

Guía de instalación de NSX-T Data Center

Modificado el 28 de febrero de 2020
VMware NSX-T Data Center 2.4



vmware®

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

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

Si tiene comentarios relacionados con esta documentación, envíelos a:

docfeedback@vmware.com

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

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

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

Contenido

Guía de instalación de NSX-T Data Center	7
1 Descripción general de NSX-T Data Center	8
Conceptos clave	9
Descripción general de NSX Manager	12
2 Flujos de trabajo de instalación de NSX-T Data Center	16
Flujo de trabajo de NSX-T Data Center para vSphere	16
Flujo de trabajo de instalación de NSX-T Data Center para KVM	17
Flujo de trabajo de configuración de NSX-T Data Center para un servidor sin sistema operativo	18
3 Preparación para la instalación	19
Requisitos del sistema	19
Requisitos del sistema de máquinas virtuales de NSX Manager	19
Requisitos del sistema de máquinas virtuales de NSX Edge	22
Requisitos de NSX Edge sin sistema operativo	23
Requisitos del sistema del servidor sin sistema operativo	26
Requisitos de los contenedores Linux sin sistema operativo	26
Puertos y protocolos	26
Puertos TCP y UDP usados por NSX Manager	28
Puertos TCP y UDP usados por NSX Edge	29
Puertos TCP y UDP utilizados por ESXi, hosts de KVM y servidor nativo	31
Instalar componentes de NSX-T Data Center	32
Instalación de NSX Manager	32
Instalación de NSX Edge	35
4 Instalar NSX-T Data Center en vSphere	39
Instalar NSX Manager y los dispositivos disponibles	39
Instalar NSX Manager en ESXi utilizando la herramienta OVF de la línea de comandos	42
Configurar NSX-T Data Center para que aparezca el menú GRUB durante el arranque	47
Iniciar sesión en la instancia de NSX Manager recién creada	48
Agregar un administrador de equipos	48
Implementar nodos de NSX Manager para formar un clúster mediante la interfaz de usuario	50
Configurar una dirección IP virtual (VIP) para un clúster	54
Instalar una instancia de NSX Edge en ESXi utilizando una GUI de vSphere	56
Instalar NSX Edge en ESXi utilizando la herramienta OVF de la línea de comandos	59
5 Instalar NSX-T Data Center en KVM	63

Configurar KVM	63
Administrar sus VM invitadas en la CLI de KVM	69
Instalar NSX Manager en KVM	70
Iniciar sesión en la instancia de NSX Manager recién creada	74
Instalar paquetes de terceros en un host de KVM	74
Comprobar la versión de Open vSwitch en los hosts de KVM de RHEL	76
Implementar nodos de NSX Manager para formar un clúster mediante la CLI	77
Instalar NSX Edge mediante un archivo ISO o con PXE	78
Instalar NSX Edge mediante un archivo ISO como un dispositivo virtual	78
Instalar NSX Edge mediante un archivo ISO sin sistema operativo	82
Instalar NSX Edge en el servidor PXE	84
6 Configurar el servidor sin sistema operativo para usar NSX-T Data Center	90
Instalar paquetes de terceros en un servidor sin sistema operativo	90
Crear una interfaz de aplicación para cargas de trabajo de servidor nativo	92
7 Configurar el clúster de NSX Manager	94
Requisitos del clúster de NSX Manager	94
Requisitos del clúster de NSX Manager para sitios únicos, dobles y múltiples	95
8 Zonas de transporte y nodos de transporte	98
Crear zonas de transporte	98
Crear un grupo de direcciones IP para direcciones IP de endpoints de túneles	101
Ruta de datos mejorada	102
Configurar perfiles	105
Crear un perfil de vínculo superior	105
Configurar perfiles de Network I/O Control	108
Agregar un perfil de clúster de NSX Edge	118
Agregar un perfil de puente de NSX Edge	119
Agregar perfil de nodo de transporte	120
Migrar VMkernel a un conmutador de N-VDS	124
Errores de migración de VMkernel	130
Crear un host independiente o un nodo de transporte sin sistema operativo	133
Configurar un nodo de transporte de host administrado	141
Configurar un nodo de transporte de host ESXi con agregado de enlaces	143
Implementación de clúster de vSphere totalmente contraído en NSX-T	144
Comprobar el estado de nodos de transporte	155
Representación visual de N-VDS	158
Instalación manual de módulos kernel NSX-T Data Center	159
Instalar manualmente módulos kernel de NSX-T Data Center en hipervisores de ESXi	159
Instalar manualmente módulos kernel de NSX-T Data Center en hipervisores de KVM en Ubuntu	162

Instalar manualmente módulos kernel de NSX-T Data Center en hipervisores de KVM en RHEL y CentOS	164
Configuración de red de NSX Edge	165
Crear un nodo de transporte de NSX Edge	171
Crear un clúster de NSX Edge	174
9 Clúster sin estado con Auto Deploy	176
Tareas de alto nivel para un clúster sin estado con Auto Deploy	176
Requisitos previos y versiones admitidas	177
Crear un perfil de imagen personalizada para hosts sin estado	178
Asociar la imagen personalizada con el host de referencia y los hosts de destino	180
Establecer la configuración de red en el host de referencia	181
Configurar el host de referencia como un nodo de transporte en NSX-T	181
Extraer el perfil de host y verificarlo	184
Verificar la asociación del perfil de host con el clúster sin estado	185
Actualizar las personalizaciones de host	186
Activar la implementación automática en los hosts de destino	187
Reiniciar hosts antes de aplicar el TNP	188
Aplicar un TNP a un clúster sin estado	188
Reiniciar hosts después de aplicar el TNP	191
Escenarios en los que el host sin estado está dentro del clúster de destino	192
Escenarios en los que el host sin estado está fuera del clúster de destino	194
Solucionar problemas del perfil de host y el perfil de nodo de transporte	196
10 Desinstalar NSX-T Data Center de un nodo de transporte de host	199
Comprobar las asignaciones de red de host para la desinstalación	199
Desinstalar NSX-T Data Center de un clúster de vSphere	201
Desinstalar NSX-T Data Center de un host en un clúster de vSphere	202
Desinstalar NSX-T Data Center de un host independiente	203
11 Instalar componentes de NSX Cloud	205
Arquitectura y componentes de NSX Cloud	205
Descripción general de la instalación y la configuración de componentes de NSX Cloud para la nube pública	207
Flujo de trabajo de día 0 para conectar NSX Cloud con la nube pública	207
Instalar CSM y conectar con NSX Manager	208
Instalar CSM	208
Unirse a CSM con NSX Manager	208
(Opcional) Configurar servidores proxy	209
(Opcional) Configurar vIDM para Cloud Service Manager	210
Conectar la nube pública con una implementación local	211
Habilitar el acceso a puertos y protocolos en CSM para conectividad híbrida	211

Conectar la red de Microsoft Azure con la implementación de NSX-T Data Center local	212
Conectar la red de Amazon Web Services (AWS) con la implementación de NSX-T Data Center local	213
Agregar la cuenta de nube pública	214
Configurar el acceso seguro a su inventario de Microsoft Azure	214
Configurar el acceso seguro a su inventario de AWS	221
Implementar o vincular NSX Public Cloud Gateway	225
Implementar PCG en una VNet de tránsito o autoadministrada	227
Implementar PCG en una VPC de tránsito o autoadministrada	229
Vincular a una VPC o VNet de tránsito	231
Entidades lógicas creadas automáticamente y grupos de seguridad nativos de la nube	233
Anular la implementación de PCG	238
Desetiquetar máquinas virtuales en la nube pública	240
Deshabilitar la directiva de cuarentena, si está habilitada	240
Eliminar entidades lógicas creadas por el usuario	241
Anular implementación de CSM	241

Guía de instalación de NSX-T Data Center

La *Guía de instalación de NSX-T Data Center* describe cómo instalar el producto VMware NSX-T™ Data Center. La información incluye instrucciones de configuración paso a paso y prácticas recomendadas.

Público objetivo

Esta información está dirigida a quien desee instalar o utilizar NSX-T Data Center. Esta información está destinada a los administradores de sistemas con experiencia que estén familiarizados con la tecnología de máquinas virtuales y los conceptos de virtualización de red.

Glosario de publicaciones técnicas

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-T Data Center

1

De la misma forma que la virtualización del servidor crea y administra máquinas virtuales de forma programática, la virtualización de redes de NSX-T Data Center crea y administra redes virtuales basadas en software de forma programática.

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]). Como consecuencia, estos servicios pueden ensamblarse mediante programación en cualquier combinación arbitraria para producir redes virtuales únicas y aisladas en cuestión de segundos.

NSX-T Data Center funciona implementando tres planos independientes pero integrados, que son los planos de administración, control y datos. Estos planos se implementan como un conjunto de procesos, módulos y agentes que residen en dos tipos de nodos: nodos de NSX Manager y de transporte.

- Cada nodo aloja un agente del plano de administración.
- Los nodos de NSX Manager alojan servicios API y los demonios del clúster del plano de administración.
- Los nodos de NSX Controller alojan los demonios del clúster del plano de control central.
- Los nodos de transporte alojan demonios del plano de control local y motores de reenvío.

NSX Manager ofrece compatibilidad de agrupación en clústeres de tres nodos que combina el administrador de directivas, la administración y los servicios de control central en un clúster de nodos. La agrupación en clústeres de NSX Manager proporciona alta disponibilidad para la interfaz de usuario y la API. La convergencia de los nodos de administración y del plano de control reduce la cantidad de dispositivos virtuales que debe implementar y administrar el administrador de NSX-T Data Center.

El dispositivo de NSX Manager está disponible en tres tamaños diferentes para diferentes escenarios de implementación. Un dispositivo pequeño para las implementaciones de laboratorio o de prueba de concepto. Un dispositivo mediano para las implementaciones de hasta 64 hosts, y un dispositivo grande para los clientes que realizan implementaciones en entornos a gran escala. Consulte [Requisitos del sistema de máquinas virtuales de NSX Manager](#) y la herramienta [Valores máximos de configuración](#).

Este capítulo incluye los siguientes temas:

- [Conceptos clave](#)

■ Descripción general de NSX Manager

Conceptos clave

Los conceptos comunes de NSX-T Data Center que se utilizan en la documentación y la interfaz de usuario.

Administrador de equipo	Un administrador de equipos es una aplicación que administra recursos, como hosts y máquinas virtuales. Un ejemplo es vCenter Server.
Plano de control	Calcula el estado de ejecución basándose en la configuración del plano de administración. El plano de control difunde la información sobre la topología notificada por los elementos del plano de datos e inserta una configuración sin estado en los motores de reenvío.
Plano de datos	Realiza el reenvío sin estado o la transformación de paquetes basándose en tablas rellenas por el plano de control. El plano de datos suministra información sobre la topología al plano de control y conserva las estadísticas relativas al nivel de los paquetes.
Red externa	Una red física o VLAN no administrada por NSX-T Data Center. Puede vincular su red lógica o red superpuesta a una red externa mediante un NSX Edge. Por ejemplo, una red física en un centro de datos de cliente o una VLAN en un entorno físico.
Nodo de tejido	Host registrado con el plano de administración de NSX-T Data Center y que tiene instalados módulos de NSX-T Data Center. Para que un host de hipervisor o NSX Edge forme parte de la superposición de NSX-T Data Center, debe agregarse al tejido de NSX-T Data Center.
Salida de puertos lógicos	El tráfico de red saliente que abandona la máquina virtual o una red lógica se denomina tráfico de salida porque sale de la red virtual e ingresa en el centro de datos.
Entrada de puertos lógicos	El tráfico de red entrante que abandona el centro de datos e ingresa en la máquina virtual se denomina tráfico de entrada.
Enrutador lógico	Entidad de enrutamiento de NSX-T Data Center.
Puerto de enrutador lógico	Puerto de red lógica al que puede adjuntar un puerto de conmutador lógico o un puerto de vínculo superior a una red física.
Conmutador lógico	Entidad que proporciona conmutación virtual de Capa 2 para interfaces de máquina virtual e interfaces de puerta de enlace. Un conmutador lógico da a los administradores de la red de arrendatarios el equivalente lógico de un conmutador de Capa 2 físico, lo que les permite conectar un conjunto de VM a un dominio de difusión común. Un conmutador lógico es una entidad lógica independiente de la infraestructura de hipervisor física y abarca a

muchos hipervisores, conectando VM independientemente de su ubicación física.

