

Guía de instalación de NSX

Actualización 9

Modificado el 21 de febrero de 2020

VMware NSX Data Center for vSphere 6.3



vmware®

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

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

Si tiene comentarios relacionados con esta documentación, envíelos a:

docfeedback@vmware.com

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

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

Copyright © 2010 - 2020 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

Guía de instalación de NSX	5
1 Descripción general de NSX for vSphere	6
Componentes de NSX for vSphere	8
Plano de datos	8
Plano de control	9
Plano de administración	10
Plataforma de consumo	11
NSX Edge	11
NSX Services	14
2 Preparación para la instalación	16
Requisitos del sistema para NSX	16
Puertos y protocolos requeridos por NSX for vSphere	19
Conmutadores distribuidos de vSphere y NSX	21
Ejemplo: Trabajar con un conmutador distribuido de vSphere	24
Comprender los modos de replicación	32
Topología de ejemplo y flujo de trabajo de instalación de NSX	34
Cross-vCenter NSX y Enhanced Linked Mode	36
3 Instalar NSX Manager Virtual Appliance	38
4 Registrar vCenter Server con NSX Manager	44
5 Configurar inicio de sesión único	47
6 Configurar un servidor syslog para NSX Manager	50
7 Instalar y asignar licencia de NSX for vSphere	52
8 Implementar clúster de NSX Controller	54
9 Excluir las máquinas virtuales de la protección de firewall	59
10 Preparar clústeres de hosts para NSX	61
11 Agregar un host a un clúster preparado	65

- 12** Quitar un host de un clúster NSX preparado 66
- 13** Configurar parámetros de transporte de VXLAN 68
- 14** Asignar un grupo de identificadores de segmento y un rango de direcciones de multidifusión 72
- 15** Agregar una zona de transporte 74
- 16** Agregar un conmutador lógico 79
- 17** Agregar un enrutador lógico distribuido 86
- 18** Agregar una puerta de enlace de servicios Edge 100
- 19** Configurar OSPF en un enrutador lógico (distribuido) 112
- 20** Configurar el protocolo OSPF en una puerta de enlace de servicios Edge 118
- 21** Instalar Guest Introspection en los clústeres de host 125
- 22** Desinstalar componentes de NSX 128
 - Desinstalar un módulo de Guest Introspection 128
 - Desinstalar un enrutador lógico distribuido o una puerta de enlace de servicios NSX Edge 129
 - Desinstalar un conmutador lógico 129
 - Desinstalar NSX de los clústeres de hosts 130
 - Quitar una instalación de NSX de forma segura 131

Guía de instalación de NSX

En este manual, la *Guía de instalación de NSX*, se describe cómo instalar el sistema VMware NSX[®] for vSphere[®] mediante la interfaz de usuario de NSX Manager y vSphere Web Client. La información incluye instrucciones de configuración paso a paso y prácticas recomendadas.

Público objetivo

Este manual está destinado a quienes deseen instalar o utilizar NSX en un entorno de VMware vCenter. La información de este manual está escrita para administradores de sistemas con experiencia que estén familiarizados con la tecnología de máquinas virtuales y las operaciones de centros de datos. En este manual se da por sentado que está familiarizado con VMware vSphere, incluidos VMware ESXi, vCenter Server y vSphere Web Client.

Glosario de publicaciones técnicas de VMware

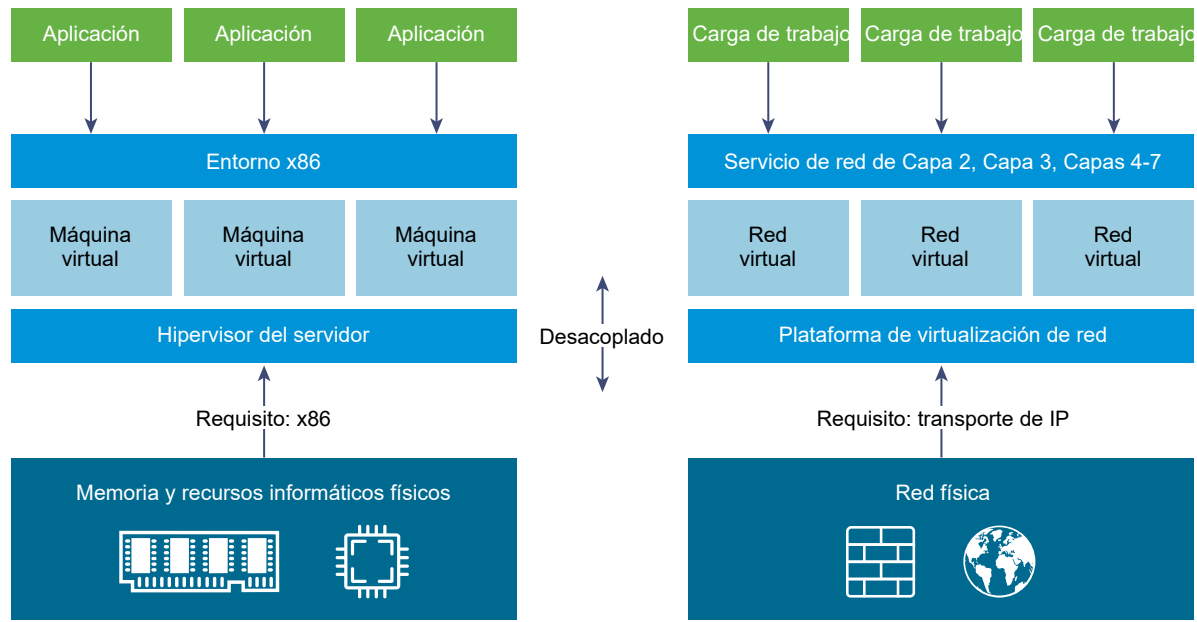
Publicaciones técnicas de VMware proporciona un glosario de términos que podrían resultarle desconocidos. Si desea ver las definiciones de los términos que se utilizan en la documentación técnica de VMware, acceda a la página <http://www.vmware.com/support/pubs>.

Descripción general de NSX for vSphere

1

Las organizaciones de TI han obtenido beneficios importantes como resultado directo de la virtualización de servidores. La consolidación de servidores redujo la complejidad física, aumentó la eficiencia operativa y la capacidad de reasignar dinámicamente los recursos subyacentes para cumplir, de forma rápida y óptima, las necesidades de las aplicaciones empresariales cada vez más dinámicas.

La arquitectura del centro de datos definido por software (SDDC) de VMware ahora extiende las tecnologías de virtualización a toda la infraestructura del centro de datos físico. NSX for vSphere es un producto clave de la arquitectura del SDDC. Con NSX for vSphere, la virtualización aporta a las redes lo que ya se ofrece en términos de capacidad informática y almacenamiento. De manera muy similar al modo en que la virtualización del servidor, mediante programación, crea, elimina y restaura máquinas virtuales basadas en software, así como crea instantáneas de ellas, la virtualización de redes de NSX for vSphere, mediante programación, crea, elimina y restaura redes virtuales basadas en software, y crea instantáneas de ellas. El resultado es un enfoque de redes transformador que no solo permite que los administradores del centro de datos alcancen muchísima mayor agilidad y mejor economía, sino que también permite la implementación de un modelo operativo muy simplificado para la red física subyacente. Gracias a que se puede implementar en cualquier red IP, incluidos los modelos de redes tradicionales existentes y las arquitecturas de tejido de última generación de cualquier proveedor, NSX for vSphere es una solución que no provoca interrupciones. De hecho, con NSX for vSphere, la infraestructura de red física existente es todo lo que se necesita para implementar un centro de datos definido por software.



La imagen de arriba establece una analogía entre la virtualización informática y de red. Con la virtualización del servidor, una capa de abstracción de software (hipervisor de servidor) reproduce los atributos conocidos de un servidor físico x86 (por ejemplo, CPU, RAM, disco, NIC) en el software; de este modo, esos atributos pueden ensamblarse programáticamente en cualquier combinación arbitraria para producir una única máquina virtual en cuestión de segundos.

Con la virtualización de red, el equivalente funcional de un hipervisor de red reproduce en el software el conjunto completo de servicios de red de Capa 2 a Capa 7 (por ejemplo, conmutación, enrutamiento, control de acceso, protección de firewall, calidad de servicio [QoS] y equilibrio de carga). Como consecuencia, estos servicios pueden ensamblarse mediante programación en cualquier combinación arbitraria para producir redes virtuales únicas y aisladas en cuestión de segundos.

Con la virtualización de red se obtienen beneficios similares a los que ofrece la virtualización del servidor. Por ejemplo, así como las máquinas virtuales son independientes de la plataforma x86 subyacente y permiten que TI trate los hosts físicos como un grupo con capacidad informática, las redes virtuales son independientes del hardware de red IP subyacente y permiten que TI trate la red física como un grupo con capacidad de transporte que puede consumirse y reasignarse a petición. A diferencia de las arquitecturas heredadas, las redes virtuales pueden aprovisionarse, cambiarse, almacenarse, eliminarse y restaurarse de forma programática sin volver a configurar la topología o el hardware físico subyacente. Al combinar las capacidades y los beneficios que ofrecen las soluciones conocidas de virtualización de almacenamiento y del servidor, este enfoque de redes transformador despliega todo el potencial del centro de datos definido por software.

NSX for vSphere puede configurarse mediante vSphere Web Client, una interfaz de línea de comandos (CLI) y una REST API.

Este capítulo incluye los siguientes temas:

- [Componentes de NSX for vSphere](#)
- [NSX Edge](#)

■ NSX Services

Componentes de NSX for vSphere

En esta sección se describen los componentes de la solución NSX for vSphere.



Debe tener en cuenta que una Cloud Management Platform (CMP) no es un componente de NSX for vSphere. Sin embargo, NSX for vSphere proporciona integración con casi cualquier CMP a través de la REST API e integración inmediata con las CMP de VMware.

Plano de datos

El plano de datos de NSX consiste en NSX vSwitch, que se basa en vSphere Distributed Switch (VDS) con otros componentes que permiten habilitar servicios. Los módulos de kernel de NSX, los agentes de espacio de usuarios, los archivos de configuración y los scripts de instalación están empaquetados en VIB y se ejecutan dentro del kernel del hipervisor a fin de proveer servicios, como el enrutamiento distribuido y el firewall lógico, y habilitar capacidades de puente con VXLAN.

NSX vSwitch (basado en VDS) abstrae la red física y proporciona conmutación en el hipervisor en el nivel de acceso. Es fundamental para la virtualización de red, ya que habilita redes lógicas que son independientes de las construcciones físicas, como las VLAN. Algunos de los beneficios de vSwitch son los siguientes:

- Compatibilidad con redes de superposición con protocolos (como VXLAN) y configuración de red centralizada. Las redes de superposición habilitan las siguientes capacidades:
 - Uso reducido de identificadores de VLAN en la red física
 - Creación de una superposición de Capa 2 (L2) lógica flexible en las redes IP existentes de la infraestructura física existente sin que sea necesario volver a establecer la arquitectura de las redes del centro de datos
 - Aprovisionamiento de comunicación (Este-Oeste y Norte-Sur) a la vez que se mantiene el aislamiento entre las empresas
 - Cargas de trabajo y máquinas virtuales de aplicaciones que son independientes de la red de superposición y funcionan como si estuvieran conectadas a una red física de Capa 2
- Escala masiva facilitada de hipervisores
- Varias características, como la creación de reflejo del puerto, NetFlow/IPFIX, la restauración y la copia de seguridad de la configuración, la comprobación del estado de red y la calidad de servicio (QoS) y LACP, proporcionan un kit de herramientas integral para la administración del tráfico, la supervisión y la solución de problemas de una red virtual

Los enrutadores lógicos pueden proporcionar un puente de Capa 2 desde el espacio de red lógica (VXLAN) hasta la red física (VLAN).

El dispositivo de puerta de enlace generalmente es un dispositivo virtual NSX Edge. NSX Edge ofrece servicios de Capa 2 y Capa 3, firewall perimetral, equilibrio de carga y otros, como SSL VPN y DHCP.

Plano de control

El plano de control de NSX se ejecuta en el clúster de NSX Controller. NSX Controller es un sistema de administración de estado avanzado que proporciona funciones en el plano de control para el enrutamiento y la conmutación lógica de NSX. Es el punto de control central para todos los conmutadores lógicos de una red, además de que conserva la información de todos los hosts, conmutadores lógicos (VXLAN) y enrutadores lógicos distribuidos.

El clúster de controladoras se encarga de administrar los módulos de conmutación y enrutamiento distribuido de los hipervisores. Por la controladora no pasa ningún tráfico del plano de datos. Los nodos de controladora se implementan en un clúster de tres miembros para habilitar la escala y la alta disponibilidad. Cualquier error en los nodos no afecta el tráfico del plano de datos.

NSX Controller funciona distribuyendo la información de red a los hosts. A fin de alcanzar un alto nivel de resiliencia, NSX Controller se integra en un clúster para ofrecer escalabilidad horizontal y HA. NSX Controller debe implementarse en un clúster de tres nodos. Los tres dispositivos virtuales proporcionan, mantienen y actualizan el estado de funcionamiento de las redes del dominio NSX. Se utiliza NSX Manager para implementar los nodos de NSX Controller.

Los tres nodos de NSX Controller forman un clúster de control. El clúster de controladoras requiere cuórum (también llamado mayoría) para poder evitar una situación de "cerebro dividido". En ese tipo de situaciones, las incoherencias de datos surgen del mantenimiento de dos conjuntos de datos distintos que se superponen. Las inconsistencias pueden deberse a condiciones de error y a problemas con la sincronización de datos. Al tener tres nodos de controladora se garantiza la redundancia de datos en caso de que ocurra un error en un nodo de NSX Controller.

Un clúster de controladoras tiene varias funciones, entre ellas:

- Proveedor de API
- Servidor de persistencia
- Administrador de conmutadores
- Administrador lógico
- Servidor de directorio

A cada función le corresponde un nodo de controladora maestro. Si se producen errores en un nodo de controladora maestro para un rol, el clúster elige un nuevo nodo maestro para ese rol entre los nodos disponibles de NSX Controller. El nuevo nodo maestro de NSX Controller para ese rol vuelve a asignar las porciones perdidas de trabajo entre los nodos de NSX Controller restantes.

NSX admite tres modos para el plano de control de conmutadores lógicos: multidifusión, unidifusión e híbrido. Al utilizar un clúster de controladoras para administrar los conmutadores lógicos basados en VXLAN deja de ser necesaria la compatibilidad de multidifusión de la infraestructura de red física. No es necesario proporcionar direcciones IP para un grupo de multidifusión ni habilitar las características de enrutamiento de PMI o de intromisión de IGMP en los enrutadores o los conmutadores físicos. Por lo tanto, los modos híbrido y de unidifusión desacoplan a NSX de la red física. Las VXLAN que están en el modo de unidifusión del plano de control no requieren que la red física admita la multidifusión para poder administrar el tráfico de difusión, de unidifusión desconocida y de multidifusión (BUM) dentro de un conmutador lógico. El modo de unidifusión replica todo el tráfico BUM localmente en el host y no requiere la configuración de la red física. En el modo híbrido, parte de la replicación del tráfico BUM se descarga en el conmutador físico del primer salto para lograr un mejor rendimiento. El modo híbrido requiere la intromisión de IGMP en el conmutador del primer salto y el acceso a un solicitante de IGMP en cada subred de VTEP.

Plano de administración

La creación del plano de administración de NSX se realiza mediante NSX Manager, el componente de administración de red centralizada de NSX. Proporciona el único punto de configuración y los puntos de entrada de la API de REST.

NSX Manager se instala como dispositivo virtual en cualquier host ESX™ del entorno de vCenter Server. NSX Manager y vCenter tienen una relación uno a uno. Para cada instancia de NSX Manager, hay una de vCenter Server. Esto es cierto incluso en un entorno de Cross-vCenter NSX.

En un entorno de Cross-vCenter NSX, hay una instancia principal de NSX Manager y una o más instancias secundarias de NSX Manager. La instancia principal de NSX Manager permite crear y administrar conmutadores lógicos universales, enrutadores lógicos (distribuidos) universales y reglas de firewall universales. Las instancias secundarias de NSX Manager se utilizan para administrar servicios de red que corresponden localmente a la instancia específica de NSX Manager. Puede haber hasta siete instancias secundarias de NSX Manager asociadas con la instancia principal en un entorno de Cross-vCenter NSX.

Plataforma de consumo

El consumo de NSX puede impulsarse directamente desde la interfaz de usuario de NSX Manager, disponible en vSphere Web Client. En general, los usuarios finales unen la virtualización de red con Cloud Management Platform (CMP) para implementar aplicaciones. NSX proporciona una integración completa en prácticamente cualquier CMP a través de las API de REST. La integración inmediata también está disponible mediante VMware vCloud Automation Center, vCloud Director y OpenStack con el complemento Neutron para NSX.

NSX Edge

Puede instalar NSX Edge como una puerta de enlace de servicios Edge (ESG) o un enrutador lógico distribuido (DLR).

Puerta de enlace de servicios Edge

La ESG brinda acceso a todos los servicios de NSX Edge, como firewall, NAT, DHCP, VPN, equilibrio de carga y alta disponibilidad. Puede instalar varios dispositivos virtuales de ESG en un centro de datos. Cada dispositivo virtual de ESG puede tener un total de diez interfaces de red interna y vínculo superior. Con un tronco, una ESG puede tener hasta 200 subinterfaces. Las interfaces internas se conectan a grupos de puertos protegidos y actúan como puerta de enlace para todas las máquinas virtuales protegidas del grupo de puertos. La subred asignada a la interfaz interna puede ser un espacio de IP enrutado públicamente o un espacio de direcciones privado (RFC 1918) con uso de NAT. Las reglas de firewall y otros servicios NSX Edge se aplican en el tráfico entre las interfaces de red.

Las interfaces de vínculo superior de las ESG se conectan a grupos de puertos de vínculo superior que tienen acceso a una red compartida de la empresa o a un servicio que proporciona redes de capa de acceso. Se pueden configurar varias direcciones IP externas para los servicios de NAT, VPN de sitio a sitio y equilibrador de carga.

Enrutador lógico distribuido

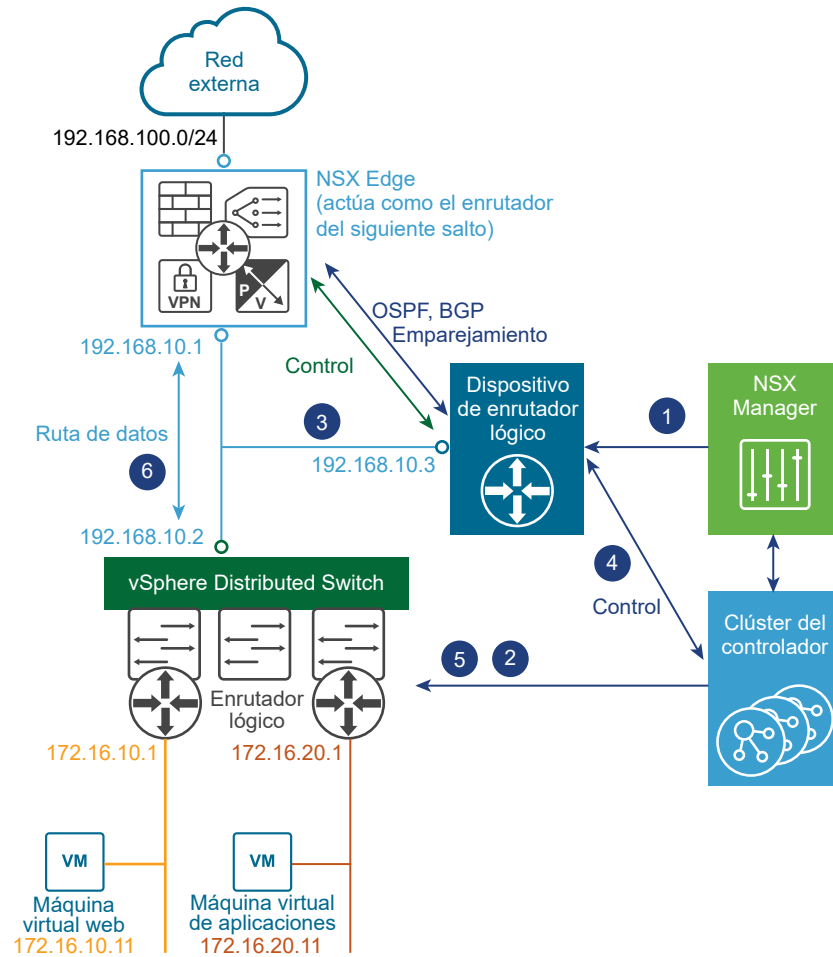
El DLR proporciona enrutamiento distribuido de Este a Oeste con espacio de dirección IP de empresa y aislamiento de ruta de acceso de datos. Las máquinas virtuales o cargas de trabajo que residen en el mismo host, en diferentes subredes, pueden comunicarse entre sí sin necesidad de atravesar una interfaz de enrutamiento tradicional.

Un enrutador lógico puede tener ocho interfaces de vínculo superior y hasta mil interfaces internas. Una interfaz de vínculo superior de un DLR generalmente se empareja con una ESG, con un conmutador de tránsito lógico de Capa 2 interviniente entre el DLR y la ESG. Una interfaz interna de un DLR se empareja con una máquina virtual alojada en un hipervisor ESXi, mediante un conmutador lógico interviniente entre la máquina virtual y el DLR.

El DLR tiene dos componentes principales:

- El plano de control del DLR es un elemento que proporciona el dispositivo virtual del DLR (también denominado máquina virtual de control). Esta máquina virtual es compatible con los protocolos de enrutamiento dinámico (BGP y OSPF), intercambia actualizaciones de enrutamiento con el dispositivo de salto de Capa 3 siguiente (generalmente, la puerta de enlace de servicios Edge) y se comunica con NSX Manager y el clúster de NSX Controller. La alta disponibilidad para el dispositivo virtual del DLR se admite mediante la configuración activo-en espera: se proporciona un par de máquinas virtuales que funcionan en los modos activo/en espera cuando se crea el DLR con la característica HA habilitada.
- En el nivel del plano de datos, hay módulos de kernel del DLR (VIB) que se instalan en los hosts ESXi que son parte del dominio NSX. Los módulos de kernel son similares a las tarjetas de línea de un chasis modular que admite el enrutamiento de Capa 3. Los módulos de kernel tienen una base de información de enrutamiento (RIB) (también conocida como tabla de enrutamiento) que se inserta desde el clúster de controladoras. Las funciones del plano de datos de búsqueda de rutas y búsqueda de entradas de ARP se ejecutan mediante los módulos de kernel. Los módulos de kernel están equipados con interfaces lógicas (denominadas LIF) que se conectan a diferentes conmutadores lógicos y a cualquier grupo de puertos respaldado por VLAN. Cada LIF tiene asignada una dirección IP que representa la puerta de enlace IP predeterminada del segmento de Capa 2 lógico al que se conecta y una dirección vMAC. La dirección IP es única para cada LIF, mientras que la misma vMAC se asigna a todas las LIF definidas.

Figura 1-1. Componentes de enrutamiento lógico



- 1 Una instancia de DLR se crea a partir de la interfaz de usuario de NSX Manager (o con llamadas API) usando el enrutamiento, con lo cual se aprovechan OSPF o BGP.
- 2 NSX Controller usa el plano de control con los hosts ESXi para insertar la nueva configuración del DLR, incluidas las LIF y sus direcciones IP y vMAC asociadas.
- 3 Si asumimos que el protocolo de enrutamiento también está habilitado en el dispositivo de salto siguiente (NSX Edge [ESG] en este ejemplo), el emparejamiento OSPF o BGP se establece entre la ESG y la máquina virtual de control del DLR. Posteriormente, la ESG y el DLR pueden intercambiar información de enrutamiento:
 - La máquina virtual de control del DLR se puede configurar para redistribuir en OSPF los prefijos IP de todas las redes lógicas conectadas (172.16.10.0/24 y 172.16.20.0/24 en este ejemplo). Como consecuencia, esta máquina virtual inserta esos anuncios de ruta en NSX Edge. Observe que el salto siguiente de esos prefijos no es la dirección IP asignada a la máquina virtual de control (192.168.10.3), sino la dirección IP que identifica el componente del plano de datos del DLR (192.168.10.2). La primera se conoce como la "dirección del protocolo" del DLR, mientras que la segunda es la "dirección de reenvío".

- NSX Edge inserta en la máquina virtual de control los prefijos para comunicarse con las redes IP de la red externa. En la mayoría de los casos, es posible que NSX Edge envíe una sola ruta predeterminada, porque representa el único punto de salida hacia la infraestructura de red física.
- 4 La máquina virtual de control del DLR inserta las rutas IP conocidas por NSX Edge en el clúster de controladoras.
 - 5 El clúster de controladoras es el responsable de distribuir las rutas conocidas de la máquina virtual de control del DLR a los hipervisores. Cada nodo de controladora del clúster es responsable de distribuir la información de una instancia de enrutador lógico en particular. En una implementación con varias instancias de enrutador lógico implementadas, la carga se distribuye entre los nodos de controladora. Una instancia de enrutador lógico distinta generalmente se asocia con cada empresa implementada.
 - 6 Los módulos de kernel de enrutamiento del DLR de los hosts controlan el tráfico de la ruta de acceso de datos para la comunicación con la red externa mediante NSX Edge.

NSX Services

Los componentes de NSX trabajan juntos para brindar los servicios funcionales siguientes.

Conmutadores lógicos

Una implementación de nube o un centro de datos virtual tiene una variedad de aplicaciones en varias empresas. Estas aplicaciones y empresas requieren un aislamiento entre sí por motivos de seguridad, aislamiento de errores y direcciones IP que no se superpongan. NSX permite la creación de varios conmutadores lógicos, cada uno de los cuales es un dominio de difusión lógico único. Una máquina virtual de aplicaciones o empresa se puede conectar de forma lógica a un conmutador lógico. Esto permite flexibilidad y velocidad de implementación, al mismo tiempo que brinda todas las características de los dominios de difusión de una red física (VLAN) sin los problemas físicos de árbol de expansión o dispersión en la Capa 2.

Un conmutador lógico se distribuye a todos los hosts de vCenter (o todos los hosts de un entorno de Cross-vCenter NSX) y puede abarcar todos estos hosts. Esto permite la movilidad de la máquina virtual (vMotion) dentro del centro de datos sin las restricciones del límite de la Capa 2 física (VLAN). La infraestructura física no está limitada por los límites de la tabla de MAC/FIB, dado que el conmutador lógico contiene el dominio de difusión en software.

Enrutadores lógicos

El enrutamiento proporciona la información de reenvío necesaria entre los dominios de difusión de Capa 2 y permite disminuir el tamaño de los dominios de difusión de Capa 2, así como mejorar la eficiencia y la escala de la red. NSX amplía esta inteligencia hasta donde residen las cargas de trabajo para el enrutamiento de Este a Oeste. Esto permite una comunicación más directa de una máquina virtual a otra sin la costosa necesidad en cuanto a tiempo y dinero de ampliar los saltos. Al mismo tiempo, los enrutadores lógicos de NSX proporcionan conectividad de Norte a Sur y permiten que las empresas accedan a redes públicas.

Firewall lógico

El firewall lógico proporciona mecanismos de seguridad para los centros de datos virtuales dinámicos. El componente firewall distribuido del firewall lógico permite segmentar entidades del centro de datos virtual, como máquinas virtuales basadas en nombres y atributos de máquinas virtuales, identidad del usuario, objetos de vCenter (por ejemplo, centros de datos) y hosts, así como atributos de redes tradicionales (direcciones IP, VLAN, etc.). El componente firewall de Edge ayuda a cumplir con los requisitos clave de seguridad de perímetro, como la creación de DMZ según las construcciones de IP/VLAN, y permite el aislamiento de empresa a empresa en los centros de datos virtuales de varias empresas.

La característica de supervisión de flujo muestra la actividad de red entre las máquinas virtuales en el nivel del protocolo de aplicaciones. Puede utilizar esta información para auditar el tráfico de red, definir y refinar las directivas de firewall, e identificar amenazas a la red.

Redes privadas virtuales (VPN) lógicas

SSL VPN-Plus permite a los usuarios remotos acceder a aplicaciones privadas de la empresa. La VPN IPsec ofrece conectividad de sitio a sitio entre una instancia de NSX Edge y sitios remotos con NSX o con enrutadores de hardware/puertas de enlace VPN de terceros. La VPN de Capa 2 permite ampliar el centro de datos permitiendo que las máquinas virtuales mantengan la conectividad de red al mismo tiempo que mantienen la misma dirección IP en los límites geográficos.

Equilibrador de carga lógico

El equilibrador de carga de NSX Edge distribuye las conexiones de cliente dirigidas a una sola dirección IP virtual (VIP) en varios destinos configurados como miembros de un grupo de equilibrio de carga. Distribuye las solicitudes de servicio entrante de manera uniforme entre varios servidores de forma tal que la distribución de carga sea transparente para los usuarios. Así, el equilibrio de carga ayuda a lograr una utilización de recursos óptima, maximizar la capacidad de proceso, minimizar el tiempo de respuesta y evitar la sobrecarga.

Service Composer

Service Composer permite aprovisionar y asignar los servicios de red y seguridad a las aplicaciones en una infraestructura virtual. Estos servicios se asignan a un grupo de seguridad y los servicios se aplican a las máquinas virtuales del grupo de seguridad por medio de una directiva de seguridad.

Extensibilidad de NSX

Los proveedores de soluciones de terceros pueden integrar sus soluciones con la plataforma de NSX para permitir que los clientes tengan una experiencia integrada en todos los productos de VMware y las soluciones de partners. Los operadores del centro de datos pueden aprovisionar redes virtuales complejas de varios niveles en cuestión de segundos, independientemente de los componentes o la topología de red subyacente.

Preparación para la instalación

2

En esta sección se describen los requisitos del sistema para NSX for vSphere y los puertos que deben estar abiertos.

Este capítulo incluye los siguientes temas:

- [Requisitos del sistema para NSX](#)
- [Puertos y protocolos requeridos por NSX for vSphere](#)
- [Conmutadores distribuidos de vSphere y NSX](#)
- [Ejemplo: Trabajar con un conmutador distribuido de vSphere](#)
- [Comprender los modos de replicación](#)
- [Topología de ejemplo y flujo de trabajo de instalación de NSX](#)
- [Cross-vCenter NSX y Enhanced Linked Mode](#)

Requisitos del sistema para NSX

Antes de instalar o actualizar NSX, tenga en cuenta los recursos y la configuración de red. Puede instalar un NSX Manager por cada vCenter Server, una instancia de Guest Introspection por cada host ESXi™ y varias instancias de NSX Edge por cada centro de datos.

Hardware

Esta tabla muestra los requisitos de hardware para los dispositivos de NSX.

Tabla 2-1. Requisitos de hardware para dispositivos

Dispositivo	Memoria	vCPU	Espacio de disco
NSX Manager	16 GB (24 GB para implementaciones de NSX de mayor tamaño)	4 (8 para implementaciones de NSX de mayor tamaño)	60 GB
NSX Controller	4 GB	4	28 GB

Tabla 2-1. Requisitos de hardware para dispositivos (continuación)

Dispositivo	Memoria	vCPU	Espacio de disco
NSX Edge	Compacto: 512 MB	Compacto: 1	Compacto, grande: 1 disco de 584 MB + 1 disco de 512 MB
	Grande: 1 GB	Grande: 2	
	Cuádruple: 2 GB	Tamaño cuádruple: 4	Cuádruple, grande: 1 disco de 584 MB + 2 discos de 512 MB
	Extra grande: 8 GB	Extra grande: 6	Extra grande: 1 disco de 584 MB + 1 disco de 2 GB + 1 disco de 512 MB
Guest Introspection	2 GB	2	5 GB (el espacio aprovisionado es 6,26 GB)

Como regla general, aumente los recursos de NSX Manager a 8 vCPU y 24 GB de RAM si el entorno administrado de NSX contiene más de 256 hipervisores o más de 2.000 máquinas virtuales.

Para conocer los detalles de tamaño específicos, póngase en contacto con el servicio de soporte técnico de VMware.

Para obtener información sobre aumentar la asignación de memoria y vCPU para sus dispositivos virtuales, consulte Asignar recursos de memoria y Cambiar el número de CPU virtuales en *Administración de máquinas virtuales de vSphere*.

El espacio aprovisionado para un dispositivo de Guest Introspection aparece como 6,26 GB para Guest Introspection. Esto ocurre porque vSphere ESX Agent Manager crea una instantánea de la máquina virtual de servicio para crear clones más rápidos si varios hosts de un clúster comparten el almacenamiento. Para obtener más información sobre cómo deshabilitar esta opción mediante ESX Agent Manager, consulte la documentación de *ESX Agent Manager*.

Latencia de red

Debe asegurarse de que la latencia de red entre los componentes sea igual o inferior a la máxima latencia descrita.

Tabla 2-2. Máxima latencia de red entre los componentes

Componentes	Máxima latencia
Instancias de NSX Controller y NSX Manager	150 ms RTT
NSX Manager y hosts ESXi	150 ms RTT
Sistema vCenter Server y NSX Manager	150 ms RTT
NSX Manager y NSX Manager en un entorno cross-vCenter NSX	150 ms RTT
NSX Controller y hosts ESXi	150 ms RTT

Software

Para ver la información de interoperabilidad más reciente, consulte la sección sobre matrices de interoperabilidad del producto en http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Para las versiones recomendadas de NSX, de vCenter Server y de ESXi, consulte las notas de la versión de NSX a la que va a actualizar. Las notas de la versión están disponibles en el sitio web de documentación de NSX for vSphere: <https://docs.vmware.com/es/VMware-NSX-for-vSphere/index.html>.

Para que una instancia de NSX Manager participe en una implementación de Cross-vCenter NSX, se deben dar las condiciones siguientes:

Componente	Versión
NSX Manager	6.2 o posterior
NSX Controller	6.2 o posterior
vCenter Server	6.0 o posterior
ESXi	<ul style="list-style-type: none"> ■ ESXi 6.0 o versiones posteriores ■ Clústeres de host que cuentan con NSX 6.2 o VIB posteriores

Para administrar todas las instancias de NSX Manager en una implementación de Cross-vCenter NSX desde una sola instancia de vSphere Web Client, debe conectar vCenter Server en Enhanced Linked Mode. Consulte Usar Modo vinculado mejorado (Enhanced Linked Mode) en *Administración de vCenter Server y hosts*.

Para verificar la compatibilidad de las soluciones de partners con NSX, consulte la Guía de compatibilidad de VMware para Networking and Security en <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security>.

Acceso de clientes y usuarios

Los siguientes elementos son necesarios para administrar el entorno de NSX:

- Resolución de nombres directa e inversa. Esta opción es necesaria si se agregaron hosts ESXi por nombre al inventario de vSphere; en caso contrario, NSX Manager no podrá resolver las direcciones IP.
- Permisos para agregar y encender máquinas virtuales.
- Acceda al almacén de datos en el que almacena archivos de máquina virtual y a los permisos de cuenta para copiar los archivos en ese almacén de datos.
- Las cookies deben estar habilitadas en el explorador web para acceder a la interfaz de usuario de NSX Manager.
- El puerto 443 debe estar abierto entre NSX Manager y el host ESXi, vCenter Server y los dispositivos de NSX que se implementarán. Este puerto debe descargar el archivo OVF en el host ESXi para la implementación.
- Un navegador web que sea compatible con la versión de vSphere Web Client que está utilizando. Consulte Usar vSphere Web Client en la documentación de *Administración de vCenter Server y hosts* para obtener información detallada.

Puertos y protocolos requeridos por NSX for vSphere

Los siguientes puertos deben estar abiertos para que NSX for vSphere funcione correctamente.

Nota Si cuenta con un entorno cross-vCenter NSX y sus sistemas vCenter Server están en Modo vinculado mejorado (Enhanced Linked Mode), cada dispositivo NSX Manager debe tener la conectividad necesaria con cada sistema vCenter Server del entorno para gestionar cualquier NSX Manager desde cualquier sistema vCenter Server.

