

# Guía de instalación de Cross-vCenter 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](mailto:docfeedback@vmware.com)

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

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

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

# Contenido

<b>1</b>	<b>Guía de instalación de Cross-vCenter</b>	<b>5</b>
<b>2</b>	<b>Descripción general de NSX for vSphere</b>	<b>6</b>
	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
<b>3</b>	<b>Descripción general de Cross-vCenter Networking and Security</b>	<b>16</b>
	Beneficios de Cross-vCenter NSX	16
	Cómo funciona Cross-vCenter NSX	17
	Matriz de compatibilidad de NSX Services en Cross-vCenter NSX	19
	Clúster de controladoras universal	20
	Zona de transporte universal	20
	Conmutadores lógicos universales	20
	Enrutadores lógicos (distribuidos) universales	21
	Reglas de firewall universal	21
	Objetos de seguridad y red universal	22
	Topologías de Cross-vCenter NSX	23
	Cross-vCenter NSX de varios sitios y de un solo sitio	23
	Salida local	25
	Modificar los roles de NSX Manager	26
<b>4</b>	<b>Preparación para la instalación</b>	<b>28</b>
	Requisitos del sistema para NSX	28
	Puertos y protocolos requeridos por NSX for vSphere	31
	Conmutadores distribuidos de vSphere y NSX	33
	Ejemplo: Trabajar con un conmutador distribuido de vSphere	36
	Topología de ejemplo y flujo de trabajo de instalación de NSX	44
	Cross-vCenter NSX y Enhanced Linked Mode	45
<b>5</b>	<b>Tareas para las instancias de NSX Manager principales y secundarias</b>	<b>47</b>
	Instalar NSX Manager Virtual Appliance	47
	Configurar inicio de sesión único	52
	Registrar vCenter Server con NSX Manager	54

- Configurar un servidor syslog para NSX Manager 56
- Instalar y asignar licencia de NSX for vSphere 57
- Excluir las máquinas virtuales de la protección de firewall 58

## 6 Configurar la instancia principal de NSX Manager 60

- Implementar NSX Controller en la instancia de NSX Manager principal 60
- Preparar hosts en la instancia de NSX Manager principal 64
- Configurar VXLAN desde la instancia principal de NSX Manager 67
- Asignar un grupo de ID de segmentos y la dirección de multidifusión en el NSX Manager principal 71
- Asignar función principal a NSX Manager 73
- Asignar un grupo universal de ID de segmentos y la dirección de multidifusión en el NSX Manager principal 74
- Agregar una zona de transporte universal en la instancia de NSX Manager principal 76
- Agregar un conmutador lógico universal en la instancia de NSX Manager principal 78
- Conectar máquinas virtuales a un conmutador lógico 80
- Agregar un enrutador lógico (distribuido) universal en la instancia de NSX Manager principal 80

## 7 Configurar instancias secundarias de NSX Manager 93

- Agregar una instancia de NSX Manager secundaria 93
- Preparar hosts en una instancia de NSX Manager secundaria 95
- Configurar VXLAN desde la instancia de NSX Manager secundaria 97
- Asignar un grupo de ID de segmentos y la dirección de multidifusión en el NSX Manager secundario 99
- Agregar clústeres a la zona de transporte universal 100

## 8 Después de configurar las instancias de NSX Manager primaria y secundaria 101

## 9 Desinstalar componentes de NSX 102

- Quitar un host de un clúster NSX preparado 102
- Desinstalar un enrutador lógico distribuido o una puerta de enlace de servicios NSX Edge 103
- Desinstalar un conmutador lógico 104
- Desinstalar NSX de los clústeres de hosts 104
- Quitar una instalación de NSX de forma segura 106

# Guía de instalación de Cross-vCenter



En este manual se describe cómo instalar VMware NSX<sup>®</sup> for vSphere<sup>®</sup> en el entorno de Cross-vCenter NSX. La información incluye instrucciones de configuración paso a paso y prácticas recomendadas.

## Público objetivo

Este manual está destinado a quienes deseen instalar NSX en un entorno de Cross-vCenter NSX. 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

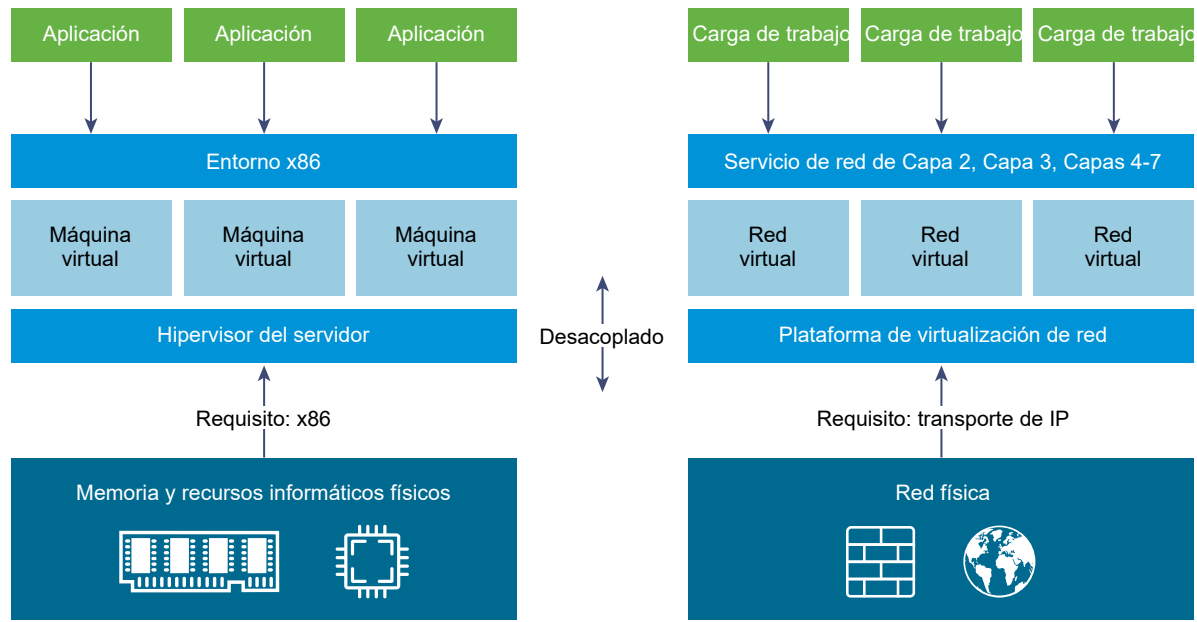
Publicaciones técnicas de VMware proporciona un glosario de términos que podrían resultarle desconocidos. Si desea ver las definiciones de los términos que se utilizan en la documentación técnica de VMware, acceda a la página <http://www.vmware.com/support/pubs>.

# Descripción general de NSX for vSphere

## 2

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

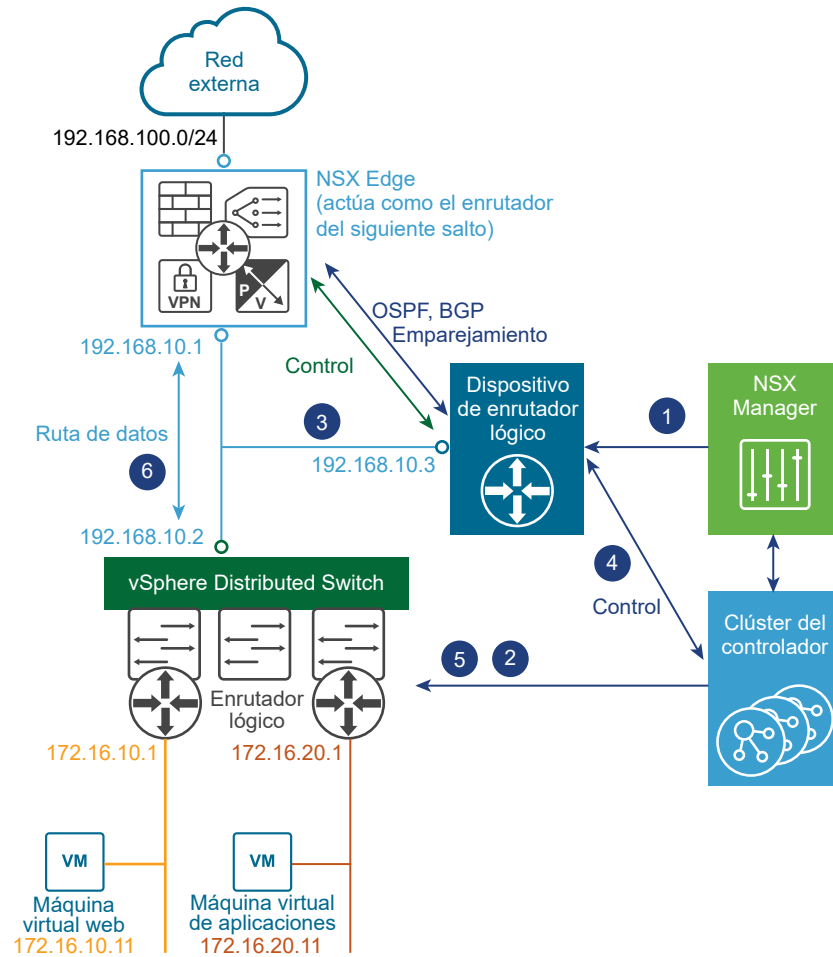
El DLR proporciona enrutamiento distribuido de Este a Oeste con espacio de dirección IP de empresa y aislamiento de ruta de acceso de datos. Las máquinas virtuales o cargas de trabajo que residen en el mismo host, en diferentes subredes, pueden comunicarse entre sí sin necesidad de atravesar una interfaz 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 2-1. 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.

# Descripción general de Cross-vCenter Networking and Security

## 3

NSX 6.2 y las versiones posteriores permiten administrar varios entornos de vCenter NSX desde un único NSX Manager principal.

Este capítulo incluye los siguientes temas:

- [Beneficios de Cross-vCenter NSX](#)
- [Cómo funciona Cross-vCenter NSX](#)
- [Matriz de compatibilidad de NSX Services en Cross-vCenter NSX](#)
- [Clúster de controladoras universal](#)
- [Zona de transporte universal](#)
- [Conmutadores lógicos universales](#)
- [Enrutadores lógicos \(distribuidos\) universales](#)
- [Reglas de firewall universal](#)
- [Objetos de seguridad y red universal](#)
- [Topologías de Cross-vCenter NSX](#)
- [Modificar los roles de NSX Manager](#)

## Beneficios de Cross-vCenter NSX

Los entornos de NSX que contienen más de un sistema vCenter Server pueden administrarse de manera centralizada.

Hay varios motivos por los que pueden requerirse varios sistemas vCenter Server. Por ejemplo:

- Para superar límites de escala de vCenter Server
- Para admitir productos que requieren varios sistemas vCenter Server o sistemas vCenter Server dedicados, como Horizon View o Site Recovery Manager
- Para separar entornos, por ejemplo, por unidad de negocios, arrendatario, organización o tipo de entorno



En NSX 6.1 y anteriores, si se implementan varios entornos de vCenter NSX, estos deben administrarse por separado. En NSX 6.2 y versiones posteriores, puede crear objetos universales en el NSX Manager primario, que se sincronizan en todos los sistemas vCenter Server del entorno.

Cross-vCenter NSX incluye estas características:

- Mayor expansión de las redes lógicas de NSX. Las mismas redes lógicas están disponibles en el entorno de vCenter NSX, por lo que es posible que las máquinas virtuales en cualquier clúster de cualquier sistema vCenter Server se conecten con la misma red lógica.
- Administración centralizada de directivas de seguridad. Las reglas de firewall se administran desde una ubicación centralizada y se aplican a la máquina virtual independientemente de la ubicación o del sistema vCenter Server.
- Compatibilidad con los nuevos límites de movilidad en vSphere 6, incluidos Cross vCenter y vMotion de larga distancia en todos los conmutadores lógicos.
- Mayor compatibilidad con entornos de varios sitios, desde distancia de metros hasta 150 ms RTT. Esto incluye centros de datos activo-activo y activo-pasivo.

Los entornos de Cross-vCenter NSX ofrecen varios beneficios:

- Administración centralizada de objetos universales, lo que reduce el esfuerzo de administración.
- Mayor movilidad de las cargas de trabajo. Las máquinas virtuales pueden migrarse mediante vMotion en todas las instancias de vCenter Server sin necesidad de volver a configurar la máquina virtual o cambiar las reglas de firewall.
- Capacidades mejoradas de NSX de varios sitios y recuperación de desastres.

---

**Nota** Se admite la funcionalidad Cross-vCenter NSX en vSphere 6.0 y versiones posteriores.

---

## Cómo funciona Cross-vCenter NSX

En un entorno de Cross-vCenter NSX, puede haber varias instancias de vCenter Server, cada una emparejado con su propia instancia de NSX Manager. A una instancia de NSX Manager se le asigna el rol de instancia principal y a las otras se les asigna el rol de instancias secundarias.

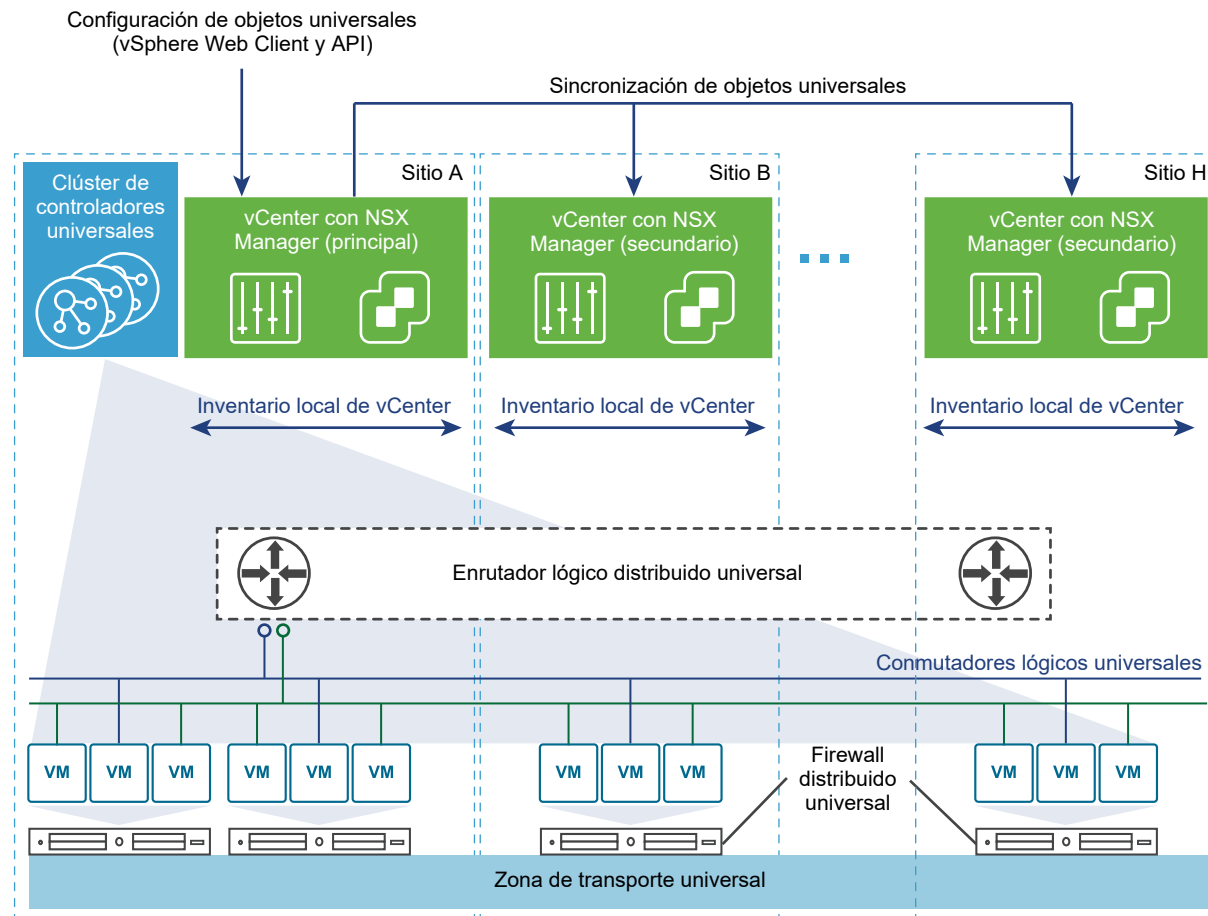
La instancia principal de NSX Manager se utiliza para implementar un clúster de controladoras universales que proporciona el plano de control al entorno de Cross-vCenter NSX. Las instancias secundarias de NSX Manager no tienen su propio clúster de controladoras.

La instancia principal de NSX Manager puede crear objetos universales, como conmutadores lógicos universales. Estos objetos se sincronizan con las instancias secundarias de NSX Manager mediante el servicio de sincronización universal de NSX. Puede ver los objetos desde las instancias secundarias de NSX Manager, pero no puede editarlos. Debe utilizar la instancia principal de NSX Manager para administrar objetos universales. La instancia principal de NSX Manager puede utilizarse para configurar cualquiera de las instancias secundarias de NSX Manager en el entorno.