En una nube de múltiples arrendatarios, pueden existir muchos conmutadores lógicos lado a lado en el mismo hardware de hipervisor, con cada segmento de Capa 2 aislado del resto. Los conmutadores lógicos se pueden conectar mediante enrutadores lógicos y los enrutadores lógicos pueden proporcionar puertos de vínculos superiores conectados a la red física externa.

Puerto de conmutador lógico

Punto de conexión de conmutador lógico para establecer una conexión a una interfaz de red de máquina virtual o una interfaz de enrutador lógico. El puerto de conmutador lógico indica el perfil de conmutación aplicado, el estado del puerto y el estado del vínculo.

Plano de administración

Proporciona un punto de entrada único de la API al sistema, persiste la configuración de los usuarios, administra las solicitudes de los usuarios y realiza tareas operacionales en todos los nodos de administración, control y plano de datos del sistema. El plano de administración también es responsable de consultar, modificar y persistir la configuración de los usuarios.

Clúster de NSX Edge

Colección de dispositivos de nodos de NSX Edge que tienen la misma configuración que los protocolos implicados en la supervisión de alta disponibilidad.

Nodo de NSX Edge

Parte integrante del objetivo funcional es el proporcionar potencia de cálculo para suministrar las funciones de servicios IP y enrutamiento IP.

Conmutador virtual distribuido administrado por NSX u Open vSwitch de KVM

El conmutador virtual distribuido administrado de NSX (N-VDS, anteriormente conocido como conmutador de host) u OVS se utilizan para las instancias compartidas de NSX Edge y el clúster de proceso. N-VDS es obligatorio para la configuración del tráfico de superposición.

Un N-VDS tiene dos modos: estándar y ruta de datos mejorada. Un N-VDS de ruta de datos mejorada tiene las capacidades de rendimiento para admitir cargas de trabajo de virtualización de funciones de red (Network Functions Virtualization, NFV).

NSX Manager

Nodo que aloja los servicios API, el plano de administración y los servicios de agente. NSX Manager es un dispositivo incluido en el paquete de instalación de NSX-T Data Center. Puede implementar el dispositivo en la función de nsx-manager nsx-controller o nsx-cloud-service-manager. Actualmente, el dispositivo solo admite una función a la vez.

Clúster de NSX Manager

Un clúster de NSX Manager que puede proporcionar alta disponibilidad.

Open vSwitch (OVS)	Conmutador de software de código abierto que actúa como conmutador de host del hipervisor dentro de XenServer, Xen, KVM y otros hipervisores basados en Linux.
Red lógica superpuesta	Red lógica implementada mediante el uso de tunelización de Capa2 en Capa 3 de tal modo que la topología vista por las VM se desacopla de la de la red física.
Interfaz física (pNIC)	Interfaz de red en un servidor físico en el que se instaló un hipervisor.
Segmento	<p>Entidad que proporciona conmutación virtual de Capa 2 para interfaces de máquina virtual e interfaces de puerta de enlace. Un segmento da a los administradores de la red de arrendatarios el equivalente lógico de un conmutador de Capa 2 físico, lo que les permite conectar un conjunto de máquinas virtuales a un dominio de difusión común. Un segmento es una entidad lógica independiente de la infraestructura de hipervisor física y abarca a muchos hipervisores, conectando máquinas virtuales independientemente de su ubicación física. A los segmentos también se los conoce como conmutadores lógicos.</p> <p>En una nube de múltiples arrendatarios, pueden existir muchos segmentos lado a lado en el mismo hardware de hipervisor, con cada segmento de Capa 2 aislado del resto. Los segmentos se pueden conectar mediante puertas de enlace, que pueden proporcionar conectividad a la red física externa.</p>
Puerta de enlace de nivel 0 o enrutador lógico de nivel 0	La puerta de enlace de nivel 0 se denomina enrutador lógico de nivel 0 en la pestaña Opciones avanzadas de redes y seguridad . Interactúa con la red física y se puede realizar como un clúster activo-activo o activo-en espera. La puerta de enlace de nivel 0 ejecuta BGP y pares con enrutadores físicos. En el modo activo-en espera, la puerta de enlace también puede proporcionar servicios con estado.
Puerta de enlace de nivel 1 o enrutador lógico de nivel 1	La puerta de enlace de nivel 1 se denomina enrutador lógico de nivel 1 en la pestaña Opciones avanzadas de redes y seguridad . Se conecta a una puerta de enlace de nivel 0 para la conectividad en dirección norte y una o más redes de superposición para la conectividad en dirección sur. Una puerta de enlace de nivel 1 puede ser un clúster activo-en espera que proporciona servicios con estado.
Zona de transporte	Colección de nodos de transporte que define el alcance máximo de conmutadores lógicos. Una zona de transporte representa un conjunto de hipervisores suministrados de manera similar y los conmutadores lógicos que conectan VM en dichos hipervisores.
Nodo de transporte	Un nodo capaz de participar en una superposición de NSX-T Data Center o en redes VLAN NSX-T Data Center. Para un host de KVM, puede preconfigurar el N-VDS o puede hacer que NSX Manager realice la

configuración. Para un host ESXi, NSX Manager siempre configura el N-VDS.

Perfil de vínculo superior

Define políticas para los vínculos que llevan desde los hosts del hipervisor a los conmutadores lógicos de NSX-T Data Center, o bien desde los nodos de NSX Edge a los conmutadores de la parte superior del rack. La configuración definida por los perfiles de vínculo superior podrían incluir políticas de formación de equipos, vínculos activos/en espera, el ID de la red VLAN de transporte y la configuración de MTU. La VLAN de transporte establecida en las etiquetas de perfil de vínculo superior solo superponen el tráfico, y el TEP utiliza el identificador de VLAN.

Interfaz de VM (vNIC)

Interfaz de red en una máquina virtual que proporciona conectividad entre el sistema operativo del invitado virtual y el vSwitch estándar o el conmutador distribuido vSphere. La vNIC se puede adjuntar a un puerto lógico. Puede identificar una vNIC basándose en su ID exclusivo (UUID).

Endpoint de túnel virtual

Cada hipervisor tiene un endpoint de túnel virtual (VTEP) responsable de encapsular el tráfico de máquina virtual dentro de un encabezado VLAN y enrutar el paquete a un VTEP de destino para su posterior procesamiento. Puede enrutar el tráfico a un VTEP de otro host o a la puerta de enlace de NSX Edge para acceder a la red física.

Descripción general de NSX Manager

NSX Manager proporciona una interfaz de usuario basada en web en la que puede administrar el entorno de NSX-T. También aloja el servidor de API que procesa las llamadas de API.

La interfaz de usuario web de NSX Manager proporciona dos métodos para configurar recursos.

- Interfaz de directivas: pestañas **Redes**, **Seguridad**, **Inventario** y **Planificar y solucionar problemas**.
- Interfaz avanzada: pestaña **Opciones avanzadas de redes y seguridad**.

Cuándo utilizar la interfaz de directivas y la interfaz avanzada

Sea coherente respecto a la interfaz de usuario que utilice. Existen algunos motivos para usar una interfaz de usuario en lugar de la interfaz avanzada.


- Si va a implementar un nuevo entorno de con NSX-T Data Center 2.4 o una versión posterior, el uso de la nueva interfaz de usuario basada de directivas para crear y administrar su entorno es la mejor opción en la mayoría de las situaciones.
 - Algunas funciones no están disponibles en la interfaz de usuario basada en directivas. Si necesita estas funciones, utilice la interfaz de usuario avanzada para todas las configuraciones.
- Si va a actualizar a NSX-T Data Center 2.4 o una versión posterior, continúe para realizar cambios de configuración mediante la interfaz de usuario **Opciones avanzadas de redes y seguridad**.

Tabla 1-1. Cuándo utilizar la interfaz de directivas y la interfaz avanzada

Interfaz de directivas	Interfaz avanzada
La mayoría de las nuevas implementaciones deben utilizar la interfaz basada en directivas.	Las implementaciones que se crearon con la interfaz avanzada, por ejemplo, se actualizan desde versiones anteriores a la interfaz basada en directivas.
Implementaciones de NSX Cloud	Implementaciones que se integran con otros complementos. Por ejemplo, NSX Container Plug-in, OpenStack y otras plataformas de administración de la nube.
<p>Funciones de redes disponibles solo en la interfaz de directivas:</p> <ul style="list-style-type: none"> ■ Servicios de DNS y zonas de DNS ■ VPN ■ Directivas de reenvío para NSX Cloud 	<p>Funciones de redes disponibles solo en la interfaz avanzada:</p> <ul style="list-style-type: none"> ■ Reenvío de capa 3 para IPv4 e IPv6 ■ Temporizador de reenvío ■ Cambiar IP de red de tránsito interno ■ Compatibilidad con VIP HA en el nivel 0 ■ Reubicación en espera ■ Filtrado de anuncios de rutas según la lista de prefijos en el nivel 1 ■ Creación de bucle invertido ■ Salto entre redes de BGP ■ Direcciones de origen de BGP ■ Rutas estáticas con BFD e interfaz como salto siguiente ■ Proxy de metadatos ■ Servidor DHCP adjunto a un segmento aislado y enlace estático
<p>Funciones de seguridad disponibles solo en la interfaz de directivas:</p> <ul style="list-style-type: none"> ■ Protección de endpoints ■ Introspección de red (inserción de servicios de este a oeste) ■ Perfiles de contexto <ul style="list-style-type: none"> ■ Aplicaciones de capa 7 ■ FQDN ■ Nuevo diseño de firewall distribuido y firewall de puerta de enlace <ul style="list-style-type: none"> ■ Categorías ■ Reglas de autoservicio 	<p>Funciones de seguridad disponibles solo en la interfaz avanzada:</p> <ul style="list-style-type: none"> ■ Capacidad para habilitar o deshabilitar el firewall distribuido, el firewall de identidad y el firewall de puerta de enlace ■ Temporizadores de sesión de firewall distribuido ■ Listas de exclusión ■ Umbrales de CPU y de memoria ■ Secciones para reglas sin estado ■ Firewall de puente ■ Bloqueo de sección ■ Identificadores de reglas de firewall distribuido ■ Reglas de firewall distribuido basadas en direcciones IP en el origen y el destino

Uso de la interfaz de directivas

Si decide utilizar la interfaz de directivas, utilícela para crear todos los objetos. No utilice la interfaz de opciones avanzadas para crear objetos.

Puede utilizar la interfaz avanzada para modificar los objetos que se crearon en la interfaz de directivas. La configuración de un objeto creado con directivas puede incluir un vínculo de **Configuración avanzada**. Este vínculo le dirige a la interfaz avanzada en la que puede ajustar la configuración. También puede ver los objetos creados por directivas directamente en la interfaz avanzada. Los ajustes administrados por directiva, pero que están visibles en la interfaz avanzada, muestra este icono: . No se pueden modificar desde la interfaz de usuario avanzada.

Dónde encontrar las interfaces de directivas y las interfaces avanzadas

Las interfaces basadas en directivas y las interfaces avanzadas aparecen en distintas partes de la interfaz de usuario de NSX Manager y utilizan diferentes URI de API.

Tabla 1-2. Interfaces de directivas e interfaces avanzadas

Interfaz de directivas	Interfaz avanzada
<ul style="list-style-type: none"> ■ Pestaña Redes ■ Pestaña Seguridad ■ Pestaña Inventario ■ Pestaña Planificar y solucionar problemas 	Pestaña Opciones avanzadas de redes y seguridad
URI de API que comienzan con <code>/policy/api</code>	URI de API que comienzan con <code>/api</code>

Nota La pestaña **Sistema** se utiliza para todos los entornos. Si modifica los nodos de Edge, los clústeres de Edge o las zonas de transporte, los cambios pueden tardar hasta 5 minutos en verse en la interfaz de usuario basada en directivas. Puede sincronizar inmediatamente mediante POST `/policy/api/v1/infra/sites/default/enforcement-points/default?action=reload`.

Para obtener más información sobre el uso de la API de directiva, consulte la [Guía de introducción de la API de directiva de NSX-T](#).

Nombres de los objetos creados en las interfaces de directiva y avanzada

Los objetos que cree tienen nombres diferentes según la interfaz que se utilizó para crearlos.

Tabla 1-3. Nombres de objetos

Objetos creados mediante la interfaz de directivas	Objetos creados mediante la interfaz avanzada
Segmento	Conmutador lógico
Puerta de enlace de nivel 1	Enrutador lógico de nivel 1
Puerta de enlace de nivel 0	Enrutador lógico de nivel 0
Grupo	Grupo de NS, conjuntos de direcciones IP, conjuntos de direcciones MAC
Directiva de seguridad	Sección de firewall

Tabla 1-3. Nombres de objetos (continuación)

Objetos creados mediante la interfaz de directivas	Objetos creados mediante la interfaz avanzada
Regla	Regla de firewall
Firewall de puerta de enlace	Firewall de Edge

Flujos de trabajo de instalación de NSX-T Data Center

2

NSX-T Data Center se puede instalar en los hosts de vSphere o de KVM. También se puede configurar un servidor sin sistema operativo para usar NSX-T Data Center.