Tabla 2-3. Puertos y protocolos requeridos por NSX for vSphere

Origen	Destino	Puerto	Protocolo (Protocol)	Propósito	Sensible	TLS	Autenticación
PC cliente	NSX Manager	443	TCP	Interfaz administrativa de NSX Manager	No	Sí	Autenticación PAM
PC cliente	NSX Manager	443	TCP	Acceso a VIB de NSX Manager	No	No	Autenticación PAM
Host ESXi	vCenter Server	443	TCP	Preparación del host ESXi	No	No	
vCenter Server	Host ESXi	443	TCP	Preparación del host ESXi	No	No	
Host ESXi	NSX Manager	5671	TCP	RabbitMQ	No	Sí	Usuario y contraseña de RabbitMQ
Host ESXi	NSX Controller	1234	TCP	Conexión del agente del ámbito del usuario	No	Sí	
NSX Controller	NSX Controller	2878, 2888, 3888	TCP	Clúster de controladores, sincronización de estado	No	Sí	IPsec
NSX Controller	NSX Controller	7777	TCP	Puerto RPC entre controladores	No	Sí	IPsec
NSX Controller	NSX Controller	30865	TCP	Clúster de controladores, sincronización de estado	No	Sí	IPsec
NSX Manager	NSX Controller	443	TCP	Comunicación de controlador a Manager	No	Sí	Usuario/contraseña
NSX Manager	vCenter Server	443	TCP	vSphere Web Access	No	Sí	
NSX Manager	vCenter Server	902	TCP	vSphere Web Access	No	Sí	

Tabla 2-3. Puertos y protocolos requeridos por NSX for vSphere (continuación)

Origen	Destino	Puerto	Protocolo (Protocol)	Propósito	Sensible	TLS	Autenticación
NSX Manager	Host ESXi	443	TCP	Conexión de aprovisionamiento y administración	No	Sí	
NSX Manager	Host ESXi	902	TCP	Conexión de aprovisionamiento y administración	No	Sí	
NSX Manager	Servidor DNS	53	TCP	Conexión de cliente DNS	No	No	
NSX Manager	Servidor DNS	53	UDP	Conexión de cliente DNS	No	No	
NSX Manager	Servidor syslog	514	TCP	Conexión de Syslog	No	No	
NSX Manager	Servidor syslog	514	UDP	Conexión de Syslog	No	No	
NSX Manager	Servidor horario NTP	123	TCP	Conexión de cliente NTP	No	Sí	
NSX Manager	Servidor horario NTP	123	UDP	Conexión de cliente NTP	No	Sí	
vCenter Server	NSX Manager	80	TCP	Preparación del host	No	Sí	
Ciente REST	NSX Manager	443	TCP	API de REST de NSX Manager	No	Sí	Usuario/contraseña
Terminal de túnel de VXLAN (VTEP)	Terminal de túnel de VXLAN (VTEP)	8472 (valor predeterminado antes de NSX 6.2.3) o 4789 (valor predeterminado en las instalaciones nuevas de NSX 6.2.3 y versiones posteriores)	UDP	Encapsulación de red de transporte entre VTEP	No	Sí	

Tabla 2-3. Puertos y protocolos requeridos por NSX for vSphere (continuación)

Origen	Destino	Puerto	Protocolo (Protocol)	Propósito	Sensible	TLS	Autenticación
Host ESXi	Host ESXi	6999	UDP	ARP en LIF de VLAN	No	Sí	
Host ESXi	NSX Manager	8301, 8302	UDP	Sincronización de DVS	No	Sí	
NSX Manager	Host ESXi	8301, 8302	UDP	Sincronización de DVS	No	Sí	
Máquina virtual de Guest Introspection	NSX Manager	5671	TCP	RabbitMQ	No	Sí	Usuario y contraseña de RabbitMQ
NSX Manager principal	NSX Manager secundario	443	TCP	Servicio de sincronización Universal de Cross-vCenter NSX	No	Sí	
NSX Manager principal	vCenter Server	443	TCP	vSphere API	No	Sí	
NSX Manager secundario	vCenter Server	443	TCP	vSphere API	No	Sí	
NSX Manager principal	Clúster de controladores universal de NSX	443	TCP	API de REST de NSX Controller	No	Sí	Usuario/contraseña
NSX Manager secundario	Clúster de controladores universal de NSX	443	TCP	API de REST de NSX Controller	No	Sí	Usuario/contraseña
Host ESXi	Clúster de controladores universal de NSX	1234	TCP	Protocolo del plano de control de NSX	No	Sí	
Host ESXi	NSX Manager principal	5671	TCP	RabbitMQ	No	Sí	Usuario y contraseña de RabbitMQ
Host ESXi	NSX Manager secundario	5671	TCP	RabbitMQ	No	Sí	Usuario y contraseña de RabbitMQ

Conmutadores distribuidos de vSphere y NSX

En un dominio NSX, NSX vSwitch es el software que funciona en los hipervisores del servidor para formar una capa de abstracción de software entre los servidores y la red física.

NSX vSwitch está basado en los conmutadores distribuidos de vSphere (VDS), que proporcionan vínculos superiores para la conectividad del host con los conmutadores físicos ubicados en la parte superior del bastidor (ToR). Como práctica recomendada, VMware aconseja planificar y preparar los conmutadores distribuidos de vSphere antes de instalar NSX for vSphere.

NSX Services no son compatibles con vSphere Standard Switch. Las cargas de trabajo de las VM se deben conectar a conmutadores distribuidos de vSphere para poder usar los servicios y características de NSX.

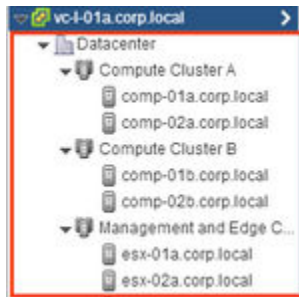
Se puede asociar un solo host a varios VDS. Un solo VDS puede abarcar varios hosts en varios clústeres. Para cada clúster de hosts que participará en NSX, se deben asociar todos los hosts del clúster a un VDS común.

Por ejemplo, supongamos que tiene un clúster con los hosts Host1 y Host2. Host1 está conectado a VDS1 y VDS2. Host2 está conectado a VDS1 y VDS3. Al preparar un clúster para NSX, solo se puede asociar NSX con el VDS1 del clúster. Si agrega otro host (Host3) al clúster y Host3 no está conectado a VDS1, la configuración no es válida y Host3 no está listo para la funcionalidad NSX.

Por lo general, para simplificar una implementación, cada clúster de hosts se asocia solamente a un VDS, aunque algunos VDS abarquen varios clústeres. Por ejemplo, supongamos que vCenter contiene los clústeres de hosts siguientes:

- Clúster de proceso A para hosts de nivel de aplicaciones
- Clúster de proceso B para hosts de nivel web
- Clúster de Edge y de administración para hosts Edge y de administración

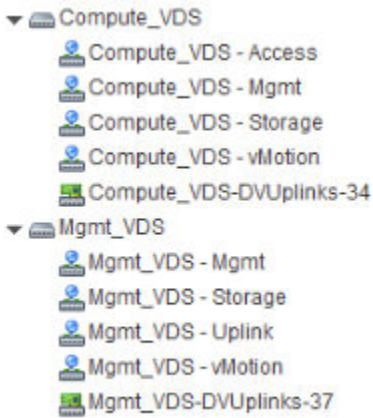
La pantalla siguiente muestra cómo aparecen estos clústeres en vCenter.



Para un diseño de clúster como este, es posible que haya dos VDS denominados Compute_VDS y Mgmt_VDS. Compute_VDS abarca ambos clústeres de proceso y Mgmt_VDS está asociado solo con el clúster de Edge y de administración.

Cada VDS contiene grupos de puertos distribuidos para los distintos tipos de tráfico que se deben transportar. Los tipos de tráfico típicos incluyen administración, almacenamiento y vMotion. Generalmente, también se necesitan puertos de acceso y vínculo superior. Por lo general, se crea un grupo de puertos para cada tipo de tráfico en cada VDS.

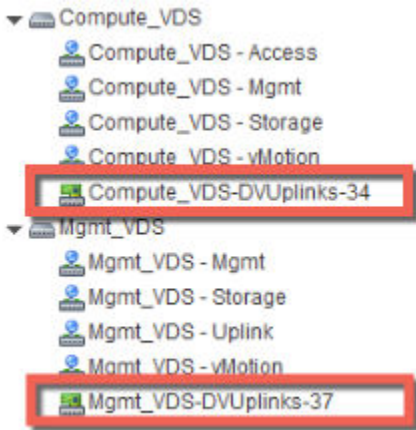
Por ejemplo, la pantalla siguiente muestra cómo aparecen estos puertos y conmutadores distribuidos en vCenter.



Cada grupo de puertos puede, opcionalmente, configurarse con un identificador de VLAN. La lista siguiente muestra un ejemplo de cómo las VLAN pueden asociarse con los grupos de puertos distribuidos para proporcionar un aislamiento lógico entre los distintos tipos de tráfico:

- Compute_VDS - Acceso---VLAN 130
- Compute_VDS - Admin---VLAN 210
- Compute_VDS - Almacenamiento---VLAN 520
- Compute_VDS - vMotion---VLAN 530
- Mgmt_VDS - Vínculo superior---VLAN 100
- Mgmt_VDS - Admin---VLAN 110
- Mgmt_VDS - Almacenamiento---VLAN 420
- Mgmt_VDS - vMotion---VLAN 430

El grupo de puertos DVUplinks es un tronco de VLAN que se crea automáticamente cuando se crea un VDS. Como puerto troncal, envía y recibe tramas etiquetadas. De forma predeterminada, lleva todos los identificadores de VLAN (0-4094). Esto significa que el tráfico con cualquier identificador de VLAN puede transmitirse por los adaptadores de red vmnic asociados con la ranura DVUplink y que los hosts del hipervisor pueden filtrarlo a medida que el conmutador distribuido determina qué grupo de puertos debe recibir el tráfico.



Si el entorno de vCenter existente contiene vSwitch estándar en lugar de conmutadores distribuidos, puede migrar los hosts a conmutadores distribuidos.

Ejemplo: Trabajar con un conmutador distribuido de vSphere

Este ejemplo muestra cómo crear un nuevo conmutador distribuido de vSphere (VDS); cómo agregar grupos de puertos para los tipos de tráfico de administración, almacenamiento y vMotion; y cómo migrar hosts en un conmutador vSwitch estándar al nuevo conmutador distribuido.

Tenga en cuenta que este es solo un ejemplo para demostrar el procedimiento. Para obtener detalles sobre el vínculo superior lógico y físico del VDS, consulte la *Guía de diseño de virtualización de red de VMware NSX for vSphere* disponible en <https://communities.vmware.com/docs/DOC-27683>.

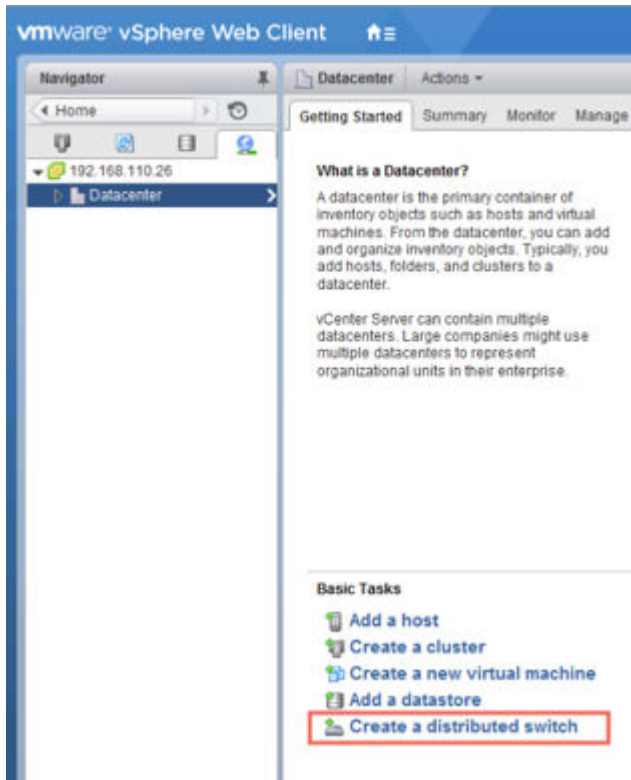
Requisitos previos

Este ejemplo da por sentado que cada host ESX que se conectará al conmutador distribuido de vSphere tiene al menos una conexión con un conmutador físico (un vínculo superior vmnic). Este vínculo superior puede utilizarse para el conmutador distribuido y el tráfico VXLAN de NSX.

Procedimiento

- 1 En vSphere Web Client, desplácese hasta el centro de datos.

- 2 Haga clic en **Crear un conmutador distribuido** (Create a Distributed Switch).



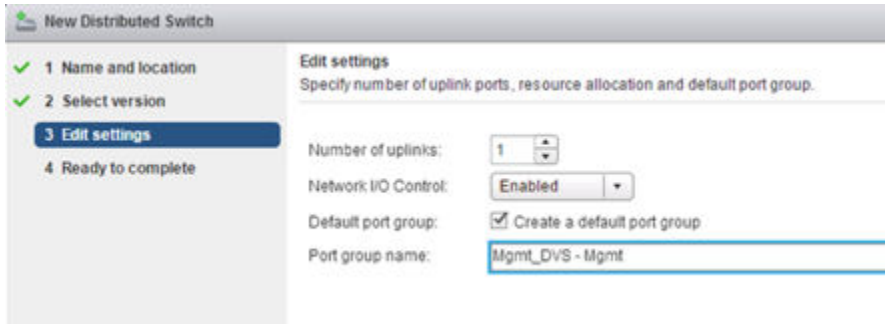
- 3 Asígnale al conmutador un nombre significativo basado en el clúster de hosts que se asociará con este conmutador.

Por ejemplo, si un conmutador distribuido estará asociado con un clúster de hosts de administración de centro de datos, puede asignarle el nombre VDS_Admin.

- 4 Proporcione al menos un vínculo superior para el conmutador distribuido, mantenga habilitado el control de E/S y asígnele un nombre significativo al grupo de puertos predeterminado. Tenga en cuenta que no es obligatorio crear el grupo de puertos predeterminado. Puede crearlo manualmente más adelante.

De forma predeterminada, se crean cuatro vínculos superiores. Ajuste la cantidad de vínculos superiores para reflejar el diseño del VDS. En general, la cantidad de vínculos superiores requerida es igual a la cantidad de NIC físicas que se asigna al VDS.

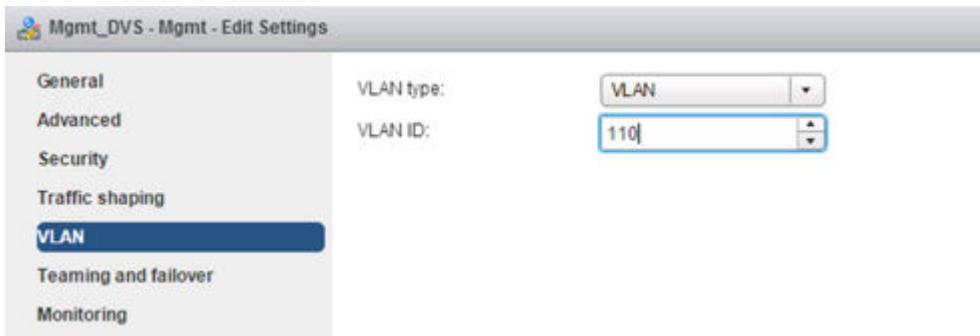
La siguiente pantalla muestra una configuración de ejemplo para el tráfico de administración del clúster de hosts de administración.



El grupo de puertos predeterminado es solo uno de los grupos que contiene el conmutador. Una vez creado el conmutador, tendrá la posibilidad de agregar grupos de puertos para los diferentes tipos de tráfico. De manera opcional, puede desmarcar la opción **Crear un grupo de puertos predeterminado** (Create a default port group) al crear un nuevo VDS. En realidad, esta puede ser la práctica recomendada; es mejor ser explícito a la hora de crear grupos de puertos.

- 5 (opcional) Una vez que finaliza el asistente Nuevo conmutador distribuido (New Distributed Switch), edite la configuración del grupo de puertos predeterminado para colocarlo en la VLAN correcta para el tráfico de administración.

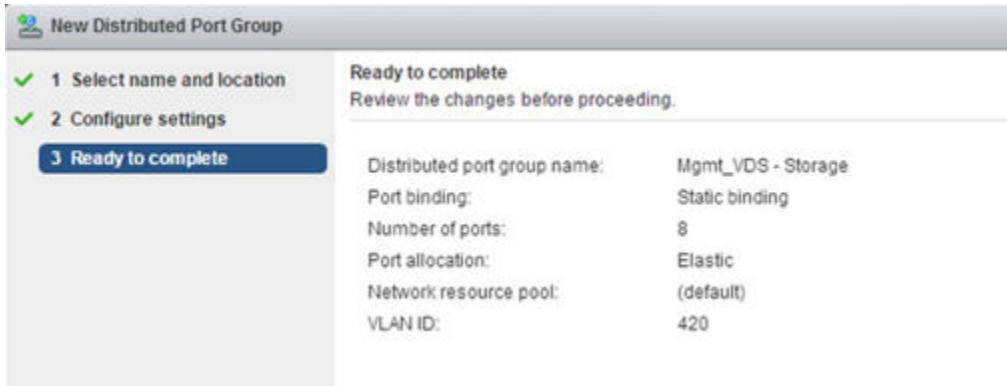
Por ejemplo, si las interfaces de administración de hosts están en la VLAN 110, coloque el grupo de puertos predeterminado en la VLAN 110. Si las interfaces de administración de hosts no están en una VLAN, omita este paso.



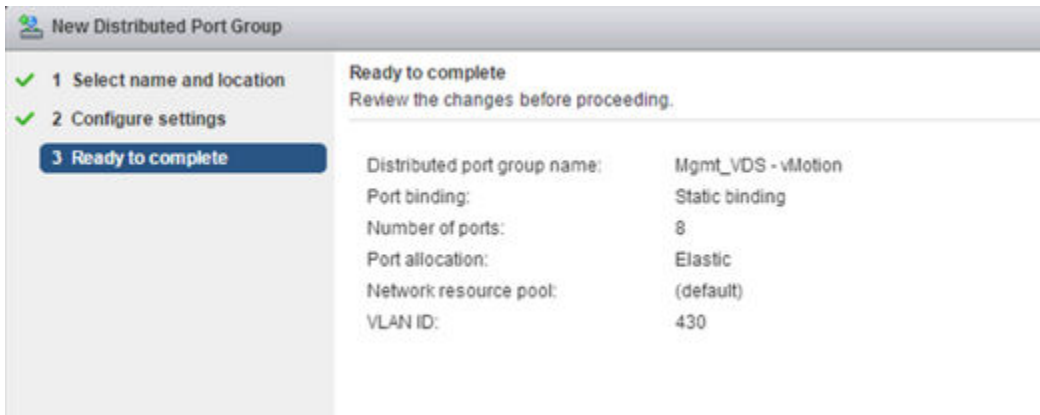
- 6 Una vez que finaliza el asistente Nuevo conmutador distribuido (New Distributed Switch), haga clic con el botón derecho en el conmutador distribuido y seleccione **Nuevo grupo de puertos distribuidos** (New Distributed Port Group).

Repita este paso con cada tipo de tráfico, asigne un nombre significativo a cada grupo de puertos y configure el identificador de VLAN correspondiente según los requisitos de separación de tráfico de la implementación.

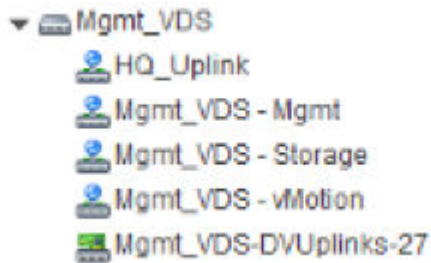
Configuración de grupo de ejemplo para almacenamiento.



Configuración de grupo de ejemplo para el tráfico vMotion.

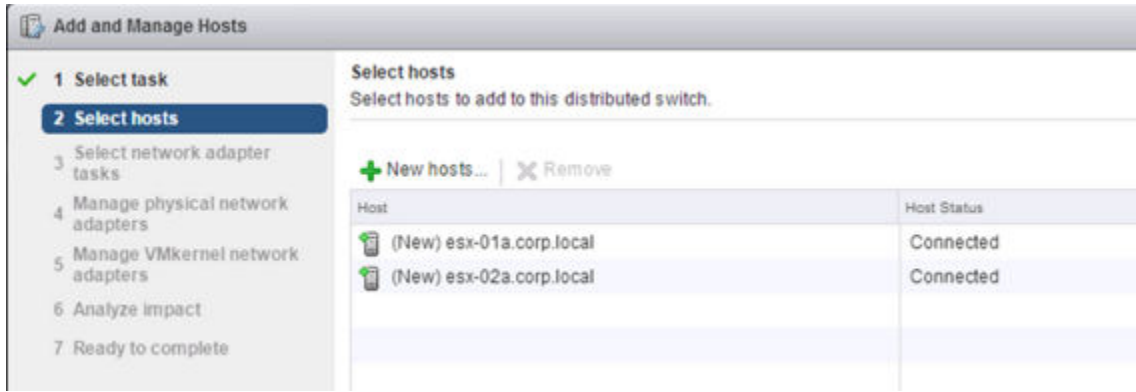


La configuración terminada del conmutador distribuido y de los grupos de puertos se ve así.

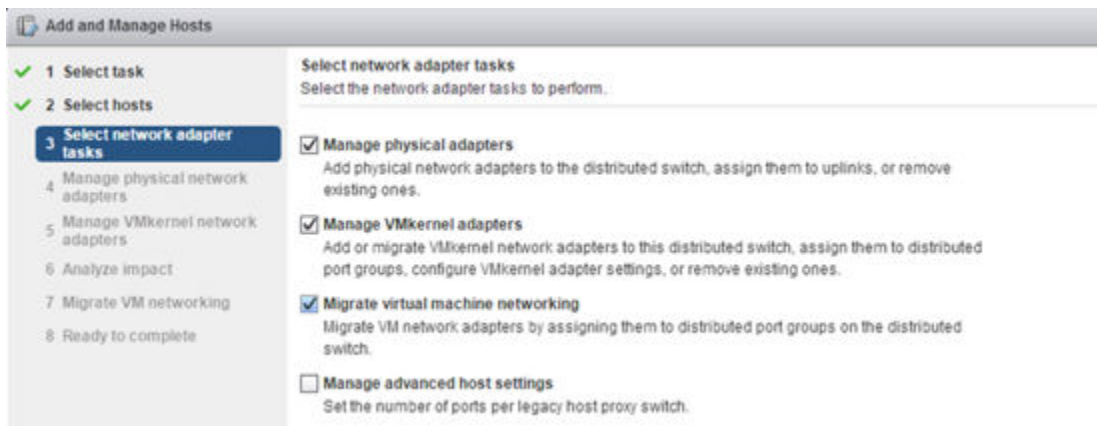


- Haga clic con el botón derecho en el conmutador distribuido, seleccione **Agregar y administrar hosts** (Add and Manage Hosts) y, a continuación, **Agregar hosts** (Add Hosts).

Conecte todos los hosts que están en el clúster asociado. Por ejemplo, si se trata de un conmutador para hosts de administración, seleccione todos los hosts del clúster de administración.

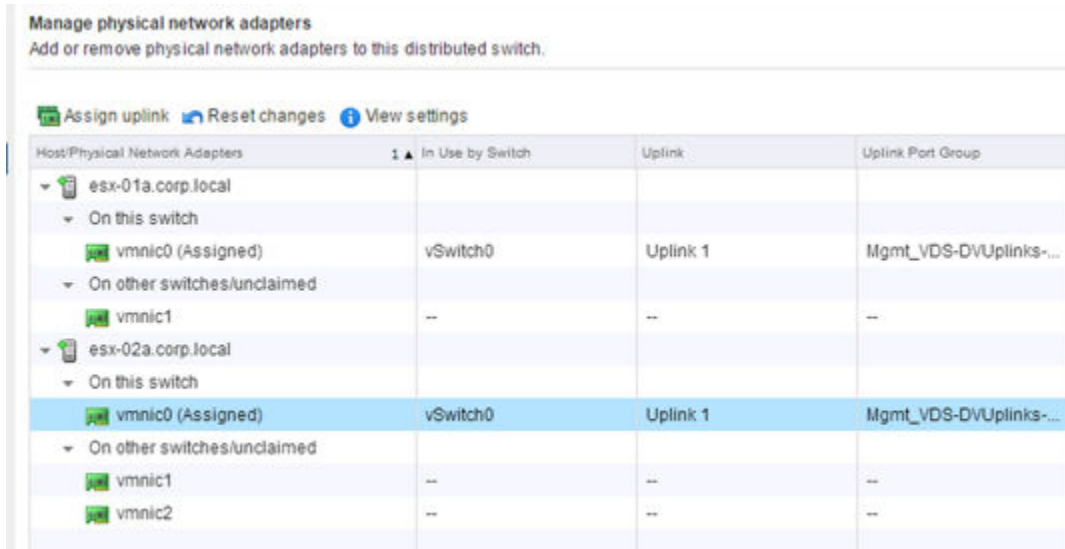


- 8 Seleccione las opciones para migrar los adaptadores físicos, los adaptadores VMkernel y las redes de la máquina virtual.



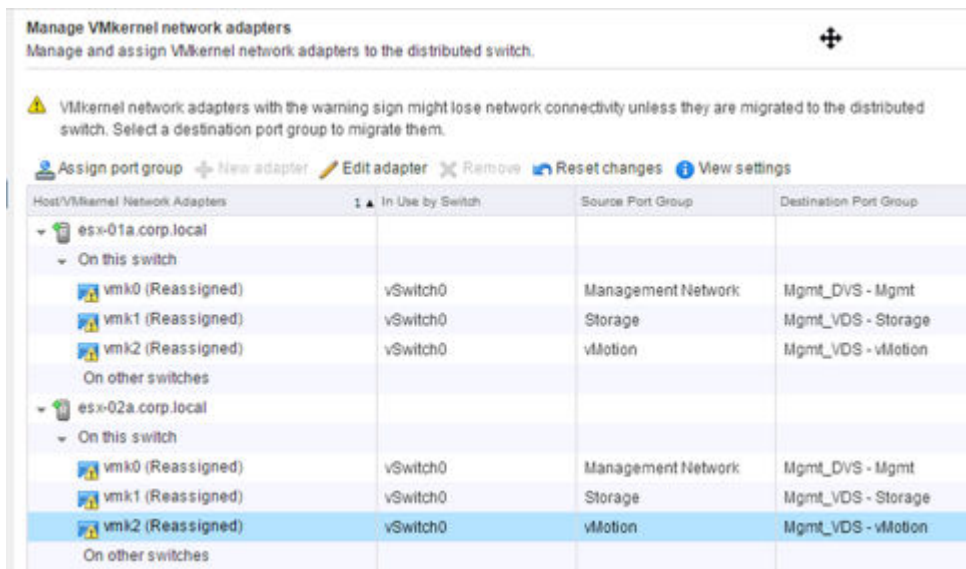
- 9 Seleccione un vínculo superior vmnic y haga clic en **Asignar vínculo superior** (Assign uplink) para migrar el vmnic desde el conmutador vSwitch estándar al conmutador distribuido. Repita este paso con cada host que vaya a conectar al conmutador vSwitch distribuido.

Por ejemplo, esta pantalla muestra dos hosts con sus vínculos superiores vmnic0 configurados para migrar desde sus respectivos conmutadores vSwitch estándar hacia el grupo de puertos distribuidos Mgmt_VDS-DVUplinks, un puerto troncal que puede transportar cualquier identificador de VLAN.



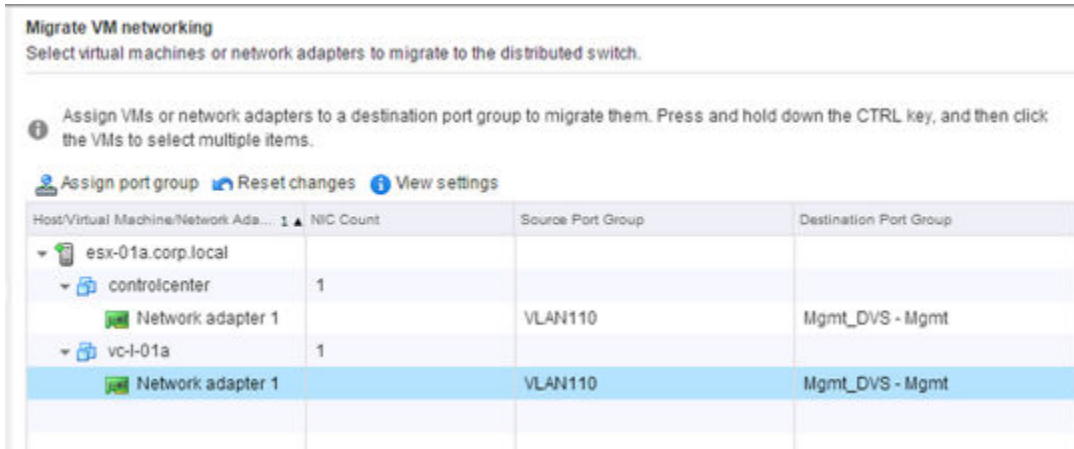
- 10 Seleccione un adaptador de red VMkernel y haga clic en **Asignar grupo de puertos** (Assign port group). Repita este paso con todos los adaptadores de red de todos los hosts que vaya a conectar al conmutador vSwitch distribuido.

Por ejemplo, esta pantalla muestra tres adaptadores de red vmk en dos hosts configurados para migrarse desde los grupos de puertos estándar hacia los nuevos grupos de puertos distribuidos.



- 11 Mueva las máquinas virtuales que están en los hosts a un grupo de puertos distribuidos.

Por ejemplo, esta pantalla muestra dos máquinas virtuales en un solo host configuradas para migrarse desde el grupo de puertos estándar hacia el nuevo grupo de puertos distribuidos.



Resultados

Una vez finalizado el procedimiento, puede comprobar los resultados en la interfaz de línea de comandos del host con la ejecución de los siguientes comandos:

```
~ # esxcli network vswitch dvs vmware list
Mgmt_VDS
  Name: Mgmt_VDS
  VDS ID: 89 78 26 50 98 bb f5 1e-a5 07 b5 29 ff 86 e2 ac
  Class: etherswitch
  Num Ports: 1862
  Used Ports: 5
  Configured Ports: 512
  MTU: 1600
  CDP Status: listen
  Beacon Timeout: -1
  Uplinks: vmnic0
  VMware Branded: true
  DVPort:
    Client: vmnic0
    DVPortgroup ID: dvportgroup-306
    In Use: true
    Port ID: 24

    Client: vmk0
    DVPortgroup ID: dvportgroup-307
    In Use: true
    Port ID: 0

    Client: vmk2
    DVPortgroup ID: dvportgroup-309
    In Use: true
    Port ID: 17

    Client: vmk1
    DVPortgroup ID: dvportgroup-308
    In Use: true
    Port ID: 9
```

■ ~ # esxcli network ip interface list

vmk2

```
Name: vmk2
MAC Address: 00:50:56:6f:2f:26
Enabled: true
Portset: DvsPortset-0
Portgroup: N/A
Netstack Instance: defaultTcpipStack
VDS Name: Mgmt_VDS
VDS UUID: 89 78 26 50 98 bb f5 1e-a5 07 b5 29 ff 86 e2 ac
VDS Port: 16
VDS Connection: 1235399406
MTU: 1500
TSO MSS: 65535
Port ID: 50331650
```

vmk0

```
Name: vmk0
MAC Address: 54:9f:35:0b:dd:1a
Enabled: true
Portset: DvsPortset-0
Portgroup: N/A
Netstack Instance: defaultTcpipStack
VDS Name: Mgmt_VDS
VDS UUID: 89 78 26 50 98 bb f5 1e-a5 07 b5 29 ff 86 e2 ac
VDS Port: 2
VDS Connection: 1235725173
MTU: 1500
TSO MSS: 65535
Port ID: 50331651
```

vmk1

```
Name: vmk1
MAC Address: 00:50:56:6e:a4:53
Enabled: true
Portset: DvsPortset-0
Portgroup: N/A
Netstack Instance: defaultTcpipStack
VDS Name: Mgmt_VDS
VDS UUID: 89 78 26 50 98 bb f5 1e-a5 07 b5 29 ff 86 e2 ac
VDS Port: 8
VDS Connection: 1236595869
MTU: 1500
TSO MSS: 65535
Port ID: 50331652
```

Pasos siguientes

Repita el proceso de migración con todos los conmutadores distribuidos de vSphere.

Comprender los modos de replicación

Cuando cree una zona de transporte o un conmutador lógico, debe seleccionar un modo de replicación. Comprender los diferentes modos puede ayudarle a decidir cuál es el más apropiado para su entorno.

Cada host ESXi preparado para NSX se configura con un endpoint de túnel VXLAN (VTEP). Cada endpoint de túnel VXLAN tiene una dirección IP. Estas direcciones IP pueden estar en la misma subred o en subredes diferentes.

Cuando dos máquinas virtuales en hosts ESXi diferentes se comunican directamente, el tráfico de encapsulación unidifusión se intercambia entre las dos direcciones IP de VTEP sin necesidad de que se produzcan inundaciones. Sin embargo, como con cualquier red de capa 2, a veces el tráfico desde una máquina virtual se debe inundar o se envía a otras máquinas virtuales que pertenecen al mismo conmutador lógico. La difusión de capa 2, la unidifusión desconocida y el tráfico multidifusión se conocen como tráfico BUM. El tráfico BUM desde una máquina virtual en un host determinado se debe replicar a otros hosts que tengan las máquinas virtuales conectadas al mismo conmutador lógico. NSX for vSphere admite tres modos de replicación diferentes:

- Modo de replicación unidifusión
- Modo de replicación multidifusión
- Modo de replicación híbrido

Resumen de los modos de replicación

Tabla 2-4. Resumen de los modos de replicación

Modo de replicación	Método de replicación BUM a VTEP en la misma subred	Método de replicación BUM a VTEP en una subred diferente	Requisitos de red física
Unidifusión (Unicast)	Unidifusión (Unicast)	Unidifusión (Unicast)	<ul style="list-style-type: none"> ■ Enrutamiento entre subredes VTEP
Multidifusión (Multicast)	Multidifusión de Capa 2	Multidifusión de Capa 3	<ul style="list-style-type: none"> ■ Enrutamiento entre subredes VTEP ■ Multidifusión de Capa 2, IGMP ■ Multidifusión de Capa 3, PIM ■ Asignación de grupos de multidifusión a conmutadores lógicos
Híbrido	Multidifusión de Capa 2	Unidifusión (Unicast)	<ul style="list-style-type: none"> ■ Enrutamiento entre subredes VTEP ■ Multidifusión de Capa 2, IGMP

Modo de replicación unidifusión

El modo de replicación unidifusión no requiere que la red física admita la multidifusión de capa 2 o capa 3 para gestionar el tráfico BUM en un conmutador lógico. El uso del modo unidifusión independiza completamente las redes lógicas de la red física. El modo de unidifusión replica todo el tráfico BUM de forma local en el host de origen y envía el tráfico BUM en un paquete unidifusión a los hosts remotos. En el modo de unidifusión, puede tener todos los VTEP en una subred o en varias.

Escenario de una subred: si todas las interfaces VTEP pertenecen a una subred única, la VTEP de origen envía el tráfico BUM a todos los VTEP remotos. Esto se conoce como replicación de cabecera. La replicación de cabecera puede resultar en una sobrecarga de host no deseada y en un mayor uso de ancho de banda. El impacto depende de la cantidad de tráfico BUM y el número de hosts y VTEP en la subred.

Escenario de varias subredes: si las interfaces VTEP del host se agrupan en varias subredes IP, el host de origen gestiona el tráfico BUM en dos partes. El VTEP de origen reenvía el tráfico BUM a cada VTEP de la misma subred (la misma que el escenario de una subred). Para los VTEP en subredes remotas, el VTEP de origen reenvía el tráfico BUM a un host de cada subred VTEP remota y configura que cada bit de replicación marque este paquete para la replicación local. Cuando un host de la subred remota recibe este paquete y encuentra el bit de replicación configurado, envía el paquete al resto de VTEP de esta subred donde existe el conmutador lógico.

Por lo tanto, el modo de replicación unidifusión se amplía correctamente en las arquitecturas de red con varias subredes de IP de VTEP, ya que la carga se distribuye en varios hosts.

Modo de replicación multidifusión

El modo de replicación multidifusión requiere que tanto la multidifusión de capa 3 como la de capa 2 estén habilitadas en la infraestructura física. Para configurar el modo de multidifusión, el administrador de red asocia cada conmutador lógico a un grupo de multidifusión de IP. Para los hosts ESXi que alojan máquinas virtuales en un conmutador lógico específico, los VTEP asociados se unen al grupo de multidifusión usando IGMP. Los enrutadores realizan un seguimiento de las uniones de IGMP y crean un árbol de distribución de multidifusión entre ellos usando un protocolo de enrutamiento de multidifusión.

Cuando los hosts replican el tráfico BUM a los VTEP en la misma subred de IP, usan una multidifusión de capa 2. Cuando los hosts replican el tráfico BUM a los VTEP en diferentes subredes de IP, usan una multidifusión de capa 3. En ambos casos, la infraestructura física gestiona la replicación del tráfico BUM a los VTEP remotos.

Aunque la multidifusión de IP es una tecnología conocida, la implementación de multidifusión de IP en el centro de datos se suele considerar un obstáculo por diferentes motivos administrativos, operativos o técnicos. El administrador de red debe tener cuidado con la multidifusión máxima admitida que aparece en la infraestructura física para habilitar la asignación uno a uno entre el conmutador lógico y el grupo de multidifusión. Uno de los beneficios de la virtualización es que permite ampliar la infraestructura virtual sin exponer estados adicionales a la infraestructura física. La asignación de conmutadores lógicos a grupos de multidifusión "físicos" rompe este modelo.

Nota En el modo de replicación multidifusión, el clúster de NSX Controller no se usa para la conmutación lógica.

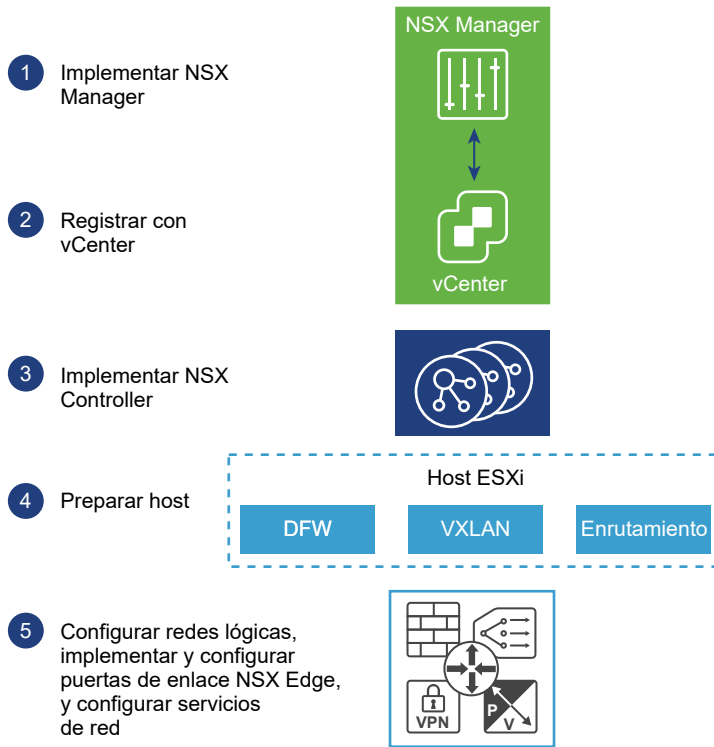
Modo de replicación híbrido

El modo híbrido es un híbrido entre los modos de replicación multidifusión y unidifusión. En el modo de replicación híbrido, el host de VTEP usa la multidifusión de Capa 2 para distribuir el tráfico BUM a los VTEP al mismo nivel en la misma subred. Cuando los VTEP de host replican el tráfico BUM a VTEP en diferentes subredes, reenvían el tráfico como paquetes de unidifusión a un host por subred de VTEP. Este host de destino usa la multidifusión de Capa 2 para enviar paquetes a otros VTEP en su subred.

