Acceso a entidades definidas

Dos mecanismos complementarios controlan el acceso a las RDE.

- **Derechos:** cuando un proveedor de servicios crea un tipo de RDE, se crea un paquete de derechos para el tipo. Un proveedor de servicios debe asignarle uno o varios de los cinco derechos específicos del tipo: **Ver: Tipo**, **Editar: Tipo**, **Control total: Tipo**, **Vista de administración: Tipo** y **Control total de administración: Tipo**.
Ver: Tipo, **Editar: Tipo** y **Control total: Tipo** solo funcionan en combinación con una entrada de ACL.
- **Lista de control de acceso (ACL):** la tabla de ACL contiene entradas que definen el acceso que tienen los usuarios a entidades específicas del sistema. Proporciona un nivel de control adicional para las entidades. Por ejemplo, mientras que el derecho **Editar: Tipo** especifica que un usuario puede modificar las entidades a las que tiene acceso, la tabla de ACL define las entidades a las que tiene acceso el usuario.

Tabla 18-1. Derechos y entradas de ACL para operaciones de RDE

Operación de entidad	Opción	Descripción
Leer	Derecho Vista de administración: Tipo	Los usuarios con este derecho pueden ver todas las RDE de este tipo dentro de una organización.
	Derecho Ver: Tipo y entrada de ACL >= Ver	Los usuarios con este derecho y una ACL de nivel de lectura pueden ver RDE de este tipo.
Modificar	Derecho Control total de administración: Tipo	Los usuarios con este derecho pueden crear, ver, modificar y eliminar RDE de este tipo en todas las organizaciones.
	Derecho Editar: Tipo y entrada de ACL >= Cambiar	Los usuarios con este derecho y una ACL de nivel de modificación pueden crear, ver y modificar RDE de este tipo.
Eliminar	Derecho Control total de administración: Tipo	Los usuarios con este derecho pueden crear, ver, modificar y eliminar RDE de este tipo en todas las organizaciones.
	Derecho Control total: Tipo y entrada de ACL = Control total	Los usuarios con este derecho y una ACL de nivel de control total pueden crear, ver, modificar y eliminar RDE de este tipo.

Compartir entidades definidas con otro usuario

Si un **administrador del sistema** publicó el paquete de derechos de un tipo de entidad definida y le otorgó a usted acceso de `ReadWrite` o `FullControl`, o si usted es el propietario de la entidad definida, puede compartir el acceso a esas entidades con otros usuarios.

- 1 Asigne el derecho **Ver: Tipo**, **Editar: Tipo** o **Control total: Tipo** del paquete a las funciones de usuario que desee que tengan un nivel específico de acceso a la entidad definida.

Nota Debe iniciar sesión como **administrador del sistema** o **administrador de la organización** para asignar derechos.

Por ejemplo, si desea que los usuarios con la función **tkg_viewer** vean los clústeres de Tanzu Kubernetes dentro de la organización, debe agregar el derecho **Ver: Clúster invitado de Tanzu Kubernetes** a la función. Si desea que los usuarios con la función **tkg_author** creen, vean y modifiquen clústeres de Tanzu Kubernetes dentro de esta organización, agregue

Editar: Clúster invitado de Tanzu Kubernetes a esa función. Si desea que los usuarios con la función **tkg_admin** creen, vean, modifiquen y eliminen clústeres de Tanzu Kubernetes dentro de esta organización, agregue el derecho **Control total: Clúster invitado de Tanzu Kubernetes** a la función.

- Otorgue a un usuario específico una lista de control de acceso (ACL) a través de la siguiente llamada de REST API.

```
POST https://[address]/cloudapi/1.0.0/entities/urn:vcloud:entity:[vendor]:[type name]:
[version]:[UUID]/accessControls
{
  "grantType" : "MembershipAccessControlGrant",
  "accessLevelId" : "urn:vcloud:accessLevel:[Access_level]",
  "memberId" : "urn:vcloud:user:[User_ID]"
}
```

Access_level debe ser `ReadOnly`, `ReadWrite` o `FullControl`. *User_ID* debe ser el identificador del usuario al que desea conceder acceso a la entidad definida.

Debe tener acceso de `ReadWrite` o `FullControl` a una entidad para conceder acceso a la ACL a esa entidad.

Los usuarios con la función **tkg_viewer**, que se describe en el ejemplo, no pueden conceder acceso a la ACL. Los usuarios con la función **tkg_author** o **tkg_admin** pueden compartir el acceso a una entidad VMWARE:TKGCLUSTER con usuarios que tengan la función **tkg_viewer**, **tkg_author** o **tkg_admin**, al concederles acceso a la ACL a través de la solicitud de API.