Para instalar o configurar cualquiera de los hipervisores o hacerlo sin sistema operativo, siga las tareas recomendadas en los flujos de trabajo.

Este capítulo incluye los siguientes temas:

- [Flujo de trabajo de NSX-T Data Center para vSphere](#)
- [Flujo de trabajo de instalación de NSX-T Data Center para KVM](#)
- [Flujo de trabajo de configuración de NSX-T Data Center para un servidor sin sistema operativo](#)

Flujo de trabajo de NSX-T Data Center para vSphere

Utilice la lista de comprobación para realizar un seguimiento del progreso de la instalación en un host vSphere.

Siga el orden recomendado de los procedimientos.

- 1 Revise los requisitos de instalación de NSX Manager. Consulte [Instalación de NSX Manager](#).
- 2 Configure los puertos y los protocolos necesarios. Consulte [Puertos y protocolos](#).
- 3 Instale NSX Manager. Consulte [Instalar NSX Manager y los dispositivos disponibles](#).
- 4 Inicie sesión en la instancia de NSX Manager recién creada. Consulte [Iniciar sesión en la instancia de NSX Manager recién creada](#).
- 5 Configure un administrador de equipos. Consulte [Agregar un administrador de equipos](#).
- 6 Implemente nodos adicionales de NSX Manager para crear un clúster. Consulte [Implementar nodos de NSX Manager para formar un clúster mediante la interfaz de usuario](#).
- 7 Revise los requisitos de instalación de NSX Edge. Consulte [Instalación de NSX Edge](#).
- 8 Instale las instancias de NSX Edge. Consulte [Instalar una instancia de NSX Edge en ESXi utilizando una GUI de vSphere](#).
- 9 Cree un clúster de NSX Edge. Consulte [Crear un clúster de NSX Edge](#).
- 10 Cree zonas de transporte. Consulte [Crear zonas de transporte](#).

- 11 Cree nodos de transporte de host. Consulte [Crear un host independiente o un nodo de transporte sin sistema operativo](#) o [Configurar un nodo de transporte de host administrado](#).

Se crea un conmutador virtual en cada host. El plano de administración envía los certificados de host al plano de control y el plano de administración inserta la información del plano de control en los hosts. Cada uno de los hosts se conecta al plano de control mediante SSL presentando su certificado. El plano de control valida el certificado cotejándolo con el certificado de host proporcionado por el plano de administración. Las controladoras aceptan la conexión si la validación se realizó correctamente.

Tras la instalación

Cuando los hosts son nodos de transporte, puede crear en cualquier momento zonas de transporte, conmutadores lógicos, enrutadores lógicos y otros componentes de red a través de la UI o la API de NSX Manager. Cuando NSX Edge y los hosts se unen al plano de administración, las entidades lógicas de NSX-T Data Center y el estado de configuración se insertan en NSX Edge y los hosts de forma automática.

Para obtener más información, consulte la *Guía de administración de NSX-T Data Center*.

Flujo de trabajo de instalación de NSX-T Data Center para KVM

Utilice la lista de comprobación para realizar un seguimiento del progreso de la instalación en un host de KVM.

Siga el orden recomendado de los procedimientos.

- 1 Prepare el entorno de KVM. Consulte [Configurar KVM](#).
- 2 Revise los requisitos de instalación de NSX Manager. Consulte [Instalación de NSX Manager](#).
- 3 Configure los puertos y los protocolos necesarios. Consulte [Puertos y protocolos](#).
- 4 Instale NSX Manager. Consulte [Instalar NSX Manager en KVM](#).
- 5 Inicie sesión en la instancia de NSX Manager recién creada. Consulte [Iniciar sesión en la instancia de NSX Manager recién creada](#).
- 6 Configure los paquetes de terceros en el host de KVM. Consulte [Instalar paquetes de terceros en un host de KVM](#).
- 7 Implemente nodos adicionales de NSX Manager para crear un clúster. Consulte [Implementar nodos de NSX Manager para formar un clúster mediante la CLI](#).
- 8 Revise los requisitos de instalación de NSX Edge. Consulte [Instalación de NSX Edge](#).
- 9 Instale las instancias de NSX Edge. Consulte [Instalar NSX Edge mediante un archivo ISO o con PXE](#).
- 10 Cree un clúster de NSX Edge. Consulte [Crear un clúster de NSX Edge](#).
- 11 Cree zonas de transporte. Consulte [Crear zonas de transporte](#).

- 12 Cree nodos de transporte de host. Consulte [Crear un host independiente o un nodo de transporte sin sistema operativo](#).

Se crea un conmutador virtual en cada host. El plano de administración envía los certificados de host al plano de control y el plano de administración inserta la información del plano de control en los hosts. Cada uno de los hosts se conecta al plano de control mediante SSL presentando su certificado. El plano de control valida el certificado cotejándolo con el certificado de host proporcionado por el plano de administración. Las controladoras aceptan la conexión si la validación se realizó correctamente.

Tras la instalación

Cuando los hosts son nodos de transporte, puede crear en cualquier momento zonas de transporte, conmutadores lógicos, enrutadores lógicos y otros componentes de red a través de la UI o la API de NSX Manager. Cuando NSX Edge y los hosts se unen al plano de administración, las entidades lógicas de NSX-T Data Center y el estado de configuración se insertan en NSX Edge y los hosts de forma automática.

Para obtener más información, consulte la *Guía de administración de NSX-T Data Center*.

Flujo de trabajo de configuración de NSX-T Data Center para un servidor sin sistema operativo

Utilice la lista de comprobación para realizar un seguimiento del progreso al configurar un servidor sin sistema operativo para usar NSX-T Data Center.

Siga el orden recomendado de los procedimientos.

- 1 Revise los requisitos del servidor sin sistema operativo. Consulte [Requisitos del sistema del servidor sin sistema operativo](#).
- 2 Configure los puertos y los protocolos necesarios. Consulte [Puertos y protocolos](#).
- 3 Instale NSX Manager. Consulte [Instalar NSX Manager en KVM](#).
- 4 Configure los paquetes de terceros en el servidor sin sistema operativo. Consulte [Instalar paquetes de terceros en un servidor sin sistema operativo](#).
- 5 Cree nodos de transporte de host. Consulte [Crear un host independiente o un nodo de transporte sin sistema operativo](#).

Se crea un conmutador virtual en cada host. El plano de administración envía los certificados de host al plano de control y el plano de administración inserta la información del plano de control en los hosts. Cada uno de los hosts se conecta al plano de control mediante SSL presentando su certificado. El plano de control valida el certificado cotejándolo con el certificado de host proporcionado por el plano de administración. Las controladoras aceptan la conexión si la validación se realizó correctamente.

- 6 Cree una interfaz de aplicación para cargas de trabajo del servidor sin sistema operativo. Consulte [Crear una interfaz de aplicación para cargas de trabajo de servidor nativo](#).

Preparación para la instalación

3

Antes de instalar NSX-T Data Center, asegúrese de que su entorno esté preparado.

Este capítulo incluye los siguientes temas:

- [Requisitos del sistema](#)
- [Puertos y protocolos](#)
- [Instalar componentes de NSX-T Data Center](#)

Requisitos del sistema

Antes de instalar NSX-T Data Center, el entorno debe cumplir los requisitos de hardware y recursos específicos.

Requisitos del sistema de máquinas virtuales de NSX Manager

Antes de instalar una instancia de NSX Manager, asegúrese de que el entorno cumpla los requisitos de compatibilidad.

Requisitos de host del hipervisor para los nodos de transporte

Hipervisor	Versión	Núcleos de CPU	Memoria
vSphere	Versión de vSphere admitida	4	16 GB
CentOS Linux KVM	7.4	4	16 GB
Red Hat Enterprise Linux (RHEL) KVM	7.6, 7.5 y 7.4	4	16 GB
SUSE Linux Enterprise Server KVM	12 SP3, SP4	4	16 GB
KVM en Ubuntu	18.04 y 16.04.2 LTS	4	16 GB

Tabla 3-1. Hosts admitidos para instancias de NSX Manager

Descripción del soporte	Hipervisor
ESXi	Para consultar los hosts admitidos, consulte las Matrices de interoperabilidad de productos de VMware .
KVM	RHEL 7.4 y Ubuntu 16.04 LTS

Para los hosts de ESXi, NSX-T Data Center admite las funciones de perfiles de host e implementación automática en vSphere 6.7 U1 o una versión posterior. Consulte más información en el apartado sobre *vSphere Auto Deploy* en la documentación de *Instalación y configuración de VMware ESXi*.

Precaución En RHEL, el comando `yum update` podría actualizar la versión del kernel y acabar con la compatibilidad con NSX-T Data Center. Deshabilite la actualización automática del kernel cuando ejecute `yum update`. Además, después de ejecutar `yum install`, compruebe que NSX-T Data Center es compatible con la versión del kernel.

Requisitos de red del host del hipervisor

Los hosts del hipervisor que ejecuten NSX-T Data Center deben tener una tarjeta NIC compatible. Para obtener información sobre las tarjetas NIC compatibles, consulte la [Guía de compatibilidad de VMware](#).

Sugerencia Para identificar rápidamente las tarjetas compatibles en la Guía de compatibilidad, aplique los siguientes criterios:

- En **Tipo de dispositivo de E/S**, seleccione **Red**.
- También puede seleccionar las opciones de GENEVE en **Funciones** si desea utilizar la encapsulación GENEVE compatible.
- De forma opcional, puede seleccionar **Ruta de datos mejorada de N-VDS** si desea utilizar dicha la ruta.

Controladores de NIC de ruta de datos mejorada

Descargue los controladores de NIC compatibles de la página [My VMware](#).

Tarjeta NIC	Controlador de NIC
Intel 82599	ixgben 1.1.0.26-1OEM.670.0.0.7535516
Controlador Ethernet X710 de Intel(R) para 10 GbE SFP+	i40en 1.2.0.0-1OEM.670.0.0.8169922
Controlador Ethernet XL710 de Intel(R) para 40 GbE QSFP+	

Requisitos de recursos de máquina virtual de NSX Manager

El tamaño del disco virtual fino es 3,8 GB y el tamaño del disco virtual grueso es 200 GB.

Tamaño del dispositivo (Appliance Size)	Memoria	vCPU	Espacio de disco	Versión de hardware de la máquina virtual
NSX Manager extra pequeño	8 GB	2	200 GB	10 o posterior
Máquina virtual pequeña de NSX Manager	16 GB	4	200 GB	10 o posterior

Tamaño del dispositivo (Appliance Size)	Memoria	vCPU	Espacio de disco	Versión de hardware de la máquina virtual
Máquina virtual mediana de NSX Manager	24 GB	6	200 GB	10 o posterior
Máquina virtual grande de NSX Manager	48 GB	12	200 GB	10 o posterior

Nota A partir de NSX-T 2.4, NSX Manager ofrece varias funciones que antes requerían dispositivos independientes. Esto incluye la función de directiva, la función del plano de administración y la función del plano de control central. La función del plano de control central estaba incluida anteriormente en el dispositivo NSX Controller.

- Los requisitos de los recursos de la máquina virtual extra pequeña de NSX Manager se aplican solo a Cloud Service Manager.
- El tamaño de dispositivo de máquina virtual pequeño de NSX Manager es adecuado para implementaciones de prueba de concepto y laboratorio, y no se debe usar en producción.
- El tamaño de dispositivo de máquina virtual mediano de NSX Manager es adecuado para entornos de producción típicos y puede admitir hasta 64 hipervisores.
- El tamaño de dispositivo de máquina virtual grande de NSX Manager es adecuado para implementaciones de gran escala con más de 64 hipervisores.

Para la escala máxima con el tamaño de dispositivo de máquina virtual grande de NSX Manager, vaya a la herramienta de valores máximos de configuración de VMware en <https://configmax.vmware.com/guest> y seleccione NSX-T Data Center en la lista de productos.

Exploradores compatibles con NSX Manager

Se recomiendan los siguientes navegadores para trabajar con NSX Manager.