La multidifusión de Capa 2 es más común en las redes de cliente que la multidifusión de Capa 3, ya que suele ser más fácil de implementar. La replicación a diferentes VTEP en la misma subred se realiza en la red física. La replicación híbrida puede suponer un descanso importante para el host de origen del tráfico BUM si existen varios VTEP al mismo nivel en la misma subred. Gracias a la replicación híbrida, puede realizar una escalabilidad vertical de un entorno denso con poca segmentación o sin ella.

Topología de ejemplo y flujo de trabajo de instalación de NSX

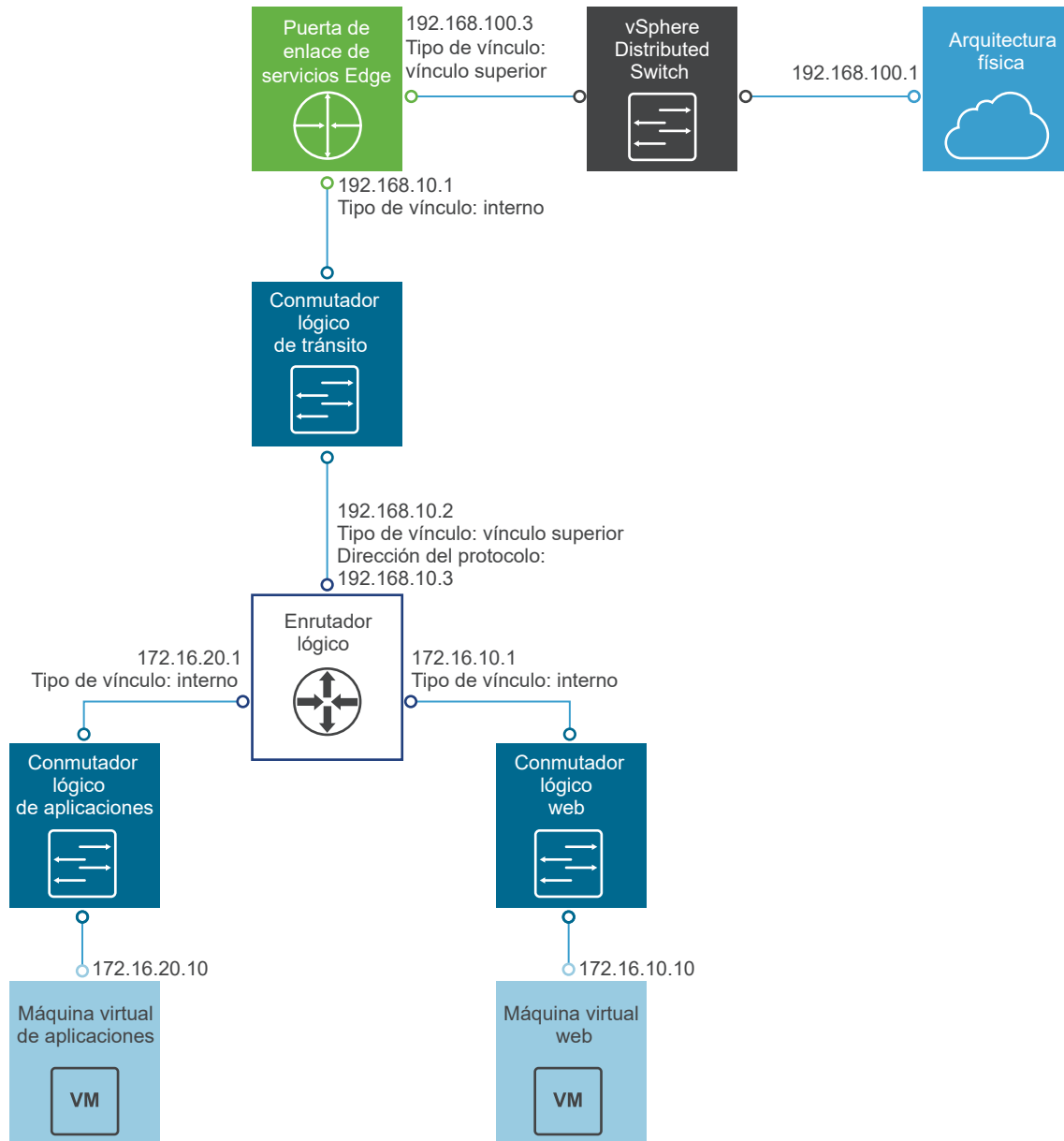
Para instalar NSX, es necesario implementar varios dispositivos virtuales, preparar los hosts ESX y realizar cierta configuración para permitir la comunicación en todos los dispositivos físicos y virtuales.



En la primera parte del proceso, se debe implementar una plantilla de OVF/OVA de NSX Manager y comprobar que NSX Manager tenga conectividad completa con las interfaces de administración de los hosts ESX que administrará. En el siguiente paso, NSX Manager y una instancia de vCenter deben vincularse entre sí mediante un proceso de registro. Esto posteriormente permite la implementación de un clúster de NSX Controller. NSX Controller, así como NSX Manager, se ejecutan como dispositivos virtuales en los hosts ESX. A continuación, se deben preparar los hosts ESX para NSX mediante la instalación de varios VIB en los hosts. Estos VIB habilitan la funcionalidad de VXLAN de Capa 2, el enrutamiento distribuido y el firewall distribuido. Después de configurar las VXLAN, especificar los rangos de interfaz de red virtual (VNI) y crear zonas de transporte, puede crear la topología de superposición de NSX.

Esta guía de instalación describe en detalle cada paso del proceso.

Si bien esta guía es aplicable a cualquier implementación de NSX, también se la puede consultar a modo de ayuda durante el proceso de creación de una topología de superposición de NSX de ejemplo que se puede utilizar con fines de práctica, instrucciones y referencia. La superposición de ejemplo tiene un solo enrutador lógico distribuido NSX (a veces denominado DLR), una puerta de enlace de servicios Edge (ESG) y un conmutador de tránsito lógico NSX que conecta los dos dispositivos de enrutamiento de NSX. La topología de ejemplo también incluye elementos de una base, que incluye dos máquinas virtuales de ejemplo. Cada una de estas máquinas virtuales está conectada a un conmutador lógico NSX distinto que permite la conectividad mediante el enrutador lógico NSX (DLR).



Cross-vCenter NSX y Enhanced Linked Mode

vSphere 6.0 presenta la característica Enhanced Linked Mode, que vincula varios sistemas de vCenter Server mediante una o más instancias de Platform Services Controller. De este forma, es posible ver y buscar los inventarios de todos los sistemas vCenter Server vinculados dentro de vSphere Web Client. En un entorno de Cross-vCenter NSX, Enhanced Linked Mode permite administrar todas las instancias de NSX Manager desde una única instancia de vSphere Web Client.

En las grandes implementaciones, donde hay varias instancias de vCenter Server, puede resultar lógico utilizar Cross-vCenter NSX con Enhanced Linked Mode para vCenter. Estas dos características son complementarias, pero distintas.

Combinar Cross-vCenter NSX y Enhanced Linked Mode

En Cross-vCenter NSX, tiene una instancia principal de NSX Manager y varias instancias secundarias de NSX Manager. Cada una de las instancias de NSX Manager está vinculada con una instancia de vCenter Server distinta. En la instancia principal de NSX Manager, se pueden crear componentes universales de NSX (como conmutadores y enrutadores) que es posible ver desde las instancias secundarias de NSX Manager.

Cuando se implementan las instancias individuales de vCenter Server con Enhanced Linked Mode, todas las instancias de vCenter Server pueden verse y administrarse desde una única instancia de vCenter Server (a veces llamada vista integral).

Por lo tanto, cuando Cross-vCenter NSX se combina con Enhanced Linked Mode para vCenter, es posible ver y administrar cualquiera de las instancias de NSX Manager y todos los componentes universales de NSX desde cualquiera de las instancias de vCenter Server vinculadas.

Utilizar Cross-vCenter NSX sin Enhanced Linked Mode

Enhanced Linked Mode no es un requisito previo para Cross-vCenter NSX. Sin Enhanced Linked Mode, aún es posible crear zonas de transporte universales para Cross-vCenter, conmutadores universales, enrutadores universales y reglas de firewall universales. No obstante, sin Enhanced Linked Mode, se debe iniciar sesión en las instancias individuales de vCenter Server para poder acceder a cada instancia de NSX Manager.

Más información sobre vSphere y Enhanced Linked Mode

Si decide utilizar Enhanced Linked Mode, consulte la *Guía de instalación y configuración de vSphere* o la *Guía de actualización de vSphere* para ver los requisitos más recientes de vSphere y de Enhanced Linked Mode.

Instalar NSX Manager Virtual Appliance

3

NSX Manager se instala como dispositivo virtual en cualquier host ESX del entorno de vCenter.

NSX Manager proporciona la interfaz de usuario gráfica (GUI) y las API de REST para crear, configurar y supervisar los componentes de NSX, como controladores, conmutadores lógicos y puertas de enlace de servicios Edge. NSX Manager proporciona una vista de sistema agregada y es el componente de administración de red centralizada de NSX. La máquina virtual de NSX Manager está incluida en un archivo OVA, lo que permite utilizar vSphere Web Client para importar NSX Manager en el almacén de datos y el inventario de la máquina virtual.

Para obtener alta disponibilidad, VMware recomienda implementar NSX Manager en un clúster configurado con HA y DRS. Como opción, puede instalar NSX Manager en una instancia de vCenter diferente de la instancia con la que operará NSX Manager. Una única instancia de NSX Manager sirve como entorno único de vCenter Server.

En las instalaciones de Cross-vCenter NSX, asegúrese de que cada instancia de NSX Manager tenga un UUID único. Las instancias de NSX Manager implementadas desde los archivos OVA tienen UUID únicos. Una instancia de NSX Manager implementada desde una plantilla (como cuando se convierte una máquina virtual a una plantilla) tendrá el mismo UUID que la instancia de NSX Manager original que se utilizó para crear la plantilla. Estas dos instancias de NSX Manager no pueden utilizarse en la misma instalación de Cross-vCenter NSX. En otras palabras: para cada instancia de NSX Manager, debe instalar un nuevo dispositivo desde cero, como se describe en este procedimiento.

La instalación de la máquina virtual NSX Manager incluye VMware Tools. No intente actualizar ni instalar VMware Tools en NSX Manager.

Durante la instalación, es posible unirse al Programa de mejora de la experiencia de cliente (CEIP) de NSX. Consulte el Programa de mejora de la experiencia de cliente en *Guía de administración de NSX* para obtener más información acerca del programa, incluyendo cómo unirse o salir de él.

Requisitos previos

- Antes de instalar NSX Manager, asegúrese de que los puertos requeridos estén abiertos. Consulte [Puertos y protocolos requeridos por NSX for vSphere](#).
- Asegúrese de que haya un almacén de datos configurado y accesible en el host ESX de destino. Se recomienda el almacenamiento compartido. HA requiere almacenamiento compartido, de modo que el dispositivo NSX Manager puede reiniciarse en otro host si se producen errores en el host original.

- Asegúrese de conocer la dirección IP y la puerta de enlace, las direcciones IP del servidor DNS, la lista de búsqueda de dominios y la dirección IP del servidor NTP que utilizará NSX Manager.
- Decida si NSX Manager tendrá únicamente direcciones IPv4, únicamente direcciones IPv6 o una configuración de red de doble pila. El nombre de host de NSX Manager se utilizará en otras entidades. Por lo tanto, el nombre de host de NSX Manager debe asignarse a la dirección IP correcta de los servidores DNS utilizados en la red.
- Prepare un grupo de puertos distribuidos para tráfico de administración en el que se comunicará NSX Manager. Consulte [Ejemplo: Trabajar con un conmutador distribuido de vSphere](#). La interfaz de administración de NSX Manager, vCenter Server y las interfaces de administración de hosts ESXi deben poder comunicarse con las instancias de NSX Guest Introspection.
- Debe estar instalado el complemento de integración de clientes. El asistente Implementar plantilla de OVF (Deploy OVF template) funciona mejor en el explorador web Firefox. A veces, en el explorador web Chrome, aparece un mensaje de error sobre la instalación del complemento de integración de clientes aunque el complemento ya esté instalado correctamente. Para instalar el complemento de integración de clientes:
 - a Abra un explorador web y escriba la URL de vSphere Web Client.
 - b En la parte inferior de la página de inicio de sesión de vSphere Web Client, haga clic en Descargar complemento de integración de clientes (Download Client Integration Plug-in).

Si el complemento de integración de clientes ya está instalado en el sistema, no verá el vínculo para descargarlo. Si desinstala el complemento de integración de clientes, el vínculo para descargarlo aparecerá en la página de inicio de sesión de vSphere Web Client.

Procedimiento

- 1 Busque el archivo de dispositivo de virtualización abierto (OVA) de NSX Manager.
Puede copiar la URL de descarga, o bien descargar el archivo OVA en el equipo.
- 2 En Firefox, abra vCenter.
- 3 Seleccione **Máquinas virtuales y plantillas** (VMs and Templates), haga clic con el botón secundario en el centro de datos y seleccione **Implementar plantilla de OVF** (Deploy OVF Template).
- 4 Pegue la URL de descarga o haga clic en **Examinar** (Browse) para seleccionar el archivo en el equipo.

Nota Si no se realiza la instalación debido a un error Expiró el tiempo de espera (Operation timed out), compruebe si el almacenamiento y los dispositivos de red tienen problemas de conectividad. Esta situación se produce cuando existe un problema con la infraestructura física, como la pérdida de conectividad con el dispositivo de almacenamiento o un problema de conectividad con el conmutador o la NIC física.

- 5 Active la casilla **Aceptar opciones de configuración adicionales** (Accept extra configuration options).

De este modo, puede establecer direcciones IPv4 e IPv6, así como propiedades de puerta de enlace predeterminada, DNS, NTP y SSH durante la instalación, en lugar de configurar estas opciones manualmente después de la instalación.

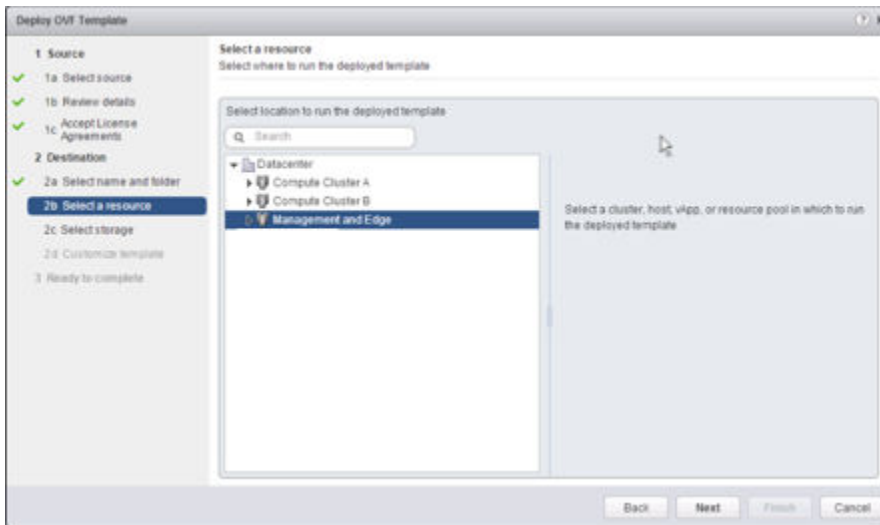
- 6 Acepte los contratos de licencia de VMware.
- 7 Edite el nombre de NSX Manager (si se lo requiere). Seleccione la ubicación para la instancia de NSX Manager implementada.

El nombre que escriba aparecerá en el inventario de vCenter.

La carpeta que seleccione se utilizará para aplicar permisos a NSX Manager.

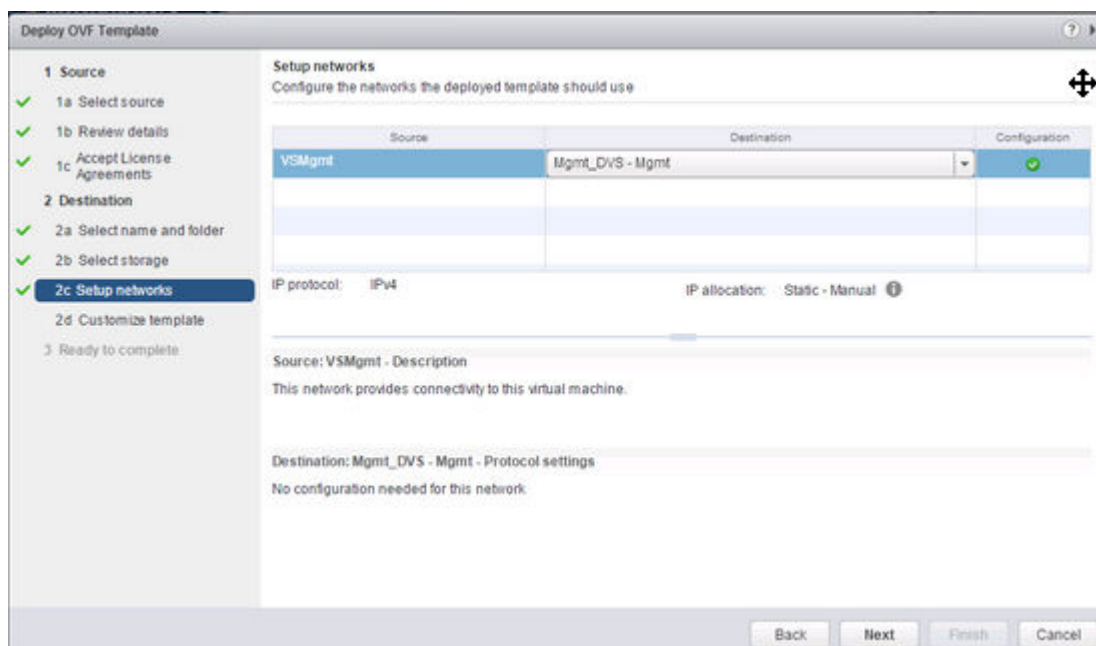
- 8 Seleccione un host o un clúster donde implementará el dispositivo NSX Manager.

Por ejemplo:



- 9 Cambie el formato de disco virtual a **Aprovisionamiento grueso** (Thick Provision) y seleccione el almacén de datos de destino para los discos virtuales y los archivos de configuración de la máquina virtual.
- 10 Seleccione el grupo de puertos de NSX Manager.

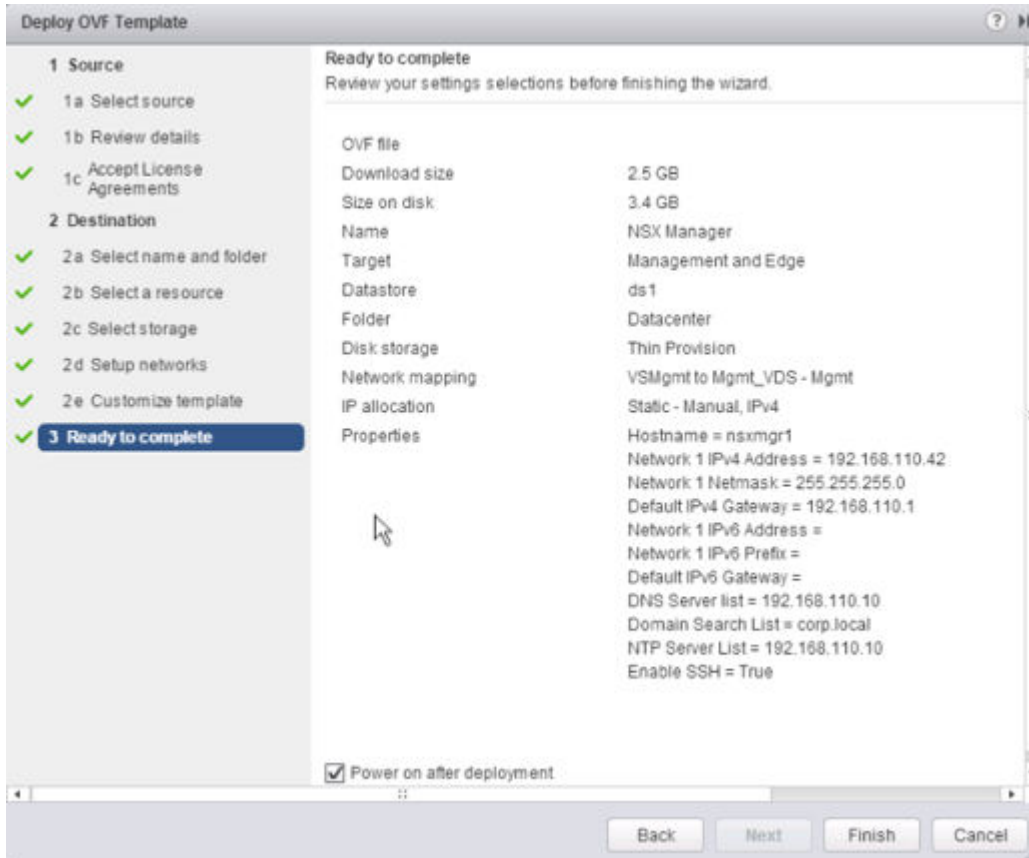
Por ejemplo, esta captura de pantalla muestra la selección del grupo de puertos Mgmt_DVS - Mgmt.



11 (opcional) Seleccione la casilla de verificación **Unirse al programa de mejora de la experiencia de cliente** (Join the Customer Experience Improvement Program).

12 Establezca las opciones de configuración adicionales de NSX Manager.

Por ejemplo, esta pantalla muestra la pantalla de revisión final una vez que se configuraron todas las opciones en una implementación de IPv4 únicamente.



Resultados

Abra la consola de NSX Manager para hacer un seguimiento del proceso de arranque.

Una vez que NSX Manager haya terminado de arrancar, inicie sesión en la interfaz de línea de comandos y ejecute el comando `show interface` para comprobar que la dirección IP se aplicó según lo esperado.

```
nsxmgr1> show interface
Interface mgmt is up, line protocol is up
index 3 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
HWaddr: 00:50:56:8e:c7:fa
inet 192.168.110.42/24 broadcast 192.168.110.255
inet6 fe80::250:56ff:fe8e:c7fa/64
Full-duplex, 0Mb/s
input packets 1370858, bytes 389455808, dropped 50, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 1309779, bytes 2205704550, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0
```

Asegúrese de que NSX Manager pueda hacer ping en su puerta de enlace predeterminada, su servidor NTP, vCenter Server y la dirección IP de la interfaz de administración en todos los hosts del hipervisor que administrará.

Para conectarse a la GUI del dispositivo NSX Manager, abra un explorador web y desplácese hasta el nombre de host o la dirección IP de NSX Manager.

Después de iniciar sesión como **admin** con la contraseña que estableció durante la instalación, en la página Inicio (Home), haga clic en **Ver resumen** (View Summary) y compruebe que los siguientes servicios se estén ejecutando:

- vPostgres
- RabbitMQ
- NSX Management Services

A fin de obtener un rendimiento óptimo, VMware recomienda que reserve memoria para el dispositivo virtual NSX Manager. Una reserva de memoria es un límite inferior garantizado para la cantidad de memoria física que el host reserva para una máquina virtual, incluso cuando la memoria está sobrecomprometida. Establezca la reserva en un nivel que garantice que NSX Manager tenga suficiente memoria como para ejecutarse de forma eficiente.

Pasos siguientes

Registre vCenter Server con NSX Manager.

Registrar vCenter Server con NSX Manager

4

NSX Manager y vCenter Server tienen una relación uno a uno. En cada instancia de NSX Manager existe un vCenter Server, incluso en un entorno de cross-vCenter NSX.

Solo puede registrarse una instancia de NSX Manager en un sistema vCenter Server. No es posible cambiar el registro de vCenter de un NSX Manager configurado.

Si desea cambiar el registro de vCenter de una instancia de NSX Manager existente, en primer lugar debe eliminar toda la configuración de NSX for vSphere y, a continuación, eliminar el complemento NSX Manager del sistema vCenter Server. Para obtener instrucciones, consulte [Quitar una instalación de NSX de forma segura](#). También puede implementar un nuevo dispositivo de NSX Manager para registrarlo en el nuevo sistema vCenter Server.

Si es necesario, puede cambiar la cuenta de usuario de vCenter Server que se utilice para registrarse en NSX Manager. La cuenta de usuario vCenter Server que se utilice para el registro debe pertenecer al grupo **Administradores (Administrators)** de vCenter Single Sign-On.

Requisitos previos

- El servicio de administración de NSX debe estar en ejecución. En la interfaz web de NSX Manager disponible en `https://<nsx-manager-ip>`, haga clic en **Inicio (Home) > Ver resumen (View Summary)** para ver el estado del servicio.
- Debe utilizar una cuenta de usuario de vCenter Server que pertenezca al grupo **Administradores (Administrators)** de vCenter Single Sign-On para sincronizar NSX Manager con el sistema vCenter Server. Si la contraseña de la cuenta tiene caracteres no ASCII, deberá cambiarla antes de sincronizar la instancia de NSX Manager con el sistema vCenter Server. No utilice la cuenta raíz.

Consulte "Administrar usuarios y grupos de vCenter Single Sign-On" en la documentación *Administrar Platform Services Controller* para obtener más información sobre cómo agregar usuarios.
- Compruebe que la resolución de nombres directa e inversa funciona y que los siguientes sistemas pueden resolver los nombres DNS del resto:
 - Dispositivos NSX Manager
 - Sistemas vCenter Server
 - Sistemas de Platform Services Controller
 - Hosts ESXi

Procedimiento

- 1 Inicie sesión en el dispositivo virtual NSX Manager.

En un navegador web, entre en la interfaz gráfica de usuario del dispositivo de NSX Manager en <https://<ip-nsx-manager>> o <https://<nombrehost-nsx-manager>> e inicie sesión como **administrador** o con una cuenta que tenga la función **administrador de Enterprise**.

- 2 En la página de inicio, haga clic en **Administrar registro de vCenter** (Manage vCenter Registration).

- 3 Edite el elemento de vCenter Server para que se dirija al nombre de host o a la dirección IP del sistema vCenter Server y, a continuación, introduzca el nombre de usuario y la contraseña del sistema vCenter Server.

- 4 Compruebe si la huella digital de certificado coincide con el certificado del sistema vCenter Server.

Si instaló un certificado firmado por la entidad de certificación en el sistema de vCenter Server, verá la huella digital del certificado firmado por la entidad de certificación. De lo contrario, verá un certificado autofirmado.

- 5 No seleccione la opción **Modificar ubicación de descarga de script de complemento**, (Modify plugin script download location) a menos que NSX Manager esté protegido por un tipo de firewall de dispositivo de enmascaramiento.

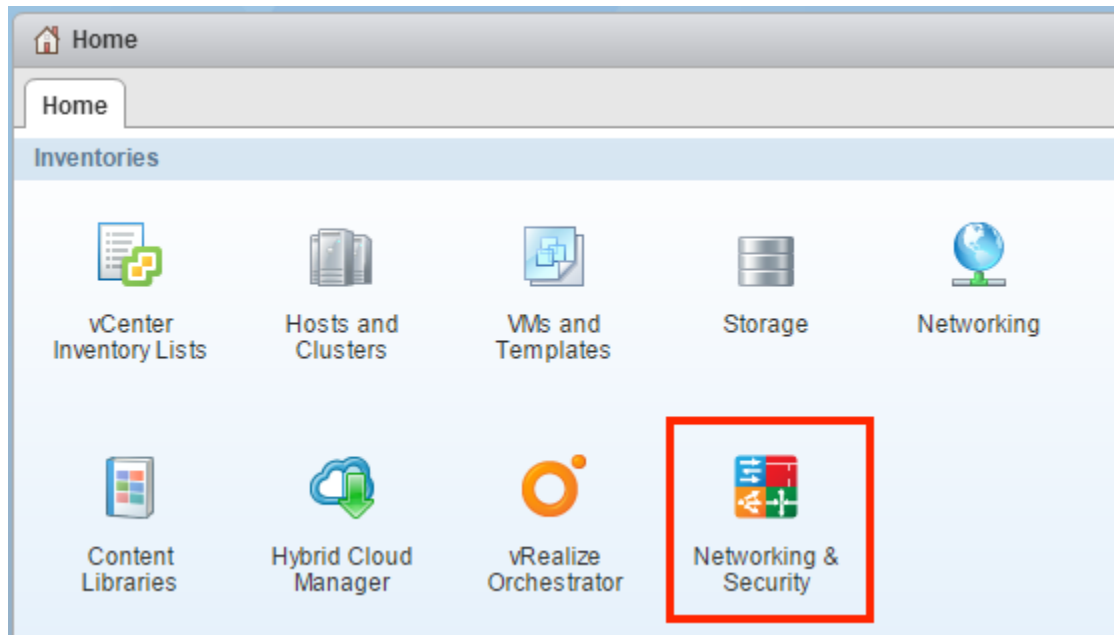
Esta opción le permite introducir una dirección IP alternativa para NSX Manager. No se recomienda poner NSX Manager detrás de un firewall de este tipo.

- 6 Confirme que el estado del sistema vCenter Server sea **Conectado (Connected)**.

- 7 Si vSphere Web Client ya está abierto, cierre sesión y vuelva a iniciarla con la cuenta que utilizara para registrar NSX Manager en vCenter Server.

Si no cierra sesión y vuelve a iniciarla, no aparecerá el icono **Redes y seguridad (Networking & Security)** en la pestaña **Inicio (Home)** de vSphere Web Client.

Haga clic en el icono **Redes y seguridad (Networking & Security)** y confirme que puede ver la nueva instancia de NSX Manager implementada.



Pasos siguientes

Programe una copia de seguridad de los datos de NSX Manager tras instalar NSX Manager. Consulte cómo restaurar y realizar una copia de seguridad de NSX en la *Guía de administración de NSX*.

Si tiene una solución de partners de NSX for vSphere, consulte la documentación del partner para obtener información sobre cómo registrar la consola del partner con NSX Manager.

Ya puede instalar y configurar los componentes de NSX for vSphere.

Configurar inicio de sesión único

5

SSO hace que vSphere y NSX sean más seguros, ya que permite que distintos componentes se comuniquen entre sí mediante un mecanismo de intercambio de token seguro, en lugar de solicitar que cada componente autentique un usuario por separado.

Puede configurar un servicio de búsqueda en NSX Manager y proporcionar las credenciales de administrador de SSO para registrar NSX Management Service como usuario de SSO. La integración del servicio Single Sign-On (SSO) con NSX mejora la seguridad de la autenticación de usuarios en vCenter y permite que NSX autentique usuarios de otros servicios de identidad, como AD, NIS y LDAP. Con SSO, NSX admite la autenticación mediante tokens autenticados de lenguaje de marcado de aserción de seguridad (SAML) de una fuente confiable mediante llamadas API de REST. NSX Manager también puede adquirir tokens de autenticación SAML para utilizarlos con las soluciones de VMware.

NSX almacena en la memoria caché la información grupal de los usuarios de SSO. Los cambios en los miembros de grupos tardan hasta 60 minutos en propagarse desde el proveedor de identidad (por ejemplo, Active Directory) hasta NSX.

Requisitos previos

- Para utilizar SSO en NSX Manager, es necesario tener la versión vCenter Server 5.5 o posterior, y el servicio de autenticación Single Sign-On (SSO) debe estar instalado en vCenter Server. Tenga en cuenta que esto aplica al servicio SSO integrado. En cambio, la implementación debe utilizar un servidor SSO externo centralizado.

Para obtener información sobre los servicios SSO que ofrece vSphere, consulte <http://kb.vmware.com/kb/2072435> y <http://kb.vmware.com/kb/2113115>.

- Debe especificarse el servidor NTP para que la hora del servidor SSO y la hora de NSX Manager estén sincronizadas.

Por ejemplo:

Time Settings		Unconfigure NTP Servers	Edit
Specify NTP server below. For SSO configuration to work correctly it is required that the time on this virtual appliance and NTP server should be in sync. It is recommended to use the same NTP server used by the SSO server.			
NTP Server	192.168.110.10		
Timezone	UTC		
Date/Time	12/28/2016 21:31:49		

Procedimiento

- 1 Inicie sesión en el dispositivo virtual NSX Manager.

En un navegador web, entre en la interfaz gráfica de usuario del dispositivo de NSX Manager en <https://<ip-nsx-manager>> o <https://<nombrehost-nsx-manager>> e inicie sesión como **administrador** o con una cuenta que tenga la función **administrador de Enterprise**.

- 2 Inicie sesión en el dispositivo virtual NSX Manager.

- 3 En la página de inicio, haga clic en **Administrar configuración de dispositivos (Manage Appliance Settings) > Servicio de administración de NSX (NSX Management Service)**.

- 4 Haga clic en **Editar** (Edit) en la sección URL de servicio de búsqueda (Lookup Service URL).

- 5 Escriba el nombre o la dirección IP del host que tiene el servicio de búsqueda.

- 6 Escriba el número de puerto.

Escriba 443 si va a utilizar vSphere 6.0. Para la versión vSphere 5.5, escriba el número de puerto 7444.

Se mostrará la URL de Lookup Service según el host y el puerto especificados.

- 7 Introduzca el nombre de usuario y la contraseña del Administrador SSO y haga clic en **Aceptar** (OK).


Se mostrará la huella digital del certificado del servidor SSO.

- 8 Compruebe si la huella digital del certificado coincide con el certificado del servidor SSO.

Si instaló un certificado firmado por la entidad de certificación en el servidor de la entidad de certificación, verá la huella digital del certificado firmado por la entidad de certificación. De lo contrario, verá un certificado autofirmado.

- 9 Confirme que el estado de Lookup Service sea **Conectado** (Connected).

Por ejemplo:

Lookup Service URL:	https://psc-01a.corp.local:443/lookupservice/sdk
SSO Administrator User Name:	administrator@vsphere.local
Status:	● Connected 

Pasos siguientes

Consulte Asignar una función a un usuario de vCenter en la *Guía de administración de NSX*.

Configurar un servidor syslog para NSX Manager

6

Si especifica un servidor syslog, NSX Manager envía todos los registros de auditoría y los eventos del sistema al servidor syslog.

Los datos de Syslog son útiles para solucionar problemas y revisar los datos registrados durante la instalación y la configuración.

NSX Edge es compatible con dos servidores syslog. NSX Manager y las instancias de NSX Controller son compatibles con un servidor syslog.

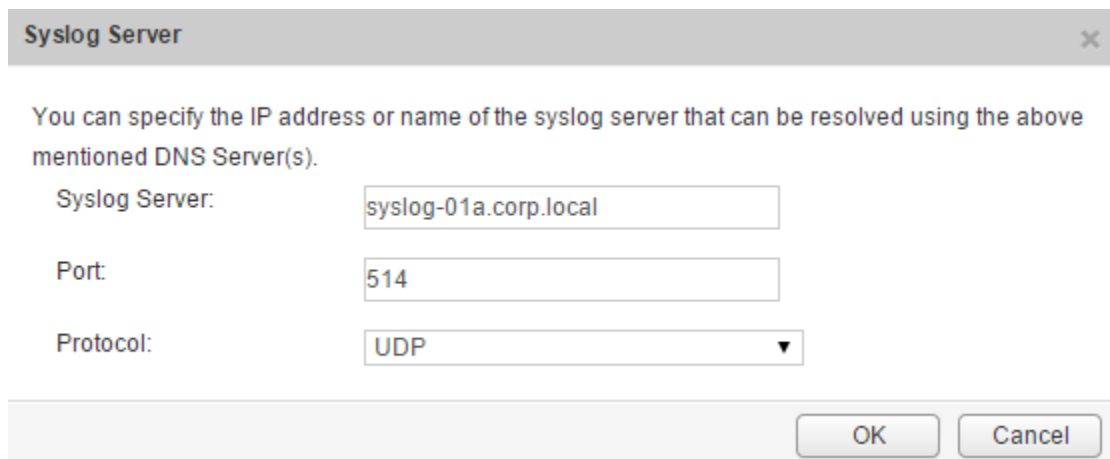
Procedimiento

- 1 Inicie sesión en el dispositivo virtual NSX Manager.

En un navegador web, entre en la interfaz gráfica de usuario del dispositivo de NSX Manager en <https://<ip-nsx-manager>> o <https://<nombrehost-nsx-manager>> e inicie sesión como **administrador** o con una cuenta que tenga la función **administrador de Enterprise**.

- 2 En la página de inicio, haga clic en **Administrar configuración de dispositivos (Manage Appliance Settings) > General**.
- 3 Haga clic en **Editar** (Edit) junto a **Servidor syslog** (Syslog Server).
- 4 Escriba el nombre del host o la dirección IP, el puerto y el protocolo del servidor syslog.

Por ejemplo:



Syslog Server [X]

You can specify the IP address or name of the syslog server that can be resolved using the above mentioned DNS Server(s).

Syslog Server:

Port:

Protocol:

OK Cancel

5 Haga clic en **Aceptar** (OK).

Resultados

Se habilita el registro remoto en NSX Manager y los registros se almacenan en el servidor syslog independiente.

Instalar y asignar licencia de NSX for vSphere

7

Una vez finalizada la instalación de NSX Manager se puede instalar y asignar una licencia de NSX for vSphere mediante vSphere Web Client.

Al iniciar NSX 6.2.3, la licencia predeterminada al completar la instalación será NSX para vShield Endpoint. Esta licencia habilita el uso de NSX para implementar y administrar vShield Endpoint solo para descarga de antivirus y tiene un cumplimiento forzado para restringir el uso de VXLAN, firewall y servicios Edge, bloqueando la preparación del host y la creación de instancias de NSX Edge.

Si necesita otras funciones de NSX, incluidos conmutadores lógicos, enrutadores lógicos, firewall distribuido o NSX Edge, puede adquirir una licencia de NSX para utilizar dichas funciones o bien solicitar una licencia de evaluación para evaluar estas características a corto plazo.

Para obtener información sobre las ediciones de licencias de NSX y sus características asociadas, consulte <https://kb.vmware.com/kb/2145269>.