Los usuarios con el derecho **Control total: Clúster invitado de Tanzu Kubernetes** pueden conceder acceso a la ACL a cualquier entidad VMWARE:TKGCLUSTER.

También puede utilizar llamadas de REST API para revocar el acceso o para ver quién tiene acceso a la entidad. Consulte la documentación de REST API de VMware Cloud Director en code.vmware.com.

Cambiar el propietario de una entidad definida

El propietario de una entidad definida o un usuario con el derecho **Control total de administración: Tipo** puede transferir la propiedad a otro usuario actualizando el modelo de entidad definido y cambiando el campo de propietario por el ID del nuevo propietario.

Este capítulo incluye los siguientes temas:

- [Trabajar con definiciones de entidad personalizada](#)

Trabajar con definiciones de entidad personalizada

Las definiciones de entidad personalizada de VMware Cloud Director son tipos de objeto enlazados a tipos de objeto de vRealize Orchestrator. Los usuarios en una organización de VMware Cloud Director pueden poseer, administrar y cambiar dichos tipos en función de sus

necesidades. Mediante la ejecución de los servicios, los usuarios de la organización pueden crear instancias de las entidades personalizadas y aplicar acciones a las instancias de los objetos.

Buscar una entidad personalizada

Puede buscar esas entidades personalizadas que se han publicado en la organización.

Requisitos previos

Esta operación requiere que los derechos de la entidad personalizada se incluyan en la función de usuario predefinida.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en **Servicios**, seleccione **Definiciones de entidades personalizadas**.

La lista de entidades personalizadas aparece en una vista de tarjeta con 12 elementos por página, organizados por nombre en orden alfabético. Cada tarjeta muestra el nombre de la entidad personalizada, el tipo de vRealize Orchestrator al que se ha asignado la entidad, el tipo de la entidad y una descripción, si hay una disponible.

- 2 En el cuadro de texto **Buscar** de la parte superior de la página, introduzca una palabra o un carácter del nombre de la entidad que desea buscar.

Los resultados de la búsqueda se muestran en una vista de tarjetas con doce elementos por página organizados por nombre y en orden alfabético.

Editar una definición de entidad personalizada

Puede modificar el nombre y la descripción de una entidad personalizada. No es posible modificar el tipo de la entidad o el tipo de objeto de vRealize Orchestrator, al cual esté enlazada la entidad. Son las propiedades predeterminadas de la entidad personalizada. Si desea modificar cualquiera de las propiedades predeterminadas, debe eliminar la definición de entidad personalizada y volver a crearla.

Requisitos previos

Esta operación requiere que los derechos de la entidad personalizada se incluyan en la función de usuario predefinida.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en **Servicios**, seleccione **Definiciones de entidades personalizadas**.

La lista de entidades personalizadas aparece en una vista de tarjeta con 12 elementos por página, organizados por nombre en orden alfabético. Cada tarjeta muestra el nombre de la entidad personalizada, el tipo de vRealize Orchestrator al que se ha asignado la entidad, el tipo de la entidad y una descripción, si hay una disponible.

- 2 En la tarjeta de la entidad personalizada seleccionada, elija **Acciones > Editar**.
Se abrirá un cuadro de diálogo nuevo.
- 3 Modifique el nombre o la descripción de la definición de entidad personalizada.
- 4 Haga clic en **Aceptar** para confirmar el cambio.

Agregar una definición de entidad personalizada

Puede crear una entidad personalizada y asignarla a un tipo de objeto de vRealize Orchestrator existente.

Requisitos previos

Esta operación requiere que los derechos de la entidad personalizada se incluyan en la función de usuario predefinida.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en **Servicios**, seleccione **Definiciones de entidades personalizadas**.

La lista de entidades personalizadas aparece en una vista de tarjeta con 12 elementos por página, organizados por nombre 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 Para agregar una nueva entidad personalizada, haga clic en **Nueva**.
Se abrirá un cuadro de diálogo nuevo.
- 3 Siga los pasos del asistente de **definición de entidad personalizada**.

Paso	
Nombre y descripción	<p>Introduzca un nombre y, si lo desea, una descripción para la nueva entidad.</p> <p>Introduzca un nombre para el tipo de entidad (por ejemplo, <code>sshHost</code>).</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 objetos 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, <code>SSH:Host</code>.</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 VMware Cloud Director muestra el parámetro de salida como una instancia de una entidad personalizada.