Explorador	Windows 10	Mac OS X 10.13, 10.14	Ubuntu 18.04
Google Chrome 76	Sí	Sí	Sí
Mozilla Firefox 68	Sí	Sí	Sí
Microsoft Edge 44	Sí		
Apple Safari 12		Sí	

Nota

- Internet Explorer no es compatible.
- La resolución mínima de explorador admitida es 1280 x 800 píxeles.
- Idiomas admitidos: NSX Manager se ha localizado a los siguientes idiomas: inglés, alemán, francés, japonés, chino simplificado, coreano, chino tradicional y español. Sin embargo, como la localización de NSX Manager utiliza la configuración de idioma del navegador, asegúrese de que la configuración coincida con el idioma deseado. La interfaz de NSX Manager no incluye ninguna opción de preferencias de idioma.

Requisitos de latencia de red

La latencia de red máxima entre las instancias de NSX Manager en un clúster de NSX Manager es 10 ms.

La latencia de red máxima entre las instancias de NSX Manager y los nodos de transporte es de 150 ms.

Requisitos de almacenamiento

- La latencia máxima de acceso de disco es inferior a 10 milisegundos.
- Se recomienda que las instancias de NSX Manager se coloquen en el almacenamiento compartido.
- El almacenamiento debe tener alta disponibilidad para evitar su interrupción, ya que si se produce un fallo de almacenamiento todos los sistemas de archivos NSX Manager se pondrían en modo de solo lectura.

Para obtener información sobre cómo diseñar mejor una solución de almacenamiento de alta disponibilidad, consulte la documentación de su tecnología de almacenamiento.

Requisitos del sistema de máquinas virtuales de NSX Edge

Antes de instalar NSX Edge, asegúrese de que el entorno cumpla los requisitos compatibles.

Los nodos de NSX Edge solo se admiten en hosts basados en ESXi con chipsets basados en Intel. De lo contrario, el modo EVC de vSphere puede evitar que se inicien los nodos de NSX Edge, tras lo que la consola mostrará un mensaje de error.

Nota Solo vNIC VMXNET 3 es compatible con la máquina virtual de NSX Edge.

Nota sobre NSX Cloud Si se utiliza NSX Cloud, ten en cuenta que NSX Public Cloud Gateway (PCG) se implementa en un único tamaño predeterminado para cada nube pública compatible: Consulte [Implementar o vincular NSX Public Cloud Gateway](#) para obtener información detallada.

Requisitos de recursos de máquina virtual de NSX Edge

Tamaño del dispositivo (Appliance Size)	Memoria	vCPU	Espacio de disco	Versión de hardware de la máquina virtual
NSX Edge pequeño	4 GB	2	200 GB	11 o posterior (vSphere 6.0 o posterior)
NSX Edge mediano	8 GB	4	200 GB	11 o posterior (vSphere 6.0 o posterior)
NSX Edge grande	32 GB	8	200 GB	11 o posterior (vSphere 6.0 o posterior)

Nota

- El tamaño de dispositivo de máquina virtual pequeña de NSX Edge es adecuada para implementaciones de prueba de concepto y laboratorio.
- El tamaño de dispositivo mediano de NSX Edge es adecuado para entornos de producción típicos.
- El tamaño de dispositivo grande de NSX Edge es adecuado para entornos con equilibrio de carga. Consulte la sección sobre cómo [escalar los recursos del equilibrador de carga](#) en la *Guía de administración de NSX-T Data Center*.

Requisitos de CPU de máquina virtual de NSX Edge

Para admitir DPDK, la plataforma de subyacente debe cumplir los siguientes requisitos:

- La CPU debe tener capacidad de AES-NI.
- La CPU debe admitir 1 GB de Huge Page.

Hardware	Tipo
CPU	<ul style="list-style-type: none"> ■ Intel Xeon E7-xxxx (Westmere-EX y generación posterior de CPU) ■ Intel Xeon 56xx (Westmere-EP) ■ Intel Xeon E5-xxxx (Sandy Bridge y generación posterior de CPU) ■ Intel Xeon Platinum (todas las generaciones) ■ Intel Xeon Gold (todas las generaciones) ■ Intel Xeon Silver (todas las generaciones) ■ Intel Xeon bronze (todas las generaciones)

Requisitos de NSX Edge sin sistema operativo

Antes de configurar NSX Edge sin sistema operativo, asegúrese de que el entorno cumpla los requisitos compatibles.

Los nodos de NSX Edge solo se admiten en hosts basados en ESXi con chipsets basados en Intel. De lo contrario, el modo EVC de vSphere puede evitar que se inicien los nodos de Edge, tras lo que la consola mostrará un mensaje de error.

Requisitos de disco, CPU y memoria de NSX Edge sin sistema operativo

Memoria	Núcleos de CPU	Espacio de disco
32 GB	8	200 GB

Requisitos de CPU de DPDK de NSX Edge sin sistema operativo

Para admitir DPDK, la plataforma de subyacente debe cumplir los siguientes requisitos:

- La CPU debe tener capacidad de AES-NI.
- La CPU debe admitir 1 GB de Huge Page.

Hardware	Tipo
CPU	<ul style="list-style-type: none"> ■ Intel Xeon E7-xxxx (Westmere-EX y generación posterior de CPU) ■ Intel Xeon 56xx (Westmere-EP) ■ Intel Xeon E5-xxxx (Sandy Bridge y generación posterior de CPU) ■ Intel Xeon Platinum (todas las generaciones) ■ Intel Xeon Gold (todas las generaciones) ■ Intel Xeon Silver (todas las generaciones) ■ Intel Xeon bronce (todas las generaciones)

Requisitos de hardware de NSX Edge sin sistema operativo

Compruebe que el hardware de NSX Edge sin sistema operativo aparezca en esta URL <https://certification.ubuntu.com/server/models/?release=18.04%20LTS&category=Server>. Si el hardware no aparece, es posible que el almacenamiento, el adaptador de vídeo o los componentes de la placa base podrían no funcionen en el dispositivo de NSX Edge.

Requisitos de NIC de NSX Edge sin sistema operativo

Tipo de NIC	Descripción	Identificador de dispositivo PCI
Intel XXV710	I40E_DEV_ID_25G_B	0x158A
	I40E_DEV_ID_25G_SFP28	0x158B
Intel X520/Intel 82599	IXGBE_DEV_ID_82599_KX4	0x10F7
	IXGBE_DEV_ID_82599_KX4_MEZZ	0x1514
	IXGBE_DEV_ID_82599_KR	0x1517
	IXGBE_DEV_ID_82599_COMBO_BACK PLANE	0x10F8
	IXGBE_DEV_ID_82599_COMBO_BACK PLANE	0x000C
	IXGBE_SUBDEV_ID_82599_KX4_KR_MEZZ	0x10F9
	IXGBE_DEV_ID_82599_CX4	0x10FB
	IXGBE_DEV_ID_82599_CX4	0x11A9
	IXGBE_DEV_ID_82599_SFP	0x1F72
	IXGBE_SUBDEV_ID_82599_SFP	0x17D0
	IXGBE_SUBDEV_ID_82599_RNDC	0x0470
	IXGBE_SUBDEV_ID_82599_560FLR	0x1507
	IXGBE_SUBDEV_ID_82599_ECNA_DP	0x154D
	IXGBE_DEV_ID_82599_SFP_EM	0x154A
	IXGBE_DEV_ID_82599_SFP_SF2	0x1558
	IXGBE_DEV_ID_82599_SFP_SF_QP	0x1557
	IXGBE_DEV_ID_82599_QSFP_SF_QP	0x10FC
	IXGBE_DEV_ID_82599EN_SFP	0x151C
	IXGBE_DEV_ID_82599_XAUI_LOM	
	IXGBE_DEV_ID_82599_T3_LOM	
Intel X540	IXGBE_DEV_ID_X540T	0x1528
	IXGBE_DEV_ID_X540T1	0x1560
Intel X550	IXGBE_DEV_ID_X550T	0x1563
	IXGBE_DEV_ID_X550T1	0x15D1
Intel X710	I40E_DEV_ID_SFP_X710	0x1572
	I40E_DEV_ID_KX_C	0x1581
	I40E_DEV_ID_10G_BASE_T	0x1586
Intel XL710	I40E_DEV_ID_KX_B	0x1580
	I40E_DEV_ID_QSFP_A	0x1583
	I40E_DEV_ID_QSFP_B	0x1584
	I40E_DEV_ID_QSFP_C	0x1585
Cisco VIC 1387	Tarjeta de interfaz virtual 1387 de Cisco UCS	0x0043

Requisitos del sistema del servidor sin sistema operativo

Antes de configurar el servidor sin sistema operativo, asegúrese de que el servidor cumpla los requisitos compatibles.

Importante El usuario que realice la instalación puede requerir permisos de comando sudo para algunos de los procedimientos. Consulte [Instalar paquetes de terceros en un servidor sin sistema operativo](#).

Requisitos del servidor sin sistema operativo

Sistema operativo	Versión	Núcleos de CPU	Memoria
CentOS Linux	7.4	4	16 GB
Red Hat Enterprise Linux (RHEL)	7.5 y 7.4	4	16 GB
SUSE Linux Enterprise Server	12 SP3	4	16 GB
Ubuntu	18.04 y 16.04.2 LTS	4	16 GB

Requisitos de los contenedores Linux sin sistema operativo

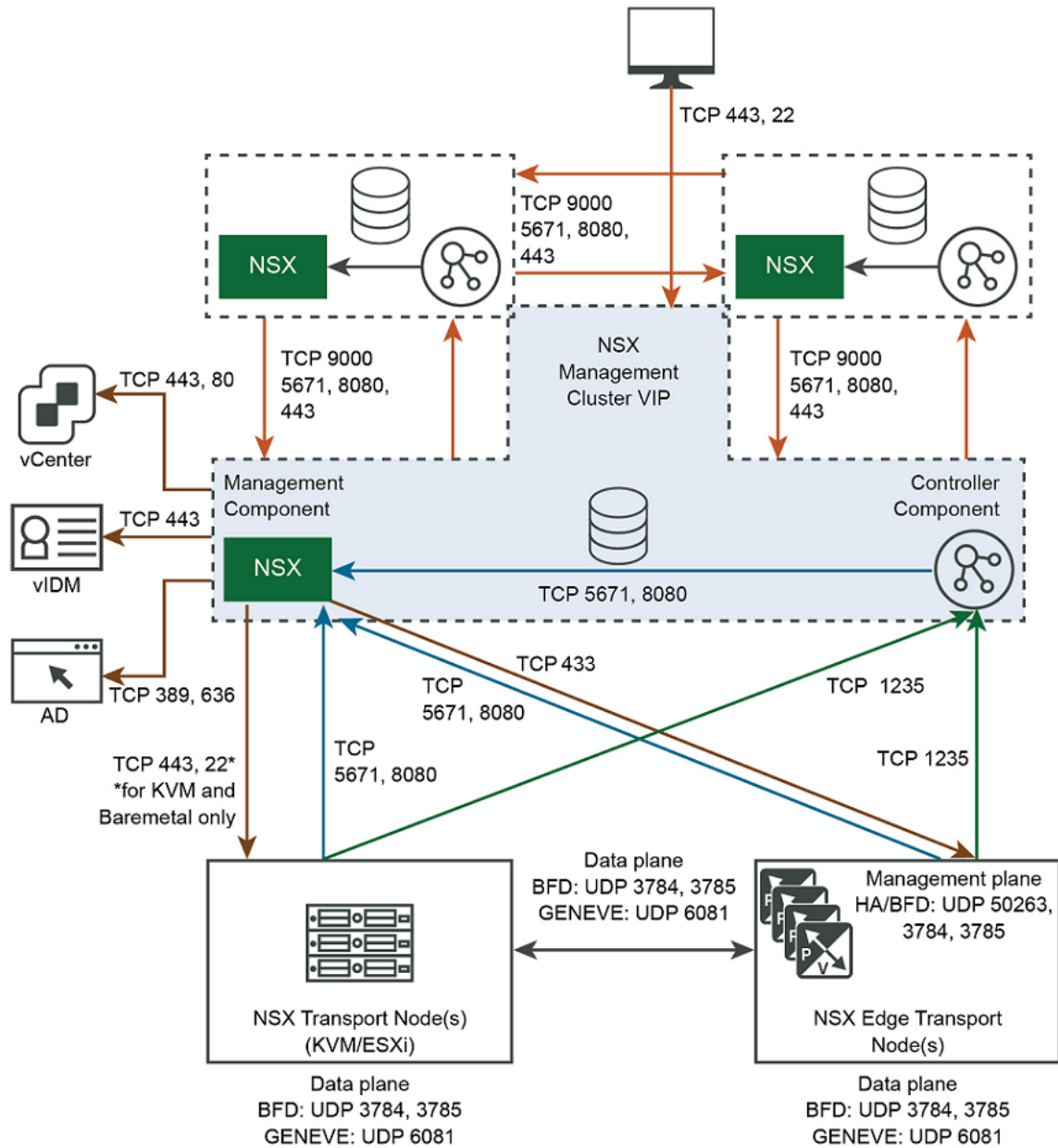
Para obtener más información sobre los requisitos de los contenedores Linux sin sistema operativo, consulte la *Guía de instalación y administración de NSX-T Container Plug-in para OpenShift*.