Procedimiento

- ◆ En vSphere 5.5, complete los siguientes pasos para agregar una licencia para NSX.
 - a Inicie sesión en vSphere Web Client.
 - b Haga clic en **Administración** (Administration) y, a continuación, en **Licencias** (Licenses).
 - c Haga clic en la pestaña **Soluciones** (Solutions).
 - d Seleccione NSX for vSphere en la lista Soluciones (Solutions). Haga clic en **Asignar una clave de licencia** (Assign a license key).
 - e Seleccione **Asignar una nueva clave de licencia** (Assign a new license key) en el menú desplegable.
 - f Escriba la clave de licencia y una etiqueta opcional para la nueva clave.
 - g Haga clic en **Descodificar** (Decode).

Descodifique la clave de licencia para comprobar que tenga el formato correcto y suficiente capacidad para conceder una licencia a los activos.
 - h Haga clic en **Aceptar** (OK).

- ◆ En vSphere 6.0, complete los siguientes pasos para agregar una licencia para NSX.
 - a Inicie sesión en vSphere Web Client.
 - b Haga clic en **Administración** (Administration) y, a continuación, en **Licencias** (Licenses).
 - c Haga clic en la pestaña **Activos** (Assets) y luego en la pestaña **Soluciones** (Solutions).
 - d Seleccione NSX for vSphere en la lista Soluciones (Solutions). En el menú desplegable **Todas las acciones** (All Actions), seleccione **Asignar licencia...** (Assign license...).
 - e Haga clic en el icono **Agregar (+)** (Add). Introduzca la clave de licencia y haga clic en **Siguiente** (Next). Agregue un nombre para las licencias y haga clic en **Siguiente** (Next). Haga clic en **Finalizar** (Finish) para agregar la licencia.
 - f Seleccione la nueva licencia.
 - g (opcional) Haga clic en el icono **Ver características** para ver qué características están habilitadas con esta licencia. Revise la columna de **Capacidad** para comprobar la capacidad de la licencia.
 - h Haga clic en **Aceptar** (OK) para asignar la nueva licencia a NSX.

Pasos siguientes

Para obtener más información sobre las licencias de NSX, consulte <http://www.vmware.com/files/pdf/vmware-product-guide.pdf>.

Implementar clúster de NSX Controller

8

NSX Controller es un sistema de administración de estado avanzado distribuido que proporciona funciones del plano de control para funciones de enrutamiento y conmutación lógicas de NSX. Sirve como punto de control central para todos los conmutadores lógicos de una red y mantiene información sobre todos los hosts, conmutadores lógicos (VXLAN) y enrutadores lógicos distribuidos. Los controladores se requieren cuando se planean implementar 1) enrutadores lógicos distribuidos o 2) VXLAN en modo híbrido o de unidifusión.

Más allá del tamaño de la implementación de NSX, VMware requiere que cada clúster de NSX Controller tenga tres nodos de controlador. No se admite otra cantidad de nodos de controlador.

El clúster requiere que el sistema de almacenamiento en disco de cada controlador tenga una latencia de escritura máxima de menos de 300 ms y una latencia de escritura media menor a 100 ms. Si el sistema de almacenamiento no cumple estos requisitos, el clúster puede volverse inestable y provocar un tiempo de inactividad del sistema.

Precaución Mientras un controlador está en estado **Implementando** (Deploying), no agregue ni modifique conmutadores lógicos o enrutamiento distribuido en el entorno. Tampoco continúe con el procedimiento de preparación del host. Después de agregar un nuevo controlador al clúster de controladores, todos los controladores quedan inactivos durante un breve período (5 minutos como máximo). Durante este tiempo de inactividad, cualquier operación relacionada con los controladores, por ejemplo, la preparación del host, puede tener resultados inesperados. Aunque parezca que la preparación del host se completó satisfactoriamente, es posible que la certificación SSL no se establezca correctamente, lo que provoca problemas en la red VXLAN.

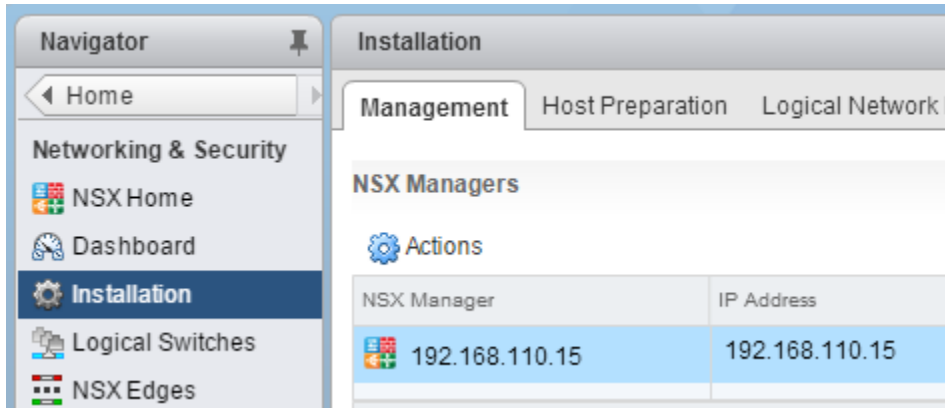
Requisitos previos

- Antes de implementar las instancias de NSX Controller, debe implementar un dispositivo NSX Manager y registrar vCenter con NSX Manager.
- Determine la configuración del grupo de direcciones IP del clúster de controlador, incluidos la puerta de enlace y el rango de direcciones IP. La configuración de DNS es opcional. La red IP de NSX Controller debe tener conexión a NSX Manager y a las interfaces de administración de los hosts ESXi.

Procedimiento

- 1 Inicie sesión en vSphere Web Client.
- 2 Desplácese hasta **Inicio > Redes y seguridad > Instalación** (Home > Networking & Security > Installation) y seleccione la pestaña **Administración** (Management).

Por ejemplo:



- 3 En la sección de nodos de NSX Controller, haga clic en el icono **Agregar nodo** (Add Node) (+).
- 4 Introduzca la configuración de NSX Controller adecuada para el entorno.

Las instancias de NSX Controller deben implementarse en un grupo del puerto de vSphere Distributed Switch o de vSphere Standard Switch que no esté basado en VXLAN y que tenga conexión a NSX Manager, a otros controladores y a hosts a través de IPv4.

Por ejemplo:

Add Controller
?

Name:

*

controller-1

NSX Manager:

*

192.168.110.15

▼

Datacenter:

*

Datacenter Site A

▼

Cluster/Resource Pool:

*

Management & Edge Cl...

▼

Datastore:

*

ds-site-a-nfs01

▼

Host:

esxmgt-01a.corp.local

▼

Folder

NSX Controllers

▼

Connected To:

*

vds-mgt_Managem

Change

Remove

IP Pool:

*

controller-pool

Select

Password:

*

Confirm password:

*

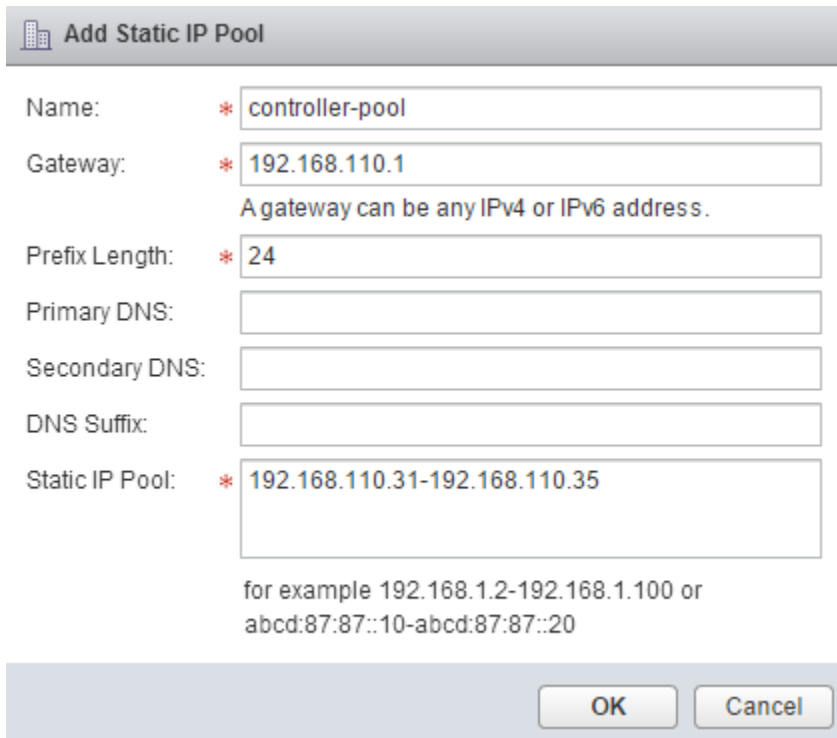
OK

Cancel

- Si todavía no configuró un grupo de direcciones IP para el clúster de controlador, haga clic en **Nuevo grupo de direcciones IP** (New IP Pool) para hacerlo.

De ser necesario, los controladores individuales pueden estar en subredes de IP distintas.

Por ejemplo:



Add Static IP Pool

Name: * controller-pool

Gateway: * 192.168.110.1
A gateway can be any IPv4 or IPv6 address.

Prefix Length: * 24

Primary DNS:

Secondary DNS:

DNS Suffix:

Static IP Pool: * 192.168.110.31-192.168.110.35

for example 192.168.1.2-192.168.1.100 or
abcd:87:87::10-abcd:87:87::20

OK Cancel

- 6 Introduzca y vuelva a introducir una contraseña para el controlador.

Nota La contraseña no debe contener el nombre de usuario como subcadena. Los caracteres no deben repetirse 3 o más veces consecutivas.

La contraseña debe tener al menos 12 caracteres y cumplir con al menos 3 de las siguientes 4 reglas:

- Al menos una letra en mayúscula
- Al menos una letra en minúscula
- Al menos un número
- Al menos un carácter especial

- 7 Una vez implementada el primer controlador, implemente otras dos más.

Es obligatorio tener tres controladores. Le recomendamos que configure una regla anticompatibilidad DRS para evitar que los controladores residan en el mismo host.

Resultados

Una vez implementados todos los controladores correctamente, estos aparecen con el estado **Conectado** (Connected) y aparece una marca de verificación de color verde.

Si la implementación no se realizó correctamente, consulte el tema Implementar instancias de NSX Controller de la *Guía para solucionar problemas de NSX*.

NSX habilita el apagado o el inicio automáticos de la máquina virtual en los hosts en los que los nodos de NSX Controller se implementan primero. Si las máquinas virtuales del nodo de controladores se migran a otros hosts posteriormente, es posible que los nuevos hosts no tengan habilitado el inicio/apagado automático de máquinas virtuales. Por este motivo, VMware recomienda que compruebe todos los hosts del clúster para asegurarse de que la opción de encendido/apagado automático esté habilitada. Consulte http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-5FE08AC7-4486-438E-AF88-80D6C7928810.html.

Ejemplo

Excluir las máquinas virtuales de la protección de firewall

9

Puede excluir un conjunto de máquinas virtuales de la protección de firewall distribuido de NSX.

NSX Manager, NSX Controller y las máquinas virtuales NSX Edge se excluyen automáticamente de la protección de firewall distribuido de NSX. Asimismo, VMware recomienda colocar las siguientes máquinas virtuales de servicio en la lista de exclusión para permitir que el tráfico circule libremente.


- vCenter Server. Puede moverse a un clúster protegido por firewall, pero ya debe existir en la lista de exclusión para evitar problemas de conectividad.

Nota Es importante agregar vCenter Server a la lista de exclusión antes de cambiar la regla predeterminada "any any" de permitir a bloquear. Si no se lleva a cabo esta acción, se bloqueará el acceso a vCenter Server tras crear una regla Denegar todo (o tras modificar la regla predeterminada para bloquear la acción). Si esto sucede, revierta el DFW a la regla de firewall predeterminada con el siguiente comando: `https://NSX_Manager_IP/api/4.0/firewall/globalroot-0/config`. La solicitud debe devolver un estado de 204. Esto restaurará la directiva predeterminada (con la regla predeterminada de permitir) para DFW y volverá a habilitar el acceso a vCenter Server y vSphere Web Client.

- Máquinas virtuales del servicio de partners.
- Máquinas virtuales que requieren el modo promiscuo. Si estas máquinas virtuales están protegidas por firewall distribuido de NSX, su rendimiento puede verse gravemente afectado.
- El servidor SQL Server que utiliza la instancia de vCenter basada en Windows.
- vCenter Web Server, si se lo va a ejecutar por separado.

Procedimiento

- 1 En vSphere Web Client, haga clic en **Redes y seguridad** (Networking & Security).
- 2 En **Inventario de redes y seguridad** (Networking & Security Inventory) haga clic en **Instancias de NSX Manager** (NSX Managers).
- 3 En la columna **Nombre** (Name), haga clic en una instancia de NSX Manager.
- 4 Haga clic en la pestaña **Administrar** (Manage) y, a continuación, en **Lista de exclusión** (Exclusion List).

- 5 Haga clic en el icono **Agregar** (Add) ().
- 6 Seleccione las máquinas virtuales que desee excluir y haga clic en **Agregar** (Add).
- 7 Haga clic en **Aceptar** (OK).

Resultados

Si una máquina virtual tiene varias NIC, todas ellas quedarán excluidas de la protección. Si agrega vNIC a una máquina virtual que ya está agregada a la lista de exclusión, el firewall se implementa automáticamente en las vNIC recientemente agregadas. Para excluir estas vNIC de la protección de firewall, debe extraer la máquina virtual de la lista de exclusión y, a continuación, volver a agregarla a la lista. Una alternativa es realizar un ciclo de energía (apagar y encender la máquina virtual), pero la primera opción es menos disruptiva.

Preparar clústeres de hosts para NSX

10

La preparación de hosts es el proceso por el cual NSX Manager 1) instala módulos de kernel en hosts ESXi que forman parte de los clústeres de vCenter y 2) compila el tejido del plano de administración y del plano de control. Los módulos de kernel de NSX for vSphere empaquetados en archivos VIB se ejecutan dentro del kernel del hipervisor y ofrecen servicios, como enrutamiento distribuido, firewall distribuido y capacidades de puente de VXLAN.

A fin de preparar el entorno para la virtualización de red, debe instalar los componentes de la infraestructura de red en cada clúster de cada instancia de vCenter Server donde sea necesario. De este modo, se implementa el software requerido en todos los hosts del clúster. Cuando se agrega un nuevo host al clúster, el software requerido se instala en ese host automáticamente.

Si va a utilizar hosts ESXi sin estado (es decir, ESXi no mantiene activamente su estado reinicio tras reinicio), debe descargar los VIB de NSX manualmente e integrarlos a la imagen del host. Puede encontrar las rutas de descarga de los VIB de NSX en la página: https://<NSX_MANAGER_IP>/bin/vdn/nwfabric.properties. Tenga en cuenta que las rutas de descarga pueden variar en cada versión de NSX. Para obtener los VIB adecuados, consulte siempre la página https://<NSX_MANAGER_IP>/bin/vdn/nwfabric.properties. Consulte cómo implementar VXLAN a través de Auto Deploy <https://kb.vmware.com/kb/2041972> para obtener más información.

Requisitos previos

- Registre vCenter Server en NSX Manager e implemente NSX Controllers.
- Compruebe si la búsqueda inversa de DNS devuelve un nombre de dominio completo cuando se consulta con la dirección IP de NSX Manager. Por ejemplo:

```
C:\Users\Administrator>nslookup 192.168.110.42
Server: localhost
Address: 127.0.0.1

Name: nsxmgr-l-01a.corp.local
Address: 192.168.110.42
```

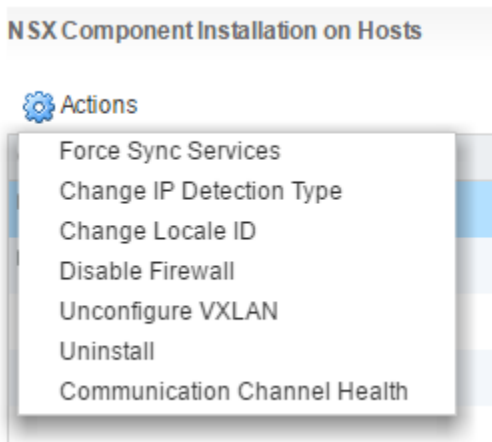
- Compruebe que los hosts puedan resolver el nombre DNS de vCenter Server.

- Compruebe si los hosts pueden conectarse a vCenter Server en el puerto 80.
- Compruebe que la hora de red en vCenter Server y los hosts ESXi esté sincronizada.
- En cada clúster del host que participará en NSX, compruebe que los hosts de ese clúster estén conectados a un vSphere Distributed Switch (VDS) común.

Por ejemplo, supongamos que tiene un clúster con los hosts Host1 y Host2. Host1 está conectado a VDS1 y VDS2. Host2 está conectado a VDS1 y VDS3. Al preparar un clúster para NSX, solo se puede asociar NSX con el VDS1 del clúster. Si agrega otro host (Host3) al clúster y Host3 no está conectado a VDS1, la configuración no es válida y Host3 no está listo para la funcionalidad NSX.

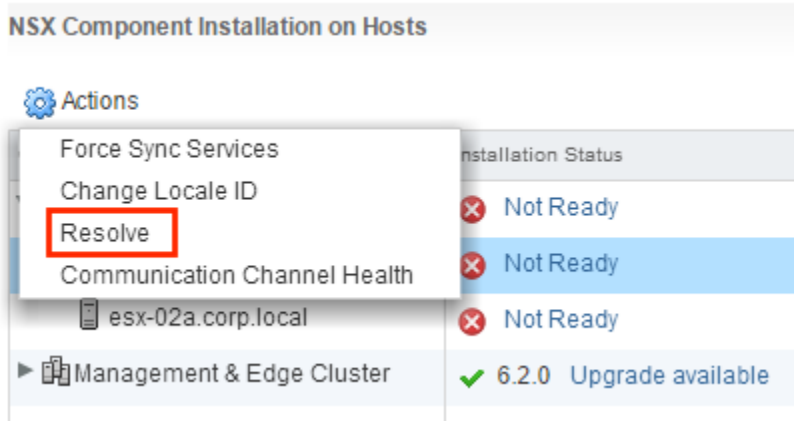
- Si tiene vSphere Update Manager (VUM) instalado en el entorno, debe deshabilitarlo a fin de poder preparar los clústeres para la virtualización de red. Para obtener más información sobre cómo comprobar si VUM está habilitado y cómo deshabilitarlo si fuera necesario, consulte <http://kb.vmware.com/kb/2053782>.
- Antes de empezar con el proceso de preparación de hosts de NSX, asegúrese siempre de que el clúster esté en estado resuelto; es decir, que la opción **Resolver** (Resolve) no aparezca en la lista **Acciones** (Actions) del clúster.

Por ejemplo:



La opción **Resolver** (Resolve) a veces aparece porque es preciso reiniciar uno o más hosts del clúster.

Otras veces, la opción **Resolver** (Resolve) aparece porque hay un error que debe solucionarse. Haga clic en el vínculo **No listo** (Not Ready) para ver el error. Si puede, borre la condición de error. Si no puede borrarla del clúster, una alternativa es mover los hosts a otro clúster o a uno nuevo y eliminar el antiguo.



Si la opción **Resolver** (Resolve) no soluciona el problema, consulte *Guía para solucionar problemas de NSX*. Para consultar una lista de problemas resueltos por la opción **Resolver** (Resolve), consulte *Eventos del sistema y de registro de NSX*.

Procedimiento

- 1 Inicie sesión en vSphere Web Client.
- 2 Diríjase a **Inicio > Redes y seguridad > Instalación** (Home > Networking & Security > Installation) y seleccione la pestaña **Preparación del host** (Host Preparation).
- 3 En todos los clústeres que requieren la conmutación lógica de NSX, el enrutamiento y los firewalls, haga clic en **Acciones** (⚙️) (Actions) y en **Instalar** (Install).

Un clúster de proceso (también conocido como clúster de carga útil) es un clúster con máquinas virtuales de aplicaciones (web, base de datos, etc.). Si un clúster de proceso tiene conmutación de NSX, enrutamiento o firewalls, haga clic en **Instalar** (Install) en el clúster de proceso.

En el clúster "Administración y Edge" (Management and Edge), como el que se muestra en el ejemplo, NSX Manager y las máquinas virtuales del controlador comparten un clúster con dispositivos Edge, como enrutadores lógicos distribuidos (DLR) y puertas de enlace de servicios Edge (ESG). En este caso, es importante que haga clic en **Instalar** (Install) en el clúster compartido.

Por el contrario, si Administración y Edge (Management and Edge) tiene un clúster dedicado y no compartido (como se recomienda para un entorno de producción), haga clic en **Instalar** (Install) en el clúster Edge, pero no en el clúster de administración.

Nota Mientras la instalación está en curso, no implemente, actualice ni desinstale servicios o componentes.

- 4 Supervise la instalación hasta que la columna **Estado de instalación** (Installation Status) muestre una marca de verificación de color verde.

Si la columna **Estado de instalación** (Installation Status) muestra un icono de advertencia rojo y el mensaje **No listo** (Not Ready), haga clic en **Resolver** (Resolve). Si hace clic en **Resolver** (Resolve) puede provocar el reinicio del host. Si la instalación todavía no se puede realizar, haga clic en el icono de advertencia. Se mostrarán todos los errores. Realice la acción requerida y haga clic de nuevo en **Resolver** (Resolve).

Cuando se completa la instalación, la columna **Estado de instalación** (Installation Status) muestra la versión y la compilación del NSX instalado y la columna **Firewall** muestra **Habilitado** (Enabled). Ambas columnas tienen una marca de verificación de color verde. Si ve Resolver (Resolve) en la columna **Estado de instalación** (Installation Status), haga clic en Resolver y, a continuación, actualice la ventana del explorador.

Resultados

Los VIB se instalan y se registran en todos los hosts del clúster preparado. Los VIB instalados varían en función de las versiones de NSX y ESXi instaladas.

Versión de ESXi	Versión de NSX	VIB instalados
5.5	Cualquier versión 6.3.x	<ul style="list-style-type: none"> ■ esx-vsip ■ esx-vxlan
6.0 o posterior	6.3.2 o anterior	<ul style="list-style-type: none"> ■ esx-vsip ■ esx-vxlan
6.0 o posterior	6.3.3 o posterior	<ul style="list-style-type: none"> ■ esx-nsxv

Para comprobarlas, asigne el protocolo SSH a cada host, ejecute el comando `esxcli software vib list` y busque los VIB correspondientes. Además de mostrar los VIB, este comando muestra la versión instalada.

```
[root@host:~] esxcli software vib list | grep esx
esx-XXXX    6.0.0-0.0.XXXXXXX  VMware  VMwareCertified  2016-12-29
```

Si agrega un host a un clúster preparado, los VIB de NSX se instalan automáticamente en el host.

Si mueve un host a un clúster no preparado, los VIB de NSX se desinstalan automáticamente del host.

Agregar un host a un clúster preparado

11

En esta sección se describe la forma de agregar un host a un clúster preparado para la virtualización de red.

Procedimiento

- 1 Agregue el host a vCenter Server como host independiente.
Consulte la *documentación de ESXi y vCenter Server*.
- 2 Agregue el host al conmutador vSphere Distributed Switch asignado al clúster donde desea agregar el host.
Todos los hosts en el clúster deben estar en el conmutador vSphere Distributed Switch que aprovecha NSX.
- 3 Haga clic con el botón secundario en el host de destino y seleccione **Modo de mantenimiento (Maintenance Mode) > Entrar en modo de mantenimiento (Enter Maintenance Mode)**.
- 4 Arrastre y suelte el host de destino en el clúster habilitado de NSX existente.
Debido a que se trata de un clúster preparado, el software requerido se instala automáticamente en el host recientemente agregado.
- 5 Haga clic con el botón secundario en el host y seleccione **Modo de mantenimiento (Maintenance Mode) > Salir del modo de mantenimiento (Exit Maintenance Mode)**.
DRS equilibra las máquinas virtuales en el host.

Quitar un host de un clúster NSX preparado

12

En esta sección se describe cómo quitar un host de un clúster preparado para la virtualización de red. Es posible que desee hacer esto si, por ejemplo, decide que el host no formará parte de NSX.

Importante Si el host tiene NSX 6.3.0 y ESXi 6.0 o versiones posteriores, no es necesario reiniciar un host para desinstalar los VIB. En las versiones anteriores de NSX y ESXi, se necesita un reinicio para completar la desinstalación del VIB.

Procedimiento

- 1 Coloque el host en modo de mantenimiento y espere a que el DRS evacue el host o realice una migración manual con vMotion de las máquinas virtuales en ejecución desde el host.
- 2 Quite los hosts del clúster preparado moviéndolos a un clúster no preparado o convirtiéndolos en hosts independientes fuera de cualquier clúster.

NSX desinstala los componentes de virtualización de red y las máquinas virtuales de servicio del host.
- 3 Si el host tiene NSX 6.2.x o versiones anteriores instaladas, o tiene ESXi 5.5 instalado, reinicie el host.
- 4 Verifique que la desinstalación de los VIB se completó.
 - a Compruebe el panel Tareas Recientes (Recent Tasks) en vSphere Web Client.
 - b En la pestaña **Preparación de host** (Host Preparation), compruebe que el estado de instalación del clúster desde el que se quitó el host tiene una marca de verificación de color verde.

Si el estado de instalación es Instalando (Installing), el proceso de desinstalación seguirá en curso.
- 5 Después de completar la desinstalación, el host puede salir del modo de mantenimiento.

Resultados

Los VIB de NSX se quitan del host. Para comprobarlo, acceda al host mediante SSH y ejecute el comando `esxcli software vib list | grep esx`. Compruebe que en el host no estén presentes los VIB siguientes:

- esx-vsip
- esx-vxlan

Si los VIB permanecen en el host, puede consultar los registros para determinar por qué no funcionó la eliminación de VIB automática.

Puede quitar los VIB manualmente si ejecuta los comandos siguientes:

- `esxcli software vib remove --vibname=esx-vxlan`
- `esxcli software vib remove --vibname=esx-vsiop`

Configurar parámetros de transporte de VXLAN

13

La red VXLAN se utiliza para la conmutación lógica de Capa 2 en todos los hosts, lo cual puede expandir varios dominios subyacentes de Capa 3. La red VXLAN se configura por clúster, donde se asigna cada clúster que participará en NSX a un conmutador distribuido de vSphere (VDS). Cuando se asigna un clúster a un conmutador distribuido, cada host del clúster queda habilitado para conmutadores lógicos. La configuración elegida aquí se utilizará para crear la interfaz del VMkernel.

Si necesita conmutación y enrutamiento lógicos, todos los clústeres que tienen VIB de NSX instalados en los hosts también deben tener configurados parámetros de transporte de VXLAN. Si desea implementar únicamente un firewall distribuido, no es necesario configurar los parámetros de transporte de VXLAN.

Cuando configura la red VXLAN, debe proporcionar un vSphere Distributed Switch, un ID de VLAN, un tamaño de MTU, un mecanismo de direcciones IP (grupo de IP o DHCP) y una directiva de formación de equipos de NIC.

La MTU de cada conmutador debe establecerse en 1.550 o superior. El valor predeterminado es 1.600. Si el tamaño de MTU de los conmutadores distribuidos de vSphere es mayor que la MTU de VXLAN, la MTU de vSphere Distributed Switch no se reducirá. Si se establece en un valor más bajo, se ajustará para que coincida con la MTU de VXLAN. Por ejemplo, si la MTU de vSphere Distributed Switch se establece en 2.000 y se acepta la MTU predeterminada de VXLAN de 1.600, la MTU de vSphere Distributed Switch no se modifica. Si la MTU de vSphere Distributed Switch es 1.500 y la MTU de VXLAN es 1.600, la MTU de vSphere Distributed Switch se cambia a este último valor.

Los VTEP tienen asociado un identificador de VLAN. Sin embargo, puede especificar el identificador de VLAN = 0 para los VTEP, lo cual indica que se quitarán las etiquetas de las tramas.

Es posible que quiera usar diferentes opciones de direcciones IP en los clústeres de administración y los clústeres de proceso. Esto depende de la forma en que esté diseñada la red física, por lo cual probablemente no sea así en las implementaciones pequeñas.

Requisitos previos

- Todos los hosts del clúster deben estar conectados a un vSphere Distributed Switch común.
- NSX Manager debe estar instalado.
- Deben estar instalados los controladores NSX Controller, a menos que se vaya a utilizar el modo de replicación de multidifusión para el plano de control.

- Planifique la directiva sobre formación de equipos de NIC. La directiva sobre formación de equipos de NIC determina el equilibrio de carga y la configuración de conmutación por error de vSphere Distributed Switch.

No mezcle distintas directivas de formación de equipos para diferentes grupos de puertos en un vSphere Distributed Switch donde algunos utilizan EtherChannel o LACPv1/LACPv2 y otros utilizan una directiva de formación de equipos diferente. Si se comparten vínculos superiores en estas distintas directivas de formación de equipos, se interrumpe el tráfico. Si hay enrutadores lógicos, habrá problemas de enrutamiento. Una configuración de este tipo no es compatible y se debe evitar.

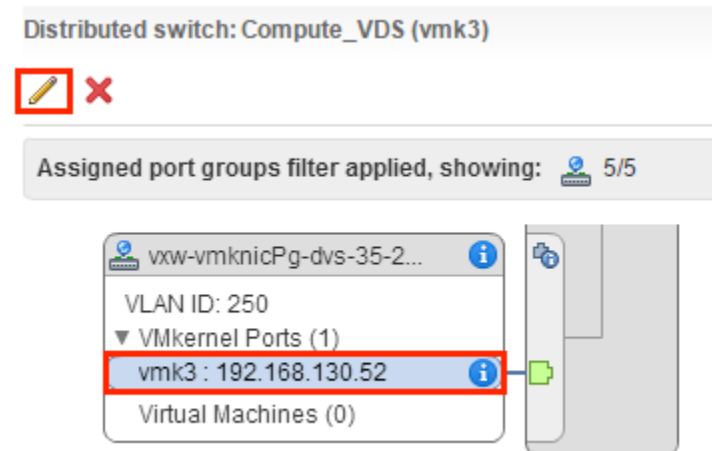
La práctica recomendada para la formación de equipos basada en hash de IP (EtherChannel, LACPv1 o LACPv2) es utilizar todos los vínculos superiores en el vSphere Distributed Switch del equipo y no tener grupos de puertos en ese vSphere Distributed Switch con diferentes directivas de formación de equipos. Para obtener más información y otras instrucciones, consulte la *Guía de diseño de virtualización de red de VMware® NSX for vSphere* en <https://communities.vmware.com/docs/DOC-27683>.

- Planifique el esquema de direcciones IP de los extremos del túnel VXLAN (VTEP). Los VTEP son las direcciones IP de origen y destino que se utilizan en el encabezado IP externo para identificar de forma única a los hosts ESX que originan y finalizan la encapsulación de tramas de VXLAN. Para las direcciones IP de VTEP puede utilizar DHCP o grupos de direcciones IP configuradas manualmente.

Si desea que una dirección IP específica se asigne a un VTEP, puede 1) utilizar una reserva o una dirección DHCP fija que asigne una dirección MAC a una dirección IP específica en el servidor DHCP o 2) utilizar un grupo de direcciones IP y, a continuación, editar manualmente la dirección IP de VTEP asignada a vmknic en **Hosts y clústers (Hosts and Clusters) > host > Administrar (Manage) > Red (Networking) > Conmutadores virtuales (Virtual Switches)**.

Nota Si edita manualmente la dirección IP, asegúrese de que la dirección IP NO sea similar al rango original del grupo de IP.

Por ejemplo:



- En los clústeres que forman parte del mismo VDS, el identificador de VLAN debe ser el mismo para los VTEP y la formación de equipos de NIC.
- La práctica recomendada consiste en exportar la configuración de conmutador distribuido de vSphere antes de preparar el clúster para VXLAN. Consulte <http://kb.vmware.com/kb/2034602>.

Procedimiento

- 1 Inicie sesión en vSphere Web Client.
- 2 Diríjase a **Inicio > Redes y seguridad > Instalación** (Home > Networking & Security > Installation) y seleccione la pestaña **Preparación del host** (Host Preparation).
- 3 Haga clic en **No configurado** (Not Configured) en la columna **VXLAN**.
- 4 Configure las redes lógicas.

Para ello, seleccione un vSphere Distributed Switch, un identificador de VLAN, un tamaño de MTU, un mecanismo de generación de direcciones IP y una directiva de formación de equipos de NIC.

Estas pantallas de ejemplo muestran la configuración de un clúster de administración con un rango de direcciones IP de 182.168.150.1-192.168.150.100, respaldado por VLAN 150, y con una directiva de formación de equipos de NIC por conmutación por error.

Configure VXLAN networking

Configuring all hosts in cluster "Management and Edge" for VXLAN networking.

Switch: * Mgmt_VDS

VLAN: * 150

MTU: * 1600

VMKNic IP Addressing: * ☐ Use DHCP
☒ Use IP Pool

IP Pool: New IP Pool...

VMKNic Teaming Policy: * Fail Over

VTEP: * 1

OK Cancel

La cantidad de VTEP no puede editarse en la interfaz de usuario. La cantidad de VTEP se establece de modo tal que coincida con la cantidad de dvUplinks en el conmutador distribuido de vSphere que se va a preparar.

Add Static IP Pool

Name: * mgmt-edge-ip-pool

Gateway: * 192.168.150.1
A gateway can be any IPv4 or IPv6 address.

Prefix Length: * 24

Primary DNS: 192.168.110.10

Secondary DNS:

DNS Suffix: corp.local

Static IP Pool: * 192.168.150.1-192.168.150.100

for example 192.168.1.2-192.168.1.100 or
abcd:87:87::10-abcd:87:87::20

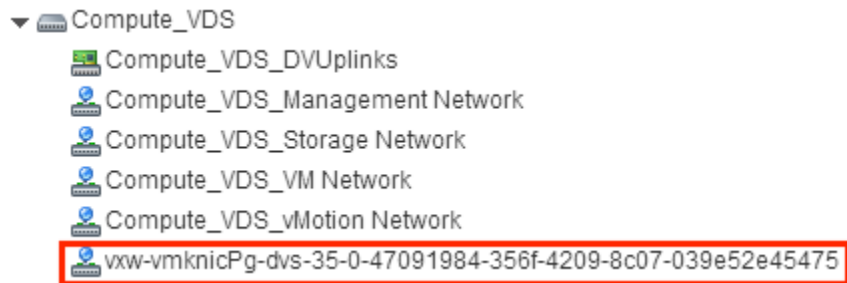
OK Cancel

En los clústeres de proceso, se puede utilizar otra configuración de direcciones IP (por ejemplo, 192.168.250.0/24 con VLAN 250). Esto depende de la forma en que esté diseñada la red física, por lo cual probablemente no sea así en las implementaciones pequeñas.

Resultados

La configuración de VXLAN tiene como resultado la creación de un nuevo grupo de puertos distribuido en el vSphere Distributed Switch especificado.

Por ejemplo:



Para obtener más información sobre cómo solucionar problemas de VXLAN, consulte *Guía para solucionar problemas de NSX*.

Asignar un grupo de identificadores de segmento y un rango de direcciones de multidifusión

14

Los segmentos de VXLAN se compilan entre los extremos de túnel de VXLAN (VTEP). Un host hipervisor es un ejemplo de un VTEP típico. Cada túnel de VXLAN tiene un identificador de segmento. Se debe especificar un grupo de identificadores de segmento para que cada NSX Manager aísle el tráfico de red. Si no hay un controlador NSX Controller implementado en el entorno, también debe agregar un rango de direcciones de multidifusión para distribuir el tráfico por la red y evitar sobrecargar una sola dirección de multidifusión.

Cuando determine el tamaño de cada grupo de identificadores de segmentos, tenga en cuenta que el rango de identificadores de segmentos controla la cantidad de conmutadores lógicos que pueden crearse. Elija un subconjunto pequeño de los 16 millones de VNI posibles. No debe configurar más de 10.000 VNI en una sola instancia de vCenter porque vCenter limita la cantidad de grupos dvPortgroups a 10.000.

Si la VXLAN se encuentra en otra implementación de NSX, considere cuáles VNI ya están en uso y evite superponerlos. Los VNI que no se superponen se aplican automáticamente en un único entorno de NSX Manager y vCenter. Los rangos de VNI locales no pueden superponerse. No obstante, es importante asegurarse de que los VNI no se superpongan en las distintas implementaciones de NSX. Los VNI que no se superponen son útiles para fines de seguimiento y permiten garantizar que las implementaciones estén preparadas para un entorno de Cross-vCenter.

Si alguna de las zonas de transporte va a utilizar el modo de replicación híbrido o de multidifusión, debe agregar una dirección de multidifusión o un rango de direcciones de multidifusión.

Contar con un rango de direcciones de multidifusión distribuye el tráfico por la red, evita la sobrecarga de una sola dirección de multidifusión y contiene mejor la replicación de BUM.

No utilice 239.0.0.0/24 o 239.128.0.0/24 como rango de direcciones de multidifusión, ya que estas redes se utilizan para el control de la subred local; es decir, los conmutadores físicos saturan todo el tráfico que utilizan estas direcciones. Para obtener más información sobre las direcciones de multidifusión inutilizables, consulte <https://tools.ietf.org/html/draft-ietf-mboned-ipv4-mcast-unusable-01>.

Cuando los modos de replicación híbrido o de multidifusión de VXLAN están configurados y funcionan correctamente, se entrega una copia del tráfico de multidifusión solamente a los hosts que enviaron mensajes de unión a IGMP. De lo contrario, la red física inunda todo el tráfico de multidifusión en todos los hosts del mismo dominio de difusión. Para evitar esa inundación, debe hacer lo siguiente:

- Asegúrese de que el conmutador físico subyacente tenga configurada una MTU mayor o igual que 1600.
- Asegúrese de que el conmutador físico subyacente tenga correctamente configurada la intromisión de IGMP y tenga establecido un solicitante de IGMP en los segmentos de red que transportan tráfico de VTEP.
- Asegúrese de que la zona de transporte esté configurada con el rango de direcciones de multidifusión recomendado. El rango de direcciones de multidifusión recomendado comienza en 239.0.1.0/24 y excluye a 239.128.0.0/24.