En las instancias principales y secundarias de NSX Manager, se pueden crear objetos locales para el entorno específico de vCenter NSX, como los conmutadores lógicos y los enrutadores lógicos (distribuidos). Existirán solo en el entorno de vCenter NSX en el que se crearon. No estarán visibles en otras instancias de NSX Manager del entorno de Cross-vCenter NSX.

A las instancias de NSX Manager se les puede asignar el rol independiente. Esto equivale a los entornos previos a NSX 6.2 con una única instancia de NSX Manager y vCenter. Una instancia de NSX Manager independiente no puede crear objetos universales.

**Nota** Si cambia el rol de una instancia principal de NSX Manager a una independiente y existen objetos universales en el entorno de NSX, se asignará el rol de tránsito a NSX Manager. Los objetos universales se mantienen, pero no pueden cambiarse, así como tampoco pueden crearse otros objetos universales. Se pueden eliminar objetos universales del rol de tránsito. El rol de tránsito solo debe utilizarse de forma temporal, por ejemplo, cuando la instancia de NSX Manager que se cambia es la principal.



## Matriz de compatibilidad de NSX Services en Cross-vCenter NSX

Hay un subconjunto de servicios NSX Services disponibles para la sincronización universal en Cross-vCenter NSX. Los servicios que no están disponibles para la sincronización universal pueden configurarse para su uso local con NSX Manager.

**Tabla 3-1. Matriz de compatibilidad de NSX Services en Cross-vCenter NSX**

NSX Service	Detalles	¿Admite la sincronización de Cross-vCenter NSX ?
Conmutador lógico	Zona de transporte	Sí
	Conmutador lógico	Sí
Puentes de Capa 2		No
Enrutamiento	Enrutador lógico (distribuido)	Sí
	Dispositivo enrutador lógico (distribuido)	No por diseño. Se deben crear dispositivos en cada instancia de NSX Manager si se necesitan varios dispositivos por enrutador lógico universal. Esto permite distintas configuraciones por dispositivo, lo que puede ser necesario en un entorno con salida local configurada.
	Puerta de enlace de servicios NSX Edge	No
Firewall lógico	Firewall distribuido	Sí
	Lista de exclusiones	No
	SpoofGuard	No
	Supervisión de flujo para flujos agregados	No
	Inserción de servicios de red	No
	Firewall de Edge	No
VPN		No
Equilibrador de carga lógico		No
Otros servicios Edge		No
Service Composer		No
Extensibilidad de la red		No
Objetos de seguridad y red	Grupos de dirección IP (conjuntos IP)	Sí
	Grupos de dirección MAC (conjuntos MAC)	Sí
	Grupos de direcciones IP	No

**Tabla 3-1. Matriz de compatibilidad de NSX Services en Cross-vCenter NSX (continuación)**

NSX Service	Detalles	¿Admite la sincronización de Cross-vCenter NSX ?
	Grupos de seguridad	Sí, pero la configuración de pertenencia a grupos varía de los grupos de seguridad universal a los de seguridad no universal. Consulte "Crear un grupo de seguridad" (Create a Security Group) en la <i>Guía de administración de NSX</i> para obtener más detalles.
	Servicios	Sí
	Grupos de servicio	Sí
Etiquetas de seguridad		Sí
Puerta de enlace de hardware (también conocida como el VTEP de hardware)		No. Consulte "Configurar una puerta de enlace de hardware" (Hardware Gateway Sample Configuration) en la <i>Guía de administración de NSX</i> para obtener más detalles.

## Clúster de controladoras universal

Cada entorno de Cross-vCenter NSX tiene un clúster de controladoras universal asociado con la instancia de NSX Manager principal. Las instancias de NSX Manager secundarias no tienen clúster de controladoras.

Dado que el clúster de controladoras universal es el único clúster de controladoras para el entorno de Cross-vCenter NSX, mantiene información sobre los conmutadores lógicos universales y los enrutadores lógicos universales al igual que sobre los conmutadores lógicos y los enrutadores lógicos que son locales en un par de NSX de vCenter.

Para evitar cualquier superposición de los identificadores de objetos, se mantienen grupos de identificadores distintos para los objetos universales y los objetos locales.

## Zona de transporte universal

En un entorno de Cross-vCenter NSX, puede haber solo una zona de transporte universal.

La zona de transporte universal se crea en la instancia de NSX Manager principal y se sincroniza en las instancias de NSX Manager secundarias. Los clústeres que deben participar en redes lógicas universales deben agregarse a la zona de transporte universal desde las instancias de NSX Manager correspondientes.

## Conmutadores lógicos universales

Los conmutadores lógicos universales permiten que las redes de Capa 2 abarquen varios sitios.

Al crear un conmutador lógico en una zona de transporte universal, se crea un conmutador lógico universal. Este conmutador está disponible en todos los clústeres de la zona de transporte universal. La zona de transporte universal puede incluir clústeres en cualquier instancia de vCenter del entorno de Cross-vCenter NSX.

El grupo de identificadores de segmentos se utiliza para asignar VNI a los conmutadores lógicos y el grupo de identificadores de segmentos universales se utiliza para asignar VNI a los conmutadores lógicos universales. Estos grupos no deben superponerse.

Debe utilizar un enrutador lógico universal para efectuar el enrutamiento entre los conmutadores lógicos universales. Si necesita realizar un enrutamiento entre un conmutador lógico universal y un conmutador lógico, debe utilizar una puerta de enlace de servicios Edge.

## Enrutadores lógicos (distribuidos) universales

Los enrutadores lógicos (distribuidos) universales ofrecen administración centralizada y una configuración de enrutamiento que se puede personalizar en el nivel del enrutador lógico universal, el clúster o el host.

Cuando crea un enrutador lógico universal, debe elegir si desea habilitar la salida local, dado que esto no se puede modificar después de la creación. La salida local permite controlar las rutas que se proporcionan a los hosts ESXi según un identificador, el identificador de región.

A cada instancia de NSX Manager se le asigna un identificador de región, que está establecido en el UUID de NSX Manager de forma predeterminada. Puede anular el identificador de región en los niveles siguientes:

- Enrutador lógico universal
- Clúster
- Host ESXi

Si no habilita la salida local, el identificador de región se omite y todos los hosts ESXi conectados al enrutador lógico universal reciben las mismas rutas. Habilitar o no la salida local en un entorno de Cross-vCenter NSX es una decisión de diseño, pero no es necesaria para todas las configuraciones de Cross-vCenter NSX.

## Reglas de firewall universal

El firewall distribuido en un entorno de Cross-vCenter NSX permite la administración centralizada de las reglas que aplican a todas las instancias de vCenter Server del entorno. Es compatible con Cross-vCenter vMotion, lo que permite mover cargas de trabajo o máquinas virtuales de una instancia de vCenter Server a otra y extender sin problemas la seguridad del centro de datos definido por software.

A medida que el centro de datos necesita escalar horizontalmente, es posible que la instancia de vCenter Server existente no escale en el mismo nivel. Esto puede requerir que se mueva un conjunto de aplicaciones a hosts más nuevos administrados por otra instancia de vCenter Server. O quizás se deban mover las aplicaciones de la etapa de copias intermedias a producción en un entorno donde los

servidores de copias intermedias sean administrados por una instancia de vCenter Server y los servidores de producción, por otra instancia de vCenter Server. El firewall distribuido es compatible con estas situaciones de Cross-vCenter vMotion, dado que replica las directivas de firewall que se definen para la instancia de NSX Manager principal en hasta siete instancias de NSX Manager secundarias.

Desde la instancia principal de NSX Manager, puede crear secciones de reglas de firewall distribuido marcadas para la sincronización universal. Puede crear más de una sección universal de reglas de Capa 2 y más de una sección universal de reglas de Capa 3. Las secciones universales siempre se muestran en la parte superior de las instancias principal y secundarias de NSX Manager. Estas secciones y sus reglas se sincronizan en todas las instancias de NSX Manager secundarias del entorno. Las reglas en otras secciones siguen siendo locales en la instancia de NSX Manager adecuada.

Las características de firewall distribuido siguientes no son compatibles en un entorno de Cross-vCenter NSX.

- Lista de exclusiones
- SpoofGuard
- Supervisión de flujo para flujos agregados
- Inserción de servicios de red
- Firewall de Edge

Service Composer no es compatible con la sincronización universal, por lo que no es posible utilizarlo para crear reglas de firewall distribuido en la sección universal.

## Objetos de seguridad y red universal

Puede crear objetos de seguridad y red personalizados para utilizarlos en las reglas de firewall distribuido en la sección universal.

Los grupos de seguridad universal (Universal Security Groups, USG) pueden tener los elementos siguientes:

- Conjuntos de direcciones IP universales
- Conjuntos de direcciones MAC universales
- Grupos de seguridad universales
- Etiquetas de seguridad universales
- Criterios dinámicos

Los objetos de seguridad y redes universales se crean, eliminan y actualizan únicamente en la instancia principal de NSX Manager, pero se pueden leer en la instancia secundaria de NSX Manager. El servicio de sincronización universal sincroniza los objetos universales en distintas instancias de vCenter de forma inmediata y bajo petición mediante el uso de la sincronización forzada.

Los grupos de seguridad universal se utilizan en dos tipos de implementación: múltiples entornos cross-vCenter NSX activos e implementaciones en espera activas de cross-vCenter NSX, donde un sitio está activo en un momento determinado y el resto se encuentra en espera. Solo las implementaciones en espera activas pueden tener grupos de seguridad universales con pertenencia dinámica basada en la pertenencia estática del nombre de la máquina virtual en función de la etiqueta de seguridad universal. Una vez que se crea un grupo de seguridad universal, este ya no se puede editar para habilitar o deshabilitar la funcionalidad de escenario en espera activo. La pertenencia se define mediante los objetos incluidos, no se pueden utilizar los objetos excluidos.

Los grupos de seguridad universales no se pueden crear desde Service Composer. Los grupos de seguridad creados desde Service Composer son locales para esa instancia de NSX Manager.

## Topologías de Cross-vCenter NSX

Se puede implementar Cross-vCenter NSX en un solo sitio físico o en varios sitios.

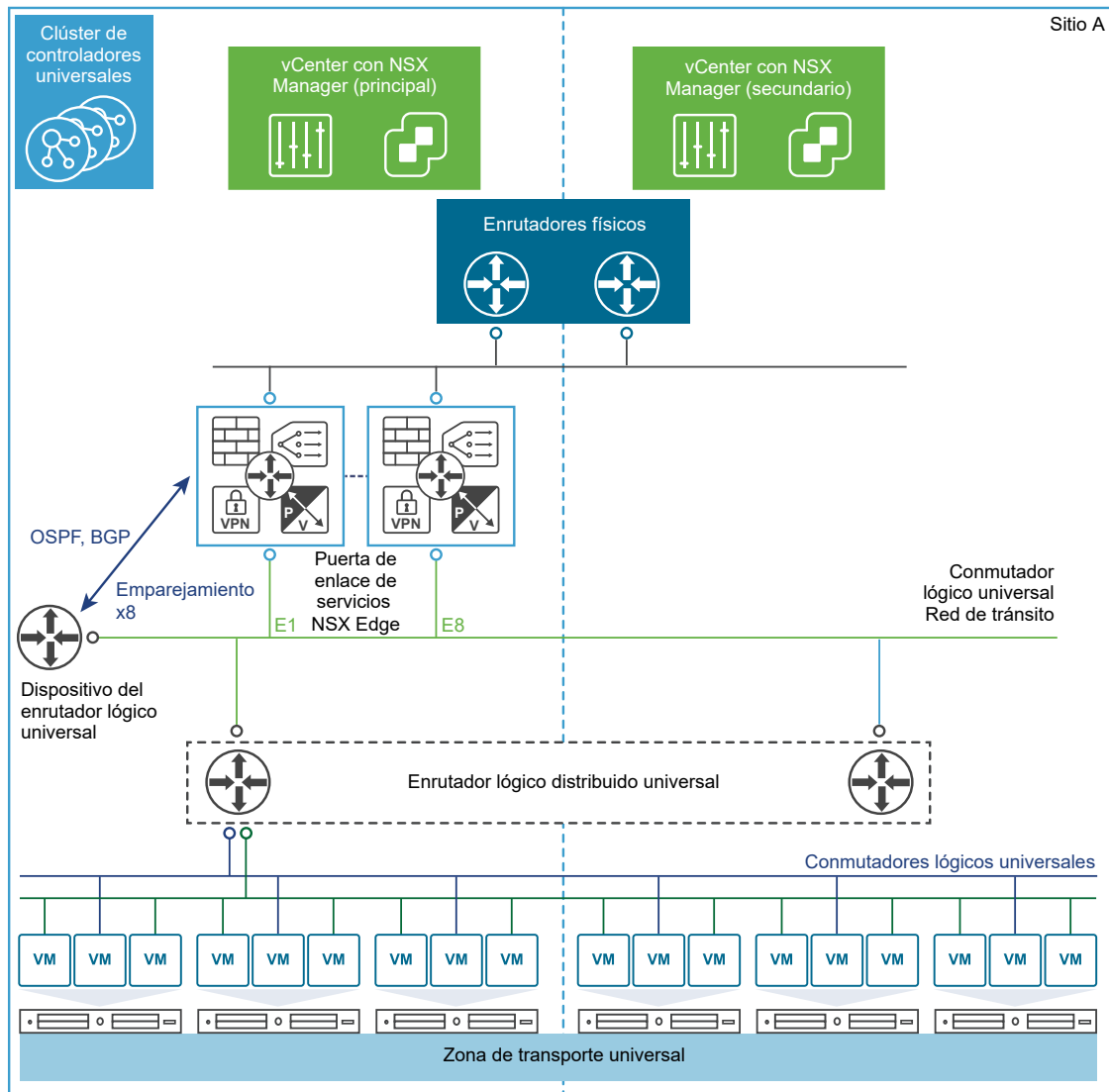
### Cross-vCenter NSX de varios sitios y de un solo sitio

Un entorno de Cross-vCenter NSX permite utilizar los mismos conmutadores lógicos y otros objetos de red en varias instalaciones de vCenter NSX. Las instancias de vCenter pueden encontrarse en el mismo sitio o en sitios diferentes.

Independientemente de que el entorno de Cross-vCenter NSX se encuentre en un solo sitio o atraviese varios sitios, se puede utilizar una configuración similar. Estas dos topologías de ejemplo consisten en lo siguiente:

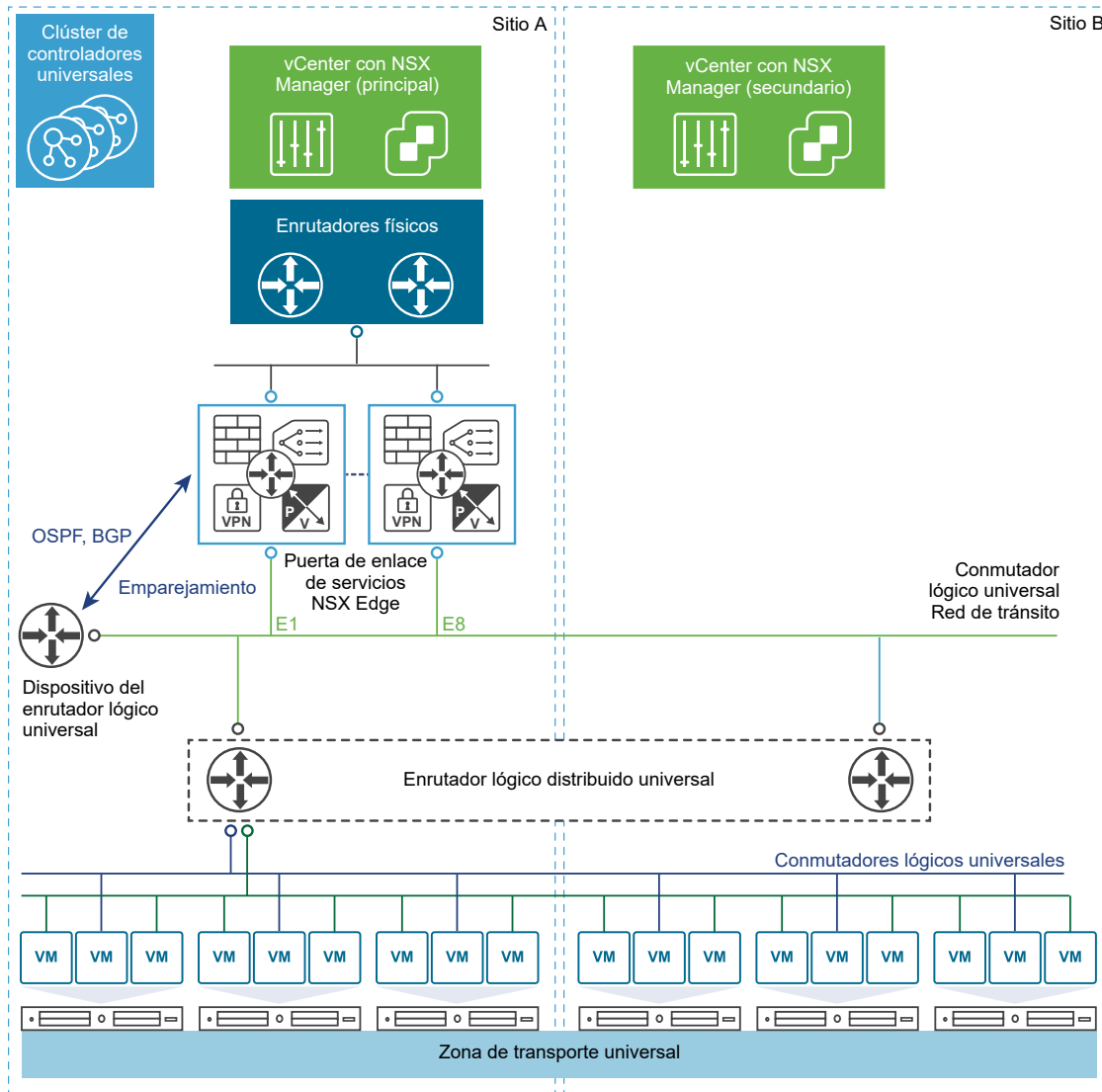
- Una zona de transporte universal que incluye todos los clústeres del sitio o de los sitios.
- Conmutadores lógicos universales asociados a la zona de transporte universal. Se utilizan dos conmutadores lógicos universales para conectar las máquinas virtuales y se utiliza uno como red de tránsito para el vínculo superior del enrutador.
- Se agregan máquinas virtuales a los conmutadores lógicos universales.
- Un enrutador lógico universal con un dispositivo NSX Edge para permitir el enrutamiento dinámico. El dispositivo de enrutamiento lógico universal tiene interfaces internas en los conmutadores lógicos universales de la máquina virtual y una interfaz de vínculo superior en el conmutador lógico universal de la red de tránsito.
- Puertas de enlace de servicios Edge (ESG) conectadas a la red de tránsito y la red física del enrutador de salida.