Puertos y protocolos

Los puertos y los protocolos habilitan rutas de comunicación de nodo a nodo en NSX-T Data Center. Las rutas están protegidas y autenticadas, y se utiliza una ubicación de almacenamiento para las credenciales con el fin de establecer una autenticación mutua.

Nota Los puertos y los protocolos requeridos deben estar abiertos en los firewalls de hipervisor físicos y de host.

Figura 3-1. Puertos y protocolos de NSX-T Data Center



De forma predeterminada, todos los certificados son certificados autofirmados. Las claves privadas y los certificados API y GUI en dirección norte se pueden reemplazar por certificados firmados por una CA.

Hay demonios internos que se comunican a través del bucle invertido o de sockets de dominio UNIX:

- KVM: MPA, netcpa, nsx-agent, OVS

- ESXi: netcpa, ESX-DP (en el kernel)

Nota Para obtener acceso a los nodos de NSX-T Data Center, debe habilitar SSH en ellos.

Nota sobre NSX Cloud Consulte [Habilitar el acceso a puertos y protocolos en CSM para conectividad híbrida](#) para obtener una lista de los puertos necesarios para la implementación de NSX Cloud.

Puertos TCP y UDP usados por NSX Manager

NSX Manager utiliza algunos puertos UDP y TCP para comunicarse con otros productos y componentes. Estos puertos deben abrirse en el firewall.

Puede usar una llamada de API o un comando de la CLI si desea especificar puertos personalizados para transferir archivos (22 es el valor predeterminado) y para exportar los datos syslog (514 y 6514 son los predeterminados). Si lo hace, es necesario que configure el firewall de acuerdo a estos cambios.

Tabla 3-2. Puertos TCP y UDP usados por NSX Manager

Origen	Destino	Puerto	Protocolo	Descripción
NSX Manager	Active Directory	389	TCP	Active Directory
Instancias de NSX Controller, nodos de NSX Edge y nodos de transporte	NSX Manager	5671	TCP	Mensajes de NSX
Instancias de NSX Controller, nodos de NSX Edge, nodos de transporte, vCenter Server	NSX Manager	8080	TCP	Instalar o actualizar el repositorio HTTP
NSX Manager	NSX Manager	9000	TCP	Acceso al almacén de datos interno
NSX Manager	Servidores DNS	53	TCP	DNS
NSX Manager	Servidores DNS	53	UDP	DNS
NSX Manager	NSX Edge	443	TCP	HTTPS
NSX Manager	Servidores SCP de administración	22	TCP	SSH (cargar paquetes de soporte, copias de seguridad, etc.)
NSX Manager	Servidores NTP	123	UDP	NTP
NSX Manager	Servidores SNMP	161, 162	TCP	SNMP
NSX Manager	Servidores SNMP	161, 162	UDP	SNMP
NSX Manager	Servidores syslog	514	TCP	Syslog
NSX Manager	Servidores syslog	514	UDP	Syslog
NSX Manager	Servidores syslog	6514	TCP	Syslog
NSX Manager	Servidores syslog	6514	UDP	Syslog

Tabla 3-2. Puertos TCP y UDP usados por NSX Manager (continuación)

Origen	Destino	Puerto	Protocolo	Descripción
NSX Manager	Destino de traceroute	3343 4 - 3352 3	UDP	Traceroute
NSX Manager	vCenter Server	80	TCP	NSX Manager para calcular la comunicación del administrador (vCenter Server) cuando se configure.
NSX Manager	vCenter Server	443	TCP	NSX Manager para calcular la comunicación del administrador (vCenter Server) cuando se configure.
NSX Manager	vIDM	443	TCP	vIDM
NSX Manager	NSX Manager	443	TCP	Comunicación de NSX Manager a NSX Manager
Clientes de administración	NSX Manager	22	TCP	SSH (deshabilitado de forma predeterminada)
Clientes de administración	NSX Manager	443	TCP	Servidor de NSX API
Servidores SNMP	NSX Manager	161	UDP	SNMP

Puertos TCP y UDP usados por NSX Edge

NSX Edge utiliza algunos puertos UDP y TCP para comunicarse con otros productos y componentes. Estos puertos deben abrirse en el firewall.

Puede usar una llamada de API o un comando de la CLI si desea especificar puertos personalizados para transferir archivos (22 es el valor predeterminado) y para exportar los datos syslog (514 y 6514 son los predeterminados). Si lo hace, es necesario que configure el firewall de acuerdo a estos cambios.

Tabla 3-3. Puertos TCP y UDP usados por NSX Edge

Origen	Destino	Puerto	Protocolo	Descripción
Clientes de administración	Nodos de NSX Edge	22	TCP	SSH (deshabilitado de forma predeterminada)
Agente NSX	Nodos de NSX Edge	5555	TCP	NSX Cloud: agente en la instancia se comunica con la puerta de enlace de NSX Cloud.
Nodos de NSX Edge	Servidores DNS	53	UDP	DNS
Nodos de NSX Edge	Servidores SCP o SSH de administración	22	TCP	SSH (cargar paquetes de soporte, copias de seguridad, etc.)
Nodos de NSX Edge	Nodos de NSX Controller	1235	TCP	netcpa

Tabla 3-3. Puertos TCP y UDP usados por NSX Edge (continuación)

Origen	Destino	Puerto	Protocolo	Descripción
Nodos de NSX Edge	Nodos de NSX Edge	1167	TCP	Backend DHCP
Nodos de NSX Edge	Nodos de NSX Edge	2480	TCP	Nestdb
Nodos de NSX Edge	Nodos de NSX Edge	6666	TCP	NSX Cloud: comunicación local de NSX Edge.
Nodos de NSX Edge	Nodos de NSX Edge	50263	UDP	Alta disponibilidad
Nodos de NSX Edge	Nodo de NSX Manager	443	TCP	HTTPS
Nodos de NSX Edge	Nodo de NSX Manager	5671	TCP	Mensajes de NSX
Nodos de NSX Edge	Nodo de NSX Manager	8080	TCP	NAPI, actualización de NSX-T Data Center
Nodos de NSX Edge	Servidores NTP	123	UDP	NTP
Nodos de NSX Edge	Servidor de la API OpenStack Nova	3000 - 9000	TCP	Proxy de metadatos
Nodos de NSX Edge	Servidores SNMP	161, 162	TCP	SNMP
Nodos de NSX Edge	Servidores SNMP	161, 162	UDP	SNMP
Nodos de NSX Edge	Servidores syslog	514	TCP	Syslog
Nodos de NSX Edge	Servidores syslog	514	UDP	Syslog
Nodos de NSX Edge	Servidores syslog	6514	TCP	Syslog
Nodos de NSX Edge	Servidores syslog	6514	UDP	Syslog
Nodos de NSX Edge	Destino de traceroute	33434 - 33523	UDP	Traceroute
Nodos de NSX Edge y nodos de transporte	Nodos de NSX Edge	3784, 3785	UDP	BFD entre la dirección IP de TEP del nodo de transporte en los datos.
Servidores SNMP	Nodos de NSX Edge	161	UDP	SNMP

Puertos TCP y UDP utilizados por ESXi, hosts de KVM y servidor nativo

ESXi, los hosts de KVM y los servidores nativos cuando se utilizan como nodos de transporte necesitan tener determinados puertos TCP y UDP disponibles.

Tabla 3-4. Puertos TCP y UDP utilizados por hosts ESXi y de KVM

Origen	Destino	Puerto	Protocolo	Descripción
Host ESXi	NSX Controller	1235	TCP	Plano de control: comunicación de LCP a CCP
Host ESXi	NSX Manager	5671	TCP	Canal de comunicación de AMQP a NSX Manager
Host ESXi	NSX Manager	8080	TCP	Instalar y actualizar el repositorio HTTP
Host ESXi y de KVM	NSX Manager	443	TCP	Conexión de aprovisionamiento y administración
Host ESXi y de KVM	NSX Manager	443	TCP	Instalar y actualizar el repositorio HTTP
Endpoint de terminación (Termination End Point, TEP) GENEVE	Endpoint de terminación (Termination End Point, TEP) GENEVE	6081	UDP	Red de transporte
host de KVM	NSX Manager	5671	TCP	Canal de comunicación de AMQP a NSX Manager
host de KVM	NSX Controller	1235	TCP	Plano de control: comunicación de LCP a CCP
host de KVM	NSX Manager	8080	TCP	Instalar y actualizar el repositorio HTTP
NSX Manager	Host ESXi	443	TCP	Conexión de aprovisionamiento y administración
NSX Manager	host de KVM	443	TCP	Conexión de aprovisionamiento y administración
Host ESXi y de KVM	Servidores syslog	514	TCP	Syslog
Host ESXi y de KVM	Servidores syslog	514	UDP	Syslog
Host ESXi y de KVM	Servidores syslog	6514	TCP	Syslog
Host ESXi y de KVM	Servidores syslog	6514	UDP	Syslog
Nodo de transporte de NSX-T Data Center	Nodo de transporte de NSX-T Data Center	3784, 3785	UDP	Sesión de BFD entre TEP, en la ruta de datos mediante la interfaz de TEP

Instalar componentes de NSX-T Data Center

Debe instalar los componentes básicos de NSX Manager y NSX Edge para usar NSX-T Data Center.

Instalación de NSX Manager

NSX Manager proporciona una interfaz gráfica de usuario (GUI) y varias API REST para crear, configurar y supervisar componentes de NSX-T Data Center, como conmutadores lógicos, enrutadores lógicos y firewalls.

NSX Manager proporciona una vista del sistema y es el componente de administración de NSX-T Data Center.

Para la alta disponibilidad, NSX-T Data Center admite un clúster de administración de tres instancias de NSX Manager. Para un entorno de producción, se recomienda implementar un clúster de administración. Para un entorno de prueba de concepto, puede implementar una sola instancia de NSX Manager.

Requisitos de instalación, de plataforma y de implementación para NSX Manager

En la siguiente tabla se detallan los requisitos de implementación, plataforma e instalación de NSX Manager

Requisitos	Descripción
Métodos de implementación admitidos	<ul style="list-style-type: none"> ■ OVA/OVF ■ QCOW2
Plataformas compatibles	<p>Consulte Requisitos del sistema de máquinas virtuales de NSX Manager.</p> <p>En ESXi, se recomienda que el dispositivo de NSX Manager se instale en el almacenamiento compartido.</p>
Dirección IP	Un NSX Manager debe disponer de una dirección IP estática. No puede cambiar la dirección IP tras la instalación.
Contraseña del dispositivo de NSX-T Data Center	<ul style="list-style-type: none"> ■ Al menos 12 caracteres ■ Al menos una letra en minúsculas ■ Al menos una letra en mayúsculas ■ Al menos un dígito ■ Al menos un carácter especial ■ Al menos cinco caracteres distintos ■ Sin palabras del diccionario ■ Sin palíndromos ■ No se admiten más de cuatro secuencias de caracteres monotónicos.
Nombre de host	<p>Cuando instale NSX Manager, especifique un nombre de host sin caracteres que no sean válidos, como, por ejemplo, guiones bajos. Si el nombre de host contiene un carácter que no sea válido, después de la implementación, el nombre de host será nsx-manager.</p> <p>Para obtener más información sobre las restricciones que se aplican al nombre de host, consulte https://tools.ietf.org/html/rfc952 y https://tools.ietf.org/html/rfc1123.</p>
VMware Tools	La máquina virtual de NSX Manager que se ejecuta en ESXi tiene VMTools instalado. No elimine ni actualice VMTools.