La interfaz de vSphere Web Client le permite configurar un único rango de ID de segmento y una única dirección de multidifusión o un rango de dirección de multidifusión. Si desea configurar varios rangos de ID de segmento o varios valores de direcciones de multidifusión, puede hacerlo usando NSX API. Consulte la *Guía de NSX API* para obtener más detalles.

Procedimiento

- 1 Inicie sesión en vSphere Web Client.
- 2 Diríjase a **Inicio > Redes y seguridad > Instalación** (Home > Networking & Security > Installation) y seleccione la pestaña **Preparación de redes lógicas** (Logical Network Preparation).
- 3 Haga clic en **Identificador de segmento > Editar** (Segment ID > Edit).
- 4 Introduzca un rango de identificadores de segmentos, por ejemplo, **5000–5999**.
- 5 (opcional) Si alguna de las zonas de transporte va a utilizar el modo de replicación híbrido o de multidifusión, debe agregar una dirección de multidifusión o un rango de direcciones de multidifusión.
 - a Seleccione la casilla de verificación **Habilitar direcciones de multidifusión** (Enable Multicast addressing).
 - b Introduzca un rango de direcciones de multidifusión o una dirección de multidifusión **239.0.0.0–239.255.255.255**.

Resultados

Al configurar los conmutadores lógicos, cada uno recibe un identificador de segmento del grupo.

Agregar una zona de transporte

15

Una zona de transporte controla con qué hosts puede comunicarse un conmutador lógico. Puede expandirse a uno o más clústeres vSphere. Las zonas de transporte establecen qué clústeres y, por lo tanto, qué máquinas virtuales pueden participar en la utilización de una red en particular.

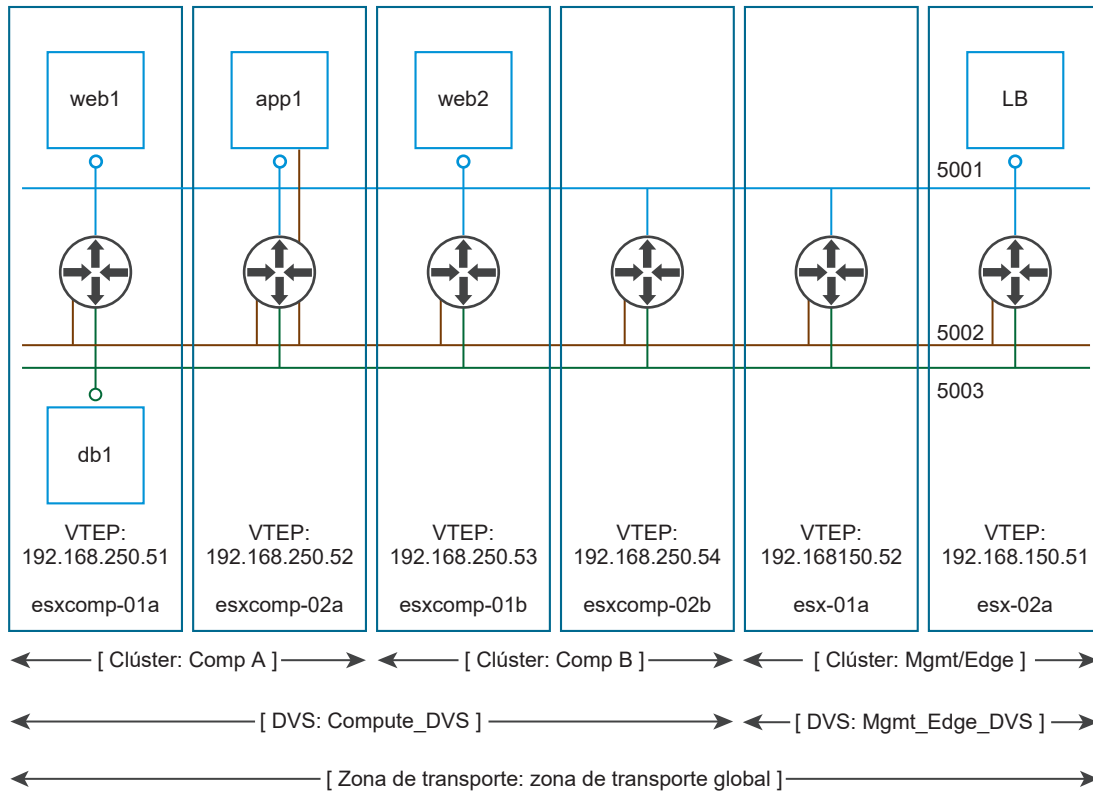
Un entorno de NSX puede contener una o más zonas de transporte según los requisitos del usuario. Un clúster de hosts puede corresponder a varias zonas de transporte. Un conmutador lógico puede corresponder a una sola zona de transporte.

NSX no permite conectar máquinas virtuales que se encuentran en diferentes zonas de transporte. La expansión de un conmutador lógico se limita a una zona de transporte, de modo que las máquinas virtuales de diferentes zonas de transporte no pueden estar en la misma red de Capa 2. Los enrutadores lógicos distribuidos no pueden conectarse a conmutadores lógicos que están en diferentes zonas de transporte. Después de desconectar el primer conmutador lógico, la selección de otros conmutadores lógicos se limita a los de la misma zona de transporte.

Las siguientes directrices ayudan a diseñar las zonas de transporte:

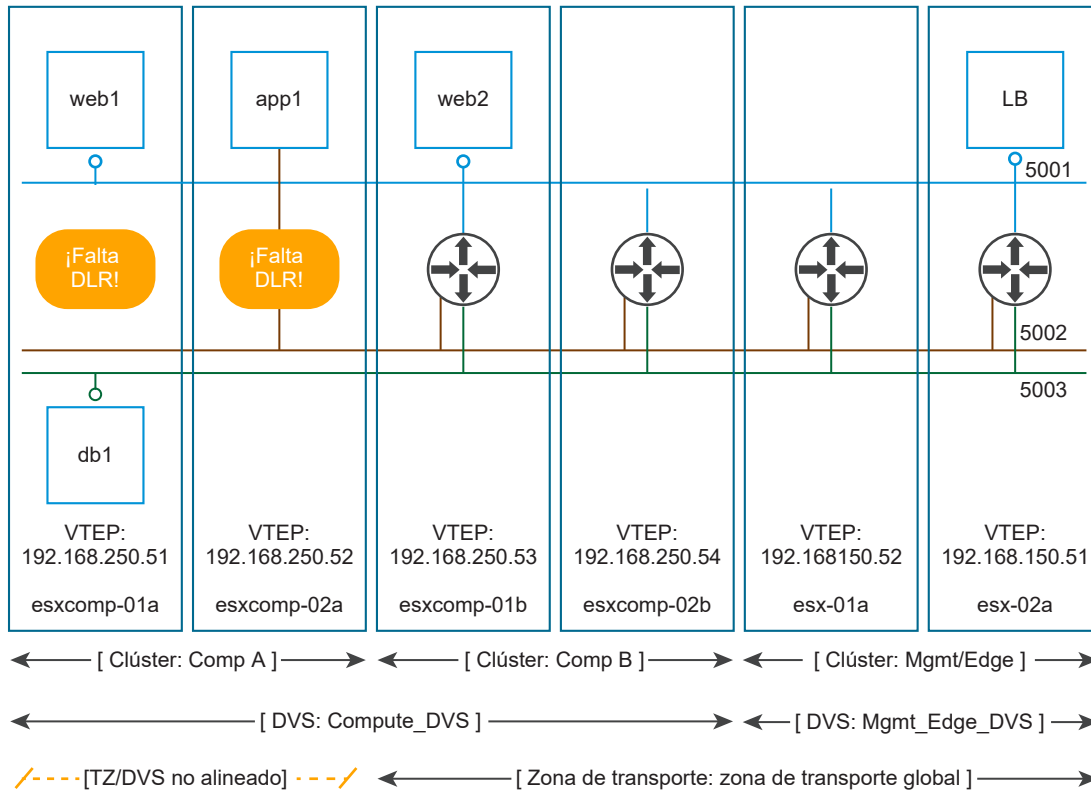
- Si un clúster requiere conectividad de Capa 3, debe estar en una zona de transporte que también incluya un clúster Edge, es decir, un clúster con dispositivos Edge de Capa 3 (enrutadores lógicos distribuidos y puertas de enlace de servicios Edge).
- Supongamos que hay dos clústeres: uno para servicios web y otro para servicios de aplicaciones. Para que haya conectividad VXLAN entre las máquinas virtuales de estos dos clústeres, ambos deben estar incluidos en la zona de transporte.
- Tenga en cuenta que todos los conmutadores lógicos incluidos en la zona de transporte estarán disponibles y serán visibles para todas las máquinas virtuales de los clústeres incluidos en la zona de transporte. Si un clúster incluye entornos protegidos, quizás no sea conveniente que este clúster esté disponible para las máquinas virtuales de otros clústeres. En cambio, puede colocar el clúster protegido en una zona de transporte más aislada.
- La expansión del conmutador distribuido de vSphere (VDS o DVS) debe coincidir con la de la zona de transporte. Al crear zonas de transporte en configuraciones de VDS de varios clústeres, asegúrese de que todos los clústeres del VDS seleccionado estén incluidos en la zona de transporte. Así se garantiza que el DLR esté disponible en todos los clústeres donde hay dvPortgroups de VDS disponibles.

El siguiente diagrama muestra una zona de transporte que está correctamente alineada con el límite de VDS.



Si no cumple con esta práctica recomendada, tenga en cuenta que si un VDS se expande en más de un clúster de hosts y la zona de transporte incluye solo uno (o un subconjunto) de estos clústeres, cualquier conmutador lógico de esa zona de transporte podrá acceder a las máquinas virtuales de todos los clústeres abarcados por el VDS. En otras palabras, la zona de transporte no podrá limitar la expansión del conmutador lógico a un subconjunto de clústeres. Si posteriormente conecta este conmutador lógico a un DLR, debe asegurarse de que las instancias del enrutador se creen únicamente en el clúster incluido en la zona de transporte, a fin de evitar problemas en la Capa 3.

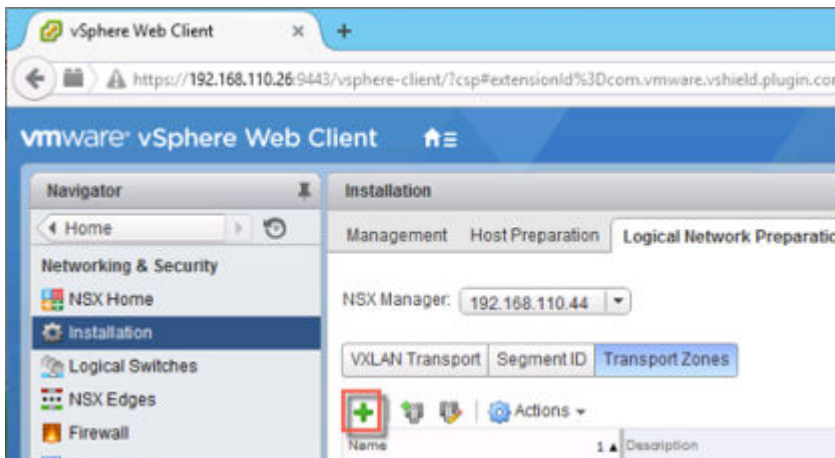
Por ejemplo, cuando una zona de transporte no está alineada con el límite del VDS, el alcance de los conmutadores lógicos (5001, 5002 y 5003) y las instancias del DLR a las que están conectados quedan desasociados; esto provoca que las máquinas virtuales del clúster Comp A no puedan acceder a las interfaces lógicas (LIF) del DLR.



Procedimiento

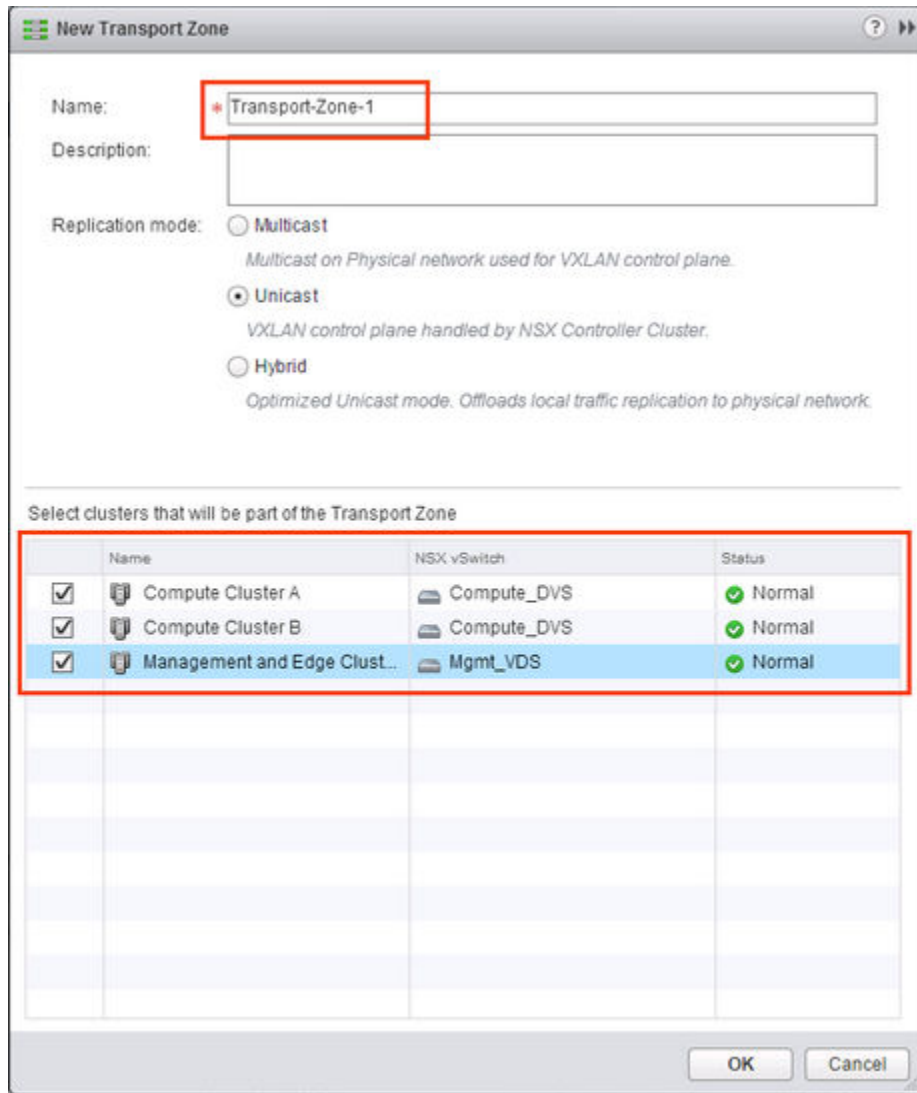
- 1 Inicie sesión en vSphere Web Client.
- 2 Diríjase a **Inicio > Redes y seguridad > Instalación** (Home > Networking & Security > Installation) y seleccione la pestaña **Preparación de redes lógicas** (Logical Network Preparation).
- 3 Haga clic en **Zonas de transporte** (Transport Zones) y en el icono **Nueva zona de transporte (+)** (New Transport Zone).

Por ejemplo:



- 4 En el cuadro de diálogo Nueva zona de transporte (New Transport Zone), escriba un nombre y una descripción (opcional) para la zona de transporte.
- 5 Seleccione el modo de plano de control según tenga un nodo de controlador en el entorno o desee utilizar direcciones de multidifusión.
 - **Multidifusión** (Multicast): para el plano de control se utilizan las direcciones IP de multidifusión de la red física. Este modo se recomienda únicamente para actualizar a partir de implementaciones de VXLAN anteriores. Se requiere PIM/IGMP en la red física.
 - **Unidifusión** (Unicast): el plano de control es operado por NSX Controller. El tráfico de unidifusión aprovecha la replicación de cabecera optimizada. No se requieren direcciones IP de multidifusión ni ninguna configuración de red especial.
 - **Híbrido** (Hybrid): descarga la replicación de tráfico local en la red física (multidifusión de Capa 2). Para esto se requiere la intromisión de IGMP en el conmutador del primer salto y el acceso a un solicitante de IGMP en cada subred de VTEP, pero no se requiere tecnología PIM. El conmutador del primer salto administra la replicación de tráfico de la subred.
- 6 Seleccione los clústeres que desea agregar a la zona de transporte.

Por ejemplo:



New Transport Zone

Name:

Description:

Replication mode: ☐ Multicast
Multicast on Physical network used for VXLAN control plane.
☒ **Unicast**
VXLAN control plane handled by NSX Controller Cluster.
☐ Hybrid
Optimized Unicast mode. Offloads local traffic replication to physical network.

Select clusters that will be part of the Transport Zone

	Name	NSX vSwitch	Status
<input checked="" type="checkbox"/>	Compute Cluster A	Compute_DVS	✓ Normal
<input checked="" type="checkbox"/>	Compute Cluster B	Compute_DVS	✓ Normal
<input checked="" type="checkbox"/>	Management and Edge Clust...	Mgmt_VDS	✓ Normal

OK Cancel

Pasos siguientes

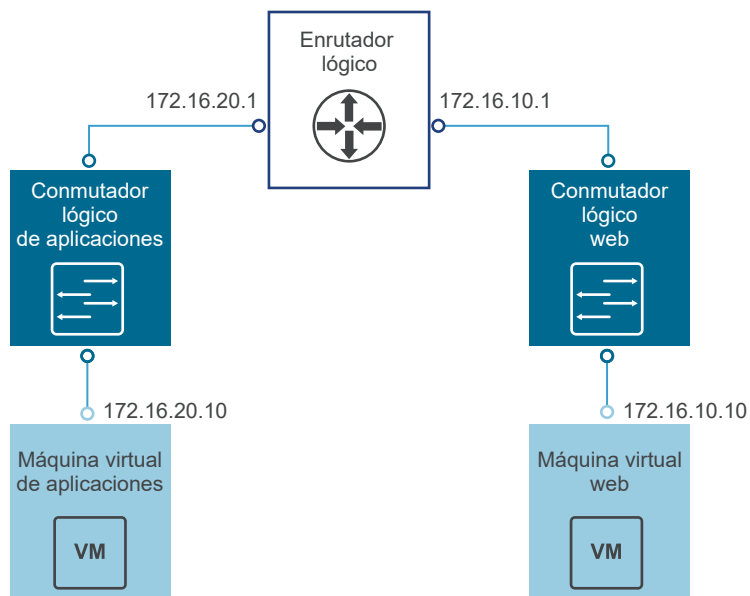
Ahora que tiene una zona de transporte, puede agregar conmutadores lógicos.

Agregar un conmutador lógico

16

Un conmutador lógico de NSX for vSphere reproduce la funcionalidad de conmutación (unidifusión, multidifusión y difusión) en un entorno virtual completamente desacoplado del hardware subyacente. Los conmutadores lógicos son similares a las VLAN en cuanto a que proporcionan conexiones de red a las que se pueden conectar máquinas virtuales. De este modo, las máquinas virtuales pueden comunicarse entre ellas mediante la VXLAN si están conectadas al mismo conmutador lógico. Cada conmutador lógico tiene un identificador de segmento, como un identificador de VLAN. A diferencia de los identificadores de VLAN, es posible tener hasta 16 millones de identificadores de segmento.

Al agregar conmutadores lógicos, es importante haber elegido una topología en particular para el diseño. Por ejemplo, la siguiente topología simple muestra dos conmutadores lógicos conectados a un solo enrutador lógico distribuido (DLR). En este diagrama, cada conmutador lógico está conectado a una sola máquina virtual. Las dos máquinas virtuales pueden estar en hosts diferentes o en el mismo host, en clústeres de hosts diferentes o en el mismo clúster de hosts. Si un DLR no separa las máquinas virtuales, las direcciones IP subyacentes configuradas en las máquinas virtuales pueden estar en la misma subred. Si una DLR las separa, las direcciones IP de las máquinas virtuales deben estar en subredes diferentes (como se muestra en el ejemplo).



Cuando cree un conmutador lógico, además de seleccionar una zona de transporte y un modo de réplica, configure dos opciones: detección de IP y detección de MAC.

La detección de IP minimiza la saturación de tráfico ARP dentro de segmentos individuales de la VXLAN; en otras palabras, entre máquinas virtuales conectadas al mismo conmutador lógico. La detección de direcciones IP está habilitada de manera predeterminada.

La detección de MAC crea una tabla de emparejamiento de VLAN/MAC en cada vNIC. Esta tabla se almacena como parte de los datos de dvfilter. Durante la ejecución de vMotion, dvfilter guarda y restaura la tabla en la nueva ubicación. A continuación, el conmutador emite RARP para todas las entradas de VLAN/MAC de la tabla. Es posible que quiera habilitar la detección de MAC si usa NIC virtuales que formen el enlace troncal de las VLAN.

Requisitos previos

- Los conmutadores distribuidos de vSphere deben estar configurados.
- NSX Manager debe estar instalado.
- Los controladoras deben estar implementados.
- Los clústeres de hosts deben estar preparados para NSX.
- VXLAN debe estar configurada.
- Debe haber un grupo de identificadores de segmentos configurado.
- Debe haber una zona de transporte configurada.

Procedimiento

- 1 Inicie sesión en vSphere Web Client.
- 2 Vaya a **Inicio > Redes y seguridad > Conmutadores lógicos** (Home > Networking & Security > Logical Switches).

- 3 Haga clic en **Nuevo conmutador lógico (+)** (New Logical Switch).

- 4 Escriba un nombre y una descripción opcional para el conmutador lógico.

- 5 Seleccione la zona de transporte en la que desea crear el conmutador lógico.

De forma predeterminada, el conmutador lógico hereda el modo de replicación del plano de control de la zona de transporte.

- 6 (opcional) Sobrescriba el modo de replicación que determina la zona de transporte.

Puede cambiarlo a uno de los otros modos disponibles. Los modos disponibles son unidifusión, híbrido y multidifusión.

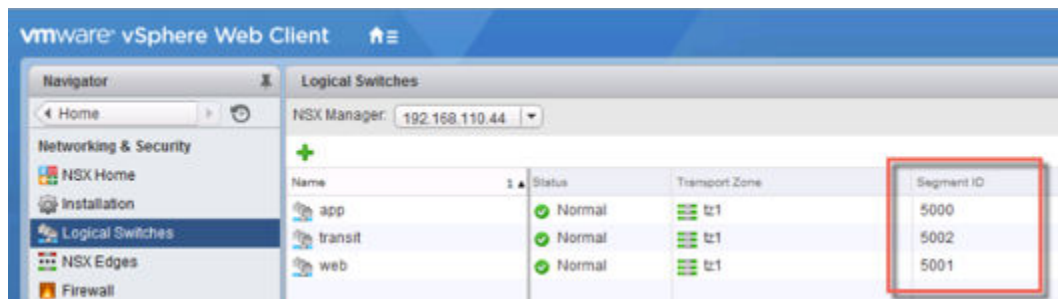
El caso en el que conviene anular el modo de replicación del plano de control heredado de la zona de transporte para un conmutador lógico individual es cuando el conmutador lógico que se crea posee características significativamente diferentes en términos de cantidad de tráfico BUM que transportará. En este caso, puede crear una zona de transporte que utilice el modo de unidifusión y utilizar el modo híbrido o de multidifusión para el conmutador lógico individual.

- 7 (Opcional) Haga clic en **Habilitar detección de direcciones IP** (Enable IP Discovery) para habilitar la supresión de ARP.
 - 8 (Opcional) Haga clic en **Habilitar detección de MAC** (Enable MAC learning).
 - 9 Para asociar una máquina virtual con el conmutador lógico, seleccione el conmutador y haga clic en **Agregar máquina virtual** (Add Virtual Machine).
 - 10 Seleccione una o varias máquinas virtuales y haga clic en el botón de la flecha hacia la derecha ().
- Las máquinas virtuales se mueven de Objetos disponibles (Available Objects) a Objetos seleccionados (Selected Objects).
- 11 Haga clic en **Siguiente** (Next) para seleccionar una vNIC para cada máquina virtual. Haga clic en **Finalizar** (Finish).

Resultados

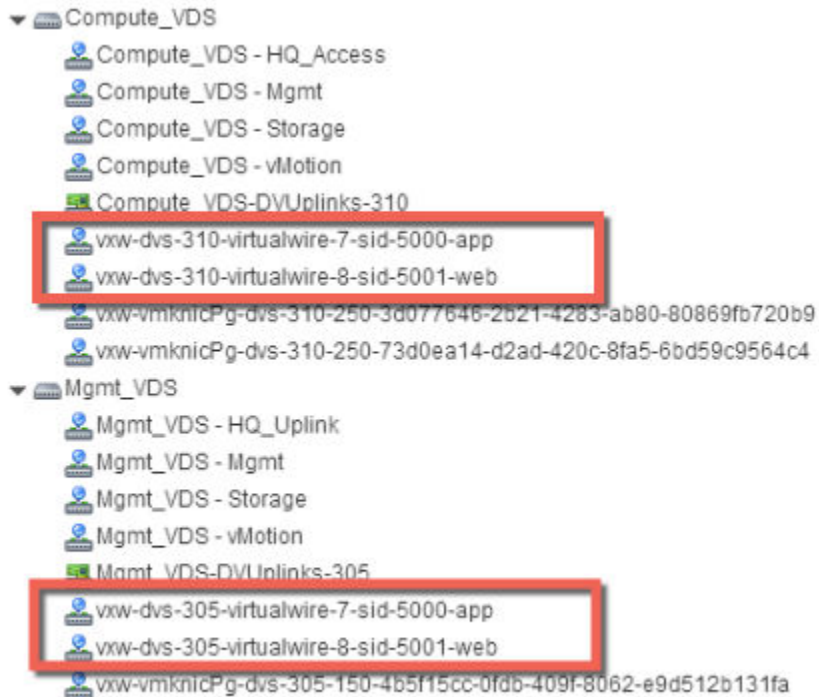
Cada conmutador lógico creado recibe un identificador del grupo de identificadores de segmentos, y se crea una instancia de cableado virtual. El cableado virtual es un dvPortgroup que se crea en cada conmutador distribuido de vSphere. El descriptor de cableado virtual contiene el nombre del conmutador lógico y el identificador de segmento del conmutador lógico. Los identificadores de segmentos asignados aparecen en varios lugares, como se muestra en los siguientes ejemplos.

En **Inicio > Redes y seguridad > Conmutadores lógicos** (Home > Networking & Security > Logical Switches):



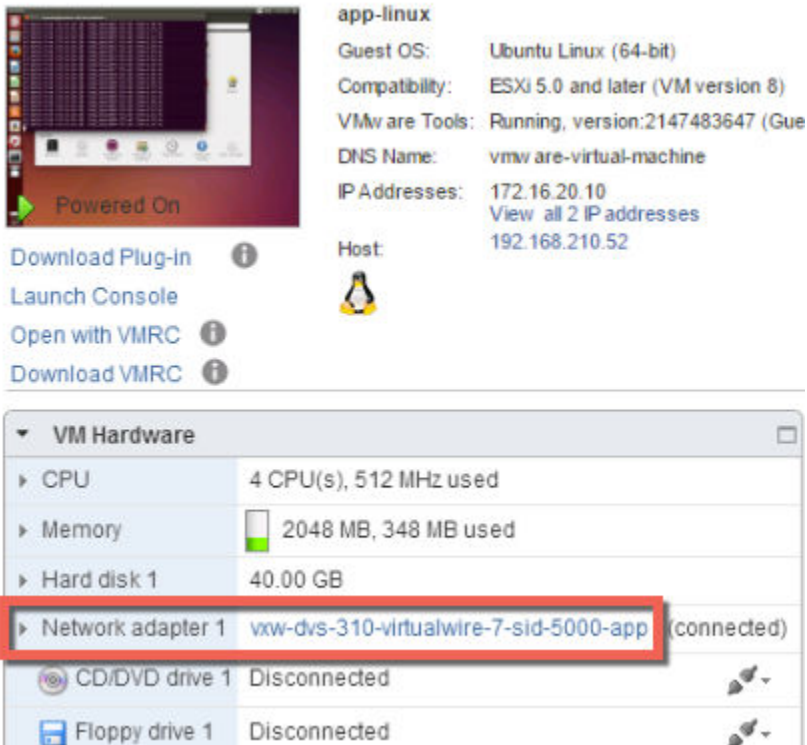
Name	Status	Transport Zone	Segment ID
app	Normal	t:1	5000
transit	Normal	t:1	5002
web	Normal	t:1	5001

En **Inicio > Redes** (Home > Networking):



Tenga en cuenta que las instancias de cableado virtual se crean en los conmutadores distribuidos de vSphere, Compute_VDS y Mgmt_VDS. Esto se debe a que estos dos conmutadores distribuidos de vSphere pertenecen a la zona de transporte que está asociada con los conmutadores lógicos de aplicaciones y web.

En **Inicio > Hosts y clústeres > VM > Resumen** (Home > Hosts and Clusters > VM > Summary):



En los hosts que ejecutan las máquinas virtuales conectadas al conmutador lógico, inicie sesión y ejecute los siguientes comandos para ver la información de estado y configuración de la VXLAN local.

- Muestra los detalles de la VXLAN específicos del host.

```
~ # esxcli network vswitch dvs vmware vxlan list
```

VDS ID	VDS Name	MTU	Segment ID	Gateway IP
88 eb 0e 50 96 af 1d f1-36 fe c1 ef a1 51 51 49 ff:ff:ff:ff:ff:ff	Compute_VDS	1600	192.168.250.0	192.168.250.1
Network Count	Vmknics Count			
0	1			

Nota Si el comando `esxcli network vswitch dvs vmware vxlan` produce el mensaje de error "Comando o espacio de nombres desconocidos" ("Unknown command or namespace"), ejecute el comando `/etc/init.d/hostd restart` en el host y vuelva a intentarlo.

El nombre de VDS aparece en el conmutador distribuido de vSphere al que está conectado el host.

El identificador de segmento es la red IP utilizada por VXLAN.

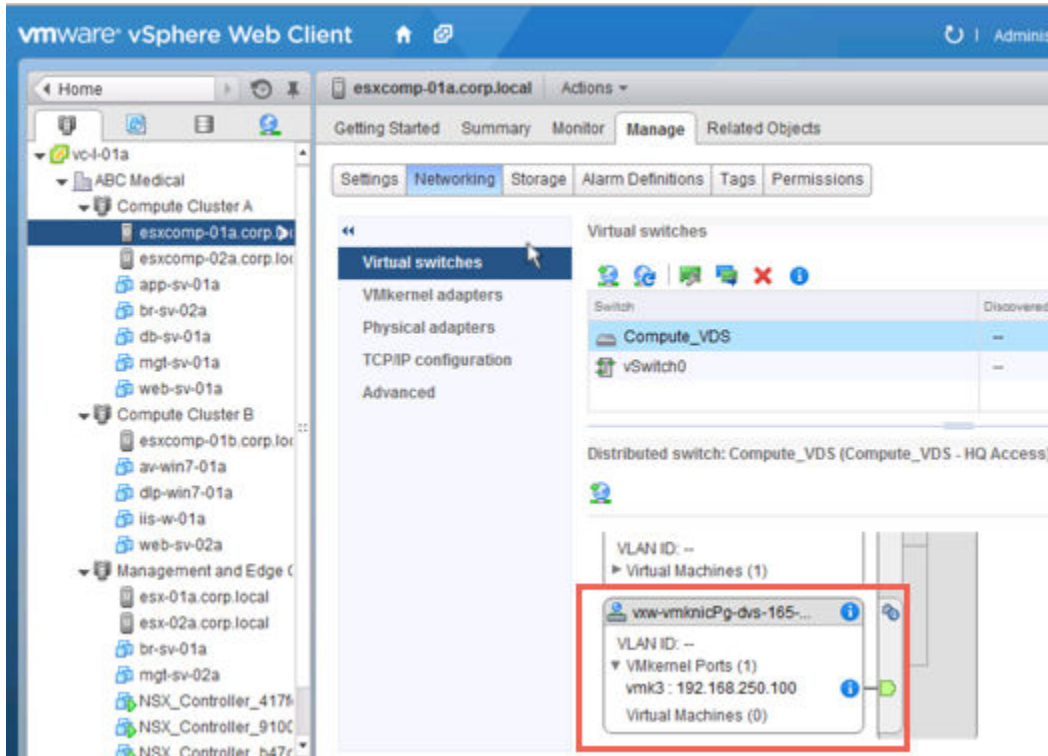
La dirección IP de la puerta de enlace es la dirección IP de la puerta de enlace utilizada por VXLAN.

La dirección MAC de la puerta de enlace sigue siendo `ff:ff:ff:ff:ff:ff`.

El recuento de red sigue siendo 0 a menos que un DLR se asocie al conmutador lógico.

El recuento de Vmknics debe coincidir con la cantidad de máquinas virtuales conectadas al conmutador lógico.

- Pruebe la conectividad de la interfaz VTEP por IP y compruebe que la MTU haya aumentado para admitir la encapsulación de VXLAN. Haga ping en la dirección IP de la interfaz, que se encuentra en la página **Administrar > Redes > Conmutadores virtuales** (Manage > Networking > Virtual switches) del host en vCenter Web Client.



La marca -d establece el bit don't-fragment (DF) en los paquetes IPv4. La marca -s establece el tamaño del paquete.

```
root@esxcomp-02a ~ # vmkping ++netstack=vxlan -d -s 1570 192.168.250.100
PING 192.168.250.100 (192.168.250.100): 1570 data bytes
1578 bytes from 192.168.250.100: icmp_seq=0 ttl=64 time=1.294 ms
1578 bytes from 192.168.250.100: icmp_seq=1 ttl=64 time=0.686 ms
1578 bytes from 192.168.250.100: icmp_seq=2 ttl=64 time=0.758 ms

--- 192.168.250.100 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.686/0.913/1.294 ms
~ #
```

```
root@esxcomp-01a ~ # vmkping ++netstack=vxlan -d -s 1570 192.168.250.101
PING 192.168.250.101 (192.168.250.101): 1570 data bytes
1578 bytes from 192.168.250.101: icmp_seq=0 ttl=64 time=0.065 ms
1578 bytes from 192.168.250.101: icmp_seq=1 ttl=64 time=0.118 ms

--- 192.168.250.101 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.065/0.091/0.118 ms
```

Pasos siguientes

Cree un enrutador lógico (distribuido) y asócielo a conmutadores lógicos para habilitar la conectividad entre las máquinas virtuales que están conectadas a diferentes conmutadores lógicos.

Agregar un enrutador lógico distribuido

17

Un enrutador lógico distribuido (distributed logical router, DLR) es un dispositivo virtual que contiene el plano de control de enrutamiento, a la vez que distribuye el plano de datos de los módulos del kernel en cada host de hipervisor. La función del plano de control del DLR depende de que el clúster de NSX Controller inserte actualizaciones de enrutamiento en los módulos del kernel.

Al implementar un nuevo enrutador lógico, considere lo siguiente:

- La versión 6.2 de NSX y las versiones posteriores permiten conectar interfaces lógicas (logical interfaces, LIF) enrutadas mediante enrutadores lógicos a una VXLAN conectada en puente con una VLAN.
- Las interfaces del enrutador lógico y las interfaces puente no pueden conectarse a un dvPortgroup si el identificador de la VLAN está establecido en 0.
- Una instancia de enrutador lógico determinada no puede conectarse a los conmutadores lógicos que existen en zonas de transporte diferentes. El objetivo de esto es garantizar que todas las instancias de conmutadores lógicos y enrutadores lógicos estén alineadas.
- No se puede conectar un enrutador lógico a grupos de puertos respaldados por VLAN si ese enrutador lógico se conecta a conmutadores lógicos que abarcan más de un vSphere Distributed Switch (VDS). Esto garantiza la correcta alineación entre instancias del enrutador lógico con dvPortgroups de conmutadores lógicos en los hosts.
- No deben crearse interfaces de enrutadores lógicos en dos grupos de puertos distribuidos (dvPortgroups) diferentes con el mismo identificador de VLAN si las dos redes están en el mismo conmutador distribuido de vSphere.
- No deben crearse interfaces de enrutadores lógicos en dos dvPortgroups diferentes con el mismo identificador de VLAN si las dos redes están en conmutadores distribuidos de vSphere diferentes, pero los dos conmutadores distribuidos de vSphere comparten los mismos hosts. En otras palabras, pueden crearse interfaces de enrutadores lógicos en dos redes diferentes con el mismo identificador de VLAN si los dos dvPortgroups están en dos conmutadores distribuidos de vSphere diferentes, siempre que los conmutadores distribuidos de vSphere no compartan un host.
- Si se configura VXLAN, las interfaces del enrutador lógico se deben conectar a grupos de puertos distribuidos en el vSphere Distributed Switch donde VXLAN esté configurado. No conecte interfaces de enrutadores lógicos a grupos de puertos en otros vSphere Distributed Switches.


En la siguiente lista se describen las características admitidas por tipo de interfaz (interna y de vínculo superior) en el enrutador lógico:

- Se admiten protocolos de enrutamiento dinámico (BGP y OSPF) solo en las interfaces de vínculo superior.
- Las reglas de firewall son aplicables solo en las interfaces de enlace ascendente, y están limitadas al tráfico de control y de administración destinado al dispositivo Edge virtual.
- Para obtener más información sobre la interfaz de administración DLR, consulte el artículo de la base de conocimiento <http://kb.vmware.com/kb/2122060> con la guía de interfaz de administración de máquinas virtuales de control DLR para NSX.