### Figura 3-1. Cross-vCenter NSX en un solo sitio





**Figura 3-2. Cross-vCenter NSX que abarca dos sitios**

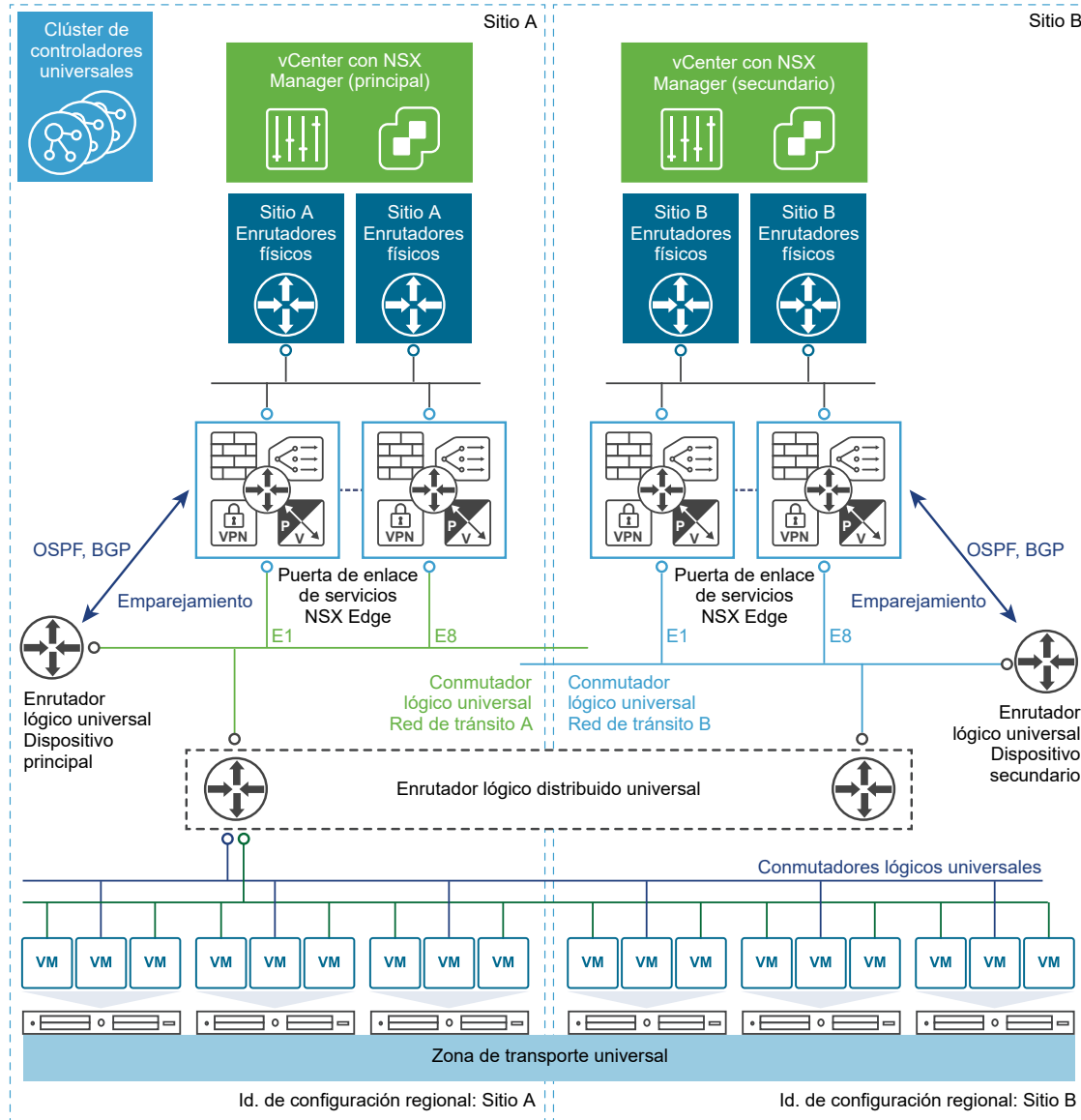


## Salida local

Todos los sitios de un entorno de Cross-vCenter NSX de varios sitios pueden utilizar los mismos enrutadores físicos para el tráfico de salida. No obstante, si es necesario personalizar las rutas de salida, debe habilitarse la característica de salida local al crear el enrutador lógico universal.

La salida local le permite personalizar las rutas en el nivel del enrutador lógico universal, del clúster o del host. Este ejemplo de un entorno de Cross-vCenter NSX en varios sitios tiene la salida local habilitada. Las puertas de enlace de servicios Edge (ESG) en cada sitio tienen una ruta predeterminada que envía tráfico saliente a través de los enrutadores físicos del sitio. El enrutador lógico universal está configurado con dos dispositivos, uno en cada sitio. Los dispositivos conocen las rutas de las ESG de su sitio. Las rutas conocidas se envían al clúster universal de controladoras. Dado que la salida local está habilitada,

el identificador de configuración regional del sitio se asocia con esas rutas. El clúster universal de controladoras envía a los hosts rutas con identificadores de configuración regional coincidentes. Las rutas conocidas del dispositivo del sitio A se envían a los hosts del sitio A y las rutas conocidas del dispositivo del sitio B se envían a los hosts del sitio B.



## Modificar los roles de NSX Manager

NSX Manager puede tener el rol principal, el rol secundario o el rol independiente. El software de sincronización especial se ejecuta en la instancia de NSX Manager principal y sincroniza todos los objetos universales con las instancias de NSX Manager secundarias.

Es importante comprender qué sucede cuando se cambia el rol de NSX Manager.

**Establecer como principal (Set as primary)**

Esta operación establece el rol de una instancia de NSX Manager como principal e inicia el software de sincronización. Se produce un error en esta operación si NSX Manager ya es una instancia principal o una secundaria.

**Establecer como independiente (desde secundaria) (Set as standalone [from secondary])**

Esta operación establece el rol de NSX Manager en modo de tránsito o independiente. Es posible que se produzca un error en esta operación si NSX Manager ya tiene el rol independiente.

**Establecer como independiente (desde principal) (Set as standalone [from primary])**

Esta operación restablece la instancia de NSX Manager principal al modo de tránsito o independiente, detiene el software de sincronización y cancela el registro de todas las instancias de NSX Manager secundarias. Es posible que se produzca un error en esta operación si NSX Manager ya es una instancia independiente o si no es posible comunicarse con las instancias de NSX Manager secundarias.

**Desconectar de principal (Disconnect from primary)**

Cuando se ejecuta esta operación en una instancia de NSX Manager secundaria, esta instancia se desconecta de forma unilateral de la instancia de NSX Manager principal. Se debe utilizar esta operación si la instancia de NSX Manager principal tuvo un error irreparable y si se desea registrar la instancia de NSX Manager secundaria en una nueva instancia principal. Si vuelve a aparecer la instancia NSX Manager principal original, su base de datos sigue mostrando la instancia de NSX Manager secundaria como registrada. Para solucionar este problema, incluya la opción **forzar** (force) cuando desconecte o cancele el registro de la instancia secundaria de la instancia principal original. La opción **forzar** (force) quita la instancia de NSX Manager secundaria de la base de datos de la instancia de NSX Manager principal original.

# Preparación para la instalación

# 4

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](#)
- [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 4-1. 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 4-1. 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 4-2. 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](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"> <li>■ ESXi 6.0 o versiones posteriores</li> <li>■ Clústeres de host que cuentan con NSX 6.2 o VIB posteriores</li> </ul>

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 4-3. 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 4-3. 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	
Cliente 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 4-3. 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.

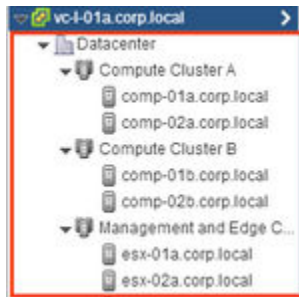
Se puede asociar un solo host a varios VDS. Un solo VDS puede abarcar varios hosts en varios clústeres. Para cada clúster de hosts que participará en NSX, se deben asociar todos los hosts del clúster a un VDS común.

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

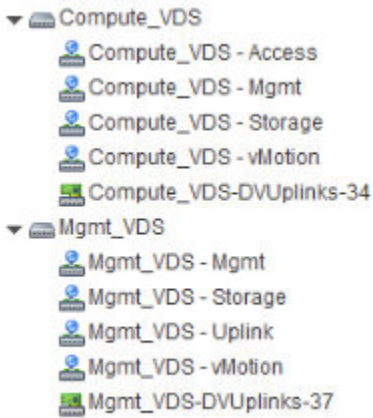
La pantalla siguiente muestra cómo aparecen estos clústeres en vCenter.



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.

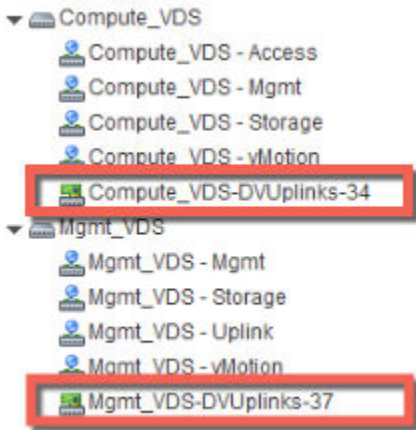
Por ejemplo, la pantalla siguiente muestra cómo aparecen estos puertos y conmutadores distribuidos en vCenter.



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>.

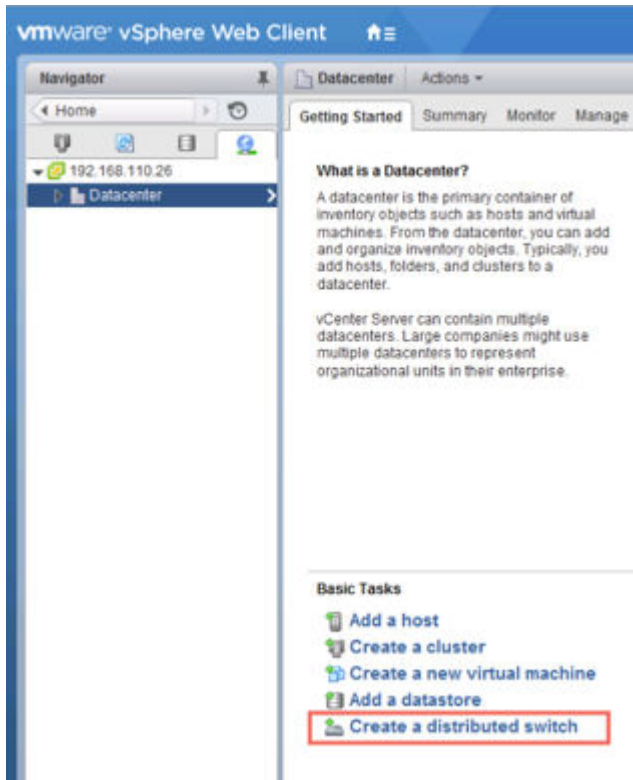
### Requisitos previos

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 asígnale 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.

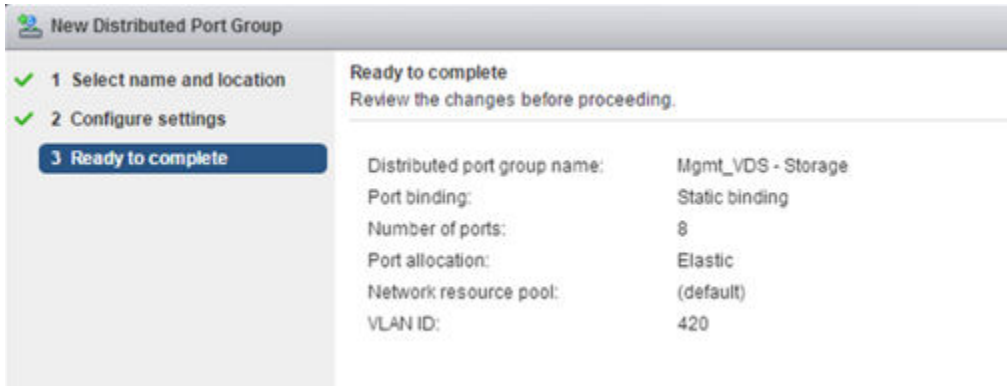
- 5 (opcional) Una vez que finaliza el asistente Nuevo conmutador distribuido (New Distributed Switch), edite la configuración del grupo de puertos predeterminado para colocarlo en la VLAN correcta para el tráfico de administración.

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.

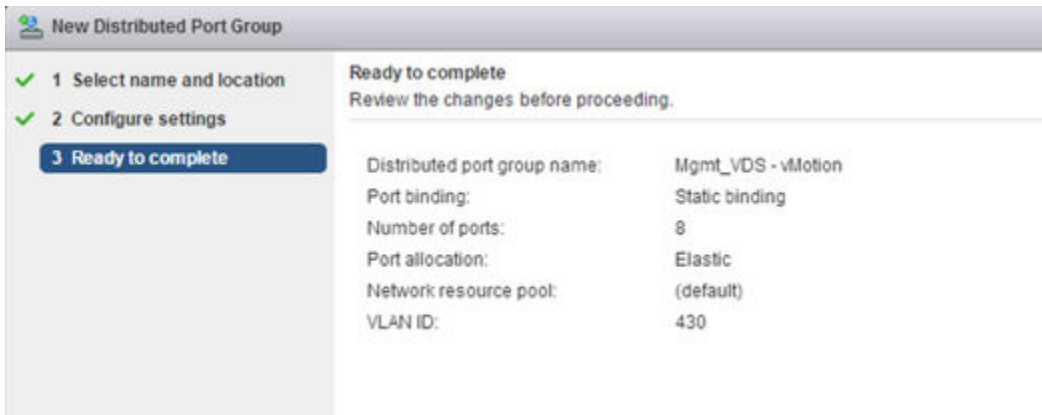
- 6 Una vez que finaliza el asistente Nuevo conmutador distribuido (New Distributed Switch), haga clic con el botón derecho en el conmutador distribuido y seleccione **Nuevo grupo de puertos distribuidos** (New Distributed Port Group).

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.

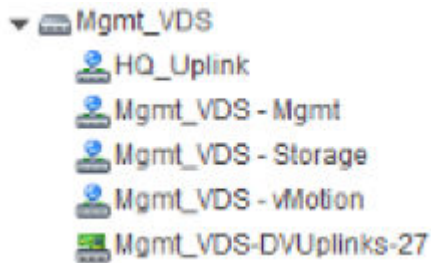
Configuración de grupo de ejemplo para almacenamiento.



Configuración de grupo de ejemplo para el tráfico vMotion.

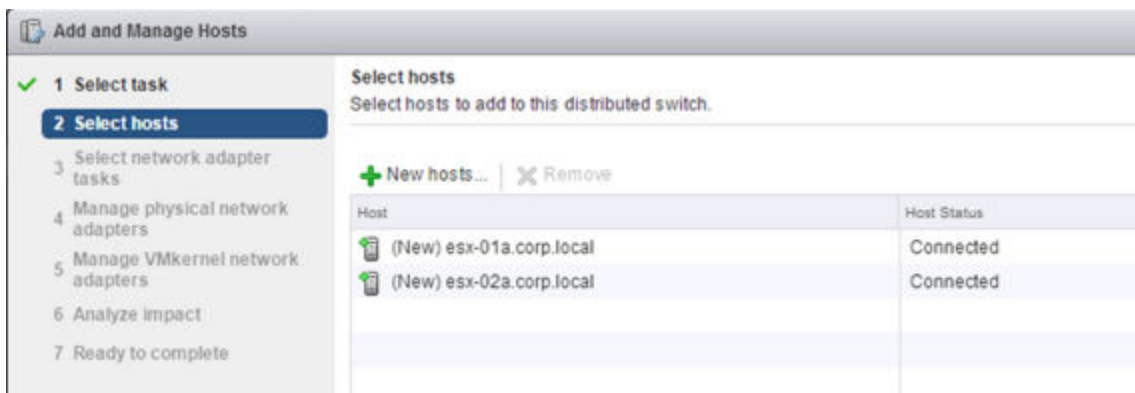


La configuración terminada del conmutador distribuido y de los grupos de puertos se ve así.