Requisitos previos

Esta operación requiere que los derechos de la entidad personalizada se incluyan en la función de usuario predefinida.


Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en **Servicios**, seleccione **Definiciones de entidades personalizadas**.

La lista de entidades personalizadas aparece en una vista de tarjeta con 12 elementos por página, organizados por nombre en orden alfabético. Cada tarjeta muestra el nombre de la entidad personalizada, el tipo de vRealize Orchestrator al que se ha asignado la entidad, el tipo de la entidad y una descripción, si hay una disponible.

- 2 En la tarjeta de la entidad personalizada seleccionada, haga clic en **Instancias**.

Las instancias disponibles se mostrarán en una vista de cuadrícula.

- 3 Haga clic en la barra de listas () que se encuentra a la izquierda de cada entidad para mostrar los flujos de trabajo asociados.

Al hacer clic en un flujo de trabajo, se iniciará una ejecución de flujo de trabajo que tomará la instancia de la entidad como un parámetro de entrada.

Asociar una acción a una entidad personalizada

Mediante la asociación de una acción a una definición de entidad personalizada, puede ejecutar un conjunto de flujos de trabajo de vRealize Orchestrator en las instancias de una entidad personalizada específica.

Requisitos previos

Esta operación requiere que los derechos de la entidad personalizada se incluyan en la función de usuario predefinida.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en **Servicios**, seleccione **Definiciones de entidades personalizadas**.

La lista de entidades personalizadas aparece en una vista de tarjeta con 12 elementos por página, organizados por nombre 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.

- En la tarjeta de la entidad personalizada seleccionada, elija **Acciones > Asociar acción**.
Se abrirá un cuadro de diálogo nuevo.
- 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 de una entidad personalizada

Puede quitar un flujo de trabajo de vRealize Orchestrator de la lista de acciones asociadas.

Requisitos previos

Esta operación requiere que los derechos de la entidad personalizada se incluyan en la función de usuario predefinida.

Procedimiento

- En la barra de navegación superior, haga clic en **Bibliotecas** y, en **Servicios**, seleccione **Definiciones de entidades personalizadas**.

La lista de entidades personalizadas aparece en una vista de tarjeta con 12 elementos por página, organizados por nombre 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.
- En la tarjeta de la entidad personalizada seleccionada, elija **Acciones > Anular asociación de acción**.

Se abrirá un cuadro de diálogo nuevo.
- Seleccione el flujo de trabajo que desea quitar y haga clic en **Anular asociación de acción**.

El flujo de trabajo de vRealize Orchestrator dejará de estar asociado a la entidad personalizada.

Publicar una entidad personalizada

Debe publicar una entidad personalizada para que los usuarios de otros tenants u otros proveedores de servicios puedan ejecutar flujos de trabajo usando las instancias de la entidad personalizada como parámetros de entrada.

Requisitos previos

Esta operación requiere que los derechos de la entidad personalizada se incluyan en la función de usuario predefinida.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en **Servicios**, seleccione **Definiciones de entidades personalizadas**.

La lista de entidades personalizadas aparece en una vista de tarjeta con 12 elementos por página, organizados por nombre en orden alfabético. Cada tarjeta muestra el nombre de la entidad personalizada, el tipo de vRealize Orchestrator al que se ha asignado la entidad, el tipo de la entidad y una descripción, si hay una disponible.

- 2 En la tarjeta de la entidad personalizada seleccionada, elija **Acciones > Publicar**.

Se abrirá un cuadro de diálogo nuevo.

- 3 Determine si desea publicar la definición de entidad personalizada en los proveedores de servicios, en todos los tenants, o solo en los tenants seleccionados.

- 4 Haga clic en **Guardar** para confirmar el cambio.

La definición de entidad personalizada estará disponible para las partes seleccionadas.

Eliminar una entidad personalizada

Puede eliminar una definición de entidad personalizada si la entidad personalizada ya no se usa, si esta se ha configurado de forma incorrecta o si desea asignar el tipo de vRealize Orchestrator a otra entidad personalizada.

Requisitos previos

Esta operación requiere que los derechos de la entidad personalizada se incluyan en la función de usuario predefinida.

Procedimiento

- 1 En la barra de navegación superior, haga clic en **Bibliotecas** y, en **Servicios**, seleccione **Definiciones de entidades personalizadas**.

La lista de entidades personalizadas aparece en una vista de tarjeta con 12 elementos por página, organizados por nombre 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.