Requisitos previos

- Se le debe asignar la función de **administrador de Enterprise** o **administrador de NSX**.
- Se debe crear un grupo de identificadores de segmentos local aunque no esté previsto crear conmutadores lógicos NSX.
- Asegúrese de que el clúster de controladores esté en funcionamiento y disponible antes de crear o modificar la configuración del enrutador lógico. Los enrutadores lógicos no pueden distribuir información de enrutamiento a hosts sin la ayuda de los controladores NSX Controller. Los enrutadores lógicos dependen de los controladores NSX Controller para funcionar, mientras que las puertas de enlace de servicios Edge (Edge Services Gateways, ESG) no.
- Si se desea conectar un enrutador lógico a los dvPortgroups de VLAN, asegúrese de que todos los hosts del hipervisor con un dispositivo de enrutador lógico instalado puedan comunicarse entre sí en el puerto UDP 6999. Es necesaria la comunicación en este puerto para que funcione el proxy ARP basado en VLAN del enrutador lógico.
- Determine dónde implementar el dispositivo de enrutador lógico.
 - El host de destino debe formar parte de la misma zona de transporte que los conmutadores lógico conectados a las interfaces del nuevo enrutador lógico.
 - Evite colocarlo en el mismo host que uno o varios de sus ESG ascendentes si utiliza ESG en una configuración ECMP. Puede utilizar reglas de antiafinidad de DRS para aplicar esto, lo que reducirá el impacto de los errores del host en el reenvío de enrutadores lógicos. Estas instrucciones no se aplican si tiene un ESG ascendente individual o en modo de alta disponibilidad. Para obtener más información, consulte la *Guía de diseño de virtualización de redes de VMware NSX for vSphere* en <https://communities.vmware.com/docs/DOC-27683>.
- Compruebe que el clúster del host en el que instala el dispositivo del enrutador lógico está preparado para NSX. Consulte cómo preparar el clúster del host para NSX en *Guía de instalación de NSX*.

Procedimiento

- 1 En vSphere Web Client, desplácese hasta **Inicio > Redes y seguridad > NSX Edge** (Home > Networking & Security > NSX Edges).
- 2 Haga clic en el icono **Agregar** (Add) (.

- 3 Seleccione **Enrutador lógico (distribuido)** (Logical [Distributed] Router) y escriba un nombre para el dispositivo.

Este nombre aparece en el inventario de vCenter. Utilice un nombre que sea único en todos los enrutadores lógicos de un solo arrendatario.

De manera opcional, también puede introducir un nombre de host. Este nombre aparece en la interfaz de línea de comandos. Si no introduce un nombre de host, la interfaz de línea de comandos muestra el identificador de Edge, que se crea automáticamente.

De manera opcional, puede introducir una descripción y un arrendatario.

Por ejemplo:

Name and description

Install Type: ☐ Edge Services Gateway
Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.

☒ Logical (Distributed) Router
Provides Distributed Routing and Bridging capabilities.

Name: *

Hostname:

Description:

Tenant:

☒ Deploy Edge Appliance
Deploys NSX Edge Appliance to support Firewall and Dynamic routing.

☐ Enable High Availability
Enable HA, for enabling and configuring High Availability.

- 4 (opcional) Implemente un dispositivo Edge.

La opción **Implementar dispositivo Edge** (Deploy Edge Appliance) está seleccionada de forma predeterminada. Se requiere un dispositivo Edge (también denominado dispositivo virtual de enrutador lógico) para el enrutamiento dinámico y para el firewall del dispositivo de enrutador lógico, que se aplica a los ping del enrutador, al acceso de SSH y al tráfico de enrutamiento dinámico.

Puede desactivar la opción de dispositivo Edge si necesita solo rutas estáticas y no desea implementar un dispositivo Edge. No puede agregar un dispositivo Edge al enrutador lógico una vez que este enrutador ya está creado.

- 5 (opcional) Habilite High Availability.

La opción **Habilitar High Availability** (Enable High Availability) no está seleccionada de forma predeterminada. Seleccione la casilla **Habilitar High Availability** (Enable High Availability) para habilitar y configurar High Availability. Se requiere High Availability si su intención es utilizar un enrutamiento dinámico.

6 Escriba y vuelva a escribir una contraseña para el enrutador lógico.

La contraseña debe tener entre 12 y 255 caracteres, y debe contener lo siguiente:

- Al menos una letra en mayúscula
- Al menos una letra en minúscula
- Al menos un número
- Al menos un carácter especial

7 (opcional) Habilite SSH.

De forma predeterminada, SSH no está habilitado. Si no habilita SSH, puede abrir la consola del dispositivo virtual para seguir accediendo al enrutador lógico. Habilitar SSH provoca que el proceso SSH se ejecute en el dispositivo virtual del enrutador. Deberá ajustar la configuración del firewall del enrutador lógico manualmente para permitir el acceso de SSH a la dirección del protocolo del enrutador lógico. La dirección del protocolo se establece cuando se configura el enrutamiento dinámico en el enrutador lógico.

8 (opcional) Habilite el modo FIPS y establezca el nivel de registro.

De forma predeterminada, el modo FIPS está deshabilitado. Seleccione la casilla **Habilitar modo FIPS** (Enable FIPS mode) para habilitar el modo FIPS. Al habilitar el modo FIPS, cualquier comunicación segura que vaya a o desde NSX Edge utiliza algoritmos o protocolos criptográficos permitidos por FIPS.

De forma predeterminada, el registro está en nivel de emergencia.

Por ejemplo:

Settings

CLI credentials will be set on the NSX Edge appliance(s). These credentials can be used to login to the read only command line interface of the appliance.

User Name: *

Password: *

Confirm password: *

☐ Enable SSH access

☐ Enable FIPS mode

Edge Control Level Logging **EMERGENCY** ▼

Set the Edge Control Level Logging

9 Configure la implementación.

- ◆ Si no seleccionó **Implementar dispositivo Edge** (Deploy Edge Appliance), el icono **Agregar** (+) (Add) está atenuado. Haga clic en **Siguiente** (Next) para continuar con la configuración.
- ◆ Si seleccionó **Implementar dispositivo Edge** (Deploy Edge Appliance), introduzca la configuración del dispositivo virtual del enrutador lógico.

Por ejemplo:

Add NSX Edge Appliance

Specify placement parameters for the NSX Edge appliance.

Cluster/Resource Pool:	*	Management & Edge ...	▼
Datastore:	*	ds-1	▼
Host:		esxmgt-01a.corp.local	▼
Folder:		Discovered virtual mac...	▼

10 Configure las interfaces. En los enrutadores lógicos, solo se admiten las direcciones IPv4.

- a Configure la conexión de la interfaz de HA y, de forma opcional, una dirección IP.

Si seleccionó **Implementar dispositivo Edge** (Deploy Edge Appliance), debe conectar la interfaz de HA a un grupo de puertos distribuidos o un conmutador lógico. Si está utilizando esta interfaz solo como una interfaz de HA, utilice un conmutador lógico. Se asigna una subred /30 desde el rango local del vínculo 169.254.0.0/16 y se utiliza para proporcionar una dirección IP para cada uno de los dos dispositivos NSX Edge.

De manera opcional, si desea utilizar esta interfaz para conectarse a NSX Edge, puede especificar una dirección IP adicional y el prefijo de la interfaz de HA.

Nota Antes de NSX 6.2, la interfaz de HA se denominaba interfaz de administración. No es posible habilitar SSH para acceder a la interfaz de HA desde ningún lugar que no se encuentre en la misma subred IP que la interfaz de HA. No se pueden configurar rutas estáticas que apunten hacia afuera de la interfaz de HA, lo que significa que RPF descartará el tráfico entrante. En teoría, se puede deshabilitar RPF, pero esto es contraproducente para la alta disponibilidad. Para el acceso SSH, también puede utilizar la dirección de protocolo del enrutador lógico, que se establece posteriormente cuando se configura el enrutamiento dinámico.

En NSX 6.2 y versiones posteriores, la interfaz de HA de un enrutador lógico se excluye automáticamente de la redistribución de rutas.

- b Configure las interfaces de esta instancia de NSX Edge.

En la sección **Configurar interfaces de esta instancia de NSX Edge** (Configure interfaces of this NSX Edge), las interfaces internas están diseñadas para conexiones a conmutadores que permiten la comunicación entre máquinas virtuales (a la que a veces se denomina comunicación este-oeste). Las interfaces internas se crean como pseudo vNIC en el dispositivo virtual del enrutador lógico. Las interfaces de vínculo superior se utilizan en la comunicación de Norte a Sur. Una interfaz de vínculo superior del enrutador lógico podría conectarse a una puerta de enlace de servicios Edge o a una máquina virtual del enrutador de terceros. Se debe tener al menos una interfaz de vínculo superior para que el enrutamiento dinámico funcione. Las interfaces de vínculo superior se crean como vNIC en el dispositivo virtual del enrutador lógico.

La configuración de la interfaz especificada en este punto se puede modificar más adelante. Es posible agregar, eliminar y modificar interfaces después de implementar un enrutador lógico.

El siguiente ejemplo muestra una interfaz de HA conectada al grupo de puertos distribuidos de administración. El ejemplo también muestra dos interfaces internas (aplicación y web) y una interfaz de vínculo superior (a ESG).

New NSX Edge

1 Name and description

2 Settings

3 Configure deployment

4 Configure interfaces

5 Default gateway settings

6 Ready to complete

Configure interfaces

HA interface Configuration

Connected To:

Mgmt_VDS - Mgmt

Change

Remove

+

x

IP Address	Subnet Prefix Length
192.168.110.60*	24

HA interface is a mandatory special-purpose interface that requires network connectivity and is configured separately from other interfaces in the Logical Router.

Configure interfaces of this NSX Edge

+

x

Name	IP Address	Subnet Prefix Length	Connected To
app	172.16.20.1*	24	app
web	172.16.10.1*	24	web
to-ESG	192.168.10.2*	29	transit

Back

Next

Finish

Cancel

11 Configure una puerta de enlace predeterminada.

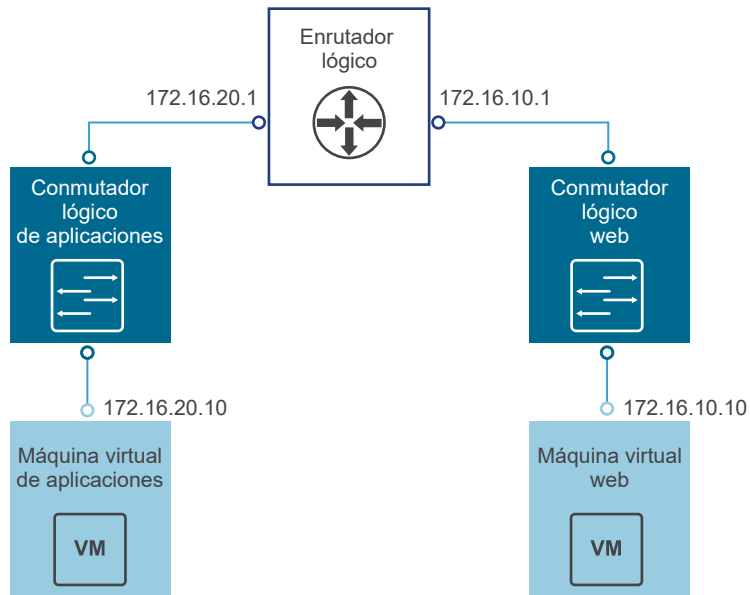
Por ejemplo:

The screenshot shows the 'New NSX Edge' configuration window. On the left, a progress bar indicates the following steps: 1 Name and description, 2 Settings, 3 Configure deployment, 4 Configure interfaces, 5 Default gateway settings (selected), and 6 Ready to complete. The main configuration area is titled 'Default gateway settings'. It includes a checkbox labeled 'Configure Default Gateway' which is checked. Below this, there are three input fields: 'vNIC' with a dropdown menu showing 'to-ESG', 'Gateway IP' with the value '192.168.10.1', and 'MTU' with the value '1500'. At the bottom of the window, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

- 12 Asegúrese de que todas las máquinas virtuales asociadas a los conmutadores lógicos tengan sus puertas de enlace predeterminadas establecidas adecuadamente en las direcciones IP de la interfaz del enrutador lógico.

Resultados

En el siguiente ejemplo de topología, la puerta de enlace predeterminada de la máquina virtual de la aplicación es 172.16.20.1. La puerta de enlace predeterminada de la máquina virtual web es 172.16.10.1. Compruebe que las máquinas virtuales puedan hacer ping en sus puertas de enlace predeterminadas y entre sí.



Conéctese a NSX Manager con SSH o la consola y ejecute los siguientes comandos:

- Vea un listado con toda la información de la instancia del enrutador lógico.

```

nsxmgr-l-01a> show logical-router list all
Edge-id      Vdr Name      Vdr id      #Lifs
edge-1       default+edge-1 0x00001388  3
  
```

- Vea un listado de los hosts que recibieron información de enrutamiento para el enrutador lógico del clúster de controladores.

```

nsxmgr-l-01a> show logical-router list dlr edge-1 host
ID      HostName
host-25 192.168.210.52
host-26 192.168.210.53
host-24 192.168.110.53
  
```

En el resultado se incluyen todos los hosts de todos los clústeres de hosts configurados como miembros de la zona de transporte a la que pertenece el conmutador lógico que está conectado al enrutador lógico especificado (en este ejemplo, edge-1).

- Vea un listado con la información de la tabla de enrutamiento que se comunica a los hosts mediante el enrutador lógico. Las entradas de la tabla de enrutamiento deben ser coherentes en todos los hosts.

```

nsx-mgr-l-01a> show logical-router host host-25 dlr edge-1 route

VDR default+edge-1 Route Table
Legend: [U: Up], [G: Gateway], [C: Connected], [I: Interface]
Legend: [H: Host], [F: Soft Flush] [!: Reject] [E: ECMP]

Destination      GenMask      Gateway      Flags      Ref Origin      UpTime      Interface
-----
0.0.0.0          0.0.0.0      192.168.10.1  UG         1  AUTO          4101      138800000002
  
```

172.16.10.0	255.255.255.0	0.0.0.0	UCI	1	MANUAL	10195	13880000000b
172.16.20.0	255.255.255.0	0.0.0.0	UCI	1	MANUAL	10196	13880000000a
192.168.10.0	255.255.255.248	0.0.0.0	UCI	1	MANUAL	10196	138800000002
192.168.100.0	255.255.255.0	192.168.10.1	UG	1	AUTO	3802	138800000002

- Vea un listado con información adicional sobre el enrutador desde el punto de vista de uno de los hosts. Este resultado es útil para saber qué controlador se está comunicando con el host.

```
nsx-mgr-l-01a> show logical-router host host-25 dlr edge-1 verbose
```

VDR Instance Information :

```
-----
Vdr Name:                default+edge-1
Vdr Id:                  0x00001388
Number of Lifs:          3
Number of Routes:        5
State:                   Enabled
Controller IP:           192.168.110.203
Control Plane IP:        192.168.210.52
Control Plane Active:    Yes
Num unique nexthops:     1
Generation Number:      0
Edge Active:             No
```

Compruebe el campo Dirección IP de controlador (Controller IP) en el resultado del comando `show logical-router host host-25 dlr edge-1 verbose`.

Acceda a un controlador mediante SSH y ejecute los siguientes comandos para mostrar la información de estado adquirida de las tablas de VNI, VTEP, MAC y ARP del controlador.

- ```
192.168.110.202 # show control-cluster logical-switches vni 5000
```

| VNI  | Controller      | BUM-Replication | ARP-Proxy | Connections |
|------|-----------------|-----------------|-----------|-------------|
| 5000 | 192.168.110.201 | Enabled         | Enabled   | 0           |

La salida para VNI 5000 muestra cero conexiones y el controlador 192.168.110.201 como propietaria de VNI 5000. Inicie sesión en ese controlador para recopilar más información de VNI 5000.

```
192.168.110.201 # show control-cluster logical-switches vni 5000
```

| VNI  | Controller      | BUM-Replication | ARP-Proxy | Connections |
|------|-----------------|-----------------|-----------|-------------|
| 5000 | 192.168.110.201 | Enabled         | Enabled   | 3           |

El resultado en 192.168.110.201 muestra tres conexiones. Compruebe las VNI adicionales.

```
192.168.110.201 # show control-cluster logical-switches vni 5001
```

| VNI  | Controller      | BUM-Replication | ARP-Proxy | Connections |
|------|-----------------|-----------------|-----------|-------------|
| 5001 | 192.168.110.201 | Enabled         | Enabled   | 3           |

```
192.168.110.201 # show control-cluster logical-switches vni 5002
```

| VNI  | Controller      | BUM-Replication | ARP-Proxy | Connections |
|------|-----------------|-----------------|-----------|-------------|
| 5002 | 192.168.110.201 | Enabled         | Enabled   | 3           |

Debido a que 192.168.110.201 es propietaria de las tres conexiones de VNI, se espera ver cero conexiones en el otro controlador 192.168.110.203.

```
192.168.110.203 # show control-cluster logical-switches vni 5000
VNI Controller BUM-Replication ARP-Proxy Connections
5000 192.168.110.201 Enabled Enabled 0
```

- Antes de comprobar las tablas de MAC y ARP, haga ping de una máquina virtual a la otra.

Desde la máquina virtual de la aplicación a la máquina virtual web:

```
vmware@app-vm$ ping 172.16.10.10
PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
64 bytes from 172.16.10.10: icmp_req=1 ttl=64 time=2.605 ms
64 bytes from 172.16.10.10: icmp_req=2 ttl=64 time=1.490 ms
64 bytes from 172.16.10.10: icmp_req=3 ttl=64 time=2.422 ms
```

Revise las tablas de MAC.

```
192.168.110.201 # show control-cluster logical-switches mac-table 5000
VNI MAC VTEP-IP Connection-ID
5000 00:50:56:a6:23:ae 192.168.250.52 7
```

```
192.168.110.201 # show control-cluster logical-switches mac-table 5001
VNI MAC VTEP-IP Connection-ID
5001 00:50:56:a6:8d:72 192.168.250.51 23
```

Revise las tablas de ARP.

```
192.168.110.201 # show control-cluster logical-switches arp-table 5000
VNI IP MAC Connection-ID
5000 172.16.20.10 00:50:56:a6:23:ae 7
```

```
192.168.110.201 # show control-cluster logical-switches arp-table 5001
VNI IP MAC Connection-ID
5001 172.16.10.10 00:50:56:a6:8d:72 23
```

Revise la información del enrutador lógico. Cada instancia del enrutador lógico se procesa en uno de los nodos del controlador.

El subcomando instance del comando `show control-cluster logical-routers` muestra un listado de los enrutadores lógicos que están conectados a este controlador.

El subcomando `interface-summary` muestra un listado de las LIF que el controlador adquirió de NSX Manager. Esta información se envía a los hosts que están en los clústeres de hosts administrados en la zona de transporte.



El subcomando `routes` muestra la tabla de enrutamiento que se envía a este controlador mediante el dispositivo virtual del enrutador lógico (también se conoce como máquina virtual de control). A diferencia de los hosts ESXi, esta tabla de enrutamiento no incluye subredes conectadas directamente, ya que la configuración de LIF proporciona esta información. La información de ruta de los hosts ESXi incluye subredes conectadas directamente porque, en ese caso, se trata de una tabla de reenvío utilizada por la ruta de datos del host ESXi.

- Vea un listado con todos los enrutadores lógicos conectados a este controlador.

```
controller # show control-cluster logical-routers instance all
LR-Id LR-Name Universal Service-Controller Egress-Locale
0x1388 default+edge-1 false 192.168.110.201 local
```

Anote el identificador de LR y utilícelo en el siguiente comando.

- `controller # show control-cluster logical-routers interface-summary 0x1388`

| Interface    | Type | Id     | IP[]            |
|--------------|------|--------|-----------------|
| 13880000000b | vxl  | 0x1389 | 172.16.10.1/24  |
| 13880000000a | vxl  | 0x1388 | 172.16.20.1/24  |
| 138800000002 | vxl  | 0x138a | 192.168.10.2/29 |

- `controller # show control-cluster logical-routers routes 0x1388`

| Destination      | Next-Hop[]   | Preference | Locale-Id                            | Source     |
|------------------|--------------|------------|--------------------------------------|------------|
| 192.168.100.0/24 | 192.168.10.1 | 110        | 00000000-0000-0000-0000-000000000000 | CONTROL_VM |
| 0.0.0.0/0        | 192.168.10.1 | 0          | 00000000-0000-0000-0000-000000000000 | CONTROL_VM |

```
[root@comp02a:~] esxcfg-route -l
```

VMkernel Routes:

| Network       | Netmask       | Gateway       | Interface |
|---------------|---------------|---------------|-----------|
| 10.20.20.0    | 255.255.255.0 | Local Subnet  | vmk1      |
| 192.168.210.0 | 255.255.255.0 | Local Subnet  | vmk0      |
| default       | 0.0.0.0       | 192.168.210.1 | vmk0      |

- Muestre las conexiones del controlador a la VNI específica.

```
192.168.110.203 # show control-cluster logical-switches connection-table 5000
```

| Host-IP        | Port  | ID |
|----------------|-------|----|
| 192.168.110.53 | 26167 | 4  |
| 192.168.210.52 | 27645 | 5  |
| 192.168.210.53 | 40895 | 6  |

```
192.168.110.202 # show control-cluster logical-switches connection-table 5001
```

| Host-IP        | Port  | ID |
|----------------|-------|----|
| 192.168.110.53 | 26167 | 4  |
| 192.168.210.52 | 27645 | 5  |
| 192.168.210.53 | 40895 | 6  |

Estas direcciones IP de hosts son interfaces `vmk0`, no VTEP. Las conexiones entre hosts y controladores ESXi se crean en la red de administración. Aquí los números de puerto son puertos TCP efímeros que asigna la pila de direcciones IP del host ESXi cuando el host establece una conexión con el controlador.

- En el host, puede ver la conexión de red del controlador vinculado al número de puerto.

```
[root@192.168.110.53:~] #esxcli network ip connection list | grep 26167
tcp 0 0 192.168.110.53:26167 192.168.110.101:1234 ESTABLISHED
96416 newreno netcpa-worker
```

- Muestre las VNI activas en el host. Observe que el resultado es diferente entre los hosts. No todas las VNI están activas en todos los hosts. Una VNI está activa en un host si ese host posee una máquina virtual conectada al conmutador lógico.

```
[root@192.168.210.52:~] # esxcli network vswitch dvs vmware vxlan network list --vds-name
Compute_VDS
```

| VXLAN ID   | Multicast IP              | Control Plane                       | Controller Connection |
|------------|---------------------------|-------------------------------------|-----------------------|
| Port Count | MAC Entry Count           | ARP Entry Count                     | VTEP Count            |
| 5000       | N/A (headend replication) | Enabled (multicast proxy,ARP proxy) | 192.168.110.203       |
| (up)       | 1                         | 0                                   | 0                     |
| 5001       | N/A (headend replication) | Enabled (multicast proxy,ARP proxy) | 192.168.110.202       |
| (up)       | 1                         | 0                                   | 0                     |

**Nota** Para habilitar el espacio de nombres vxlan en vSphere 6,0 y versiones posteriores, ejecute el comando `/etc/init.d/hostd restart`.

En el caso de conmutadores lógicos en modo híbrido o de unidifusión, el comando `esxcli network vswitch dvs vmware vxlan network list --vds-name <vds-name>` contiene el siguiente resultado:

- El plano de control está habilitado.
- El proxy de multidifusión y el proxy ARP aparecen en el listado. El proxy AARP aparece en el listado aunque se haya deshabilitado la detección de direcciones IP.
- Una dirección IP de controlador válida aparece en el listado y la conexión está activa.
- Si un enrutador lógico está conectado al host ESXi, el recuento de puertos es al menos 1, incluso si no hay máquinas virtuales en el host conectado al conmutador lógico. Este puerto es vdrPort, que es un puerto dvPort especial conectado al módulo del kernel del enrutador lógico en el host ESXi.

- En primer lugar, haga ping de una máquina virtual a otra en una subred diferente y, a continuación, muestre la tabla de MAC. Tenga en cuenta que la MAC interna es la entrada de la máquina virtual, mientras que la MAC externa y la dirección IP externa se refieren a la VTEP.

```
~ # esxcli network vswitch dvs vmware vxlan network mac list --vds-name=Compute_VDS --vxlan-id=5000
```

| Inner MAC         | Outer MAC         | Outer IP       | Flags    |
|-------------------|-------------------|----------------|----------|
| 00:50:56:a6:23:ae | 00:50:56:6a:65:c2 | 192.168.250.52 | 00000111 |

```
~ # esxcli network vswitch dvs vmware vxlan network mac list --vds-name=Compute_VDS --vxlan-id=5001
```

| Inner MAC         | Outer MAC         | Outer IP       | Flags    |
|-------------------|-------------------|----------------|----------|
| 02:50:56:56:44:52 | 00:50:56:6a:65:c2 | 192.168.250.52 | 00000101 |
| 00:50:56:f0:d7:e4 | 00:50:56:6a:65:c2 | 192.168.250.52 | 00000111 |

### Pasos siguientes

Cuando instale un dispositivo NSX Edge, NSX habilita el encendido/apagado automático de la máquina virtual en el host si vSphere HA está deshabilitado en el clúster. Si posteriormente las máquinas virtuales del dispositivo se migran a otros hosts en el clúster, es posible que los hosts nuevos no tengan habilitada la opción de encendido/apagado automático de la máquina virtual. Por este motivo, VMware recomienda que cuando instale dispositivos NSX Edge en clústeres que tienen vSphere deshabilitado, debe comprobar todos los hosts del clúster para asegurarse de que la opción de encendido/apagado automático esté habilitada. Consulte la sección sobre cómo editar la configuración de encendido y apagado de la máquina Virtual en *Administrar máquinas virtuales de vSphere*.

Después de implementar el enrutador lógico, haga doble clic en el identificador del enrutador lógico para configurar opciones adicionales, como interfaces, enrutamiento, firewall, puentes y relé DHCP.

# Agregar una puerta de enlace de servicios Edge

# 18

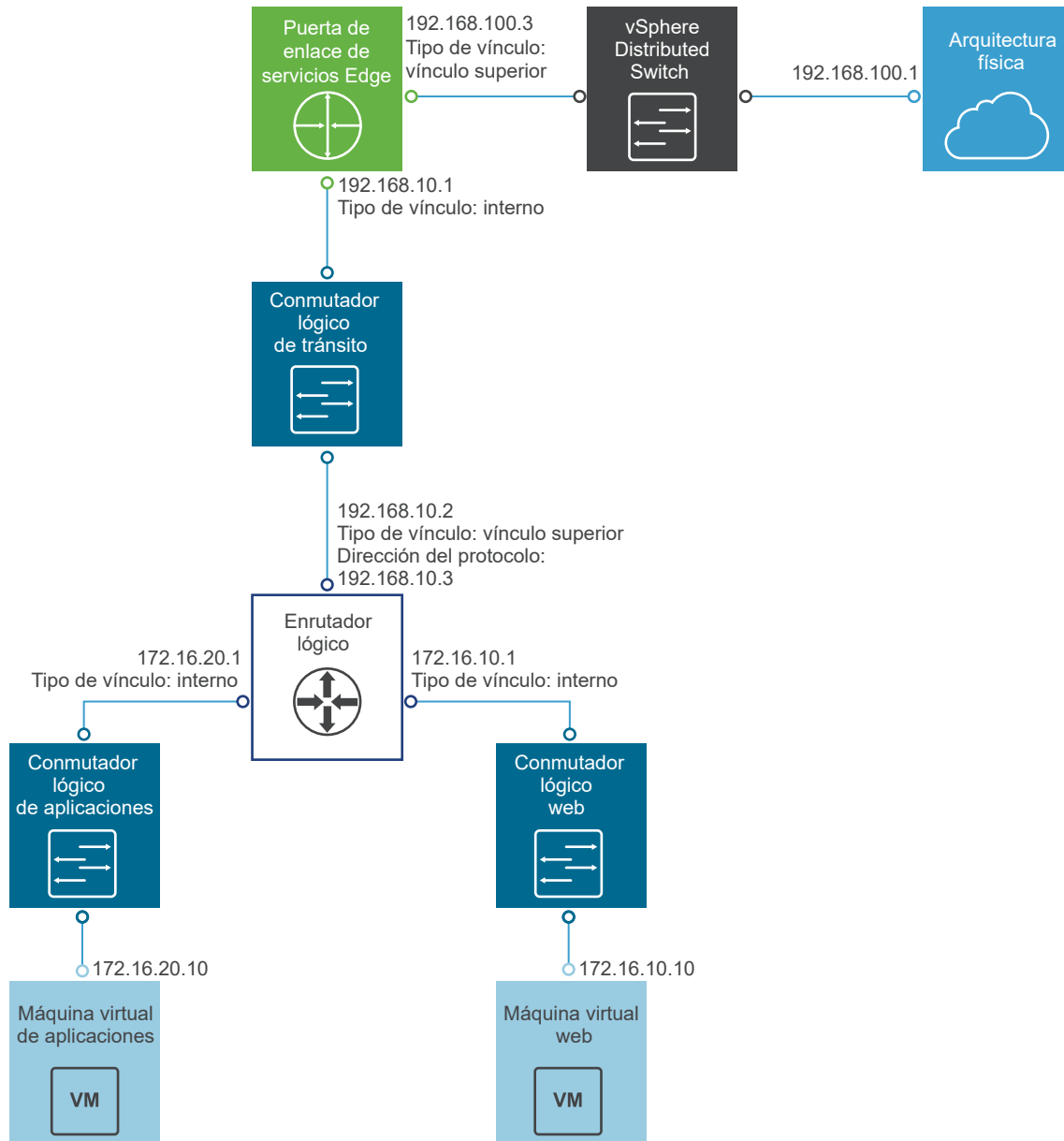
Puede instalar varios dispositivos virtuales de puertas de enlace de servicios NSX Edge en un centro de datos. Cada dispositivo virtual NSX Edge puede tener un total de diez interfaces de red de internas y de vínculo superior. Las interfaces internas se conectan a grupos de puertos protegidos y actúan como puerta de enlace para todas las máquinas virtuales protegidas del grupo de puertos. La subred asignada a la interfaz interna puede ser una dirección IP enrutada públicamente o un espacio de direcciones privado (RFC 1918) con uso de NAT. Las reglas de firewall y otros servicios NSX Edge se aplican sobre el tráfico entre interfaces.

Las interfaces de vínculo superior de una ESG se conectan a grupos de puertos de vínculo superior que tienen acceso a una red compartida de la empresa o a un servicio que ofrece redes de capa de acceso.

En la siguiente lista se describen las características admitidas por tipo de interfaz (interna y de vínculo superior) en la ESG:

- DHCP: no se admite en la interfaz de vínculo superior.
- Reenviador de DNS: no se admite en la interfaz de vínculo superior.
- HA: no se admite en la interfaz de vínculo superior, requiere al menos una interfaz interna.
- VPN SSL: la dirección IP del agente de escucha debe pertenecer a la interfaz de vínculo superior.
- VPN IPsec: la dirección IP del sitio local debe pertenecer a la interfaz de vínculo superior.
- VPN de capa 2: solo las redes internas pueden ampliarse.

En la siguiente imagen se muestra una topología de ejemplo con una interfaz de vínculo superior de ESG conectada a la infraestructura física mediante el conmutador distribuido de vSphere, y la interfaz interna de ESG conectada a un enrutador lógico de NSX mediante un conmutador de tránsito lógico de NSX.



Pueden configurarse varias direcciones IP para equilibrio de carga, VPN de sitio a sitio y servicios de NAT.

### Requisitos previos

- Se le debe haber asignado la función de administrador de Enterprise o administrador de NSX.
- Compruebe que el grupo de recursos tenga capacidad suficiente para implementar el dispositivo virtual de la puerta de enlace de servicios Edge (edge services gateway, ESG) . Consulte [Requisitos del sistema para NSX](#).
- Compruebe que los clústeres de host en los que se instalará el dispositivo NSX Edge se instalarán y preparará para NSX. Consulte cómo preparar el clúster del host para NSX (Prepare the Host Cluster for NSX) en *Guía de instalación de NSX*.

## Procedimiento

- 1 En vCenter, desplácese hasta **Inicio > Redes y seguridad > NSX Edge** (Home > Networking & Security > NSX Edges) y haga clic en el icono **Agregar** (Add) (+).
- 2 Seleccione **Puerta de enlace de servicios Edge** (Edge Services Gateway) y escriba un nombre para el dispositivo.

Este nombre aparece en el inventario de vCenter. El nombre debe ser único en todas las ESG de un mismo arrendatario.

De manera opcional, también puede introducir un nombre de host. Este nombre aparece en la interfaz de línea de comandos. Si no especifica un nombre de host, la interfaz de línea de comandos muestra el identificador de Edge, que se crea automáticamente.

De manera opcional, puede introducir una descripción y un arrendatario, y habilitar High Availability.

Por ejemplo:

**New NSX Edge**

1 Name and description

2 Settings

3 Configure deployment

4 Configure interfaces

5 Default gateway settings

6 Firewall and HA

7 Ready to complete

**Name and description**

Install Type: ☒ Edge Services Gateway  
Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.

☐ Logical (Distributed) Router  
Provides Distributed Routing and Bridging capabilities.

Name:

Hostname:

Description:

Tenant:

☒ Deploy NSX Edge  
Select this option to create a new NSX Edge in deployed mode. Appliance and interface configuration is mandatory to deploy the NSX Edge.

☐ Enable High Availability  
Enable HA, for enabling and configuring High Availability.

Back Next Finish Cancel

**3** Escriba y vuelva a escribir una contraseña para ESG.

La contraseña debe tener al menos 12 caracteres y cumplir con al menos 3 de las siguientes 4 reglas:

- Al menos una letra en mayúscula
- Al menos una letra en minúscula
- Al menos un número
- Al menos un carácter especial

**4** (opcional) Habilite SSH, High Availability, generación automática de reglas y el modo FIPS y establezca el nivel de registro.

Si no habilita la generación automática de reglas, debe agregar manualmente la configuración de firewall, NAT y enrutamiento para permitir el control de tráfico para ciertos servicios NSX Edge, incluidos el equilibrio de carga y VPN. La generación automática de reglas no crea reglas para tráfico de canal de datos.

De forma predeterminada, las opciones SSH y High Availability están deshabilitadas, y la generación automática de reglas está habilitada.

De forma predeterminada, el modo FIPS está deshabilitado.

De forma predeterminada, el registro está en nivel de emergencia.

Por ejemplo:

**New NSX Edge**

1 Name and description  
**2 Settings**  
 3 Configure deployment  
 4 Configure interfaces  
 5 Default gateway settings  
 6 Firewall and HA  
 7 Ready to complete

**Settings**

CLI credentials will be set on the NSX Edge appliance(s). These credentials can be used to login to the read only command line interface of the appliance.

User Name: \* admin

Password: \* \*\*\*\*\*

Confirm password: \* \*\*\*\*\*

☒ Enable SSH access

☒ Enable FIPS mode

☒ Enable auto rule generation  
 Enable auto rule generation, to automatically generate service rules to allow flow of control traffic.

Edge Control Level Logging **EMERGENCY**

*Set the Edge Control Level Logging*

Back Next Finish Cancel

- 5 Seleccione el tamaño de la instancia NSX Edge en función de los recursos del sistema.

La opción **Large** NSX Edge tiene más CPU, memoria y espacio en disco que la opción **Compact** NSX Edge, y admite una mayor cantidad de componentes de usuarios VPN SSL-Plus simultáneos. La opción **X-Large** NSX Edge es ideal para entornos que tienen un equilibrador de carga con millones de sesiones simultáneas. La opción Quad Large NSX Edge se recomienda cuando es necesaria una gran capacidad de proceso y requiere una alta velocidad de conexión.

Consulte [Requisitos del sistema para NSX](#).

- 6 Cree un dispositivo Edge.

Introduzca la configuración del dispositivo virtual de la ESG que se agregará al inventario de vCenter. Si no agrega un dispositivo al instalar NSX Edge, NSX Edge permanece en modo sin conexión hasta que se agrega un dispositivo.

Si habilitó HA, puede agregar dos dispositivos. Si agrega un solo dispositivo, NSX Edge replica su configuración para el dispositivo en espera y garantiza que las dos máquinas virtuales NSX Edge con HA no estén en el mismo host ESX incluso después de utilizar DRS y vMotion (a menos que la migre manualmente con vMotion al mismo host). Para que HA funcione correctamente, debe implementar los dos dispositivos en un almacén de datos compartido.

Por ejemplo:



Add NSX Edge Appliance

Specify placement parameters for the NSX Edge appliance.

|                        |   |                           |   |
|------------------------|---|---------------------------|---|
| Cluster/Resource Pool: | * | Management & Edge ...     | ▼ |
| Datastore:             | * | ds-1                      | ▼ |
| Host:                  |   | esxmgt-01a.corp.local     | ▼ |
| Folder:                |   | Discovered virtual mac... | ▼ |

- 7 Seleccione **Implementar NSX Edge** (Deploy NSX Edge) y agregue el dispositivo Edge en un modo implementado. Debe configurar dispositivos e interfaces para el dispositivo Edge para poder implementarlo.

- 8 Configure las interfaces.

En ESG, se admiten las direcciones IPv4 e IPv6.

Debe agregar al menos una interfaz interna para que HA funcione.

Una interfaz puede tener varias subredes no superpuestas.

Si introduce más de una dirección IP para una interfaz, puede seleccionar la dirección IP principal.

Un interfaz puede tener una dirección IP principal y varias secundarias. NSX Edge considera la dirección IP principal como la dirección de origen para el tráfico generado localmente, por ejemplo, servidores de Syslog remotos y pings iniciados por el operador.

Debe agregar una dirección IP con una interfaz antes de utilizarla en cualquier configuración de características.

De manera opcional, puede introducir la dirección MAC de la interfaz.

Si cambia la dirección MAC más tarde mediante una llamada API, tendrá que volver a implementar el dispositivo edge.

Si HA está habilitado, puede introducir dos direcciones IP de administración en formato CIDR si lo desea. Los latidos de las dos máquinas virtuales NSX Edge con HA se comunican por medio de estas direcciones IP de administración. Las direcciones IP de administración deben estar en la misma Capa 2/subred y poder comunicarse entre sí.

De manera opcional, puede modificar la MTU.

Habilite el ARP de proxy si desea permitir que la ESG responda a las solicitudes de ARP dirigidas a otras máquinas. Esto es útil, por ejemplo, cuando tiene la misma subred en ambos lados de una conexión WAN.

Habilite la redirección de ICMP para transmitir la información de enrutamiento a los hosts.