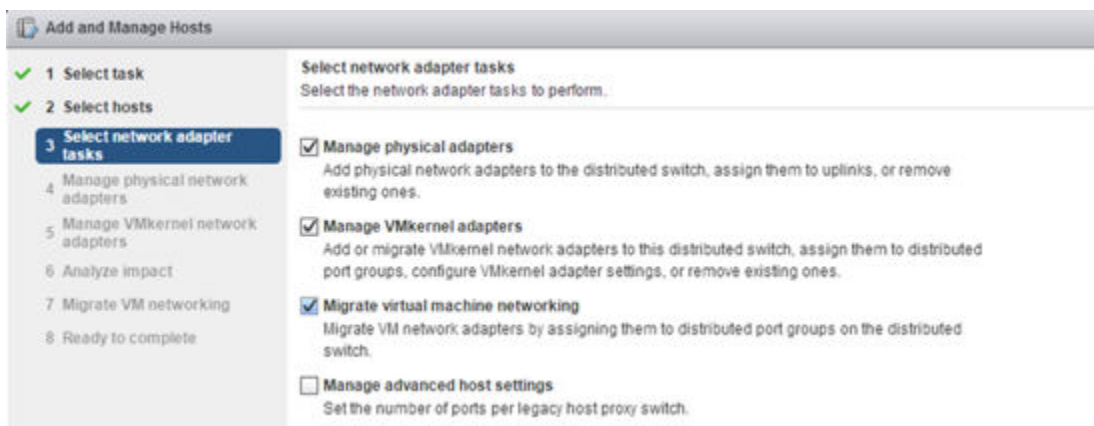


- 7 Haga clic con el botón derecho en el conmutador distribuido, seleccione **Agregar y administrar hosts** (Add and Manage Hosts) y, a continuación, **Agregar hosts** (Add Hosts).

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.



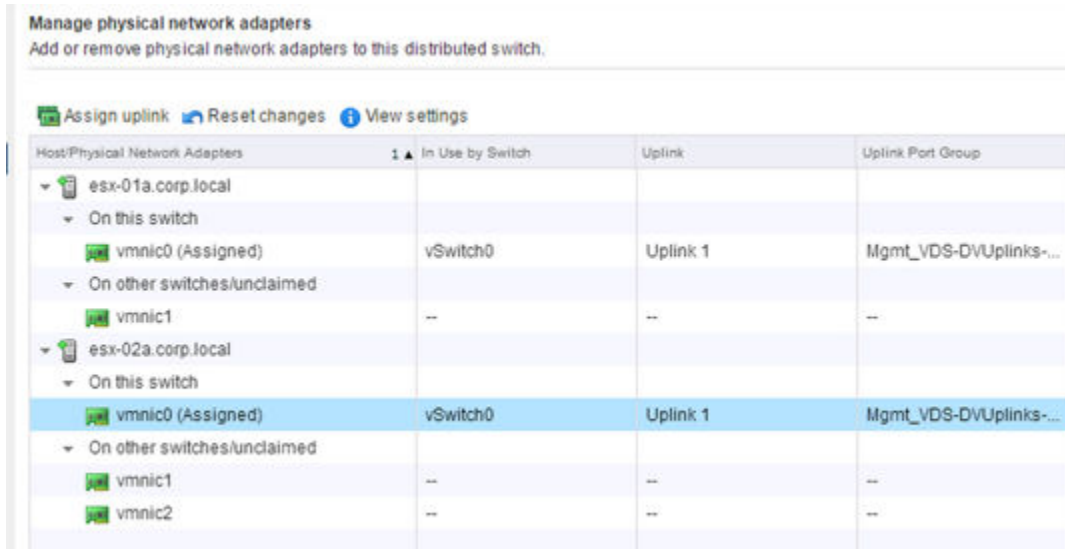
- 8 Seleccione las opciones para migrar los adaptadores físicos, los adaptadores VMkernel y las redes de la máquina virtual.



- 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.

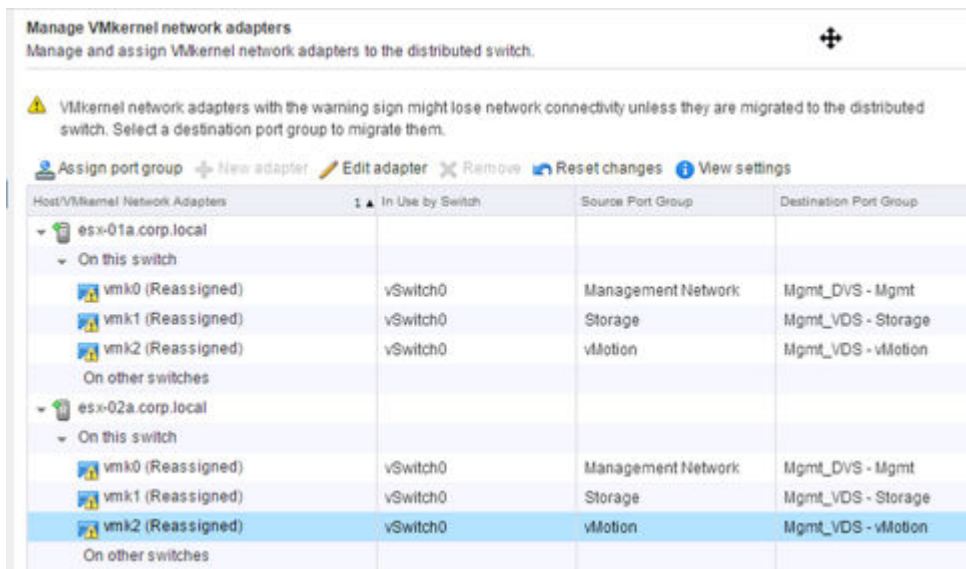
Por ejemplo, esta pantalla muestra dos hosts con sus vínculos superiores vmnic0 configurados para migrar desde sus respectivos conmutadores vSwitch estándar hacia el grupo de puertos distribuidos Mgmt\_VDS-DVUplinks, un puerto troncal que puede transportar cualquier identificador de VLAN.





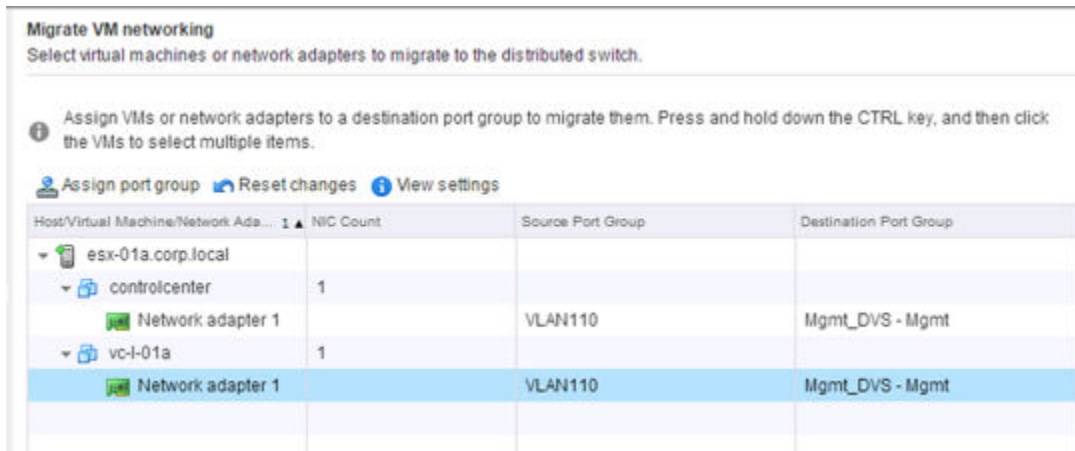
- 10 Seleccione un adaptador de red VMkernel y haga clic en **Asignar grupo de puertos** (Assign port group). Repita este paso con todos los adaptadores de red de todos los hosts que vaya a conectar al conmutador vSwitch distribuido.