Requisitos	Descripción
Sistema	<ul style="list-style-type: none"> ■ Compruebe que se cumplan los requisitos del sistema. Consulte Requisitos del sistema. ■ Compruebe que estén abiertos los puertos necesarios. Consulte Puertos y protocolos. ■ Compruebe que haya un almacén de datos configurado y accesible en el host ESXi. ■ Compruebe que tenga 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. ■ Si aún no tiene una, cree la red del grupo de puertos de máquinas virtuales de destino. Coloque los dispositivos de NSX-T Data Center en una red de máquinas virtuales de administración. <p>Si tiene varias redes de administración, puede agregar rutas estáticas a las otras redes desde el dispositivo NSX-T Data Center.</p> <ul style="list-style-type: none"> ■ Planifique su esquema de direcciones IP IPv4 o IPv6 de NSX Manager.
Privilegios de OVF	<p>Compruebe que tenga privilegios adecuados para implementar una plantilla OVF en el host ESXi.</p> <p>Una herramienta de administración que puede implementar plantillas OVF, como vCenter Server o vSphere Client. La herramienta de implementación de OVF debe admitir opciones de configuración que permitan realizar la configuración de forma manual.</p> <p>La versión de la herramienta de OVF debe ser 4.0 o posterior.</p>
Complemento de cliente	Debe estar instalado el complemento de integración de clientes.

Nota En una instalación nueva de NSX Manager, después de reiniciar el sistema o tras cambiar la contraseña de **admin** cuando se le solicita en el primer inicio de sesión, puede que NSX Manager tarde varios minutos en arrancar.

Escenarios de instalación de NSX Manager

Importante Cuando instale NSX Manager desde un archivo OVA u OVF, desde vSphere Client o desde la línea de comandos, los valores de la propiedad OVA/OVF, como nombres de usuario, contraseñas o direcciones IP, no se validan antes de que se encienda la máquina virtual.

- Si especifica un nombre de usuario para **admin** o **audit**, el nombre debe ser único. Si especifica el mismo nombre, este se ignora y se usan los nombres predeterminados (**admin** y **audit**).
- Si la contraseña para el usuario **admin** no cumple los requisitos de complejidad, debe iniciar sesión en NSX Manager mediante SSH o en la consola como usuario **admin** con la contraseña **default**. Se le solicitará que cambie la contraseña.
- Si la contraseña del usuario **audit** no cumple los requisitos de complejidad, la cuenta de usuario se deshabilita. Para habilitar la cuenta, inicie sesión en NSX Manager mediante SSH o en la consola como el usuario **admin** y ejecute el comando **set user audit** para establecer la contraseña del usuario **audit** (la contraseña actual es una cadena vacía).

- Si la contraseña para el usuario **root** no cumple los requisitos de complejidad, debe iniciar sesión en NSX Manager mediante SSH o en la consola como **root** con la contraseña **vmware**. Se le solicitará que cambie la contraseña.

Precaución Los cambios realizados en NSX-T Data Center cuando se ha iniciado sesión con las credenciales de usuario **root** pueden provocar errores en el sistema y pueden afectar a la red. Solo se pueden realizar cambios con las credenciales de usuario **root** siguiendo las instrucciones del equipo de soporte de VMware.

Nota Los servicios principales del dispositivo no se iniciarán hasta que se establezca una contraseña con un nivel de complejidad suficiente.

Después de implementar NSX Manager desde un archivo OVA, no puede cambiar la configuración de la IP de la máquina virtual si apaga esta máquina virtual y modifica la configuración OVA en vCenter Server.

Configurar NSX Manager para el acceso mediante el servidor DNS

De forma predeterminada, los nodos de transporte acceden a NSX Manager en función de sus direcciones IP. Sin embargo, pueden hacerlo en función de los nombres de DNS de las instancias de NSX Manager.

Al habilitar el uso de FQDN (DNS) en instancias de NSX Manager, la dirección IP de los administradores puede cambiar sin que eso afecte a los nodos de transporte.

Para habilitar el uso de FQDN, publique los FQDN de las instancias de NSX Manager.

Nota Es necesario habilitar el uso de FQDN (DNS) en las instancias de NSX Manager para las implementaciones de multisitio Lite y NSX Cloud. (Es opcional para los demás tipos de implementación). Consulte *Implementación multisitio de NSX-T Data Center* en la *Guía de administración de NSX-T Data Center* y [Capítulo 11 Instalar componentes de NSX Cloud](#) en esta guía.

Publicar los FQDN de las instancias de NSX Manager

Después de instalar los componentes principales de NSX-T Data Center y CSM, para permitir que NAT utilice un FQDN, debe configurar las entradas de búsqueda y búsqueda inversa en el servidor DNS de NSX-T de su implementación.

Además, también debe habilitar la publicación del FQDN de NSX Manager mediante la API de NSX-T.

Ejemplo de solicitud: PUT `https://<nsx-mgr>/api/v1/configs/management`

```
{
  "publish_fqdns": true,
  "_revision": 0
}
```

Ejemplo de respuesta:

```
{
  "publish_fqdns": true,
  "_revision": 1
}
```

Consulte la *Guía de la API de NSX-T Data Center* para obtener más detalles.

Nota Después de publicar los FQDN, valide el acceso de los nodos de transporte como se describe en la siguiente sección.

Validar el acceso a través de los nodos de transporte mediante FQDN

Después de publicar los FQDN de las instancias de NSX Manager, compruebe que los nodos de transporte accedan correctamente a las instancias de NSX Manager.

Mediante SSH, inicie sesión en un nodo de transporte, como un hipervisor o un nodo de Edge, y ejecute el comando de CLI `get controllers`.

Ejemplo de respuesta:

Controller IP	Port	SSL	Status	Is Physical Master	Session State	Controller FQDN
192.168.60.5	1235	enabled	connected	true	up	nsxmgr.corp.com

Instalación de NSX Edge

NSX Edge proporciona servicios de enrutamiento y conectividad a las instancias de NSX Edge de red que sean externas a la implementación de NSX-T Data Center. Es obligatorio contar con una instancia de NSX Edge si desea implementar un enrutador de nivel 0 o un enrutador de nivel 1 con servicios con estado, como la traducción de direcciones de red (Network Address Translation, NAT), VPN, entre otros.

Nota Solo puede haber un enrutador de nivel 0 por cada nodo de NSX Edge. Sin embargo, se pueden alojar varios enrutadores de carga de nivel 1 en un mismo nodo NSX Edge. Se pueden combinar máquinas virtuales de NSX Edge de diferentes tamaños en el mismo clúster, pero no es recomendable.

Tabla 3-5. Requisitos de instalación, de plataformas y de implementación para NSX Edge

Requisitos	Descripción
Métodos de implementación admitidos	<ul style="list-style-type: none"> ■ OVA/OVF ■ ISO con PXE ■ ISO sin PXE
Plataformas compatibles	NSX Edge solo es compatible en ESXi o sin sistema operativo. NSX Edge no es compatible con KVM.
Instalación de PXE	La cadena Contraseña debe estar cifrada con el algoritmo sha-512 para la contraseña del usuario administrador y raíz.

Tabla 3-5. Requisitos de instalación, de plataformas y de implementación para NSX Edge (continuación)

Requisitos	Descripción
Contraseña del dispositivo de NSX-T Data Center	<ul style="list-style-type: none"> ■ Al menos 12 caracteres ■ Al menos una letra en minúsculas ■ Al menos una letra en mayúsculas ■ Al menos un dígito ■ Al menos un carácter especial ■ Al menos cinco caracteres distintos ■ Sin palabras del diccionario ■ Sin palíndromos ■ No se admiten más de cuatro secuencias de caracteres monotónicos.
Nombre de host	<p>Cuando instale NSX Edge, especifique un nombre de host sin caracteres que no sean válidos, como, por ejemplo, guiones bajos. Si el nombre de host contiene un carácter no válido, después de la implementación, el nombre de host será localhost. Para obtener más información sobre las restricciones que se aplican al nombre de host, consulte https://tools.ietf.org/html/rfc952 y https://tools.ietf.org/html/rfc1123.</p>
VMware Tools	<p>La máquina virtual de NSX Edge que se ejecuta en ESXi tiene VMTools instalado. No elimine ni actualice VMTools.</p>
Sistema	<p>Compruebe que se cumplan los requisitos del sistema. Consulte Requisitos del sistema de máquinas virtuales de NSX Edge.</p>
Puertos	<p>Compruebe que estén abiertos los puertos necesarios. Consulte Puertos y protocolos.</p>
Direcciones IP	<p>Si tiene varias redes de administración, puede agregar rutas estáticas a las otras redes desde el dispositivo NSX-T Data Center.</p> <p>Planifique su esquema de direcciones IP IPv4 o IPv6 de NSX Edge.</p>
Plantilla OVF	<ul style="list-style-type: none"> ■ Compruebe que tenga privilegios adecuados para implementar una plantilla OVF en el host ESXi. ■ Compruebe que los nombres de host no incluyan guiones bajos. De lo contrario, el nombre de host se establece en <i>nsx-manager</i>. ■ Una herramienta de administración que puede implementar plantillas OVF, como vCenter Server o vSphere Client. <p>La herramienta de implementación de OVF debe admitir opciones de configuración que permitan realizar la configuración de forma manual.</p> <ul style="list-style-type: none"> ■ Debe estar instalado el complemento de integración de clientes.
Servidor NTP	<p>Debe configurarse el mismo servidor NTP en todos los servidores de NSX Edge en un clúster de servidores perimetrales.</p>

Escenarios de instalación de NSX Edge

Importante Cuando instale NSX Edge desde un archivo OVA u OVF, desde vSphere Web Client o desde la línea de comandos, los valores de la propiedad OVA/OVF, como nombres de usuario, contraseñas o direcciones IP, no se validan antes de que se encienda la máquina virtual.

- Si especifica un nombre de usuario para **admin** o **audit**, el nombre debe ser único. Si especifica el mismo nombre, este se ignora y se usan los nombres predeterminados (**admin** y **audit**).
- Si la contraseña para el usuario **admin** no cumple los requisitos de complejidad, debe iniciar sesión en NSX Edge mediante SSH o en la consola como usuario **admin** con la contraseña **default**. Se le solicitará que cambie la contraseña.
- Si la contraseña del usuario **audit** no cumple los requisitos de complejidad, la cuenta de usuario se deshabilita. Para habilitar la cuenta, inicie sesión en NSX Edge mediante SSH o en la consola como el usuario **admin** y ejecute el comando **set user audit** para establecer la contraseña del usuario **audit** (la contraseña actual es una cadena vacía).
- Si la contraseña para el usuario **root** no cumple los requisitos de complejidad, debe iniciar sesión en NSX Edge mediante SSH o en la consola como **root** con la contraseña **vmware**. Se le solicitará que cambie la contraseña.

Precaución Los cambios realizados en NSX-T Data Center cuando se ha iniciado sesión con las credenciales de usuario **root** pueden provocar errores en el sistema y pueden afectar a la red. Solo se pueden realizar cambios con las credenciales de usuario **root** siguiendo las instrucciones del equipo de soporte de VMware.

Nota Los servicios principales del dispositivo no se inician hasta que se establezca una contraseña con un nivel de complejidad suficiente.

Después de implementar NSX Edge desde un archivo OVA, no puede cambiar la configuración de la IP de la máquina virtual si apaga esta máquina virtual y modifica la configuración OVA en vCenter Server.

Unir NSX Edge al plano de administración

Unir NSX Edge al plano de administración garantiza que NSX Manager y NSX Edge se pueden comunicar entre sí.

Requisitos previos

Verifique que dispone de privilegios de administrador para iniciar sesión en las instancias de NSX Edge y el dispositivo de NSX Manager.

Procedimiento

- 1 Abra una sesión SSH en el dispositivo de NSX Manager.
- 2 Abra una sesión SSH en el NSX Edge.

- 3 En el dispositivo NSX Manager, ejecute el comando `get certificate api thumbprint`.

La salida de comandos es una cadena alfanumérica exclusiva para esta instancia de NSX Manager.

Por ejemplo:

```
NSX-Manager1> get certificate api thumbprint
...
```

- 4 En el NSX Edge, ejecute el comando **join management-plane**.

Proporcione la siguiente información:

- Nombre de host o dirección IP del NSX Manager con un número de puerto opcional
- Nombre de usuario del NSX Manager
- Huella digital del certificado del NSX Manager
- Contraseña del NSX Manager

```
NSX-Edge1> join management-plane NSX-Manager1 username admin thumbprint <NSX-Manager1's-
thumbprint>
Password for API user: <NSX-Manager1's-password>
Node successfully registered and Edge restarted
```

Repita este comando en cada nodo de NSX Edge.

- 5 Compruebe el resultado ejecutando el comando `get managers` en sus NSX Edge.

```
nsx-edge-1> get managers
- 192.168.110.47 Connected
```

- 6 En la interfaz de usuario de NSX Manager, seleccione la página **Sistema > Tejido > Nodos > Nodos de transporte de Edge**.