Habilite el filtrado inverso de rutas para comprobar la posibilidad de conexión de la dirección de origen en los paquetes que se reenvían. En el modo habilitado, el paquete debe recibirse en la interfaz que el enrutador utilizaría para reenviar el paquete de retorno. En el modo flexible, la dirección de origen debe aparecer en la tabla de enrutamiento.

Configure parámetros de contención si desea volver a utilizar las direcciones IP y MAC en diferentes entornos contenidos. Por ejemplo, en una Cloud Management Platform (CMP), la contención permite ejecutar varias instancias de nube simultáneas con las mismas direcciones IP y MAC completamente aisladas o “contenidas”.

Por ejemplo:

**Edit NSX Edge Interface**

vNIC#: 1

Name: \* Internal

Type: ☒ Internal ☐ Uplink

Connected To: transit-switch [Change](#) [Remove](#)

Connectivity Status: ☒ Connected ☐ Disconnected

Configure subnets

| IP Address    | Subnet Prefix Length |
|---------------|----------------------|
| 192.168.10.1* | 29                   |
|               |                      |
|               |                      |
|               |                      |

MAC Addresses:

You can specify a MAC address or leave it blank for auto generation. In case of HA, two different MAC addresses are required.

MTU:

Options: ☐ Enable Proxy ARP ☐ Send ICMP Redirect Reverse Path Filter [Disable](#) ▼

Fence Parameters:

Example: ethernet0.filter1.param1=1

[OK](#) [Cancel](#)

En el siguiente ejemplo se muestran dos interfaces: una conecta la ESG con el mundo exterior mediante un grupo de puertos de vínculo superior en un conmutador distribuido de vSphere, mientras que la otra conecta la ESG a un conmutador lógico de tránsito al cual también está conectado un enrutador lógico distribuido.

### New NSX Edge

- ✓ 1 Name and description
- ✓ 2 Settings
- ✓ 3 Configure deployment
- ✓ 4 **Configure interfaces**
- 5 Default gateway settings
- 6 Firewall and HA
- 7 Ready to complete

### Configure interfaces

Configure interfaces of this NSX Edge

+ ✎ ✕

| vNIC# | Name     | IP Address    | Subnet Prefix Length | Connected To         |
|-------|----------|---------------|----------------------|----------------------|
| 0     | uplink   | 192.168.100.3 | 24                   | Mgmt_VDS - HQ_Uplink |
| 1     | internal | 192.168.10.1  | 29                   | transit-switch       |
|       |          |               |                      |                      |
|       |          |               |                      |                      |
|       |          |               |                      |                      |
|       |          |               |                      |                      |
|       |          |               |                      |                      |
|       |          |               |                      |                      |
|       |          |               |                      |                      |

Back
Next
Finish
Cancel

9 Configure una puerta de enlace predeterminada.

Puede editar el valor de MTU, pero este no puede ser mayor que el valor de MTU configurado en la interfaz.

Por ejemplo:

**New NSX Edge**

✓ 1 Name and description  
 ✓ 2 Settings  
 ✓ 3 Configure deployment  
 ✓ 4 Configure interfaces  
**5 Default gateway settings**  
 6 Firewall and HA  
 7 Ready to complete

**Default gateway settings**

☒ Configure Default Gateway

vNIC: \* uplink

Gateway IP: \* 192.168.100.2

MTU: 1500

Back Next Finish Cancel

## 10 Configure la directiva de firewall, el registro y los parámetros de HA.

**Precaución** Si no configura la directiva de firewall, se establece la directiva predeterminada para denegar todo el tráfico.

De forma predeterminada, los registros están habilitados en todos los dispositivos NSX Edge nuevos. El nivel de registro predeterminado es NOTICE (ATENCIÓN). Si los registros se almacenan de forma local en la ESG, es posible que el proceso de registro genere demasiados registros y afecte al rendimiento de NSX Edge. Por este motivo, le recomendamos que configure los servidores syslog remotos y reenvíe los registros a un recopilador centralizado para que se analicen y se supervisen.

Si habilitó High Availability, complete la sección HA. De forma predeterminada, HA selecciona automáticamente una interfaz interna y asigna automáticamente direcciones IP de vínculo locales. NSX Edge admite dos máquinas virtuales para High Availability, que permanecen actualizadas con configuraciones del usuario. Si se produce un error de latido en la máquina virtual principal, el estado de la máquina virtual secundaria cambia a activo. De esa manera, una máquina virtual NSX Edge siempre está activa en la red. NSX Edge replica la configuración del dispositivo principal para el

dispositivo en espera y garantiza que las dos máquinas virtuales NSX Edge con HA no estén en el mismo host ESX, incluso después de utilizar DRS y vMotion. En vCenter, se implementan dos máquinas virtuales en el mismo grupo de recursos y almacén de datos que el dispositivo configurado. Se asignan direcciones IP de vínculo locales a máquinas virtuales con HA en NSX Edge HA para que puedan comunicarse entre sí. Seleccione la interfaz interna para la cual desea configurar parámetros de HA. Si selecciona el valor CUALQUIERA (ANY) para la interfaz, pero no hay interfaces internas configuradas, la interfaz de usuario mostrará un error. Se crean dos dispositivos Edge, pero como no hay una interfaz interna configurada, el dispositivo Edge nuevo permanece en espera y se deshabilita HA. Una vez que se configura una interfaz interna, HA se vuelve a habilitar en el dispositivo Edge. Escriba el período en segundos dentro del cual, si el dispositivo de copia de seguridad no recibe una señal de latido del dispositivo principal, este se considera inactivo y el dispositivo de copia de seguridad lo reemplaza. El intervalo predeterminado es 15 segundos. De manera opcional, puede introducir dos direcciones IP de administración en formato CIDR para anular las direcciones IP de vínculo locales asignadas a las máquinas virtuales con HA. Asegúrese de que las direcciones IP de administración no se superpongan con las direcciones IP utilizadas para ninguna otra interfaz, y que no interfieran con el enrutamiento de tráfico. No debe utilizar una dirección IP que exista en otro lugar de la red, ni siquiera si esa red no está conectada directamente con NSX Edge.

Por ejemplo:

**New NSX Edge**

- ✓ 1 Name and description
- ✓ 2 Settings
- ✓ 3 Configure deployment
- ✓ 4 Configure interfaces
- ✓ 5 Default gateway settings
- 6 Firewall and HA**
- 7 Ready to complete

### Firewall and HA

☒ **Configure Firewall default policy**

Default Traffic Policy: ☒ Accept ☐ Deny

Logging: ☐ Enable ☒ Disable

#### Configure HA parameters

Configuring HA parameters is mandatory for HA to work.

vNIC: \* internal

Declare Dead Time: 15 (seconds)

Management IPs:

You can specify pair of IPs (in CIDR format) with /30 subnet. Management IPs must not overlap with any vnic subnets.

Back Next Finish Cancel

## Resultados

Después de implementar ESG, vaya a la vista Hosts y clústeres (Hosts and Clusters) y abra la consola del dispositivo virtual Edge. Desde la consola, compruebe si puede hacer ping en las interfaces conectadas.

## Pasos siguientes

Cuando instale un dispositivo NSX Edge, NSX habilita el encendido/apagado automático de la máquina virtual en el host si vSphere HA está deshabilitado en el clúster. Si posteriormente las máquinas virtuales del dispositivo se migran a otros hosts en el clúster, es posible que los hosts nuevos no tengan habilitada la opción de encendido/apagado automático de la máquina virtual. Por este motivo, VMware recomienda que cuando instale dispositivos NSX Edge en clústeres que tienen vSphere deshabilitado, debe comprobar todos los hosts del clúster para asegurarse de que la opción de encendido/apagado automático esté habilitada. Consulte la sección sobre cómo editar la configuración de encendido y apagado de la máquina Virtual en *Administrar máquinas virtuales de vSphere*.

Ahora puede configurar el enrutamiento para permitir la conectividad de los dispositivos externos a las máquinas virtuales.

# Configurar OSPF en un enrutador lógico (distribuido)

# 19

La configuración de OSPF en un enrutador lógico permite la conectividad de la máquina virtual en todos los enrutadores lógicos, los cuales, a su vez, se conectan con las puertas de enlace de servicios Edge (ESG).

Las directivas de enrutamiento de OSPF ofrecen un proceso dinámico de equilibrio de carga de tráfico entre rutas de igual costo.

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 distinguen por un identificador de área.

## Requisitos previos

Debe configurarse un identificador de enrutador, como se muestra en [OSPF configurado en el enrutador lógico \(distribuido\)](#).

Cuando se habilita un identificador de enrutador, el campo se completa de forma predeterminada con la interfaz de vínculo superior del enrutador lógico.

## Procedimiento

- 1 Inicie sesión en vSphere Web Client.
- 2 Haga clic en **Redes y seguridad** (Networking & Security) y, a continuación, en **Instancias de NSX Edge** (NSX Edges).
- 3 Haga doble clic en un enrutador lógico.
- 4 Haga clic en **Enrutamiento** (Routing) y, a continuación, haga clic en **OSPF**.
- 5 Habilite OSPF.
  - a Haga clic en **Editar** (Edit) en la esquina superior derecha de la ventana y, a continuación, haga clic en **Habilitar OSPF** (Enable OSPF).
  - b En **Dirección de reenvío** (Forwarding Address), escriba una dirección IP que utilizará el módulo de rutas de datos del enrutador en los hosts para reenviar paquetes de rutas de datos.
  - c En **Dirección de protocolo** (Protocol Address), escriba una dirección IP única dentro de la misma subred de **Dirección de reenvío** (Forwarding Address). El protocolo utiliza la dirección de protocolo para formar adyacencias con los elementos del mismo nivel.



## 6 Configure las áreas de OSPF.

- a Como opción, puede eliminar el área Not-So-Stubby (NSSA) 51 que viene configurada de forma predeterminada.
- b En **Definiciones de área** (Area Definitions), haga clic en el icono **Agregar** (Add).
- c Escriba un identificador de área. NSX Edge admite un identificador de área en forma de número decimal. Los valores válidos van del 0 al 4294967295.
- d En **Tipo** (Type), seleccione **Normal** o **NSSA**.

Las NSSA impiden el desborde con anuncios sobre el estado del vínculo (LSA) AS externos. Las NSSA dependen del enrutamiento predeterminado en destinos externos. Por lo tanto, deben ubicarse en el extremo de un dominio de enrutamiento de OSPF. Las NSSA pueden importar rutas externas en el dominio de enrutamiento de OSPF, por lo que ofrecen un servicio de tránsito para los dominios pequeños de enrutamiento que no forman parte del dominio de enrutamiento de OSPF.

## 7 (opcional) Seleccione un tipo de autenticación en **Autenticación** (Authentication). OSPF realiza la autenticación en el nivel del área.

Todos los enrutadores dentro del área deben tener la misma autenticación y la correspondiente contraseña configurada. Para que funcione la autenticación de MD5, tanto los enrutadores de recepción como de transmisión deben tener la misma clave MD5.

- a **Ninguna** (None): no se requiere autenticación, que es el valor predeterminado.
- b **Contraseña** (Password): en este método de autenticación, se incluye una contraseña en el paquete transmitido.
- c **MD5**: este método de autenticación utiliza un cifrado MD5 (síntesis del mensaje de tipo 5). En el paquete transmitido se incluye una suma de comprobación de MD5.
- d Para la autenticación de tipo **Contraseña** (Password) o **MD5**, escriba la contraseña o la clave de MD5.

---

### Importante

- Si NSX Edge está configurado para HA con el reinicio correcto de OSPF habilitado y MD5 se usa para la autenticación, OSPF no se reinicia correctamente. Las adyacencias solo aparecen después de que caduque el período de gracia en los nodos de aplicaciones auxiliares de OSPF.
  - No puede configurar la autenticación **MD5** si está habilitado el modo FIPS.
  - NSX for vSphere siempre utiliza un valor 1 de ID de clave. Los dispositivos que no administre NSX for vSphere y que estén al mismo nivel que la puerta de enlace de servicios Edge o el enrutador lógico distribuido se deben configurar para que usen el valor 1 de la ID clave cuando se use la autenticación MD5. De lo contrario, no se puede establecer una sesión OSPF.
-

**8** Asigne interfaces a las áreas.

- a En **Asignación de interfaz a área** (Area to Interface Mapping), haga clic en el icono **Agregar** (Add) para asignar la interfaz que corresponde al área de OSPF.
- b Seleccione la interfaz que desea asignar y el área de OSPF a la cual será asignada.

**9** (opcional) Si fuera necesario, edite la configuración predeterminada de OSPF.

En la mayoría de los casos, se recomienda conservar la configuración predeterminada de OSPF. Si finalmente cambia la configuración, asegúrese de que los elementos del mismo nivel de OSPF utilicen la misma configuración.

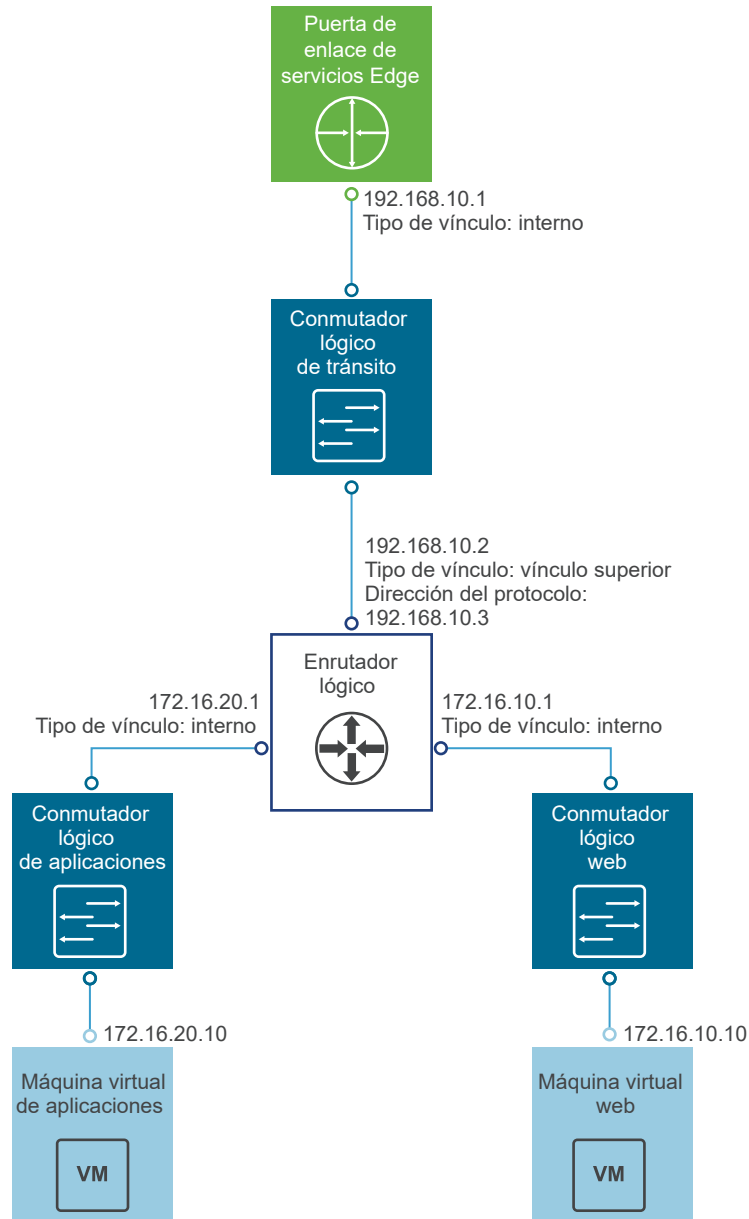
- a **Intervalo de saludo** (Hello Interval) muestra el intervalo predeterminado entre los paquetes de saludo que se envían en la interfaz.
- b **Intervalo inactivo** (Dead Interval) muestra el intervalo predeterminado durante el cual debe recibirse al menos un paquete de saludo de un vecino antes de que el enrutador declare a ese vecino como inactivo.
- c **Prioridad** (Priority) muestra la prioridad predeterminada de la interfaz. La interfaz con la prioridad más alta es el enrutador designado.
- d La opción **Costo** (Cost) de una interfaz muestra la sobrecarga predeterminada necesaria para enviar paquetes a través de esa interfaz. El costo de una interfaz es inversamente proporcional a su ancho de banda. A mayor ancho de banda, menor costo.

**10** Haga clic en **Publicar cambios** (Publish Changes).

## Ejemplo: OSPF configurado en el enrutador lógico (distribuido)

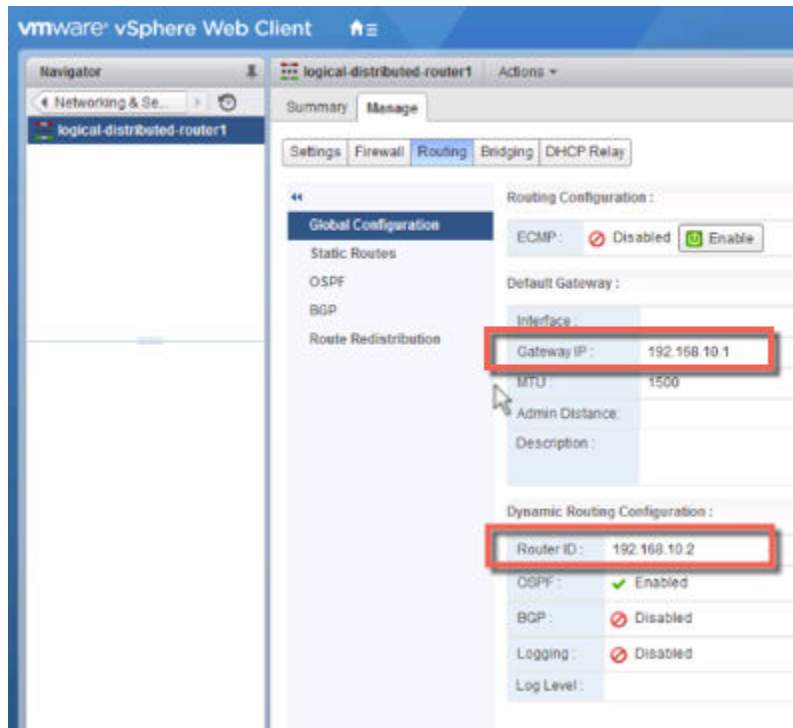
Un escenario simple de NSX for vSphere que utiliza OSPF es aquel en el que un enrutador lógico (DLR) y una puerta de enlace de servicios Edge (ESG) son vecinos de OSPF, como se muestra aquí.

**Figura 19-1. Topología de NSX for vSphere**

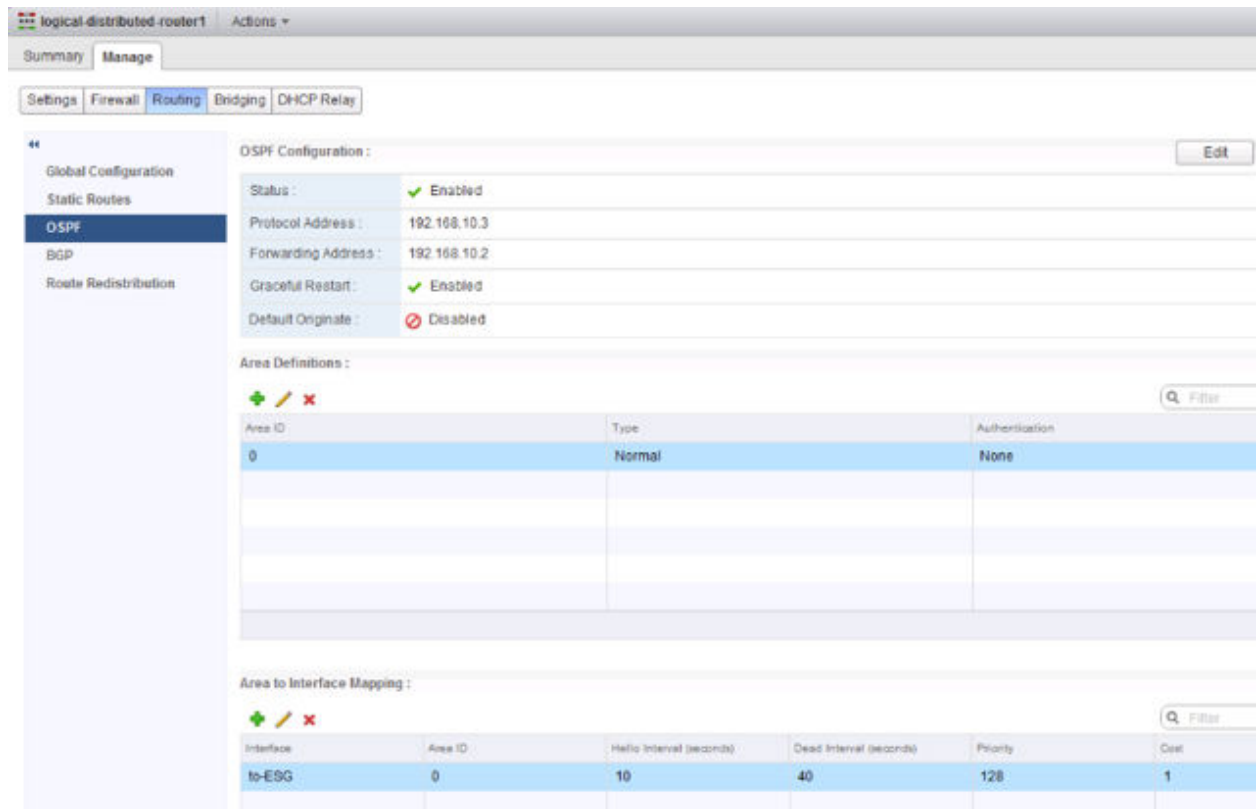


En la siguiente pantalla, la puerta de enlace predeterminada del enrutador lógico es la dirección IP de la interfaz interna de la ESG (192.168.10.1).

El identificador del enrutador es la interfaz de vínculo superior del enrutador lógico: es decir, la dirección IP que apunta a la ESG (192.168.10.2).



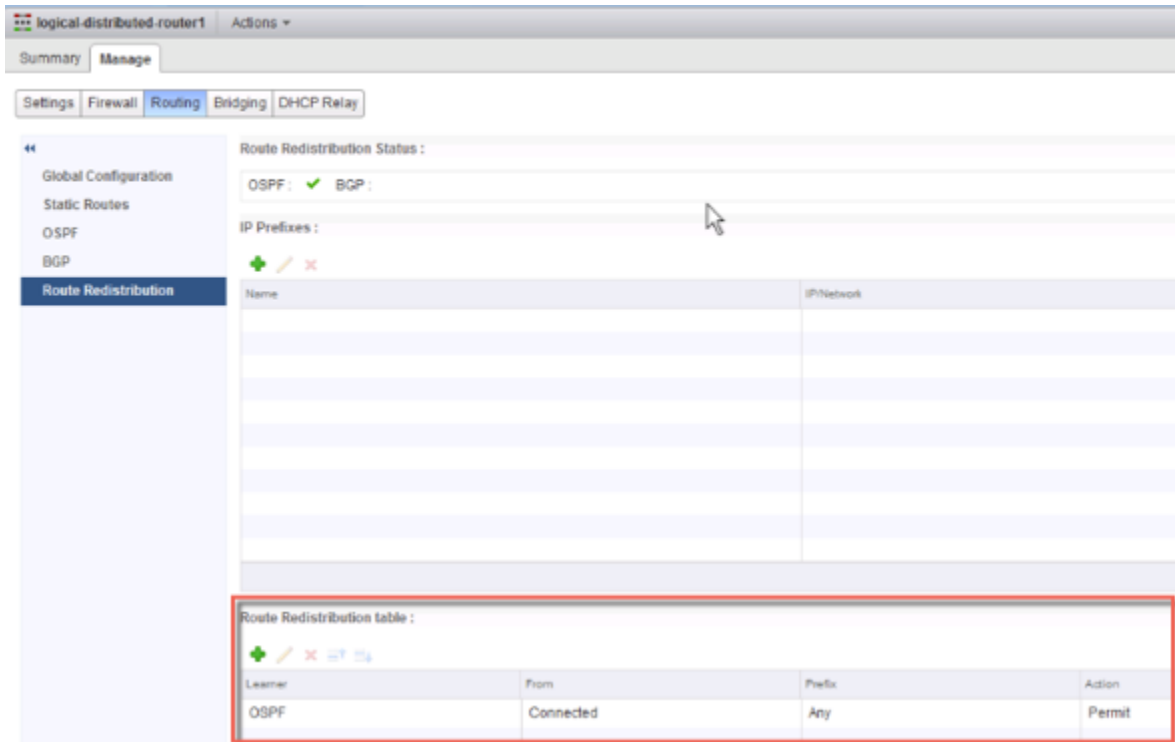
La configuración del enrutador lógico utiliza 192.168.10.2 como dirección de reenvío. La dirección del protocolo puede ser cualquier dirección IP que se encuentre en la misma subred y que no se esté utilizando en otro lugar. En este caso, está configurada la dirección 192.168.10.3. El identificador de área configurado es 0 y la interfaz de vínculo superior (la interfaz que apunta a la ESG) se asigna al área.



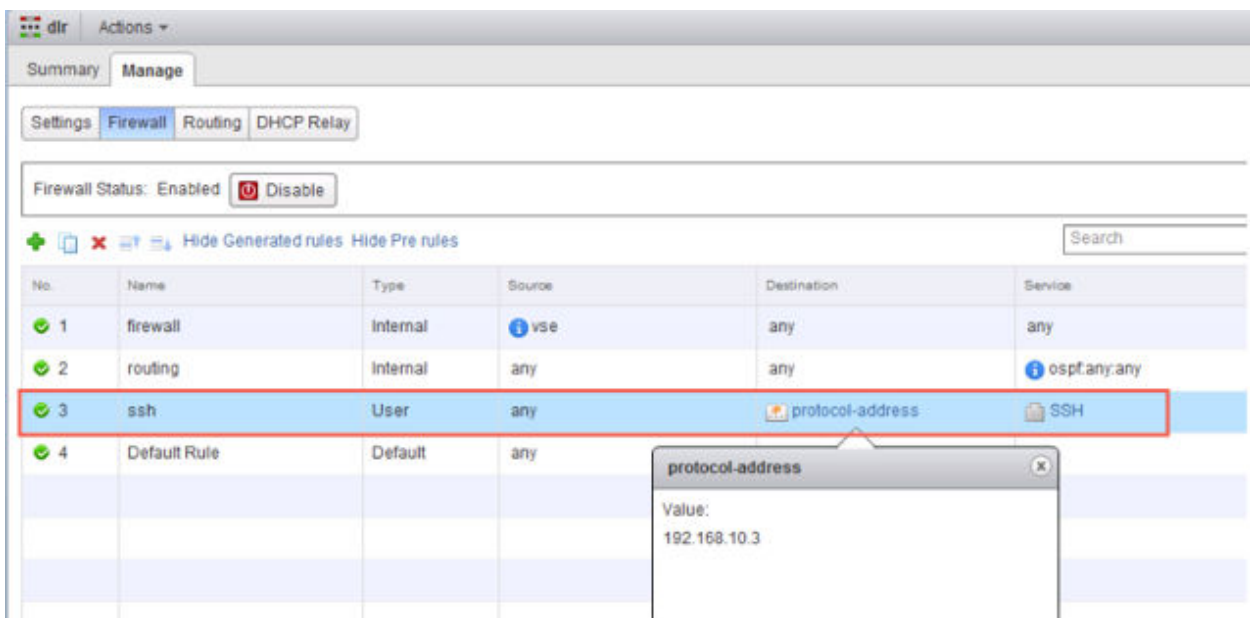
## Pasos siguientes

Asegúrese de que la redistribución de rutas y la configuración de firewall permitan anunciar las rutas correctas.

En este ejemplo, en OSPF se anuncian las rutas conectadas del enrutador lógico (172.16.10.0/24 y 172.16.20.0/24).



Si habilitó SSH al crear el enrutador lógico, también debe configurar un filtro de firewall que habilite SSH en la dirección del protocolo del enrutador lógico. Por ejemplo:



# Configurar el protocolo OSPF en una puerta de enlace de servicios Edge

## 20

La configuración de un protocolo OSPF en una puerta de enlace de servicios Edge (ESG) permite que ESG conozca y anuncie rutas. La aplicación más común de OSPF en una ESG se realiza en el vínculo entre la ESG y un enrutador lógico (distribuido). Esta acción permite que la ESG conozca las interfaces lógicas (LIFS) que están conectadas al enrutador lógico. Este objetivo puede cumplirse con OSPF, IS-IS, BGP o enrutamiento estático.

Las directivas de enrutamiento de OSPF ofrecen un proceso dinámico de equilibrio de carga de tráfico entre rutas de igual costo.

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 distinguen por un identificador de área.

### Requisitos previos

Debe configurarse un identificador de enrutador, como se muestra en [OSPF configurado en la puerta de enlace de servicios Edge](#).

Cuando se habilita un identificador de enrutador, el campo se completa de forma predeterminada con la dirección IP de la interfaz de vínculo superior de la ESG.

### Procedimiento

- 1 Inicie sesión en vSphere Web Client.
- 2 Haga clic en **Redes y seguridad** (Networking & Security) y, a continuación, en **Instancias de NSX Edge** (NSX Edges).
- 3 Haga doble clic en una ESG.
- 4 Haga clic en **Enrutamiento** (Routing) y, a continuación, haga clic en **OSPF**.

## 5 Habilite OSPF.

- a Haga clic en **Editar** (Edit) en la esquina superior derecha de la ventana y, a continuación, haga clic en **Habilitar OSPF** (Enable OSPF).
- b (opcional) Haga clic en **Habilitar reinicio correcto** (Enable Graceful Restart) para detener la interrupción del reenvío de paquetes durante el reinicio de los servicios de OSPF.
- c (opcional) Haga clic en **Habilitar origen predeterminado** (Enable Default Originate) para permitir que la ESG se anuncie como puerta de enlace predeterminada ante los elementos del mismo nivel.

## 6 Configure las áreas de OSPF.

- a (opcional) Elimine el área Not-So-Stubby (NSSA) 51 que viene configurada de forma predeterminada.
- b En **Definiciones de área** (Area Definitions), haga clic en el icono **Agregar** (Add).
- c Escriba un identificador de área. NSX Edge admite un identificador de área en forma de dirección IP o número decimal.
- d En **Tipo** (Type), seleccione **Normal** o **NSSA**.

Las NSSA impiden el desborde con anuncios sobre el estado del vínculo (LSA) AS externos. Las NSSA dependen del enrutamiento predeterminado en destinos externos. Por lo tanto, deben ubicarse en el extremo de un dominio de enrutamiento de OSPF. Las NSSA pueden importar rutas externas en el dominio de enrutamiento de OSPF, por lo que ofrecen un servicio de tránsito para los dominios pequeños de enrutamiento que no forman parte del dominio de enrutamiento de OSPF.

- 7 (opcional) Si selecciona como tipo **NSSA**, se mostrará el campo **Función de traductor de NSSA** (NSSA Translator Role). Seleccione la casilla **Siempre** (Always) para traducir LSA de tipo 7 a LSA de tipo 5. La NSSA traduce todas las LSA de tipo 7 a LSA de tipo 5.
- 8 (opcional) Seleccione un tipo de autenticación en **Autenticación** (Authentication). OSPF realiza la autenticación en el nivel del área.

Todos los enrutadores dentro del área deben tener la misma autenticación y la correspondiente contraseña configurada. Para que funcione la autenticación de MD5, tanto los enrutadores de recepción como de transmisión deben tener la misma clave MD5.

- a **Ninguna** (None): no se requiere autenticación, que es el valor predeterminado.
- b **Contraseña** (Password): en este método de autenticación, se incluye una contraseña en el paquete transmitido.

- c **MD5**: este método de autenticación utiliza un cifrado MD5 (síntesis del mensaje de tipo 5). En el paquete transmitido se incluye una suma de comprobación de MD5.
- d Para la autenticación de tipo **Contraseña** (Password) o **MD5**, escriba la contraseña o la clave de MD5.

---

#### Nota

- No puede configurar la autenticación **MD5** si está habilitado el modo FIPS.
  - NSX siempre utiliza un valor de ID de clave de 1. Cualquier emparejamiento de dispositivos que no sean NSX con NSX Edge o un enrutador lógico distribuido debe configurarse para utilizar un valor de ID de clave de 1 cuando se use la autenticación MD5. De lo contrario, no se establecerá ninguna sesión OSPF.
- 

### 9 Asigne interfaces a las áreas.

- a En **Asignación de interfaz a área** (Area to Interface Mapping), haga clic en el icono **Agregar** (Add) para asignar la interfaz que corresponde al área de OSPF.
- b Seleccione la interfaz que desea asignar y el área de OSPF a la cual será asignada.

### 10 (opcional) Edite la configuración predeterminada de OSPF.

En la mayoría de los casos, se recomienda conservar la configuración predeterminada de OSPF. Si finalmente cambia la configuración, asegúrese de que los elementos del mismo nivel de OSPF utilicen la misma configuración.

- a **Intervalo de saludo** (Hello Interval) muestra el intervalo predeterminado entre los paquetes de saludo que se envían en la interfaz.
- b **Intervalo inactivo** (Dead Interval) muestra el intervalo predeterminado durante el cual debe recibirse al menos un paquete de saludo de un vecino antes de que el enrutador declare a ese vecino como inactivo.
- c **Prioridad** (Priority) muestra la prioridad predeterminada de la interfaz. La interfaz con la prioridad más alta es el enrutador designado.
- d La opción **Costo** (Cost) de una interfaz muestra la sobrecarga predeterminada necesaria para enviar paquetes a través de esa interfaz. El costo de una interfaz es inversamente proporcional a su ancho de banda. A mayor ancho de banda, menor costo.

### 11 Haga clic en **Publicar cambios** (Publish Changes).

### 12 Asegúrese de que la redistribución de rutas y la configuración de firewall permitan anunciar las rutas correctas.

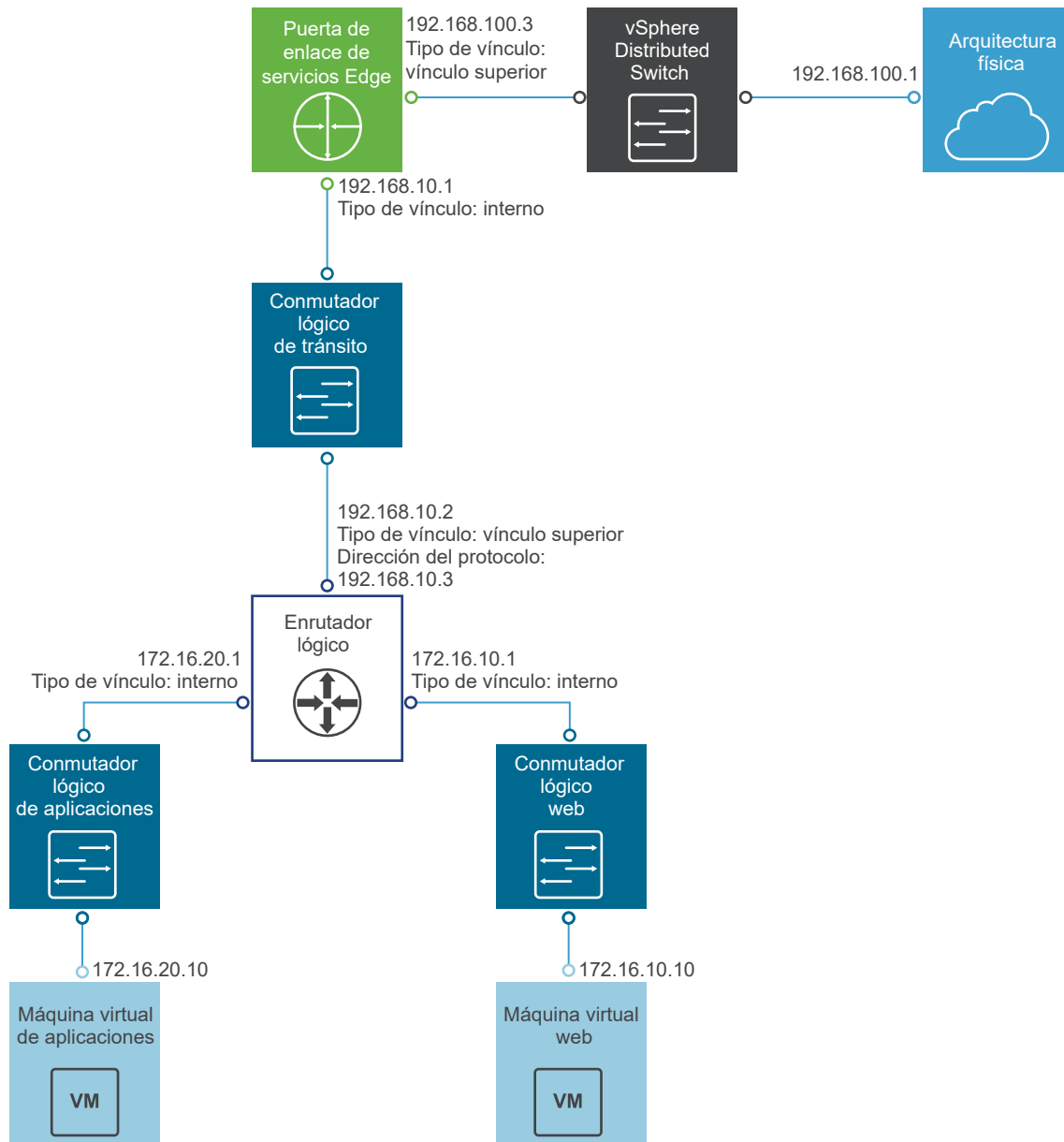
## Ejemplo: OSPF configurado en la puerta de enlace de servicios Edge

Un escenario simple de NSX que utiliza OSPF es uno donde un enrutador lógico y una puerta de enlace de servicios Edge son vecinos de OSPF, como se muestra aquí.