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

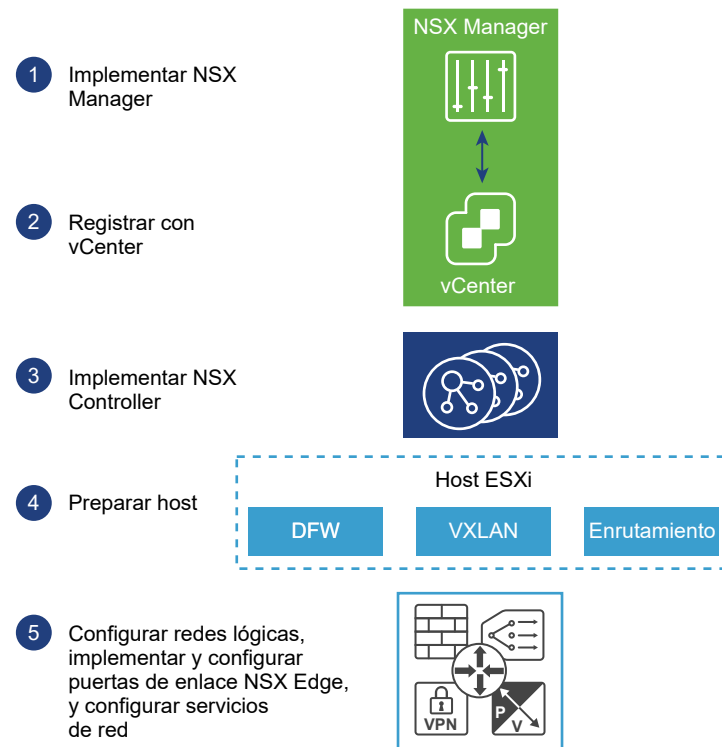
```

## Pasos siguientes

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

# 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.

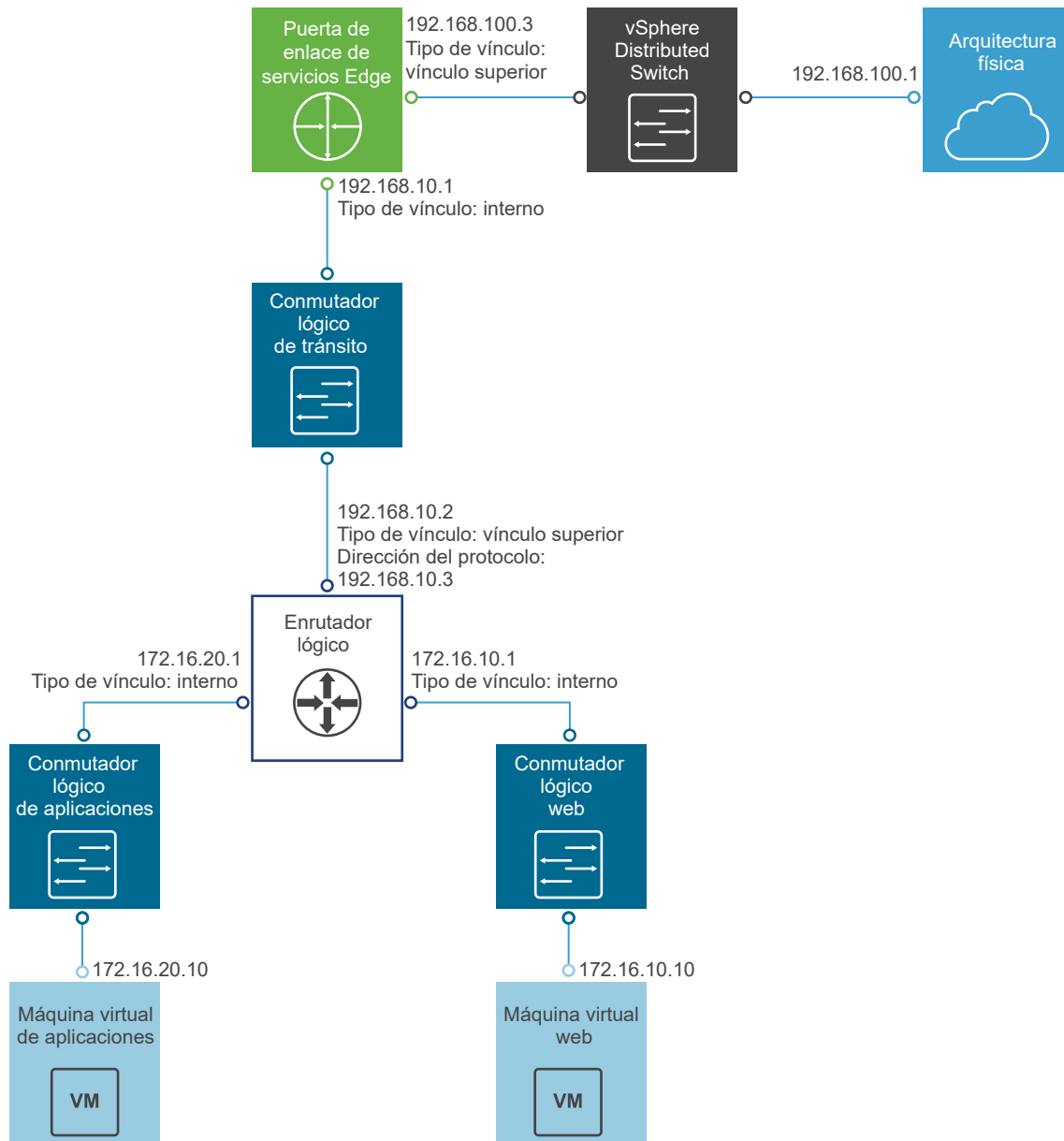


En la primera parte del proceso, se debe implementar una plantilla de OVF/OVA de NSX Manager y comprobar que NSX Manager tenga conectividad completa con las interfaces de administración de los hosts ESX que administrará. En el siguiente paso, NSX Manager y una instancia de vCenter deben vincularse entre 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.

# Tareas para las instancias de NSX Manager principales y secundarias

## 5

En un entorno de Cross-vCenter, puede haber una instancia de NSX Manager principal y hasta siete instancias de NSX Manager secundarias. Algunas tareas de instalación se realizan en cada instancia de NSX Manager, ya sea que se convierta en una instancia de NSX Manager principal o en una secundario.

Este capítulo incluye los siguientes temas:

- [Instalar NSX Manager Virtual Appliance](#)
- [Configurar inicio de sesión único](#)
- [Registrar vCenter Server con NSX Manager](#)
- [Configurar un servidor syslog para NSX Manager](#)
- [Instalar y asignar licencia de NSX for vSphere](#)
- [Excluir las máquinas virtuales de la protección de firewall](#)

## Instalar NSX Manager Virtual Appliance

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

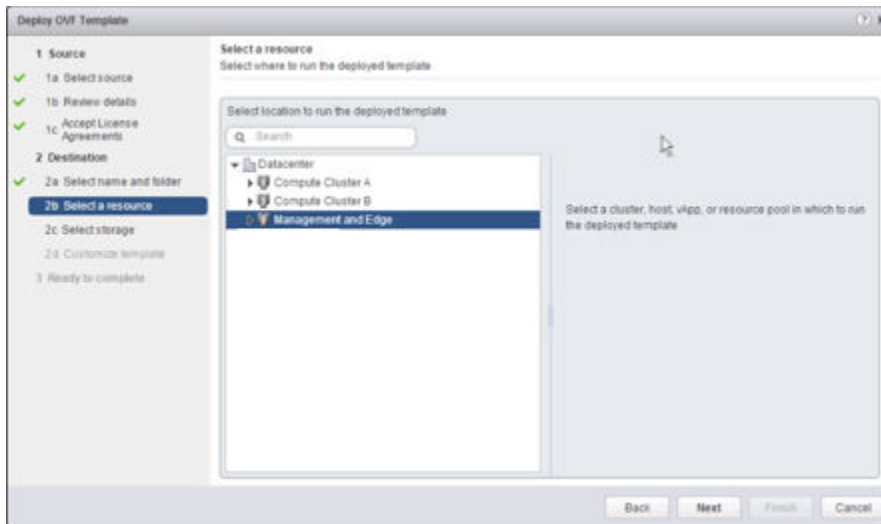
- 1 Busque el archivo de dispositivo de virtualización abierto (OVA) de NSX Manager.  
Puede copiar la URL de descarga, o bien descargar el archivo OVA en el equipo.
- 2 En Firefox, abra vCenter.
- 3 Seleccione **Máquinas virtuales y plantillas** (VMs and Templates), haga clic con el botón secundario 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.

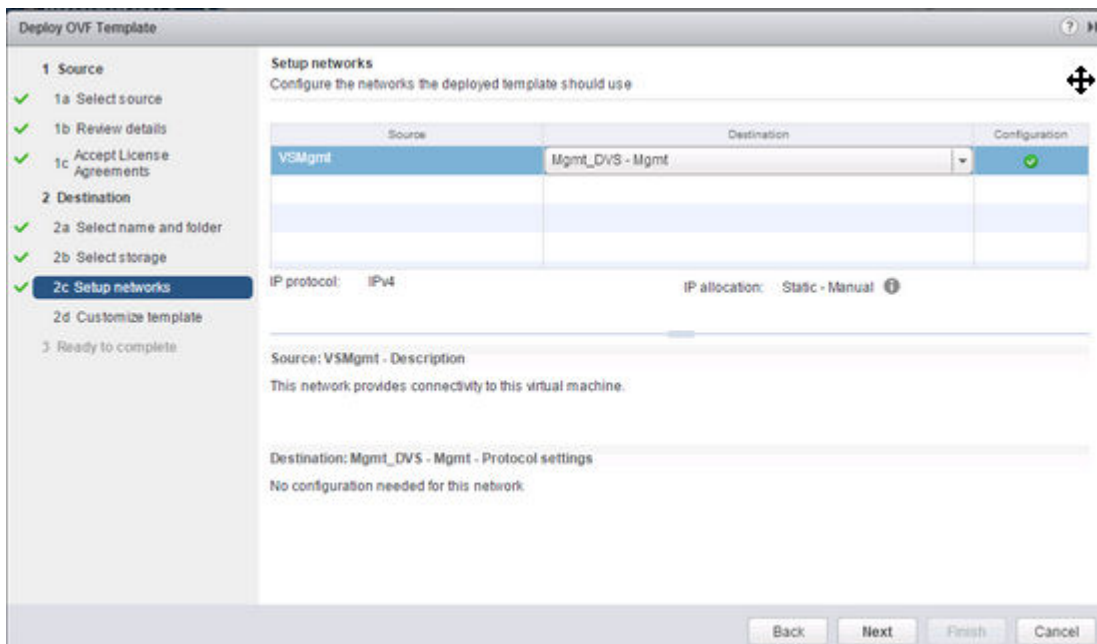
---

- 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:



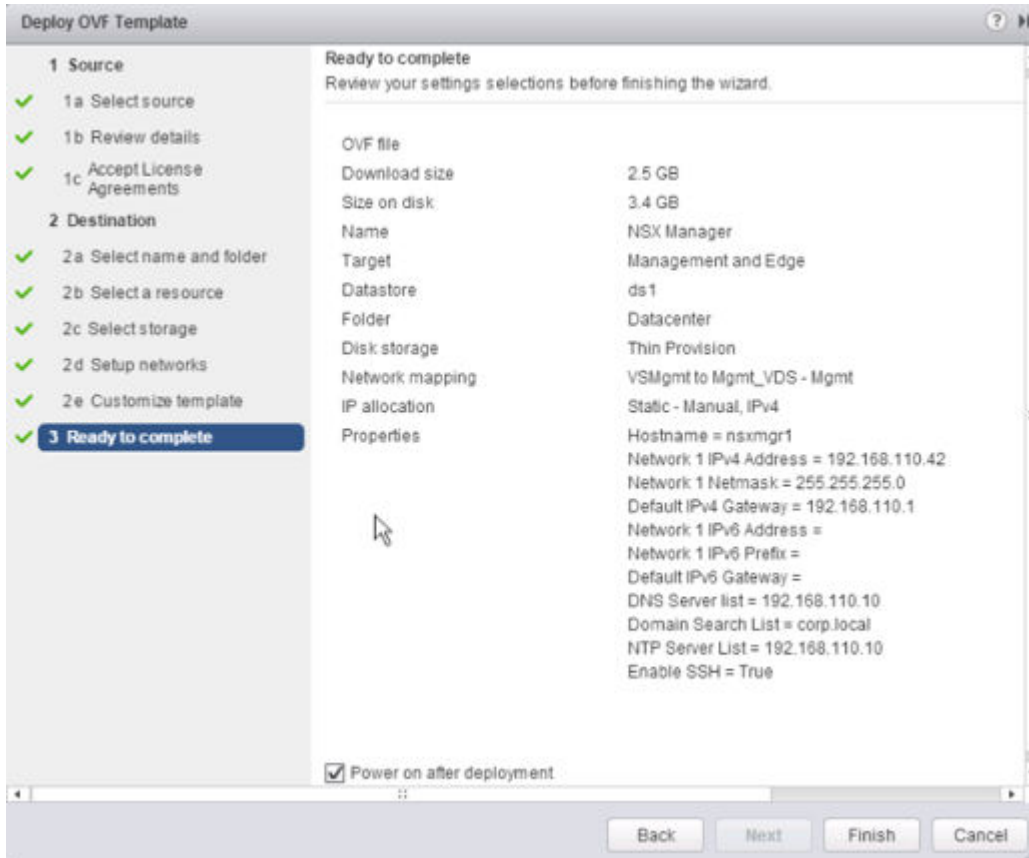
- 9 Cambie el formato de disco virtual a **Aprovisionamiento grueso** (Thick Provision) y seleccione el almacén de datos de destino para los discos virtuales y los archivos de configuración de la máquina virtual.
- 10 Seleccione el grupo de puertos de NSX Manager.

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.

## Configurar inicio de sesión único

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 explorador web, desplácese hasta la GUI del dispositivo NSX Manager en <https://<nsx-manager-ip>> o <https://<nsx-manager-hostname>> e inicie sesión como administrador con la contraseña que configuró al instalar NSX Manager.

- 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*.

## Registrar vCenter Server con NSX Manager

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 un NSX Manager existente, en primer lugar debe eliminar toda la configuración de NSX 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.

### 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 explorador web, desplácese hasta la GUI del dispositivo NSX Manager en <https://<nsx-manager-ip>> o <https://<nsx-manager-hostname>> e inicie sesión como administrador con la contraseña que configuró al instalar NSX Manager.

- 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.

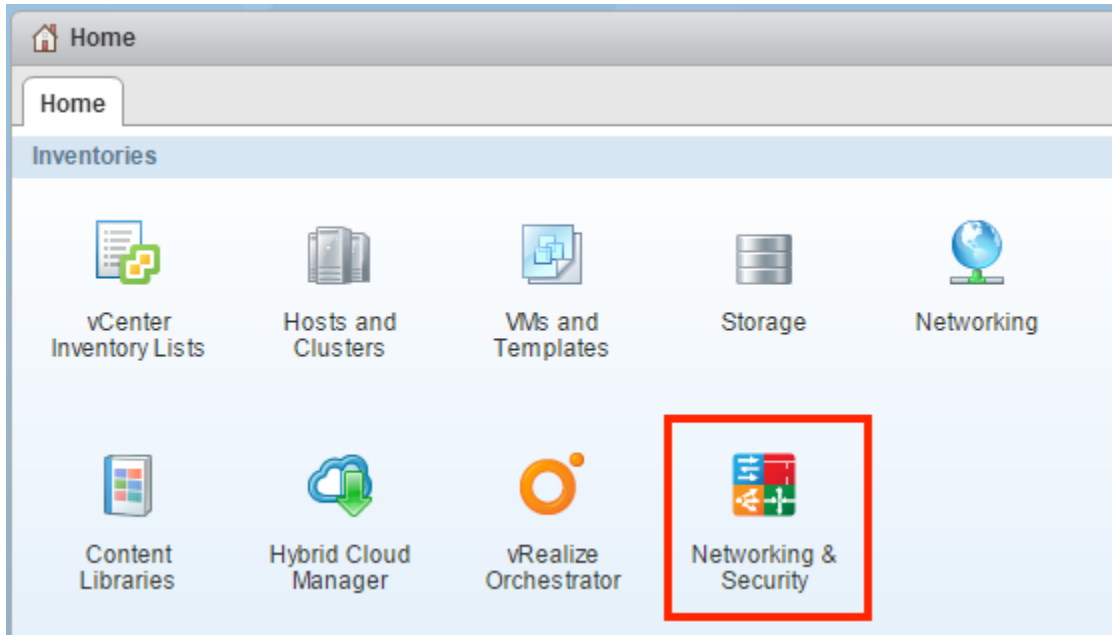
Esta opción le permite introducir una dirección IP alternativa para NSX Manager. No se recomienda poner NSX Manager detrás de un firewall de este tipo.

- 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 un servidor syslog para NSX Manager

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.

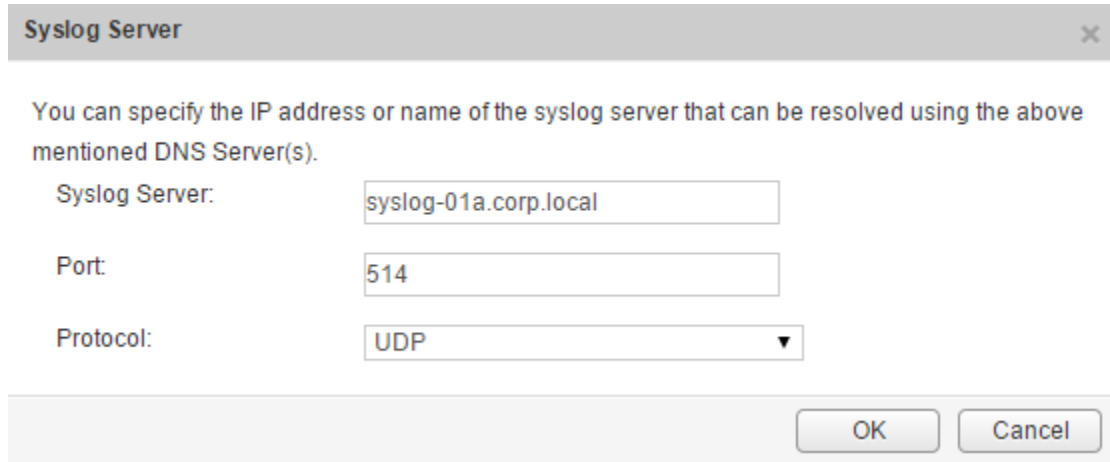
En un explorador web, desplácese hasta la GUI del dispositivo NSX Manager en <https://<nsx-manager-ip>> o <https://<nsx-manager-hostname>> e inicie sesión como administrador con la contraseña que configuró al instalar NSX Manager.

- 2 En la página de inicio, haga clic en **Administrar configuración de dispositivos (Manage Appliance Settings) > General (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

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>.

## Excluir las máquinas virtuales de la protección de firewall

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.

# Configurar la instancia principal de NSX Manager

## 6

Hay una sola instancia principal de NSX Manager en un entorno de Cross-vCenter NSX. Seleccione qué instancia de NSX Manager será la principal y realice las tareas de configuración para completar la instalación de NSX, asignar el rol principal a NSX Manager y crear objetos universales.

La instancia principal de NSX Manager se utiliza para implementar un clúster de controladoras universales que proporciona el plano de control al entorno de Cross-vCenter NSX. Las instancias secundarias de NSX Manager no tienen su propio clúster de controladoras.

Este capítulo incluye los siguientes temas:

- [Implementar NSX Controller en la instancia de NSX Manager principal](#)
- [Preparar hosts en la instancia de NSX Manager principal](#)
- [Configurar VXLAN desde la instancia principal de NSX Manager](#)
- [Asignar un grupo de ID de segmentos y la dirección de multidifusión en el NSX Manager principal](#)
- [Asignar función principal a NSX Manager](#)
- [Asignar un grupo universal de ID de segmentos y la dirección de multidifusión en el NSX Manager principal](#)
- [Agregar una zona de transporte universal en la instancia de NSX Manager principal](#)
- [Agregar un conmutador lógico universal en la instancia de NSX Manager principal](#)
- [Conectar máquinas virtuales a un conmutador lógico](#)
- [Agregar un enrutador lógico \(distribuido\) universal en la instancia de NSX Manager principal](#)

## Implementar NSX Controller en la instancia de NSX Manager principal

NSX Controller es un sistema avanzado de administración de estado distribuido que proporciona funciones del plano de control para funciones de enrutamiento lógico y conmutación lógica 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. En Cross-vCenter NSX, una vez que se asigna la función

principal a NSX Manager, su clúster de controladores se convierte en el clúster de controladores universal de todo el entorno de Cross-vCenter NSX.

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.

### Requisitos previos

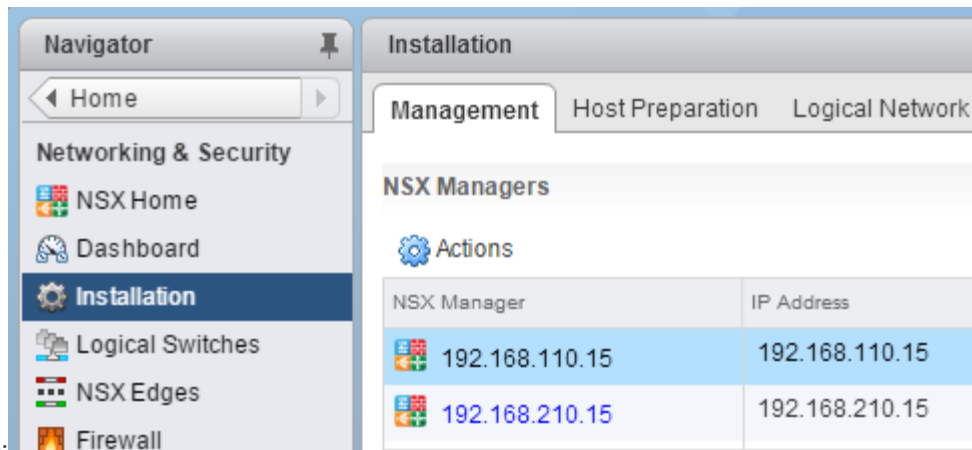
- Antes de implementar las instancias de NSX Controller, debe implementar un dispositivo NSX Manager y registrar vCenter con NSX Manager.
- Determine la configuración del grupo de direcciones IP del clúster de controlador, incluidos la puerta de enlace y el rango de direcciones IP. La configuración de 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 Con vSphere Web Client, inicie sesión en el sistema vCenter Server registrado con el NSX Manager que pasará a ser el principal.

Si los sistemas vCenter Server del entorno cross-vCenter NSX están en Enhanced Linked Mode, puede acceder a cualquier NSX Manager asociado desde todos los sistemas vCenter Server vinculados. Para ello, debe seleccionarlo en el menú desplegable **NSX Manager**.


- 2 Desplácese hasta **Inicio > Redes y seguridad > Instalación** (Home > Networking & Security > Installation) y seleccione la pestaña **Administración** (Management).



Por ejemplo:

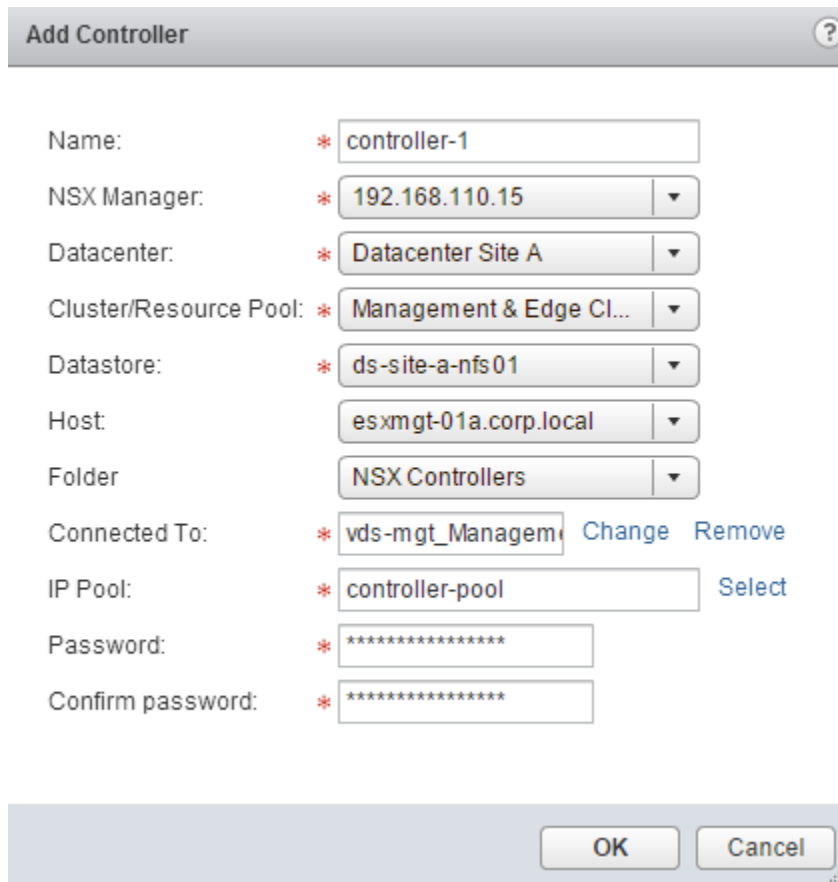
Si los sistemas vCenter Server están en Enhanced Linked Mode, aquí aparecerán todos los NSX Manager asociados.

- 3 En la sección NSX Manager, seleccione el NSX Manager que se convertirá en el primario.

- 4 En la sección de nodos de NSX Controller, haga clic en el icono **Agregar nodo** (Add Node) (  ).
- 5 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.

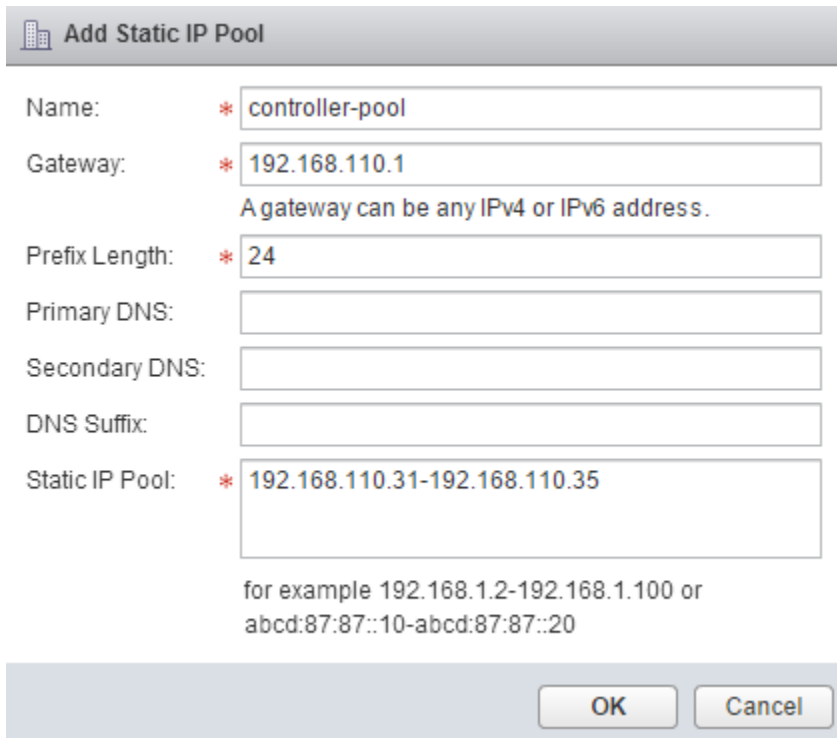
Por ejemplo:



- 6 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

- 7 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

- 8 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*.

## Preparar hosts en la instancia de NSX Manager principal

La preparación de hosts es el proceso por el cual NSX Manager 1) instala módulos de kernel de NSX 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 de NSX. Los módulos de kernel de NSX 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](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](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
```

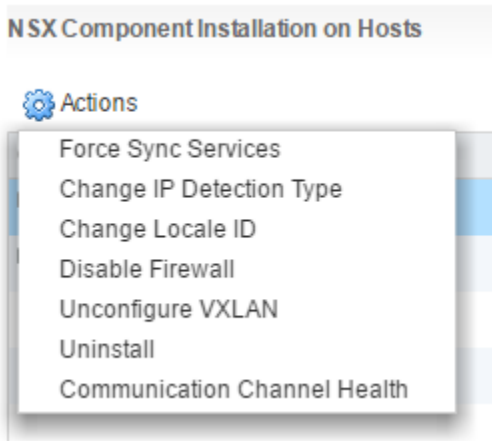
- Compruebe que los hosts puedan resolver el nombre DNS de vCenter Server.
- Compruebe si los hosts pueden conectarse a vCenter Server en el puerto 80.
- Compruebe que la hora de red en vCenter Server y los hosts ESXi esté sincronizada.
- En cada clúster del host que participará en NSX, compruebe que 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.



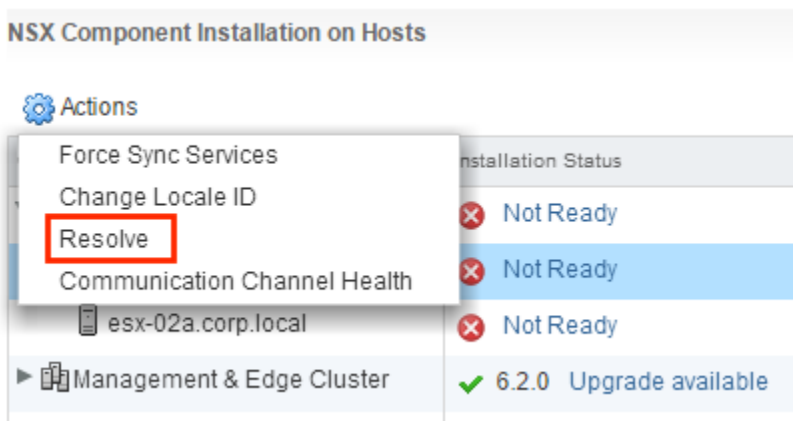
- Si tiene vSphere Update Manager (VUM) instalado en el entorno, debe deshabilitarlo a fin de poder preparar los clústeres para la virtualización de red. Para obtener más información sobre cómo comprobar si VUM está habilitado y cómo deshabilitarlo si fuera necesario, consulte <http://kb.vmware.com/kb/2053782>.
- 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 Con vSphere Web Client, inicie sesión en el sistema vCenter Server registrado con el NSX Manager que pasará a ser el principal.

Si los sistemas vCenter Server del entorno cross-vCenter NSX están en Enhanced Linked Mode, puede acceder a cualquier NSX Manager asociado desde todos los sistemas vCenter Server vinculados. Para ello, debe seleccionarlo en el menú desplegable **NSX Manager**.

- 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"> <li>■ esx-vsip</li> <li>■ esx-vxlan</li> </ul>
6.0 o posterior	6.3.2 o anterior	<ul style="list-style-type: none"> <li>■ esx-vsip</li> <li>■ esx-vxlan</li> </ul>
6.0 o posterior	6.3.3 o posterior	<ul style="list-style-type: none"> <li>■ esx-nsxv</li> </ul>

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.

## Configurar VXLAN desde la instancia principal de NSX Manager

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.

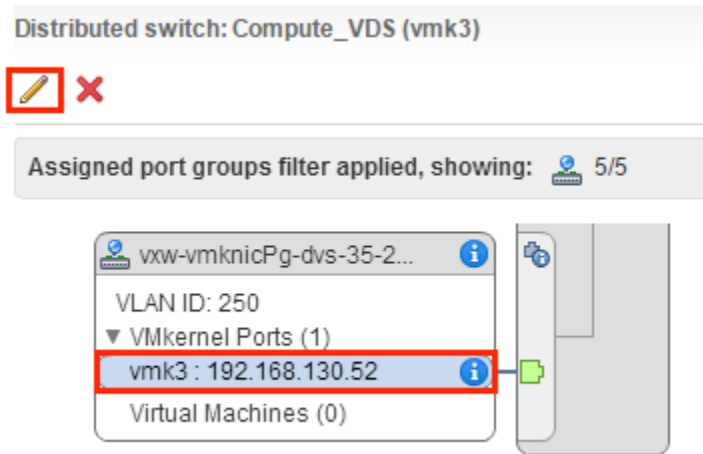
Si desea que una dirección IP específica se asigne a un VTEP, puede 1) utilizar una reserva o una dirección DHCP fija que asigne una dirección MAC a una dirección IP específica en el servidor DHCP o 2) utilizar un grupo de direcciones IP y, a continuación, editar manualmente la dirección IP de VTEP asignada a vmknics en **Hosts y clústeres (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 Con vSphere Web Client, inicie sesión en el sistema vCenter Server registrado con el NSX Manager que pasará a ser el principal.  
  
Si los sistemas vCenter Server del entorno cross-vCenter NSX están en Enhanced Linked Mode, puede acceder a cualquier NSX Manager asociado desde todos los sistemas vCenter Server vinculados. Para ello, debe seleccionarlo en el menú desplegable **NSX Manager**.
- 2 Diríjase a **Inicio > Redes y seguridad > Instalación** (Home > Networking & Security > Installation) y seleccione la pestaña **Preparación del host** (Host Preparation).
- 3 Verifique que el NSX Manager adecuado esté seleccionado en el menú desplegable **NSX Manager**.
- 4 Haga clic en **No configurado** (Not Configured) en la columna **VXLAN**.
- 5 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

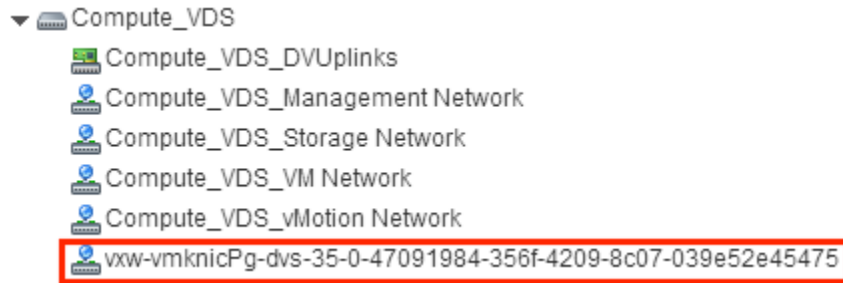
OK Cancel

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 ID de segmentos y la dirección de multidifusión en el NSX Manager principal

Los segmentos de VXLAN se compilan entre los extremos de túnel de VXLAN (VTEP). Cada túnel de VXLAN tiene un identificador de segmento. Debe especificar un grupo de identificadores de segmentos en la instancia de NSX Manager principal para aislar el tráfico de la 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.

Las instancias de NSX Manager en su entorno cross-vCenter NSX deben usar un grupo de identificadores de segmentos que no se superpongan. Además, los grupos de identificadores de segmentos universales no se deben superponer con ningún grupo de identificadores de segmentos en el entorno cross-vCenter NSX. Los VNI que no se superponen se aplican automáticamente en un único entorno de NSX Manager y vCenter. 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 cross-vCenter NSX.

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.

Debe asegurarse de que la dirección o el rango de direcciones de multidifusión especificadas no tengan conflictos con otras direcciones de multidifusión asignadas a cualquier instancia de NSX Manager en el entorno Cross-vCenter NSX.

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 Con vSphere Web Client, inicie sesión en el sistema vCenter Server registrado con el NSX Manager que pasará a ser el principal.  
  
Si los sistemas vCenter Server del entorno cross-vCenter NSX están en Enhanced Linked Mode, puede acceder a cualquier NSX Manager asociado desde todos los sistemas vCenter Server vinculados. Para ello, debe seleccionarlo en el menú desplegable **NSX Manager**.
- 2 Diríjase a **Inicio > Redes y seguridad > Instalación** (Home > Networking & Security > Installation) y seleccione la pestaña **Preparación de redes lógicas** (Logical Network Preparation).
- 3 Verifique que el NSX Manager adecuado esté seleccionado en el menú desplegable **NSX Manager**.
- 4 Haga clic en **Identificador de segmento > Editar** (Segment ID > Edit).
- 5 Introduzca un rango de identificadores de segmentos, por ejemplo, **5000–5999**.
- 6 (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.

## Asignar función principal a NSX Manager

La instancia de NSX Manager principal ejecuta el clúster de controladores. Las instancias de NSX Manager adicionales son secundarias. El clúster de controladores que se implementa mediante la instancia de NSX Manager principal es un objeto compartido y se lo denomina clúster de controladores universal. Las instancias de NSX Manager secundarias importan automáticamente el clúster de controladores universal. Puede haber una instancia de NSX Manager principal y hasta siete instancias de NSX Manager secundarias en un entorno de Cross-vCenter NSX.

Las instancias de NSX Manager tienen alguno de los cuatro roles:

- Principal
- Secundario
- Independiente
- De tránsito

Para ver la función de una instancia de NSX Manager, inicie sesión en la instancia de vCenter vinculada a ella y desplácese hasta **Inicio (Home) > Redes y seguridad (Networking & Security) > Instalación (Installation)** y, a continuación, seleccione la pestaña **Administración (Management)**. La función se muestra en la columna Función (Role) en Instancias de NSX Manager (NSX Managers). Si no se muestra ninguna columna Función (Role), NSX Manager tiene la función independiente.

### Requisitos previos

- La versión de las instancias de NSX Manager (la instancia principal de NSX Manager y las instancias que se asignarán a la función secundaria) debe coincidir.
- Los identificadores de nodo de la instancia principal de NSX Manager y las instancias de NSX Manager que se asignarán a la función secundaria deben estar presentes y ser diferentes. Las instancias de NSX Manager implementadas desde los archivos OVA tienen identificadores de nodo únicos. Una instancia de NSX Manager implementada desde una plantilla (como cuando se convierte una máquina virtual a una plantilla) tendrá el mismo identificador de nodo que la instancia de NSX Manager original que se utilizó para crearla; estas dos instancias de NSX Manager no pueden utilizarse en la misma instalación de Cross-vCenter NSX.

---

**Nota** Puede ver el identificador de nodo de NSX Manager con la siguiente llamada API de REST:

```
GET https://NSX-Manager-IP-Address/api/2.0/services/vsmconfig
```

---

- Cada NSX Manager debe registrarse con un sistema vCenter Server único y distinto.

- Los puertos UDP utilizados para la VXLAN deben ser los mismos para todas las instancias de NSX Manager.

---

**Nota** Puede ver y cambiar el puerto VXLAN usando vSphere Web Client en **Redes y seguridad (Networking & Security) > Instalación (Installation) > Preparación de redes lógicas (Logical Network Preparation)**. Consulte el apartado sobre cómo cambiar el puerto VXLAN en *Guía de administración de NSX*.

---

- Al asignar la función secundaria a un NSX Manager, el sistema de vCenter Server vinculado no debe tener ningún NSX Controller implementado.
- El grupo de identificadores de segmentos de NSX Manager que se va a asignar a la función secundaria no debe superponerse con los grupos de identificadores de segmentos de la instancia de NSX Manager principal ni con el grupo de identificadores de segmentos de otra instancia de NSX Manager secundaria.
- La instancia de NSX Manager a la que se le va a asignar la función secundaria debe tener la función independiente o de tránsito.

#### Procedimiento

- 1 Inicie sesión en la instancia de vCenter vinculada a la instancia de NSX Manager principal con vSphere Web Client.
- 2 Desplácese hasta **Inicio > Redes y seguridad > Instalación** (Home > Networking & Security > Installation) y seleccione la pestaña **Administración** (Management).
- 3 Seleccione la instancia de NSX Manager que desea asignar como principal y haga clic en **Acciones** (Actions). A continuación, haga clic en **Asignar función principal** (Assign Primary Role).

Se le asigna la función principal a la instancia de NSX Manager seleccionada. Los otros NSX Managers del entorno de cross-vCenter NSX ya muestran la función Independiente (Standalone).

## Asignar un grupo universal de ID de segmentos y la dirección de multidifusión en el NSX Manager principal

El grupo de identificadores de segmentos universales especifica un rango de uso cuando se crean segmentos de red lógicos. Las implementaciones de Cross-vCenter NSX utilizan un grupo único de identificadores de segmentos universales para garantizar que los identificadores de red de VXLAN (VNI) de los conmutadores lógicos universales sean coherentes en todas las instancias de NSX Manager secundarias.

El identificador de segmento universal se define una vez en el NSX Manager principal y, a continuación, se sincroniza en todos los NSX Manager secundarios. Tenga en cuenta que el rango de identificadores de segmentos debe ser único en cualquier instancia de NSX Manager que planee utilizar en una implementación de Cross-vCenter NSX. En este ejemplo se utiliza un rango alto para proporcionar escalabilidad en el futuro.

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.

Debe asegurarse de que la dirección o el rango de direcciones de multidifusión especificadas no tengan conflictos con otras direcciones de multidifusión asignadas a cualquier instancia de NSX Manager en el entorno Cross-vCenter NSX.

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 Con vSphere Web Client, inicie sesión en el sistema vCenter Server registrado con el NSX Manager que pasará a ser el principal.

Si los sistemas vCenter Server del entorno cross-vCenter NSX están en Enhanced Linked Mode, puede acceder a cualquier NSX Manager asociado desde todos los sistemas vCenter Server vinculados. Para ello, debe seleccionarlo en el menú desplegable **NSX Manager**.

- 2 Diríjase a **Inicio > Redes y seguridad > Instalación** (Home > Networking & Security > Installation) y seleccione la pestaña **Preparación de redes lógicas** (Logical Network Preparation).
- 3 Verifique que el NSX Manager adecuado esté seleccionado en el menú desplegable **NSX Manager**.
- 4 Haga clic en **Identificador de segmento > Editar** (Segment ID > Edit).
- 5 Escriba un rango para los identificadores de segmentos universales, por ejemplo, 900000-909999.

---

**Precaución** Verifique que el rango no se superponga con cualquier otro rango asignado en los NSX Manager del entorno de Cross-vCenter NSX.

---

- 6 (opcional) Si alguna de sus zonas de transporte utilizará multidifusión o el modo de replicación híbrido, seleccione **Habilitar direcciones de multidifusión universales** (Enable Universal multicast addressing) e introduzca una dirección de multidifusión universal o un rango de direcciones de multidifusión universales.

---

**Precaución** Compruebe que la dirección de multidifusión especificada no entra en conflicto con ninguna otra dirección de multidifusión asignada en ningún NSX Manager en el entorno cross-vCenter NSX.

---

## Resultados

Posteriormente, después de configurar los conmutadores lógicos universales, cada conmutador lógico universal recibe un identificador de segmento universal del grupo.

## Agregar una zona de transporte universal en la instancia de NSX Manager principal

Las zonas de transporte universal controlan los hosts a los que puede acceder un conmutador lógico universal. La instancia de NSX Manager principal crea la zona de transporte universal y esta se replica en las instancias de NSX Manager secundarias. Las zonas de transporte universal pueden abarcar uno o más clústeres de vSphere en el entorno de Cross-vCenter NSX.