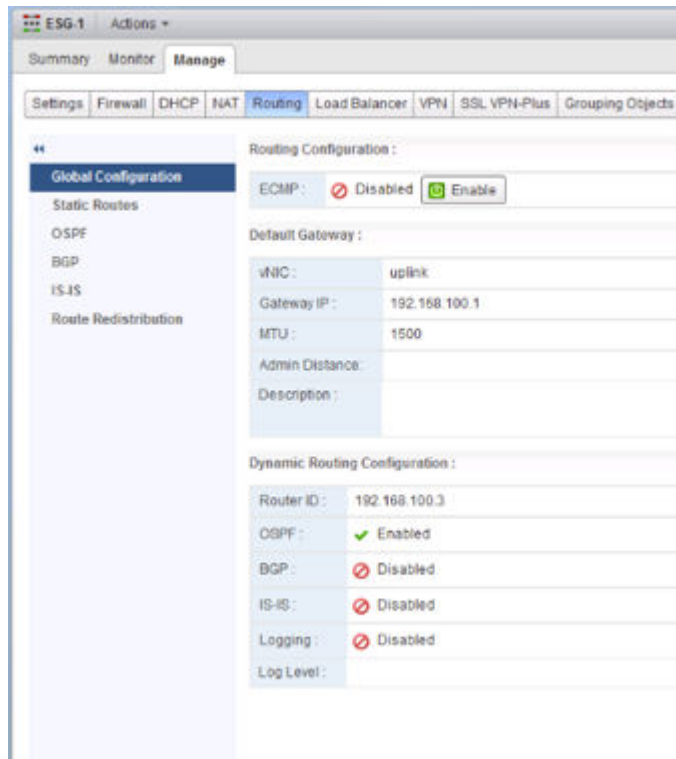
La ESG puede conectarse al exterior a través de un puente, un enrutador físico (o como se muestra aquí) mediante un grupo de puertos de vínculo superior en un conmutador distribuido de vSphere.

**Figura 20-1. Topología NSX**

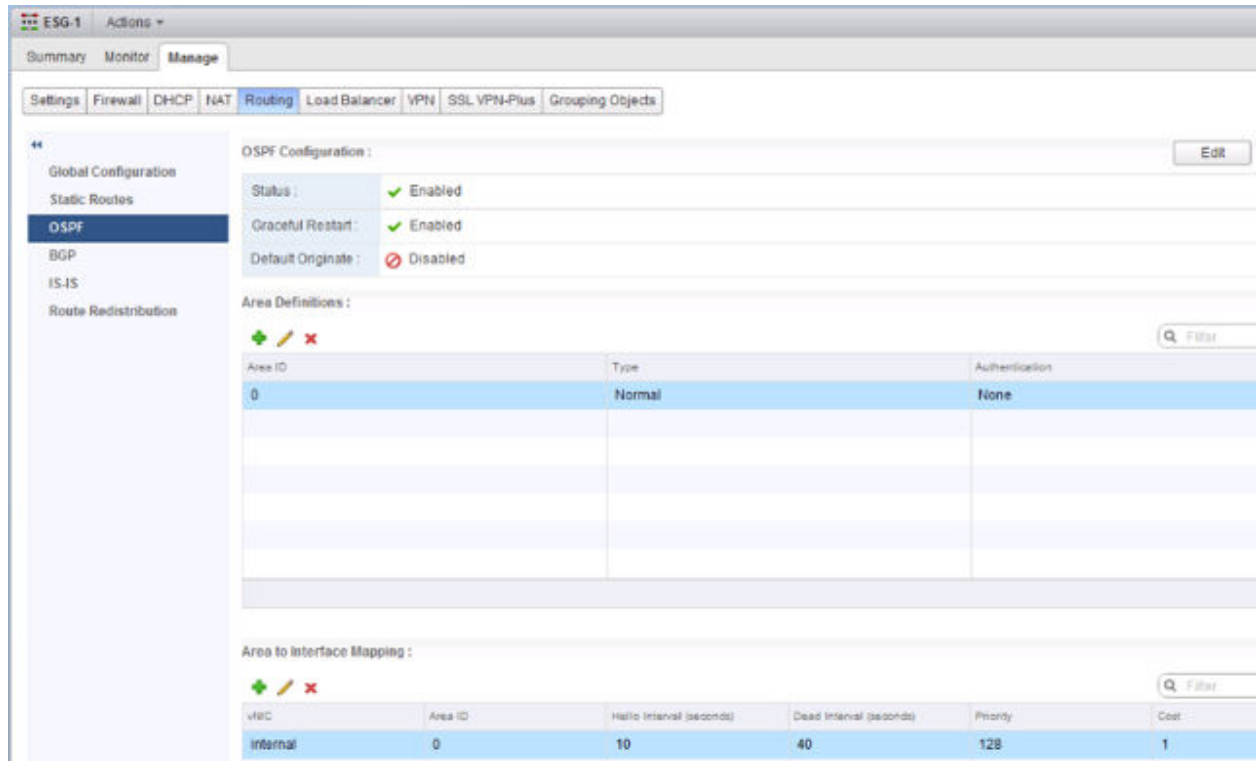


En la siguiente pantalla, la puerta de enlace predeterminada de la ESG es la interfaz de vínculo superior de la ESG con el elemento externo del mismo nivel.

El identificador de enrutador es la dirección IP de la interfaz de vínculo superior de la ESG: es decir, la dirección IP que apunta al elemento externo del mismo nivel.



El identificador de área configurado es 0 y la interfaz interna (la interfaz que apunta al enrutador lógico) se asigna al área.



Los enrutadores conectados se redistribuyen en OSPF de modo que el vecino de OSPF (el enrutador lógico) pueda conocer la red de vínculo superior de la ESG.

Summary Monitor Manage

Settings Firewall DHCP NAT **Routing** Load Balancer VPN SSL VPN-Plus Grouping Objects

Global Configuration  
Static Routes  
OSPF  
BGP  
IS-IS  
**Route Redistribution**

Route Redistribution Status:

OSPF ☒ ISIS ☐ BGP ☐

IP Prefixes:

+ - ✎ ✖

| Name | IP Network |
|------|------------|
|      |            |
|      |            |
|      |            |
|      |            |

Route Redistribution table:

+ - ✎ ✖

| Learned | From      | Prefix | Action |
|---------|-----------|--------|--------|
| OSPF    | Connected | Any    | Permit |

**Nota** Asimismo, OSPF puede configurarse entre la ESG y su enrutador externo del mismo nivel, aunque es más frecuente que el vínculo utilice el par BGP para anunciar rutas.

Asegúrese de que la ESG conozca las rutas externas de OSPF a partir del enrutador lógico.

```
NSX-edge-7-0> show ip route

Codes: 0 - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
M1 - OSPF NSSA external type 1, M2 - OSPF NSSA external type 2

Total number of routes: 5

S 0.0.0.0/0 [0/0] via 192.168.100.1
0 E2 172.16.10.0/24 [110/1] via 192.168.10.2
0 E2 172.16.20.0/24 [110/1] via 192.168.10.2
C 192.168.10.0/29 [0/0] via 192.168.10.1
C 192.168.100.0/24 [0/0] via 192.168.100.3
```

Para comprobar la conectividad, asegúrese de que haya un dispositivo externo en la arquitectura física que pueda hacer ping en las máquinas virtuales.

Por ejemplo:

```
PS C:\Users\Administrator> ping 172.16.10.10
```

```
Pinging 172.16.10.10 with 32 bytes of data:
```

```
Reply from 172.16.10.10: bytes=32 time=5ms TTL=61
```

```
Reply from 172.16.10.10: bytes=32 time=1ms TTL=61
```

```
Ping statistics for 172.16.10.10:
```

```
Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 1ms, Maximum = 5ms, Average = 3ms
```

```
PS C:\Users\Administrator> ping 172.16.20.10
```

```
Pinging 172.16.20.10 with 32 bytes of data:
```

```
Reply from 172.16.20.10: bytes=32 time=2ms TTL=61
```

```
Reply from 172.16.20.10: bytes=32 time=1ms TTL=61
```

```
Ping statistics for 172.16.20.10:
```

```
Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

# Instalar Guest Introspection en los clústeres de host

# 21

Al instalar Guest Introspection se instalan automáticamente un nuevo VIB y una máquina virtual de servicio en cada host del clúster. Se requiere Guest Introspection para la supervisión de actividad y varias soluciones de seguridad de terceros.

---

**Nota** No es posible migrar una máquina virtual de servicios (SVM) usando vMotion/SvMotion. Para que las máquinas virtuales de servicios funcionen correctamente, se deben mantener en el host en el que se implementaron.

---

## Requisitos previos

Las instrucciones de instalación a continuación dan por sentado que se cuenta con el siguiente sistema:

- Un centro de datos con versiones compatibles de vCenter Server y ESXi instalado en cada host del clúster.
- Si los hosts de los clústeres se actualizaron de vCenter Server versión 5.0 a la versión 5.5, debe abrir los puertos 80 y 443 en esos hosts.
- Los hosts del clúster donde quiere instalar Guest Introspection deben estar preparados para NSX. Consulte cómo preparar el clúster del host para NSX (Prepare the Host Cluster for NSX) en *Guía de instalación de NSX*. Guest Introspection no puede instalarse en hosts independientes. Si utiliza NSX para implementar y administrar Guest Introspection solo para la capacidad de descarga antivirus, no es necesario que prepare los hosts para NSX, acción que no está permitida por la licencia de NSX para vShield Endpoint.
- NSX Manager instalado y en ejecución.
- Asegúrese de que NSX Manager y los hosts preparados que ejecuten los servicios de Guest Introspection estén vinculados con el mismo servidor NTP y que la hora esté sincronizada. Un error al realizar esta acción puede provocar que las máquinas virtuales no estén protegidas por los servicios de antivirus, aunque el estado del clúster aparezca en verde para Guest Introspection y cualquier servicio de terceras partes.

Si se agrega un servidor NTP, VMware recomienda que se vuelva a implementar Guest Introspection y cualquier servicio de terceras partes.

Si desea asignar una dirección IP a la máquina virtual de servicio de Guest Introspection desde un grupo de IP, cree el grupo de IP antes de instalar NSX Guest Introspection. Consulte cómo trabajar con grupos IP en la *Guía de administración de NSX*.

---

**Precaución** Guest Introspection utiliza la subred 169.254.x.x para asignar las direcciones IP de forma interna para el servicio GI. Si asigna la dirección IP 169.254.1.1 a cualquier interfaz de VMkernel de un host ESXi, se producirá un error en la instalación de Guest Introspection. El servicio GI utiliza esta dirección IP para la comunicación interna.

---

vSphere Fault Tolerance no funciona con Guest Introspection.

## Procedimiento

- 1 En la pestaña **Instalación** (Installation), haga clic en **Implementaciones de servicios** (Service Deployments).
- 2 Haga clic en el icono **Nueva implementación de servicios** (New Service Deployment) (+).
- 3 En el cuadro de diálogo Implementar servicios de red y seguridad (Deploy Network and Security Services), seleccione **Guest Introspection**.
- 4 En **Especificar programación** (Specify schedule) (en la parte inferior del cuadro de diálogo), seleccione **Implementar ahora** (Deploy now) para implementar Guest Introspection en cuanto esté instalado, o bien seleccione una fecha y una hora para la implementación.
- 5 Haga clic en **Siguiente**.
- 6 Seleccione el centro de datos y los clústeres donde desea instalar Guest Introspection y haga clic en **Siguiente** (Next).
- 7 En la página Seleccionar red de administración y almacenamiento (Select storage and Management Network), seleccione el almacén de datos donde desea agregar el almacenamiento de las máquinas virtuales de servicio, o bien seleccione **Especificado en el host** (Specified on host). Se recomienda utilizar las redes y los almacenes de datos compartidos en lugar de la opción "Especificado en el host" (Specified on host) de modo que los flujos de trabajo de la implementación se automaticen.

El almacén de datos seleccionado debe estar disponible en todos los hosts del clúster elegido.

Si seleccionó **Especificado en el host** (Specified on host), siga los pasos a continuación para cada host del clúster.

- a En la página de inicio de vSphere Web Client, haga clic en **vCenter** y, a continuación, en **Hosts**.
- b Haga clic en un host en la columna **Nombre** (Name) y, a continuación, en la pestaña **Administrar** (Manage).
- c Haga clic en **Máquinas virtuales agente** (Agent VMs) y, a continuación, en **Editar** (Edit).
- d Seleccione el almacén de datos y haga clic en **Aceptar** (OK).

- 8 Seleccione el grupo de puertos virtuales distribuidos donde se alojará la interfaz de administración. Si se estableció el almacén de datos en la opción **Especificado en el host** (Specified on host), la red también debe establecerse en la opción **Especificado en el host**.

El grupo de puertos seleccionado debe poder comunicarse con el grupo de puertos de NSX Manager y estar disponible en todos los hosts del clúster seleccionado.

Si seleccionó **Especificado en el host** (Specified on host), siga los subpasos del paso 7 para seleccionar una red del host. Para agregar un host (o varios hosts) al clúster, el almacén de datos y la red deben establecerse antes de agregar cada host al clúster.

- 9 En la asignación de direcciones IP, seleccione una de las siguientes opciones:

| Seleccionar             | Para                                                                                                                                                                                                                           |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DHCP                    | Asignar una dirección IP a la máquina virtual de servicio de NSX Guest Introspection mediante el protocolo de configuración dinámica de host (DHCP). Seleccione esta opción si los hosts se encuentran en diferentes subredes. |
| Grupo de direcciones IP | Asignar una dirección IP a la máquina virtual de servicio de NSX Guest Introspection a partir del grupo de direcciones IP seleccionado.                                                                                        |

- 10 Haga clic en **Siguiente** (Next) y, a continuación, en **Finalizar** (Finish) en la página Listo para finalizar (Ready to complete).
- 11 Supervise la implementación hasta que la columna **Estado de instalación** (Installation Status) muestre **Correcto** (Succeeded).
- 12 Si la columna **Estado de instalación** (Installation Status) muestra **Con errores** (Failed), haga clic en el icono junto a Con errores. Se muestran todos los errores de implementación. Haga clic en **Resolver** (Resolve) para solucionar los errores. En algunos casos, al resolver los errores aparecen otros nuevos. Realice la acción requerida y haga clic de nuevo en **Resolver** (Resolve).

# Desinstalar componentes de NSX

# 22

En este capítulo se detallan los pasos necesarios para desinstalar los componentes de NSX desde el inventario de vCenter.

---

**Nota** No extraiga ningún dispositivo que NSX implementó (como controladores e instancias) directamente desde vCenter. Administre y elimine siempre los dispositivos de NSX a través de la pestaña **Redes y seguridad** (Networking & Security) de vSphere Web Client.

---

Este capítulo incluye los siguientes temas:

- [Desinstalar un módulo de Guest Introspection](#)
- [Desinstalar un enrutador lógico distribuido o una puerta de enlace de servicios NSX Edge](#)
- [Desinstalar un conmutador lógico](#)
- [Desinstalar NSX de los clústeres de hosts](#)
- [Quitar una instalación de NSX de forma segura](#)

## Desinstalar un módulo de Guest Introspection

Al desinstalar Guest Introspection se extrae un VIB de los hosts del clúster y se extrae la máquina virtual de servicio de cada host del clúster. Se requiere Guest Introspection para el Firewall de identidad (Identity Firewall), la Supervisión de endpoint (Endpoint Monitoring) y varias soluciones de seguridad de terceros. La desinstalación de Guest Introspection puede traer consecuencias de amplio alcance.

---

**Precaución** Antes de desinstalar un módulo de Guest Introspection del clúster, deberá desinstalar todos los productos de terceros que están utilizando Guest Introspection en los hosts de ese clúster. Siga las instrucciones del proveedor de la solución.

---

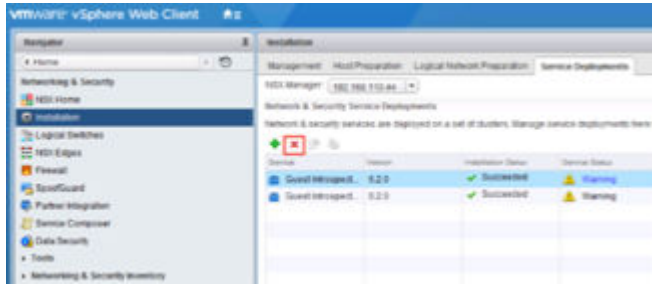
Se pierde la protección de las máquinas virtuales del clúster de NSX. Debe mover las máquinas virtuales mediante vMotion fuera del clúster antes de desinstalar.

Para desinstalar Guest Introspection:

- 1 En vCenter, desplácese hasta **Inicio > Redes y seguridad > Instalación** (Home > Networking & Security > Installation) y seleccione la pestaña **Implementaciones de servicios** (Service Deployments).
- 2 Seleccione una instancia de Guest Introspection y haga clic en el icono de eliminación.



- 3 Puede eliminarla ahora o programar la eliminación para más adelante.



## Desinstalar un enrutador lógico distribuido o una puerta de enlace de servicios NSX Edge

Puede desinstalar una instancia de NSX Edge con vSphere Web Client.

### Requisitos previos

Se le debe haber asignado el rol de administrador de Enterprise o administrador de NSX.

### Procedimiento

- 1 Inicie sesión en vSphere Web Client.
- 2 Haga clic en **Redes y seguridad** (Networking & Security) y, a continuación, en **Instancias de NSX Edge** (NSX Edges).
- 3 Seleccione una instancia de NSX Edge y haga clic en el icono **Eliminar** (Delete) (✖).

## Desinstalar un conmutador lógico

Debe eliminar todas las máquinas virtuales de un conmutador lógico antes de desinstalarlo.

### Requisitos previos

Se le debe haber asignado la función de administrador de Enterprise o administrador de NSX.

### Procedimiento

- 1 En vSphere Web Client, desplácese hasta **Inicio > Redes y seguridad > Conmutadores lógicos** (Home > Networking & Security > Logical Switches).
- 2 Elimine todas las máquinas virtuales de un conmutador lógico.
  - a Seleccione un conmutador lógico y haga clic en el icono **Eliminar máquina virtual** (Remove Virtual Machine) (✖).
  - b Mueva todas las máquinas virtuales de **Objetos disponibles** (Available Objects) a **Objetos seleccionados** (Selected Objects) y haga clic en **Aceptar** (OK).
- 3 Con el conmutador lógico seleccionado, haga clic en el icono **Eliminar** (Delete) (✖).

# Desinstalar NSX de los clústeres de hosts

Puede desinstalar NSX de todos los hosts en un clúster.

Si desea quitar NSX de los hosts individuales (y no de todo el clúster), consulte [Capítulo 12 Quitar un host de un clúster NSX preparado](#).

## Requisitos previos


- Desconecte las máquinas virtuales del clúster desde los conmutadores lógicos.

## Procedimiento

- 1 Quite el clúster de su zona de transporte.

Vaya a **Preparación de red lógica > Zonas de transporte** (Logical Network Preparation > Transport Zones) y desconecte el clúster de la zona de transporte.

Si el clúster aparece atenuado y no puede desconectarlo de la zona de transporte, esto puede deberse a que 1) un host del clúster está desconectado o no está encendido o 2) el clúster puede contener una o más máquinas virtuales o dispositivos que están asociados a la zona de transporte. Por ejemplo, si el host se encuentra en un clúster de administración y tiene instalados controladores NSX Controller, primero quite o mueva los controladores.

- 2 Desinstalar los VIB de NSX En vCenter Web Client, acceda a **Redes y seguridad (Networking & Security) > Instalación (Installation) > Preparación del host (Host Preparation)**. Seleccione un clúster y haga clic en **Acciones (Actions)** (  ) y seleccione **Desinstalar** (Uninstall).

El estado de instalación muestra **No está listo (Not Ready)**. Si hace clic en **No está listo** (Not Ready), el cuadro de diálogo muestra este mensaje: Se debe poner el host en el modo de mantenimiento para completar la instalación del el VIB/agente (Host must be put into maintenance mode to complete agent VIB installation).

- 3 Seleccione el clúster y haga clic en la acción **Resolver** (Resolve) para completar la desinstalación.
  - Si el host tiene NSX 6.2.x o versiones anteriores instaladas, o tiene instalado ESXi 5.5, se necesita un reinicio para completar la desinstalación. Si el clúster tiene DRS habilitado, el DRS intenta reiniciar los hosts de manera controlada para que las máquinas virtuales continúen en ejecución. Si se produce un error en el DRS por cualquier motivo, se detiene la acción **Resolver** (Resolve). En este caso, es posible que deba mover las máquinas virtuales manualmente y, a continuación, volver a intentar la acción **Resolver** (Resolve) o reiniciar los hosts manualmente.
  - En el caso de los hosts con NSX 6.3.0 y ESXi 6.0 o versiones posteriores de ambos, el host debe ponerse en modo de mantenimiento para completar la desinstalación. Si el clúster tiene DRS habilitado, el DRS intenta poner los hosts en el modo de mantenimiento de manera

controlada para que las máquinas virtuales continúen en ejecución. Si se produce un error en el DRS por cualquier motivo, se detiene la acción **Resolver** (Resolve). En este caso, es posible que deba mover las máquinas virtuales manualmente y, a continuación, volver a intentar la acción **Resolver** (Resolve) o poner los hosts en el modo de mantenimiento de forma manual.

---

**Importante** Si pone los hosts en el modo de mantenimiento de forma manual, debe verificar que la desinstalación de los VIB de hosts se haya completado antes de que los hosts salgan del modo de mantenimiento.

- a Compruebe el panel Tareas Recientes (Recent Tasks) en vSphere Web Client.
- b En la pestaña **Preparación de host** (Host Preparation), compruebe que el estado de instalación del clúster desde el que se quitó el host tiene una marca de verificación de color verde.

Si el estado de instalación es Instalando (Installing), el proceso de desinstalación seguirá en curso.

---

## Quitar una instalación de NSX de forma segura

Una desinstalación completa de NSX elimina los VIB del host, las instancias de NSX Manager, los controladores, toda la configuración de VXLAN, los conmutadores lógicos, los enrutadores lógicos, el firewall de NSX, Guest Introspection y el complemento NSX de vCenter. Procure seguir los pasos para todos los hosts del clúster. VMware recomienda desinstalar los componentes de virtualización de red de un clúster antes de quitar el complemento NSX de vCenter Server.

---

**Nota** No extraiga ningún dispositivo implementado por NSX (como controladores e instancias) directamente desde vCenter. Administre y elimine siempre los dispositivos de NSX a través de la pestaña **Redes y seguridad** (Networking & Security) de vSphere Web Client.

---

### Requisitos previos

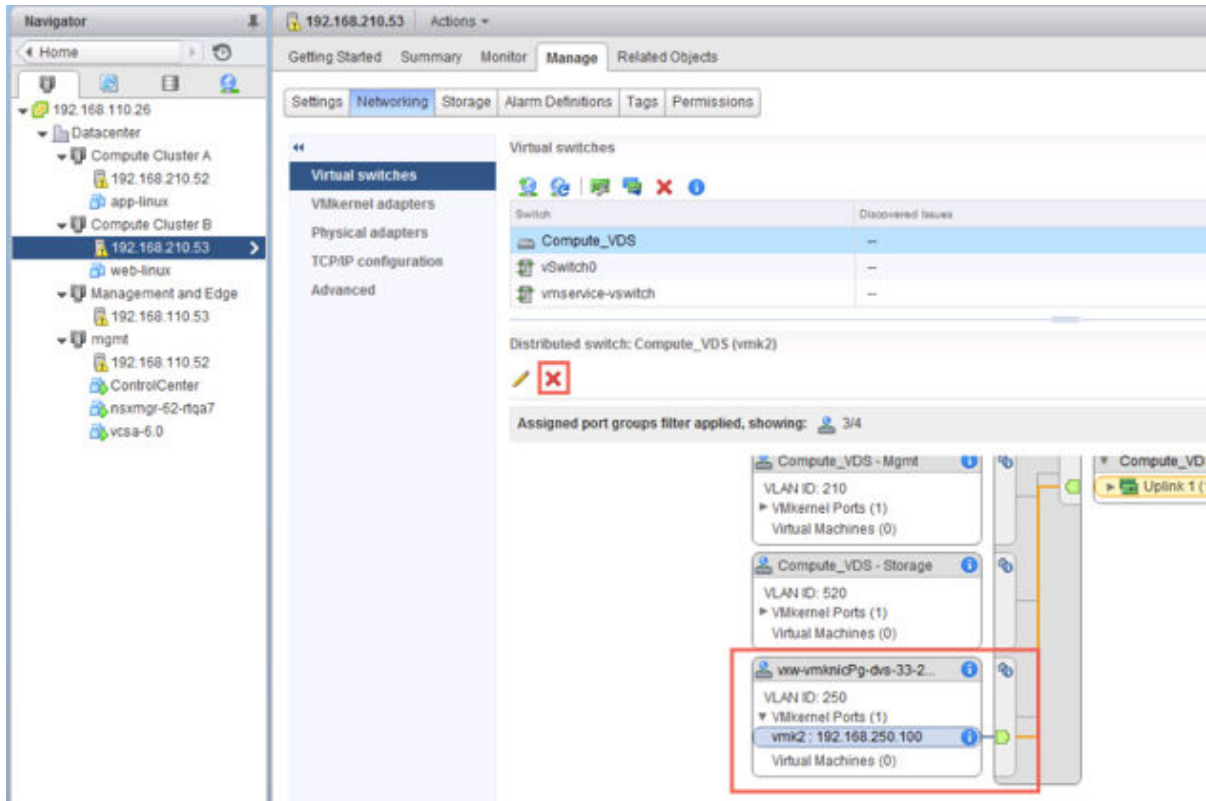
- Se le debe haber asignado la función de administrador de Enterprise o administrador de NSX.
- Quite todas las soluciones de partners registradas, al igual que los servicios de extremo, antes de revertir la preparación del host para que las máquinas virtuales de servicio del clúster se quiten correctamente.
- Elimine todas las instancias de NSX Edge. Consulte [Desinstalar un enrutador lógico distribuido o una puerta de enlace de servicios NSX Edge](#).
- Desconecte las máquinas virtuales en la zona de transporte de los conmutadores lógicos y elimine los conmutadores lógicos. Consulte [Desinstalar un conmutador lógico](#).
- Desinstalar NSX de los clústeres de host. Consulte [Desinstalar NSX de los clústeres de hosts](#).

### Procedimiento

- 1 Elimine la zona de transporte.

- 2 Elimine el dispositivo NSX Manager y todas las máquinas virtuales del dispositivo NSX Controller del disco.
- 3 Quite todas las interfaces vmkernel de VTEP que hayan quedado.

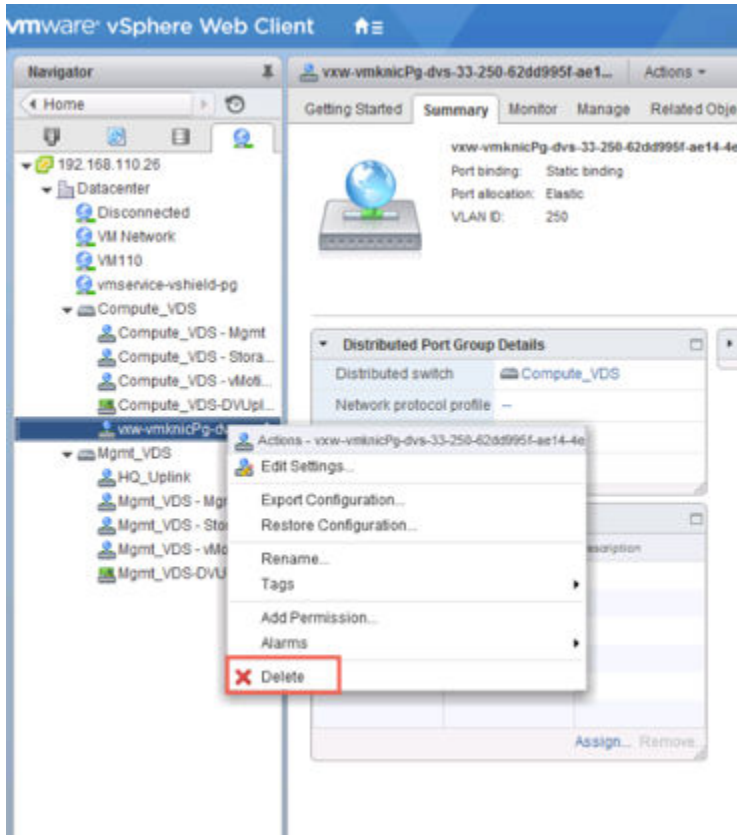
Por ejemplo:



Por lo general, las interfaces vmkernel de VTEP ya se eliminan como resultado de las operaciones de desinstalación anteriores.

- 4 Quite todos los dvPortgroups utilizados para los VTEP que hayan quedado.

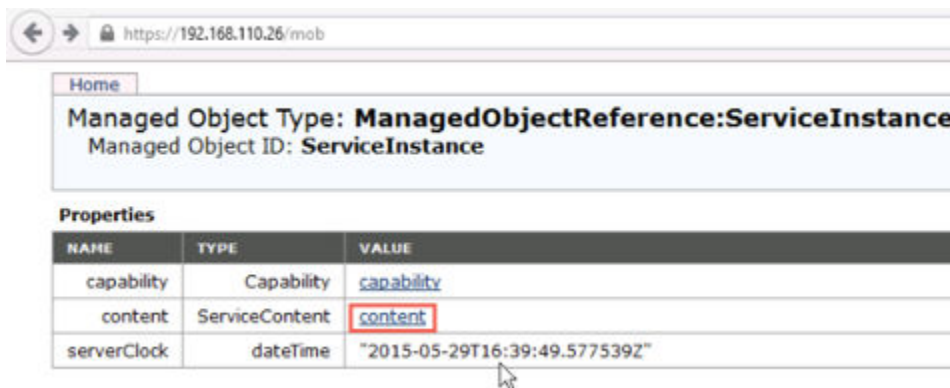
Por ejemplo:



Por lo general, los dvPortgroups utilizados para los VTEP ya se eliminan como resultado de las operaciones de desinstalación anteriores.

- 5 Si eliminó interfaces vmkernel de VTEP o dvPortgroups, reinicie los hosts.
- 6 Para la instancia de vCenter en la que desea quitar el complemento de NSX Manager, inicie sesión en el explorador de objetos administrados en [https://your\\_vc\\_server/mob](https://your_vc_server/mob).
- 7 Haga clic en **Contenido** (Content).

Por ejemplo:



8 Haga clic en **AdministradorDeExtensiones** (ExtensionManager).

← → https://192.168.110.26/mob/Tmoid=ServiceInstance&doPath=content

Home

**Data Object Type: ServiceContent**  
Parent Managed Object ID: **ServiceInstance**  
Property Path: **content**

**Properties**

| NAME                      | TYPE                                                   | VALUE                                     |
|---------------------------|--------------------------------------------------------|-------------------------------------------|
| about                     | AboutInfo                                              | <a href="#">about</a>                     |
| accountManager            | ManagedObjectReference:HostLocalAccountManager         | Unset                                     |
| alarmManager              | ManagedObjectReference:AlarmManager                    | <a href="#">AlarmManager</a>              |
| authorizationManager      | ManagedObjectReference:AuthorizationManager            | <a href="#">AuthorizationManager</a>      |
| certificateManager        | ManagedObjectReference:CertificateManager              | <a href="#">certificateManager</a>        |
| clusterProfileManager     | ManagedObjectReference:ClusterProfileManager           | <a href="#">ClusterProfileManager</a>     |
| complianceManager         | ManagedObjectReference:ProfileComplianceManager        | <a href="#">MoComplianceManager</a>       |
| customFieldsManager       | ManagedObjectReference:CustomFieldsManager             | <a href="#">CustomFieldsManager</a>       |
| customizationSpecManager  | ManagedObjectReference:CustomizationSpecManager        | <a href="#">CustomizationSpecManager</a>  |
| datastoreNamespaceManager | ManagedObjectReference:DatastoreNamespaceManager       | <a href="#">DatastoreNamespaceManager</a> |
| diagnosticManager         | ManagedObjectReference:DiagnosticManager               | <a href="#">DiagMgr</a>                   |
| dvSwitchManager           | ManagedObjectReference:DistributedVirtualSwitchManager | <a href="#">DVSManager</a>                |
| eventManager              | ManagedObjectReference:EventManager                    | <a href="#">EventManager</a>              |
| extensionManager          | ManagedObjectReference:ExtensionManager                | <a href="#">ExtensionManager</a>          |
| fileManager               | ManagedObjectReference:FileManager                     | <a href="#">FileManager</a>               |
| guestOperationsManager    | ManagedObjectReference:GuestOperationsManager          | <a href="#">questOperationsManager</a>    |
| hostProfileManager        | ManagedObjectReference:HostProfileManager              | <a href="#">HostProfileManager</a>        |

9 Haga clic en **CancelarRegistroDeExtensión** (UnregisterExtension)

**Methods**

| RETURN TYPE                            | NAME                                            |
|----------------------------------------|-------------------------------------------------|
| Extension                              | <a href="#">FindExtension</a>                   |
| string                                 | <a href="#">GetPublicKey</a>                    |
| ExtensionManagerIpAllocationUsage[]    | <a href="#">QueryExtensionIpAllocationUsage</a> |
| ManagedObjectReference:ManagedEntity[] | <a href="#">QueryManagedBy</a>                  |
| void                                   | <a href="#">RegisterExtension</a>               |
| void                                   | <a href="#">SetExtensionCertificate</a>         |
| void                                   | <a href="#">SetPublicKey</a>                    |
| void                                   | <a href="#">UnregisterExtension</a>             |
| void                                   | <a href="#">UpdateExtension</a>                 |

- 10 Escriba la cadena **com.vmware.vShieldManager** y haga clic en **Invocar método** (Invoke Method).

**Managed Object Type:**  
**ManagedObjectReference:ExtensionManager**  
 Managed Object ID: **ExtensionManager**  
 Method: **UnregisterExtension**

**void UnregisterExtension**

---

**Parameters**

| NAME                           | TYPE   | VALUE                                                                      |
|--------------------------------|--------|----------------------------------------------------------------------------|
| <b>extensionKey</b> (required) | string | <input style="width: 90%;" type="text" value="com.vmware.vShieldManager"/> |

Invoke Method

- 11 Si va a ejecutar vSphere 6 vCenter Appliance, inicie la consola y habilite el shell de BASH en **Opciones de modo de solución de problemas** (Troubleshooting Mode Options).

**Troubleshooting Mode Options**

**Disable BASH Shell**

Disable SSH

<Up/Down> Select

**Disable BASH Shell**

**BASH Shell is Enabled**  
 Change current state of the BASH Shell

<Enter> Change      <Esc>Exit

Otro modo de habilitar el shell de BASH es iniciar sesión como raíz y ejecutar el comando `shell.set --enabled true`.

- 12 Elimine los directorios de vSphere Web Client para NSX y, a continuación, reinicie el servicio Web Client.

Los directorios de vSphere Web Client para NSX se denominan `com.vmware.vShieldManager.**` y se encuentran en las ubicaciones siguientes:

- VMware vCenter Server para Windows – `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity\`



- VMware vCenter Server Appliance: /etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/

Reiniciar vCenter Server Appliance:

- En vCenter Server Appliance 6.0, inicie sesión en el shell de vCenter Server como usuario raíz y ejecute los comandos siguientes:

```
Command> shell.set --enabled True
Command> shell
localhost:~ # cd /bin
localhost:~ # service-control --stop vsphere-client
localhost:~ # service-control --start vsphere-client
```

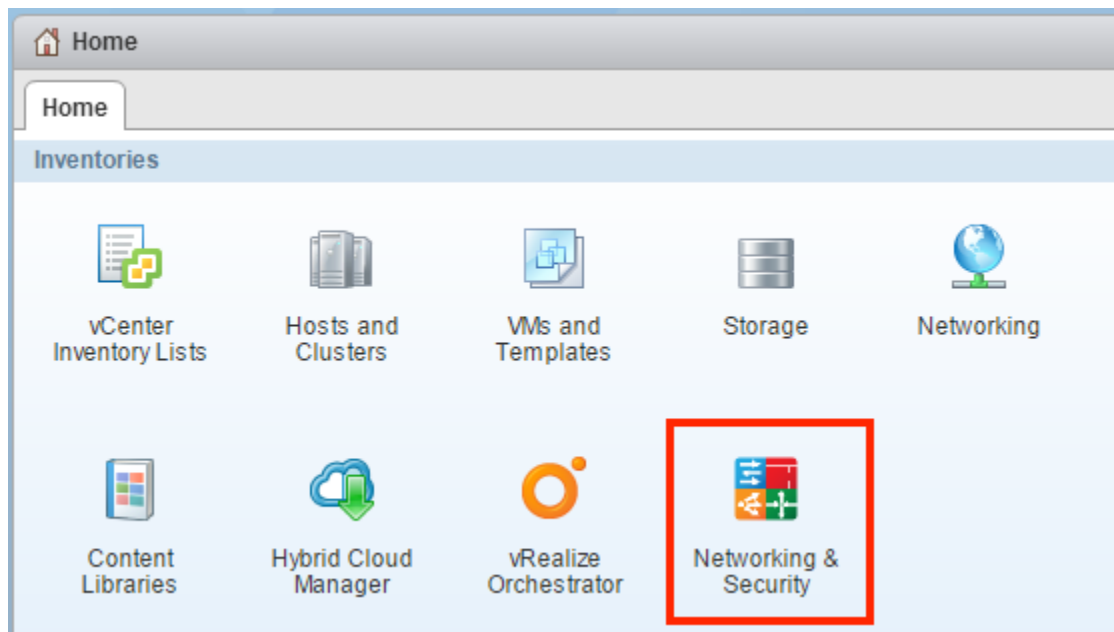
- En vCenter Server 6.0, puede ejecutar los siguientes comandos en Windows.

```
cd C:\Program Files\VMware\vCenter Server\bin
service-control --stop vspherewebclientsvc
service-control --start vspherewebclientsvc
```

## Resultados

Se quita el complemento de NSX Manager de vCenter. Para confirmarlo, cierre sesión en vCenter y vuelva a iniciarla.

El icono **Redes y seguridad** (Networking & Security) del complemento de NSX Manager ya no aparece en la pantalla de inicio de vCenter Web Client.



Vaya a **Administración > Complementos de clientes** (Administration > Client Plug-Ins) y compruebe que la lista de complementos no incluya el **Complemento de interfaz de usuario de NSX** (NSX User Interface plugin).