Después de la creación, hay una zona de transporte universal disponible en todas las instancias de NSX Manager secundarias en el entorno de Cross-vCenter NSX. Puede haber solo una zona de transporte universal.

## Requisitos previos

Configurar una zona de transporte universal después de haber creado un administrador NSX Manager principal.

## Procedimiento

- 1 Con vSphere Web Client, inicie sesión en el sistema vCenter Server registrado con el NSX Manager principal.

Si los sistemas vCenter Server del entorno cross-vCenter NSX están en Enhanced Linked Mode, puede acceder a cualquier NSX Manager asociado desde todos los sistemas vCenter Server vinculados. Para ello, debe seleccionarlo en el menú desplegable **NSX Manager**.

- 2 Diríjase a **Inicio > Redes y seguridad > Instalación** (Home > Networking & Security > Installation) y seleccione la pestaña **Preparación de redes lógicas** (Logical Network Preparation).
- 3 Verifique que el NSX Manager adecuado esté seleccionado en el menú desplegable **NSX Manager**.
- 4 Haga clic en **Zonas de transporte** (Transport Zones) y en el icono **Nueva zona de transporte (+)** (New Transport Zone).
- 5 Seleccione **Marcar este objeto para sincronización universal** (Mark this object for universal synchronization).

Esta zona de transporte se sincronizará con el NSX Manager secundario.

- 6 Seleccione el modo de plano de control:
  - **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.

- 7 Seleccione los clústeres que se agregarán a la zona de transporte.

## Resultados

La zona de transporte universal está disponible en todas las instancias de NSX Manager secundarias en el entorno de Cross-vCenter NSX.

Name	1 ▲ Description	Control Plane Mode	Logical Switches
Transport-Zone		Unicast	1
Universal-Transport-Zone		Unicast	4

**Pasos siguientes**

A continuación, cree un conmutador lógico universal.

## Agregar un conmutador lógico universal en la instancia de NSX Manager principal

En una implementación de Cross-vCenter NSX, puede crear conmutadores lógicos universales, que pueden abarcar todas las instancias de vCenter. El tipo de zona de transporte determina si el conmutador nuevo es un conmutador lógico o un conmutador lógico universal. Cuando agrega un conmutador lógico a una zona de transporte universal, el conmutador lógico es universal.

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.

**Nota** No puede deshabilitar la detección de IP cuando cree un conmutador lógico universal. Puede deshabilitar la detección de IP a través de la API después de crear el conmutador lógico universal. Esta opción se administra de forma independiente en cada NSX Manager. Consulte la *Guía de NSX API*.

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 desee habilitar la detección de MAC si las máquinas virtuales tienen varias direcciones MAC o van a utilizar NIC virtuales que son VLAN de enlace troncal.

**Requisitos previos**

**Tabla 6-1. Requisitos previos para crear un conmutador lógico o un conmutador lógico universal**

Conmutador lógico (Logical Switch)	Conmutador lógico universal
<ul style="list-style-type: none"> <li>■ Los conmutadores distribuidos de vSphere deben estar configurados.</li> <li>■ NSX Manager debe estar instalado.</li> <li>■ Los controladoras deben estar implementados.</li> <li>■ Los clústeres de hosts deben estar preparados para NSX.</li> <li>■ VXLAN debe estar configurada.</li> <li>■ Debe haber una zona de transporte configurada.</li> <li>■ Debe haber un grupo de identificadores de segmentos configurado.</li> </ul>	<ul style="list-style-type: none"> <li>■ Los conmutadores distribuidos de vSphere deben estar configurados.</li> <li>■ NSX Manager debe estar instalado.</li> <li>■ Los controladoras deben estar implementados.</li> <li>■ Los clústeres de hosts deben estar preparados para NSX.</li> <li>■ VXLAN debe estar configurada.</li> <li>■ Se debe asignar una instancia de NSX Manager principal.</li> <li>■ Se debe crear una zona de transporte universal.</li> <li>■ Se debe configurar un grupo de identificadores de segmentos universales.</li> </ul>

## Procedimiento

- 1 Vaya a **Inicio > Redes y seguridad > Conmutadores lógicos** (Home > Networking & Security > Logical Switches).
- 2 Seleccione la instancia de NSX Manager principal.
- 3 Haga clic en el icono **Nuevo conmutador lógico (+)** (New Logical Switch).
- 4 Escriba un nombre y una descripción opcional para el conmutador lógico.
- 5 En la sección Zona de transporte (Transport Zone), haga clic en **Cambiar** (Change) para seleccionar una zona de transporte. Seleccione la zona de transporte universal para crear un conmutador lógico universal.

**Importante** Si crea un conmutador lógico universal y selecciona el modo de replicación híbrido, debe asegurarse de que la dirección de multidifusión utilizada no tenga conflictos con otras direcciones de multidifusión asignadas a cualquier instancia de NSX Manager en el entorno Cross-vCenter NSX.

- 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 MAC** (Enable MAC learning).

## Ejemplo: Conmutador lógico y conmutador lógico universal

App es un conmutador lógico conectado a una zona de transporte. Solo está disponible en la instancia de NSX Manager en la que se creó.

Universal-App es un conmutador lógico universal conectado a una zona de transporte universal. Está disponible en cualquiera de las instancias de NSX Manager del entorno de Cross-vCenter NSX.

El conmutador lógico y el conmutador lógico universal tienen identificadores de segmentos de distintos grupos de identificadores de segmentos.

Virtual Wire ID	Segment ID	Name	1 ▲	Status	Transport Zone
virtualwire-1	5000	App		✓ Normal	Transport-Zone
universalwire-2	900000	Universal-App		✓ Normal	Universal-Transport-Zone

## Pasos siguientes


Agregue máquinas virtuales a un conmutador lógico universal.

De forma opcional, puede crear un enrutador lógico universal y asociarlo a los conmutadores lógicos universales para habilitar la conectividad entre las máquinas virtuales que están conectadas a diferentes conmutadores lógicos universales.

## Conectar máquinas virtuales a un conmutador lógico

Puede conectar máquinas virtuales a un conmutador lógico o a un conmutador lógico universal.

### Procedimiento

- 1 En **Conmutadores lógicos** (Logical Switches), seleccione el conmutador lógico al que desee agregar máquinas virtuales.
- 2 Haga clic en el icono **Agregar máquina virtual** (Add Virtual Machine) ()
- 3 Seleccione las máquinas virtuales que desea agregar al conmutador lógico.
- 4 Seleccione las vNIC que desea conectar.
- 5 Haga clic en **Siguiente** (Next).
- 6 Revise las vNIC que seleccionó.
- 7 Haga clic en **Finalizar** (Finish).

## Agregar un enrutador lógico (distribuido) universal en la instancia de NSX Manager principal

Los módulos de kernel del enrutador lógico del host realizan el enrutamiento entre la redes VXLAN y entre las redes virtual y física. Un dispositivo NSX Edge proporciona la capacidad de enrutamiento dinámico, cuando es necesario. Un enrutador lógico universal proporciona el enrutamiento de Este a Oeste entre los conmutadores lógicos universales.

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.

---

**Importante** Si habilita High Availability en NSX Edge en un entorno de Cross-vCenter NSX, los dispositivos NSX Edge activos y en espera deben residir en el mismo vCenter Server. Si migra uno de los miembros de un par HA de NSX Edge a un sistema de vCenter Server diferente, los dos dispositivos de HA dejarán de funcionar como un par HA, y es posible que se interrumpa el tráfico.

---

### 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*.
- Determine si necesita habilitar la salida local. La salida local permite enviar rutas a hosts de manera selectiva. Quizás sea conveniente utilizar esta opción si la implementación de NSX se expande a varios sitios. Consulte [Topologías de Cross-vCenter NSX](#) para obtener más información. No puede habilitar la salida local después de crear el enrutador lógico universal.

## Procedimiento

- 1 En vSphere Web Client, desplácese hasta **Inicio > Redes y seguridad > NSX Edge** (Home > Networking & Security > NSX Edges).
- 2 Seleccione la instancia de NSX Manager principal para agregar un enrutador lógico universal.
- 3 Haga clic en el icono **Agregar** (Add) (+).
- 4 Seleccione **Enrutador lógico (distribuido) universal** (Universal Logical [Distributed] Router).
- 5 (opcional) Habilite la salida local.
- 6 Introduzca un nombre para el dispositivo.

Este nombre aparece en el inventario de vCenter. El nombre debe ser 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 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.

- 7 (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.

## 8 (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.

## 9 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

## 10 (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.

## 11 (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

*Set the Edge Control Level Logging*

## 12 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...	▼

### 13 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:  [Change](#) [Remove](#)

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

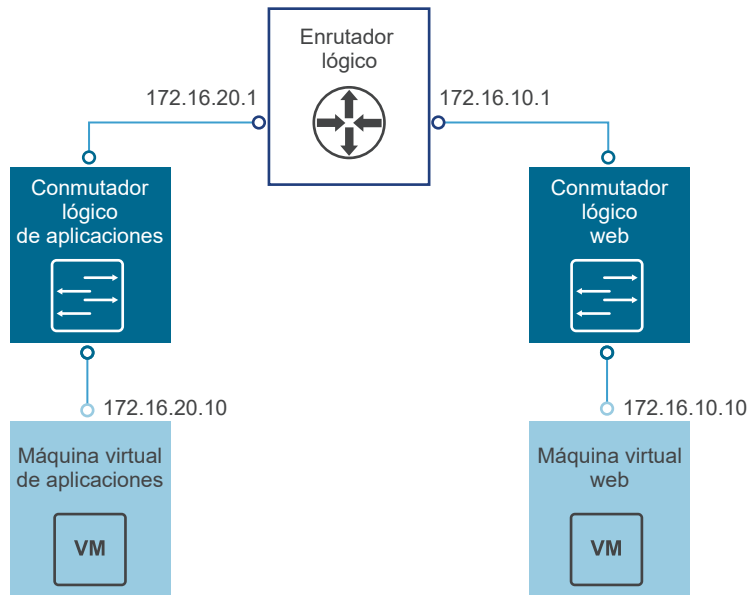
Name	IP Address	Subnet Prefix Length	Connected To
app	172.16.20.1*	24	app
web	172.16.10.1*	24	web
to-ESG	192.168.10.2*	29	transit

[Back](#) [Next](#) [Finish](#) [Cancel](#)

- Asegúrese de que todas las máquinas virtuales asociadas a los conmutadores lógicos tengan sus puertos de enlace predeterminados establecidos 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 puertos de enlace predeterminados 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 | vxlan | 0x1389 | 172.16.10.1/24  |
| 13880000000a | vxlan | 0x1388 | 172.16.20.1/24  |
| 138800000002 | vxlan | 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.

# Configurar instancias secundarias de NSX Manager

# 7

Una vez configurada una instancia principal de Cross-vCenter NSX Manager, se puede configurar una instancia secundaria. Las instancias secundarias de NSX Manager utilizan el mismo clúster de control universal que implementó la instancia principal de NSX Manager. Puede haber hasta siete instancias secundarias de NSX Manager en un entorno de Cross-vCenter NSX. Una vez que se asignó el rol secundario a una instancia de NSX Manager, puede utilizar objetos universales, como conmutadores lógicos universales.

Complete las tareas de configuración de cada instancia secundaria de NSX Manager en el entorno de Cross-vCenter NSX.

## Agregar una instancia de NSX Manager secundaria

Puede agregar hasta siete instancias de NSX Manager secundarias en un entorno de Cross-vCenter NSX. Los objetos universales configurados en la instancia de NSX Manager principal se sincronizan en las instancias de NSX Manager secundarias.

Las instancias de NSX Manager tienen alguno de los cuatro roles:

- Principal
- Secundario
- Independiente
- De tránsito

Para ver la función de una instancia de NSX Manager, inicie sesión en la instancia de vCenter vinculada a ella y desplácese hasta **Inicio (Home) > Redes y seguridad (Networking & Security) > Instalación (Installation)** y, a continuación, seleccione la pestaña **Administración (Management)**. La función se muestra en la columna Función (Role) en Instancias de NSX Manager (NSX Managers). Si no se muestra ninguna columna Función (Role), NSX Manager tiene la función independiente.

### Requisitos previos

- Debe haber dos instancias de NSX Manager como mínimo, una con una función principal y otra con una función independiente o de tránsito.
- La versión de las instancias de NSX Manager (la instancia principal de NSX Manager y las instancias que se asignarán a la función secundaria) debe coincidir.

- Los identificadores de nodo de la instancia principal de NSX Manager y las instancias de NSX Manager que se asignarán a la función secundaria deben estar presentes y ser diferentes. Las instancias de NSX Manager implementadas desde los archivos OVA tienen identificadores de nodo únicos. Una instancia de NSX Manager implementada desde una plantilla (como cuando se convierte una máquina virtual a una plantilla) tendrá el mismo identificador de nodo que la instancia de NSX Manager original que se utilizó para crearla; estas dos instancias de NSX Manager no pueden utilizarse en la misma instalación de Cross-vCenter NSX.

---

**Nota** Puede ver el identificador de nodo de NSX Manager con la siguiente llamada API de REST:

```
GET https://NSX-Manager-IP-Address/api/2.0/services/vsmconfig
```

- 
- Cada NSX Manager debe registrarse con un sistema vCenter Server único y distinto.
  - Los puertos UDP utilizados para la VXLAN deben ser los mismos para todas las instancias de NSX Manager.

---

**Nota** Puede ver y cambiar el puerto VXLAN usando vSphere Web Client en **Redes y seguridad (Networking & Security) > Instalación (Installation) > Preparación de redes lógicas (Logical Network Preparation)**. Consulte el apartado sobre cómo cambiar el puerto VXLAN en *Guía de administración de NSX*.

- 
- Al asignar la función secundaria a un NSX Manager, el sistema de vCenter Server vinculado no debe tener ningún NSX Controller implementado.
  - El grupo de identificadores de segmentos de NSX Manager que se va a asignar a la función secundaria no debe superponerse con los grupos de identificadores de segmentos de la instancia de NSX Manager principal ni con el grupo de identificadores de segmentos de otra instancia de NSX Manager secundaria.
  - La instancia de NSX Manager a la que se le va a asignar la función secundaria debe tener la función independiente o de tránsito.
  - Los NSX Manager principales y secundarios deben tener la misma versión TLS de sincronización universal para que funcionen correctamente.

Compruebe que el NSX Manager secundario esté configurado para usar al menos una de las versiones TLS configuradas en el NSX Manager principal. Consulte el documento sobre cómo cambiar la configuración del modo FIPS y TLS en NSX Manager en la *Guía de administración de NSX*.

## Procedimiento

- 1 Inicie sesión en la instancia de vCenter vinculada a la instancia de NSX Manager principal.
- 2 Desplácese hasta **Inicio (Home) > Redes y seguridad (Networking & Security) > Instalación (Installation)** y seleccione la pestaña **Administración (Management)**.
- 3 Seleccione la instancia de NSX Manager principal. A continuación, seleccione **Acciones (Actions) > Agregar instancia de NSX Manager secundaria (Add Secondary NSX Manager)**.

- 4 Escriba la dirección IP, el nombre de usuario y la contraseña de la instancia de NSX Manager secundaria.





---

**Nota** Debe usar un nombre de host para configurar una instancia secundaria de NSX Manager si la instancia principal de NSX Manager está usando una dirección IPv6.

---

- 5 Haga clic en **Aceptar** (OK).
- 6 Compruebe que la huella digital del certificado coincida con el certificado del NSX Manager secundario.
- 7 Una vez completado correctamente el registro, la función cambia de Independiente (Standalone) a Secundario (Secondary).

Si los sistemas vCenter Server se encuentran en Enhanced Linked Mode, puede ver los roles de todas las instancias de NSX Manager asociadas con esos sistemas vCenter Server en la pestaña **Inicio (Home) > Redes y seguridad (Networking & Security) > Instalación (Installation)**.

| NSX Manager                                                                                      | Role      | 1 ▲ IP Address | vCenter                                                                                                |
|--------------------------------------------------------------------------------------------------|-----------|----------------|--------------------------------------------------------------------------------------------------------|
|  192.168.110.15 | Primary   | 192.168.110.15 |  vcsa-01a.corp.local |
|  192.168.210.15 | Secondary | 192.168.210.15 |  vcsa-01b.corp.local |

Si el entorno no utiliza Enhanced Linked Mode, inicie sesión en la instancia de vCenter vinculada a la instancia de NSX Manager secundaria para ver la función de NSX Manager.

Si el cambio de función de NSX Manager no se muestra, cierre la sesión de vSphere Web Client y vuelva a iniciarla.

---

**Nota** Al principio, el controlador puede estar en estado desconectado. Espere unos segundos y, a continuación, actualice vSphere Web Client. El estado cambia a Normal.

---

## Preparar hosts en una instancia de NSX Manager secundaria

Durante la preparación del host, la instancia de NSX Manager secundaria instala módulos de kernel de NSX en los hosts ESXi que pertenecen a los clústeres vCenter, y crea el plano de control y el tejido del plano de administración de NSX. Los módulos de kernel de NSX 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.


### Requisitos previos

Para ver los detalles sobre los requisitos previos para la preparación del host, consulte [Preparar hosts en la instancia de NSX Manager principal](#)

## Procedimiento

- 1 Utilizando vSphere Web Client, inicie sesión en el sistema vCenter Server registrado con el NSX Manager que desee modificar.

Si los sistemas vCenter Server del entorno cross-vCenter NSX están en Enhanced Linked Mode, puede acceder a cualquier NSX Manager asociado desde todos los sistemas vCenter Server vinculados. Para ello, debe seleccionarlo en el menú desplegable **NSX Manager**.

- 2 Diríjase a **Inicio > Redes y seguridad > Instalación** (Home > Networking & Security > Installation) y seleccione la pestaña **Preparación del host** (Host Preparation).
- 3 Verifique que el NSX Manager adecuado esté seleccionado en el menú desplegable **NSX Manager**.
- 4 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.

---

- 5 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"> <li>■ esx-vmtoolsd</li> <li>■ esx-vxlan</li> </ul> |
| 6.0 o posterior | 6.3.2 o anterior        | <ul style="list-style-type: none"> <li>■ esx-vmtoolsd</li> <li>■ esx-vxlan</li> </ul> |
| 6.0 o posterior | 6.3.3 o posterior       | <ul style="list-style-type: none"> <li>■ esx-nsxv</li> </ul>                          |

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.XXXXXXXX  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.

## Configurar VXLAN desde la instancia de NSX Manager secundaria

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.

### Requisitos previos

Para ver los detalles sobre los requisitos previos, consulte [Configurar VXLAN desde la instancia principal de NSX Manager](#).

### Procedimiento

- 1 Utilizando vSphere Web Client, inicie sesión en el sistema vCenter Server registrado con el NSX Manager que desee modificar.

Si los sistemas vCenter Server del entorno cross-vCenter NSX están en Enhanced Linked Mode, puede acceder a cualquier NSX Manager asociado desde todos los sistemas vCenter Server vinculados. Para ello, debe seleccionarlo en el menú desplegable **NSX Manager**.

- 2 Diríjase a **Inicio (Home) > Redes y seguridad (Networking & Security) > Instalación (Installation)** y seleccione la pestaña **Preparación del host** (Host Preparation).

- 3 Verifique que el NSX Manager adecuado esté seleccionado en el menú desplegable **NSX Manager**.
- 4 Haga clic en **No configurado** (Not Configured) en la columna **VXLAN**.
- 5 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.

## Asignar un grupo de ID de segmentos y la dirección de multidifusión en el NSX Manager secundario

La instancia de NSX Manager secundaria muestra el grupo de ID de segmentos universales, que se sincroniza desde el NSX Manager principal. Además, es posible crear un grupo de ID de segmentos que sea local para el NSX Manager secundario, que se usa para crear conmutadores lógicos locales para ese NSX Manager. Si solo creará conmutadores lógicos universales, no es necesario que agregue un grupo local de ID de segmentos al NSX Manager secundario.

### Requisitos previos

Para obtener más detalles sobre los requisitos e instrucciones para la planificación de grupos de ID de segmentos y direcciones de multidifusión, consulte [Asignar un grupo de ID de segmentos y la dirección de multidifusión en el NSX Manager principal](#).

### Procedimiento

- 1 Utilizando vSphere Web Client, inicie sesión en el sistema vCenter Server registrado con el NSX Manager que desee modificar.

Si los sistemas vCenter Server del entorno cross-vCenter NSX están en Enhanced Linked Mode, puede acceder a cualquier NSX Manager asociado desde todos los sistemas vCenter Server vinculados. Para ello, debe seleccionarlo en el menú desplegable **NSX Manager**.

- 2 Vaya a **Inicio (Home) > Redes y seguridad (Networking & Security) > Instalación (Installation) > Preparación de redes lógicas (Logical Network Preparation)** y seleccione la pestaña **ID de segmentos (Segment ID)**.
- 3 Verifique que el NSX Manager adecuado esté seleccionado en el menú desplegable **NSX Manager**.
- 4 Escriba un rango para los identificadores de segmentos locales, por ejemplo, **20000–29999**.

---

**Precaución** Los rangos especificados para los identificadores de segmentos locales no se deben superponer.

---

- 5 (opcional) Si alguna de sus zonas de transporte utilizará multidifusión o el modo de replicación híbrido, seleccione **Habilitar direcciones de multidifusión** (Enable multicast addressing) y escriba una dirección de multidifusión o un rango de direcciones de multidifusión.

---

**Precaución** Compruebe que la dirección de multidifusión especificada no entra en conflicto con ninguna otra dirección de multidifusión asignada en ningún NSX Manager en el entorno cross-vCenter NSX.

---


## Resultados

Ahora, la instancia de NSX Manager secundaria tiene los identificadores de segmentos universales importados proporcionados por la instancia de NSX Manager principal y los identificadores de segmentos locales.

## Agregar clústeres a la zona de transporte universal

Debe agregar a la zona de transporte universal los clústeres asociados a los NSX Manager secundarios. Esto le permite conectar las máquinas virtuales de dichos clústeres con los conmutadores lógicos universales.

### Procedimiento

- 1 Utilizando vSphere Web Client, inicie sesión en el sistema vCenter Server registrado con el NSX Manager que desee modificar.  
  
Si los sistemas vCenter Server del entorno cross-vCenter NSX están en Enhanced Linked Mode, puede acceder a cualquier NSX Manager asociado desde todos los sistemas vCenter Server vinculados. Para ello, debe seleccionarlo en el menú desplegable **NSX Manager**.
- 2 Vaya a **Inicio (Home) > Redes y seguridad (Networking & Security) > Instalación (Installation) > Preparación de redes lógicas (Logical Network Preparation)** y seleccione la pestaña **Zona de transporte (Transport Zones)**.
- 3 Verifique que el NSX Manager adecuado esté seleccionado en el menú desplegable **NSX Manager**.
- 4 Seleccione la zona de transporte universal y haga clic en **Acciones (Actions)** (  ) > **Conectar clústeres (Connect Clusters)**. Seleccione los clústeres que desea agregar a la zona de transporte universal y haga clic en Aceptar (OK).

# Después de configurar las instancias de NSX Manager primaria y secundaria

## 8

Ahora ya tiene configuradas una instancia de NSX Manager primaria y al menos una instancia de NSX Manager secundaria. Además de crear objetos universales desde la instancia de NSX Manager principal, puede crear objetos locales a ese entorno de vCenter NSX específico, como conmutadores lógicos, enrutadores lógicos (distribuidos) y puertas de enlace de servicios Edge. Puede crearlos en una instancia de NSX Manager primaria o secundaria. Existirán solo en el entorno de vCenter NSX en el que se crearon. No serán visibles para las otras instancias de NSX Manager en el entorno de Cross-vCenter NSX. Además, puede agregar hosts a los clústeres o quitarlos.

Consulte *Guía de administración de NSX* para obtener detalles sobre las tareas administrativas adicionales que debería completar.

# Desinstalar componentes de NSX

## 9

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:

- [Quitar un host de un clúster NSX preparado](#)
- [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](#)

## Quitar un host de un clúster NSX preparado

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-vsip`

## 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. En un entorno de cross-vCenter NSX, debe eliminar todas las máquinas virtuales del conmutador lógico universal de todos los NSX Managers.


### 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).

Si está desinstalando un conmutador lógico universal, es posible que tenga máquinas virtuales conectadas al conmutador lógico universal en los NSX Managers principal y secundarios. Repita esos pasos en todos los NSX Manager de su entorno cross-vCenter NSX para eliminar todas las máquinas virtuales del conmutador lógico universal.

- 3 Con el conmutador lógico seleccionado, haga clic en el icono **Eliminar** (Delete) (.

Si está desinstalando un conmutador lógico universal, debe eliminarlo del NSX Manager principal.

## 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 [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 quita 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 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 elimine dispositivos creados por NSX directamente desde vCenter, como los dispositivos NSX Edge. Administre y elimine siempre estos dispositivos a través de la pestaña Redes y seguridad (Networking and Security) de vSphere Web Client.

---

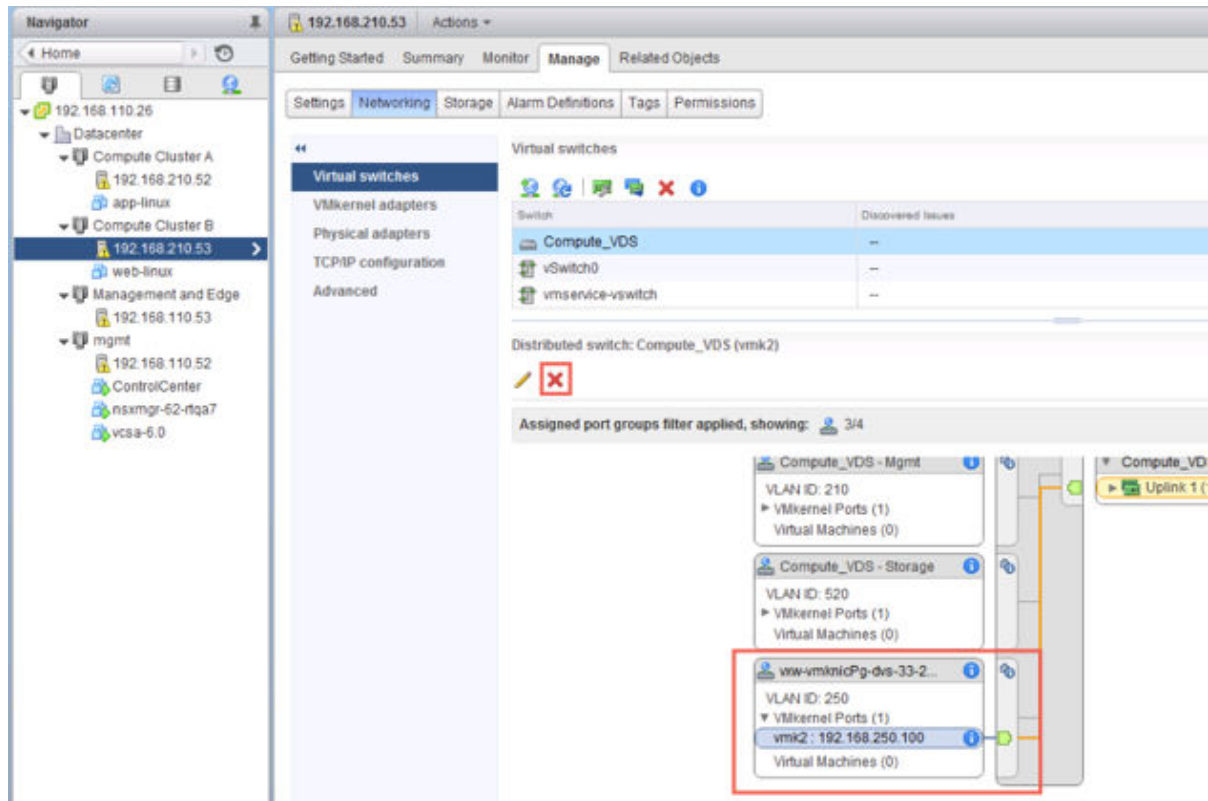
### Requisitos previos

- 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.

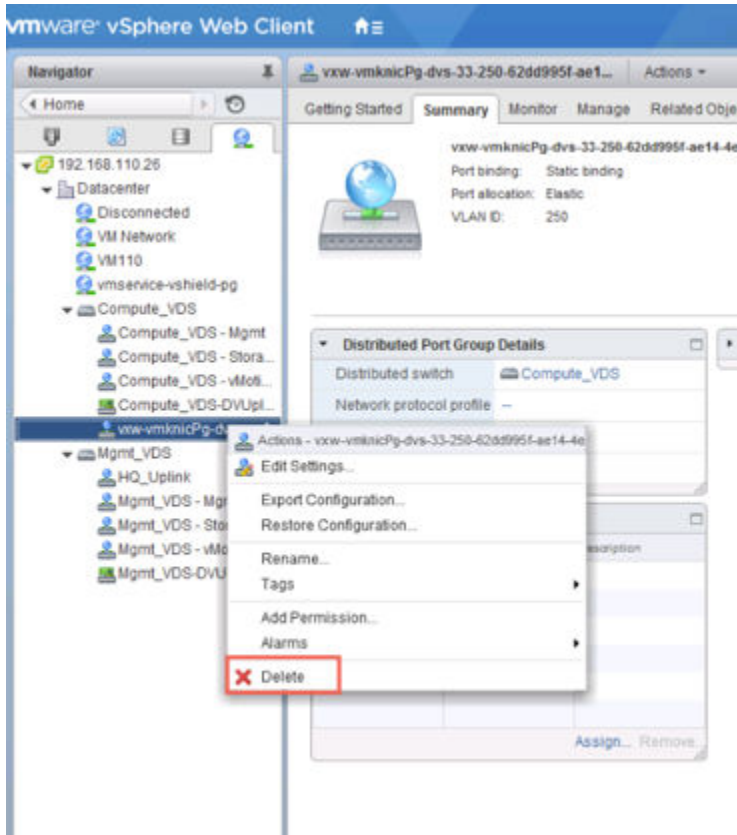
Por ejemplo:



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.

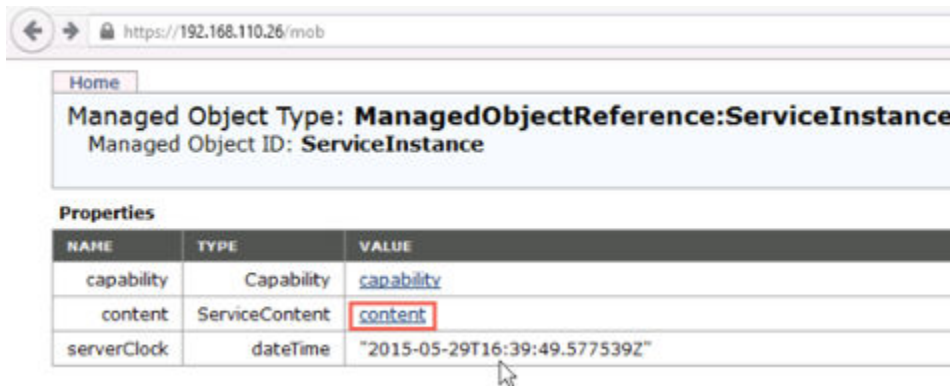
Por ejemplo:



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 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:

- vCenter Server 5.x
  - Windows 2003: `%ALLUSERSPROFILE%\Application Data\VMware\vSphere Web Client\vc-packages\vsphere-client-serenity\`
  - Windows 2008/2012: `%ALLUSERSPROFILE%\VMware\vSphere Web Client\vc-packages\vsphere-client-serenity\`
  - VMware vCenter Server Appliance: `/var/lib/vmware/vsphere-client/vc-packages/vsphere-client-serenity/`
- vCenter Server 6.0.x
  - Windows 2008/2012: `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/`

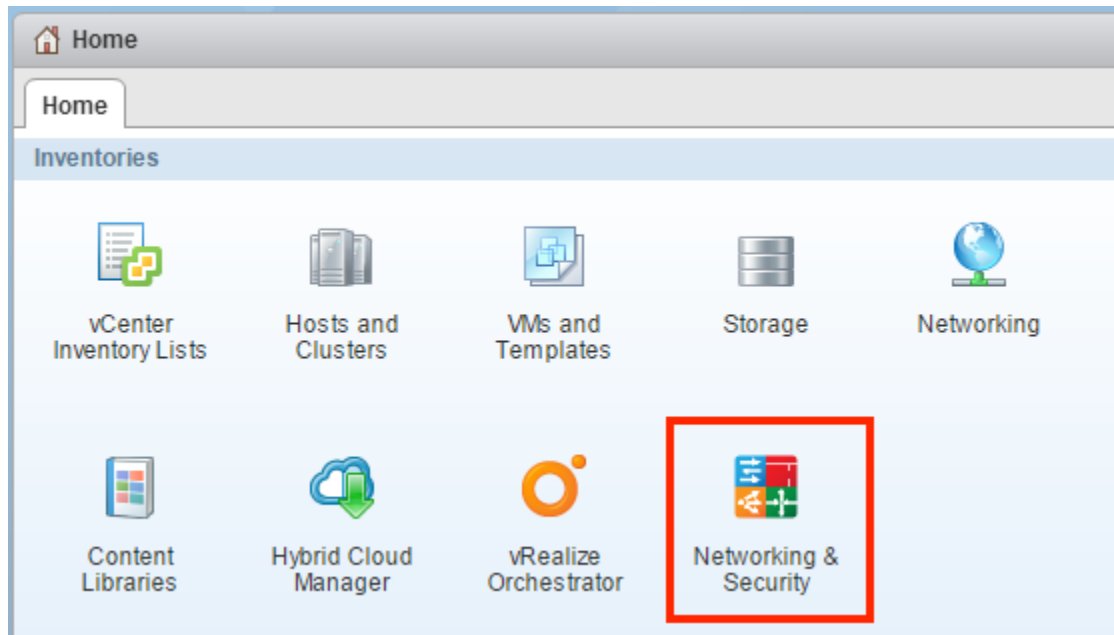
Para vCenter Server Appliance, ejecute el comando `service vsphere-client restart` en el shell del dispositivo.

Para vCenter basado en Windows, ejecute `services.msc`, haga clic con el botón secundario en **vSphere Web Client** y haga clic en **Iniciar** (Start).

### 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).