La conectividad de NSX Manager debe estar activa. Si la conectividad de NSX Manager no está activa, actualice la ventana del explorador.

Pasos siguientes

Agregue los NSX Edge como nodos de transporte. Consulte [Crear un nodo de transporte de NSX Edge](#).

Instalar NSX-T Data Center en vSphere

4

Puede instalar los componentes de NSX-T Data Center, NSX Manager y NSX Edge usando la interfaz de usuario o la CLI.

Asegúrese de que tiene la versión compatible de vSphere. Consulte [Soporte de vSphere](#).

Este capítulo incluye los siguientes temas:

- [Instalar NSX Manager y los dispositivos disponibles](#)
- [Instalar una instancia de NSX Edge en ESXi utilizando una GUI de vSphere](#)

Instalar NSX Manager y los dispositivos disponibles

Puede utilizar vSphere Client para implementar NSX Manager o Cloud Service Manager como dispositivo virtual.

Cloud Service Manager es un dispositivo virtual que utiliza componentes de NSX-T Data Center y los integra en la nube pública.

Requisitos previos

- Compruebe que se cumplan los requisitos del sistema. Consulte [Requisitos del sistema](#).
- Compruebe que estén abiertos los puertos necesarios. Consulte [Puertos y protocolos](#).
- Compruebe que haya un almacén de datos configurado y accesible en el host ESXi.
- Compruebe que tenga 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.
- Si aún no tiene una, cree la red del grupo de puertos de máquinas virtuales de destino. Coloque los dispositivos de NSX-T Data Center en una red de máquinas virtuales de administración.

Si tiene varias redes de administración, puede agregar rutas estáticas a las otras redes desde el dispositivo NSX-T Data Center.

- Planifique su esquema de direcciones IP IPv4 o IPv6 de NSX Manager.

Procedimiento

- 1 Busque el archivo OVA de NSX-T Data Center en el portal de descargas de VMware.

Puede copiar la URL de descarga, o bien descargar el archivo OVA.

- 2 En vSphere Client, seleccione el host en el que desee instalar NSX-T Data Center.
- 3 Haga clic en el botón secundario y seleccione **Implementar plantilla OVF** para iniciar el Asistente de instalación.
- 4 Introduzca la URL de descarga del archivo OVA, o desplácese hasta el archivo OVA.
- 5 Introduzca un nombre para la máquina virtual de NSX Manager.
El nombre que escriba aparecerá en el inventario de vSphere.
- 6 Seleccione un recurso informático para el dispositivo de NSX Manager.
 - ◆ Para realizar la instalación en un host de ESXi administrado por vCenter, seleccione el host en el que desee implementar el dispositivo de NSX Manager.
 - ◆ Para realizar la instalación en un host de ESXi independiente, seleccione el host en el que desee implementar el dispositivo de NSX Manager.
- 7 Compruebe los detalles de la plantilla de OVF.
- 8 Para que el rendimiento sea óptimo, reserve memoria para el dispositivo de NSX Manager.
Establezca la reserva para garantizar que NSX Manager tenga suficiente memoria como para ejecutarse de forma eficiente. Consulte [Requisitos del sistema de máquinas virtuales de NSX Manager](#).
- 9 Seleccione un almacén de datos para almacenar los archivos de dispositivos de NSX Manager.
- 10 Seleccione una red de destino para cada red de origen.
- 11 Seleccione el grupo de puertos o la red de destino de NSX Manager.
- 12 Especifique la raíz del sistema de NSX Manager, el administrador de la CLI y las contraseñas de auditoría.

Sus contraseñas deben cumplir las restricciones de seguridad para contraseñas.

- Al menos 12 caracteres
- Al menos una letra en minúsculas
- Al menos una letra en mayúsculas
- Al menos un dígito
- Al menos un carácter especial
- Al menos cinco caracteres distintos
- Sin palabras del diccionario
- Sin palíndromos
- No se admiten más de cuatro secuencias de caracteres monotónicos.

13 Escriba el nombre de host de NSX Manager.

Nota El nombre de host debe ser un nombre de dominio válido. Asegúrese de que cada parte del nombre de host (dominio y subdominio) que esté separada por el punto empiece por un carácter alfabético.

14 Acepte la función predeterminada **NSX Manager** para la máquina virtual.

Seleccione la función **nsx-cloud-service-manager** en el menú desplegable para instalar el dispositivo de NSX Cloud.

15 Introduzca la puerta de enlace predeterminada, la IPv4 de la red de administración, la máscara de red de administración, el DNS y la dirección IP de NTP.

16 Habilite SSH y permita el inicio de sesión SSH raíz en la línea de comandos de NSX Manager.

De forma predeterminada, estas opciones están deshabilitadas por motivos de seguridad.

17 Compruebe que las especificaciones de la plantilla OVF personalizada sean precisas y haga clic en **Finalizar** para iniciar la instalación.

La instalación puede durar entre 7 y 8 minutos.

18 En vSphere Client, abra la consola de máquina virtual de NSX Manager para realizar un seguimiento del proceso de arranque.

19 Una vez que NSX Manager arranque, inicie sesión en la interfaz de línea de comandos y ejecute el comando `get interface eth0` para comprobar que la dirección IP se aplicó según lo previsto.

20 Introduzca el comando `get services` para comprobar que todos los servicios se están ejecutando.

Si los servicios no se están ejecutando, espere a que todos los servicios empiecen a ejecutarse.

Nota Los siguientes servicios no se ejecutan de forma predeterminada: `liagent`, `migration-coordinator` y `snmp`. Puede iniciarlos de la siguiente forma:

- `start service liagent`
- `start service migration-coordinator`
- Para SNMP:

```
set snmp community <community-string>
start service snmp
```

21 Compruebe que NSX Manager tenga la conectividad necesaria.

Asegúrese de que puede realizar las siguientes tareas.

- Haga ping a NSX Manager desde otro equipo.
- NSX Manager puede hacer ping a la puerta de enlace predeterminada.
- NSX Manager puede hacer ping a los hosts del hipervisor que están en la misma red que NSX Manager con la interfaz de administración.

- NSX Manager puede hacer ping al servidor DNS y al servidor NTP.
- Si habilitó SSH, asegúrese de que puede utilizarlo con su NSX Manager.

Si no se estableció la conectividad, asegúrese de que el adaptador de red del dispositivo virtual esté en la VLAN o red adecuada.

Pasos siguientes

Inicie sesión en NSX Manager en un explorador web compatible. Consulte [Iniciar sesión en la instancia de NSX Manager recién creada](#) .

Instalar NSX Manager en ESXi utilizando la herramienta OVF de la línea de comandos

Si prefiere automatizar la instalación de NSX Manager o usar la CLI para este proceso, puede utilizar VMware OVF Tool, que es una utilidad de línea de comandos.

Por motivos de seguridad, `nsx_isSSHEnabled` y `nsx_allowSSHRootLogin` están deshabilitados de forma predeterminada. Cuando están deshabilitados, no puede utilizar SSH ni iniciar sesión en la línea de comandos de NSX Manager. Si habilita `nsx_isSSHEnabled` pero no habilita `nsx_allowSSHRootLogin`, podrá utilizar SSH con NSX Manager, pero no podrá iniciar sesión como raíz.

Requisitos previos

- Compruebe que se cumplan los requisitos del sistema. Consulte [Requisitos del sistema](#).
- Compruebe que estén abiertos los puertos necesarios. Consulte [Puertos y protocolos](#).
- Compruebe que haya un almacén de datos configurado y accesible en el host ESXi.
- Compruebe que tenga 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.
- Si aún no tiene una, cree la red del grupo de puertos de máquinas virtuales de destino. Coloque los dispositivos de NSX-T Data Center en una red de máquinas virtuales de administración.

Si tiene varias redes de administración, puede agregar rutas estáticas a las otras redes desde el dispositivo NSX-T Data Center.

- Planifique su esquema de direcciones IP IPv4 o IPv6 de NSX Manager.

Procedimiento

- 1 Ejecute el comando `ovftool` con los parámetros apropiados.

El proceso depende de si el host es independiente o está administrado por vCenter Server.

- Para un host independiente:

- Ejemplo de Windows:

```
C:\Program Files\VMware\VMware OVF Tool>ovftool \
--sourceType=OVA \
--name=nsx-manager \
--X:injectOvfEnv \
--X:logFile=<filepath>\nsxovftool.log \
--allowExtraConfig \
--datastore=<datastore name> \
--network=<network name> \
--acceptAllEulas \
--noSSLVerify \
--diskMode=thin \
--powerOn \
--prop:"nsx_role=nsx-manager nsx-controller" \
--prop:"nsx_ip_0=10.168.110.75" \
--prop:"nsx_netmask_0=255.255.255.0" \
--prop:"nsx_gateway_0=10.168.110.1" \
--prop:"nsx_dns1_0=10.168.110.10" \
--prop:"nsx_domain_0=corp.local" \
--prop:"nsx_ntp_0=10.168.110.10" \
--prop:"nsx_isSshEnabled=<True|False>" \
--prop:"nsx_allowSSHRootLogin=<True|False>" \
--prop:"nsx_passwd_0=<password>" \
--prop:"nsx_cli_passwd_0=<password>" \
--prop:"nsx_cli_audit_passwd_0=<password>" \
--prop:"nsx_hostname=nsx-manager" \
<nsx-unified-appliance-release>.ova \
vi://root:<password>@10.168.110.51
```

Nota El bloque de código de Windows anterior utiliza la barra diagonal inversa (\) para indicar la continuación de la línea de comandos. En uso real, omita la barra diagonal inversa y escriba el comando completo en una sola línea.

Nota En el ejemplo anterior, la dirección IP de la máquina host en la que se va a implementar NSX Manager es 10.168.110.51.

- Ejemplo de Linux:

```
mgrformfactor="small"
ipAllocationPolicy="fixedPolicy"
mgrdatastore="QNAP-Share-VMs"
mgrnetwork="Management-VLAN-210"

mgrname01="nsx-manager-01"
```

```

mgrhostname01="nsx-manager-01"
mgrip01="192.168.210.121"

mgrnetmask="255.255.255.0"
mgrgw="192.168.210.254"
mgrdns="192.168.110.10"
mgrntp="192.168.210.254"
mgrpasswd="<password>"
mgrssh="<True|False>"
mgrroot="<True|False>"
logLevel="trivia"

mgresxhost01="192.168.110.113"

ovftool --noSSLVerify --skipManifestCheck --powerOn \
--deploymentOption=$mgrformfactor \
--diskMode=thin \
--acceptAllEulas \
--allowExtraConfig \
--ipProtocol=IPv4 \
--ipAllocationPolicy=$ipAllocationPolicy \
--datastore=$mgrdatastore \
--network=$mgrnetwork \
--name=$mgrname01 \
--prop:nsx_hostname=$mgrhostname01 \
--prop:nsx_role="nsx-manager nsx-controller" \
--prop:nsx_ip_0=$mgrip01 \
--prop:nsx_netmask_0=$mgrnetmask \
--prop:nsx_gateway_0=$mgrgw \
--prop:nsx_dns1_0=$mgrdns \
--prop:nsx_ntp_0=$mgrntp \
--prop:nsx_passwd_0=$mgrpasswd \
--prop:nsx_cli_passwd_0=$mgrpasswd \
--prop:nsx_cli_audit_passwd_0=$mgrpasswd \
--prop:nsx_isSSHEnabled=$mgrssh \
--prop:nsx_allowSSHRootLogin=$mgrroot \
--X:logFile=nsxt-manager-ovf.log \
--X:logLevel=$logLevel \
/home/<user/nsxt-autodeploy/<nsx-unified-appliance-release>.ova \
vi://root:<password>@$mgresxhost01

```

El resultado debe ser similar al siguiente:

```

Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://root:<password>@10.168.110.51
Deploying to VI: vi://root:<password>@10.168.110.51
Transfer Completed
Powering on VM: nsx-manager nsx-controller
Task Completed
Completed successfully

```

- Para un host administrado por vCenter Server:
- Ejemplo de Windows:

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-manager \
--X:injectOvfEnv \
--X:logFile=ovftool.log \
  --allowExtraConfig \
--datastore=ds1 \
--network="management" \
--acceptAllEulas \
--noSSLVerify \
--diskMode=thin \
--powerOn \
--prop:"nsx_role=nsx-manager nsx-controller" \
--prop:"nsx_ip_0=10.168.110.75" \
--prop:"nsx_netmask_0=255.255.255.0" \
--prop:"nsx_gateway_0=10.168.110.1" \
--prop:"nsx_dns1_0=10.168.110.10" \
--prop:"nsx_domain_0=corp.local" \
--prop:"nsx_ntp_0=10.168.110.10" \
--prop:"nsx_isSSHEnabled=<True|False>" \
--prop:"nsx_allowSSHRootLogin=<True|False>" \
--prop:"nsx_passwd_0=<password>" \
--prop:"nsx_cli_passwd_0=<password>" \
--prop:"nsx_hostname=nsx-manager" \
<nsx-unified-appliance-release>.ova \
vi://administrator@vsphere.local:<password>@10.168.110.24/?ip=10.168.110.51
```

Nota El bloque de código de Windows anterior utiliza la barra diagonal inversa (\) para indicar la continuación de la línea de comandos. En uso real, omita la barra diagonal inversa y escriba el comando completo en una sola línea.

- Ejemplo de Linux:

```
mgrformfactor="small"
ipAllocationPolicy="fixedPolicy"
mgrdatastore="QNAP-Share-VMs"
mgrnetwork="Management-VLAN-210"

mgrname01="nsx-manager-01"
mgrhostname01="nsx-manager-01"
mgrip01="192.168.210.121"

mgrnetmask="255.255.255.0"
mgrgw="192.168.210.254"
mgrdns="192.168.110.10"
mgrntp="192.168.210.254"
mgrpasswd="<password>"
mgrssh="<True|False>"
mgrroot="<True|False>"
logLevel="trivia"
```

```

vcadmin="administrator@vsphere.local"
vcpass="<password>"
vcip="192.168.110.151"
mgresxhost01="192.168.110.113"

ovftool --noSSLVerify --skipManifestCheck --powerOn \
--deploymentOption=$mgrformfactor \
--diskMode=thin \
--acceptAllEulas \
--allowExtraConfig \
--ipProtocol=IPv4 \
--ipAllocationPolicy=$ipAllocationPolicy \
--datastore=$mgrdatastore \
--network=$mgrnetwork \
--name=$mgrname01 \
--prop:nsx_hostname=$mgrhostname01 \
--prop:nsx_role="nsx-manager nsx-controller" \
--prop:nsx_ip_0=$mgrip01 \
--prop:nsx_netmask_0=$mgrnetmask \
--prop:nsx_gateway_0=$mgrgw \
--prop:nsx_dns1_0=$mgrdns \
--prop:nsx_ntp_0=$mgrntp \
--prop:nsx_passwd_0=$mgrpasswd \
--prop:nsx_cli_passwd_0=$mgrpasswd \
--prop:nsx_cli_audit_passwd_0=$mgrpasswd \
--prop:nsx_isSSHEnabled=$mgrssh \
--prop:nsx_allowSSHRootLogin=$mgrroot \
--X:logFile=nsxt-manager-ovf.log \
--X:logLevel=$logLevel \
/home/<user/nsxt-autodeploy/<nsx-unified-appliance-release>.ova \
vi://$vcadmin:$vcpass@$vcip/?ip=$mgresxhost01

```

El resultado debe ser similar al siguiente:

```

Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://administrator@vsphere.local@10.168.110.24:443/
Deploying to VI: vi://administrator@vsphere.local@10.168.110.24:443/
Transfer Completed
Powering on VM: nsx-manager nsx-controller
Task Completed
Completed successfully

```

- 2 Para que el rendimiento sea óptimo, reserve memoria para el dispositivo de NSX Manager.

Establezca la reserva para garantizar que NSX Manager tenga suficiente memoria como para ejecutarse de forma eficiente. Consulte [Requisitos del sistema de máquinas virtuales de NSX Manager](#).

- 3 En vSphere Client, abra la consola de máquina virtual de NSX Manager para realizar un seguimiento del proceso de arranque.

- 4 Una vez que NSX Manager arranque, inicie sesión en la interfaz de línea de comandos y ejecute el comando `get interface eth0` para comprobar que la dirección IP se aplicó según lo previsto.
- 5 Compruebe que NSX Manager tenga la conectividad necesaria.

Asegúrese de que puede realizar las siguientes tareas.

- Haga ping a NSX Manager desde otro equipo.
- NSX Manager puede hacer ping a la puerta de enlace predeterminada.
- NSX Manager puede hacer ping a los hosts del hipervisor que están en la misma red que NSX Manager con la interfaz de administración.
- NSX Manager puede hacer ping al servidor DNS y al servidor NTP.
- Si habilitó SSH, asegúrese de que puede utilizarlo con su NSX Manager.

Si no se estableció la conectividad, asegúrese de que el adaptador de red del dispositivo virtual esté en la VLAN o red adecuada.

Pasos siguientes

Inicie sesión en NSX Manager en un explorador web compatible. Consulte [Iniciar sesión en la instancia de NSX Manager recién creada](#).

Configurar NSX-T Data Center para que aparezca el menú GRUB durante el arranque

Hay que configurar el dispositivo de NSX-T Data Center para que aparezca el menú GRUB en el momento del arranque es necesaria si se pretende restablecer la contraseña raíz del dispositivo de NSX-T Data Center.

Importante Si la configuración no se realiza después de implementar el dispositivo y olvida la raíz, el administrador o la contraseña de auditoría, no se podrá restablecer.

Procedimiento

- 1 Inicie sesión en la máquina virtual como raíz.
- 2 Cambie el valor del parámetro GRUB_HIDDEN_TIMEOUT en el archivo `/etc/default/grub`.
`GRUB_HIDDEN_TIMEOUT=2`
- 3 (opcional) Cambie la contraseña de GRUB en el archivo `/etc/grub.d/40_custom`.
La contraseña predeterminada es `VMware1`.
- 4 Actualice la configuración de GRUB.
`update-grub`

Iniciar sesión en la instancia de NSX Manager recién creada

Después de instalar NSX Manager, puede utilizar la interfaz de usuario para realizar otras tareas de instalación.

Después de instalar NSX Manager, puede unirse al Programa de mejora de la experiencia de cliente (Customer Experience Improvement Program, CEIP) de NSX-T Data Center. Consulte el Programa de mejora de la experiencia de cliente en *Guía de administración de NSX-T Data Center* para obtener más información acerca del programa, incluyendo cómo unirse o salir de él más adelante.

Requisitos previos

Compruebe que esté instalado NSX Manager. Consulte [Instalar NSX Manager y los dispositivos disponibles](#).

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión con privilegios de administrador en NSX Manager.
Se muestra el CLUF.
- 2 Lea y acepte las condiciones del CLUF.
- 3 Seleccione si desea unirse al programa CEIP de VMware.
- 4 Haga clic en **Guardar**

Agregar un administrador de equipos

Un administrador de equipos, por ejemplo vCenter Server, es una aplicación que administra recursos, como hosts y máquinas virtuales.

NSX-T Data Center sondea los administradores de equipos para detectar cambios, como las máquinas virtuales y los hosts agregados o eliminados, y actualiza el inventario con los resultados obtenidos. Como opción, es posible agregar un administrador de equipos, debido a que NSX-T Data Center obtiene información del inventario incluso sin un administrador de este tipo, como máquinas virtuales y hosts independientes.

Al agregar un administrador de equipo de vCenter Server, debe proporcionar las credenciales de un usuario de vCenter Server. Puede proporcionar las credenciales del administrador de vCenter Server o crear específicamente una función y un usuario para NSX-T Data Center y proporcionar las credenciales de este usuario. Esta función debe tener los siguientes privilegios de vCenter Server:

Extension.Register extension

Extension.Unregister extension

Extension.Update extension

Sessions.Message

Sessions.Validate session

Sessions.View and stop sessions

Host.Configuration.Maintenance
Host.Local Operations.Create virtual machine
Host.Local Operations.Delete virtual machine
Host.Local Operations.Reconfigure virtual machine
Tasks
Scheduled task
Global.Cancel task
Permissions.Reassign role permissions
Resource.Assign vApp to resource pool
Resource.Assign virtual machine to resource pool
Virtual Machine.Configuration
Virtual Machine.Guest Operations
Virtual Machine.Provisioning
Virtual Machine.Inventory
Network.Assign network
vApp

Para obtener más información sobre las funciones y los privilegios de vCenter Server, consulte el documento *Seguridad de vSphere* .

Requisitos previos

- Compruebe que usa la versión compatible de vSphere. Consulte [Versión de vSphere admitida](#).
- Comunicación de IPv6 e IPv4 con vCenter Server.
- Compruebe que usa el número recomendado de administradores de equipos. Consulte <https://configmax.vmware.com/home>.

Nota NSX-T Data Center no es compatible con el mismo vCenter Server para registrarse con más de un NSX Manager.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Sistema > Tejido > Administradores de equipos > Agregar**.

3 Complete la información de los administradores de equipos.

Opción	Descripción
Nombre y descripción	<p>Escriba el nombre para identificar vCenter Server.</p> <p>De forma opcional, puede incluir cualquier información especial, como el número de clústeres en vCenter Server.</p>
Dirección IP o nombre de dominio	Especifique la dirección IP de vCenter Server.
Tipo	Mantenga la opción predeterminada.
Nombre de usuario y contraseña	Escriba las credenciales para iniciar sesión en vCenter Server.
Huella digital	Escriba el valor del algoritmo de huella digital SHA-256 de vCenter Server.

Si deja el valor de huella digital en blanco, se le solicitará que acepte la huella digital que proporciona el servidor.

Tras aceptar la huella digital, NSX-T Data Center tarda unos segundos en detectar y registrar los recursos de vCenter Server.

4 Si el icono de progreso cambia de **En curso** a **No registrado**, realice los siguientes pasos para resolver el error.

- Seleccione el mensaje de error y haga clic en **Resolver**. Un posible mensaje de error será el siguiente:

```
Extension already registered at CM <vCenter Server name> with id <extension ID>
```

- Introduzca las credenciales de vCenter Server y haga clic en **Resolver**.

Si ya existe un registro, se reemplazará.

Resultados

El administrador de equipos tarda un poco en registrarse en vCenter Server, y lo mismo sucede para que el estado de conexión aparezca como **Activo**.

Puede hacer clic en el nombre del administrador de equipos para ver su información, para editarlo, o bien para administrar las etiquetas que se aplican a este.

Implementar nodos de NSX Manager para formar un clúster mediante la interfaz de usuario

Puede implementar varios nodos de NSX Manager para proporcionar alta disponibilidad y fiabilidad.

Después de implementar los nuevos nodos, estos se conectan al nodo de NSX Manager para formar un clúster. El número recomendado de nodos de NSX Manager en clúster es tres.

Nota La implementación de varios nodos de NSX Manager mediante la interfaz de usuario solo se admite para los hosts de ESXi administrados por vCenter Server.

Los detalles de repositorio y la contraseña del primer nodo de NSX Manager implementado se sincronizan con los nodos recién implementados en el clúster.

Requisitos previos

- Compruebe que haya un nodo de NSX Manager instalado. Consulte [Instalar NSX Manager y los dispositivos disponibles](#).
- Compruebe que se haya configurado el administrador de equipos. Consulte [Agregar un administrador de equipos](#).
- Compruebe que se cumplan los requisitos del sistema. Consulte [Requisitos del sistema](#).
- Compruebe que estén abiertos los puertos necesarios. Consulte [Puertos y protocolos](#).
- Compruebe que haya un almacén de datos configurado y accesible en el host ESXi.
- Compruebe que tenga 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.
- Si aún no tiene una, cree la red del grupo de puertos de máquinas virtuales de destino. Coloque los dispositivos de NSX-T Data Center en una red de máquinas virtuales de administración.

Si tiene varias redes de administración, puede agregar rutas estáticas a las otras redes desde el dispositivo NSX-T Data Center.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión con privilegios de administrador en NSX Manager.
- 2 Seleccione **Sistema > Dispositivos > Información general > Agregar nodos**.
- 3 Introduzca los detalles de atributo comunes de NSX Manager.

Opción	Descripción
Administrador de equipo	Se rellenará el administrador de equipos de recursos registrados.
Habilitar SSH	Alterne el botón para permitir el inicio de sesión SSH para el nuevo nodo de NSX Manager.
Habilitar acceso root	Alterne el botón para permitir el acceso raíz para el nuevo nodo de NSX Manager.
Confirmación de nombre de usuario y contraseña de la CLI	<p>Establezca la contraseña de la CLI y la confirmación de contraseña para el nuevo nodo.</p> <p>Su contraseña debe cumplir las restricciones de seguridad para contraseñas.</p> <ul style="list-style-type: none"> ■ Al menos 12 caracteres ■ Al menos una letra en minúsculas ■ Al menos una letra en mayúsculas ■ Al menos un dígito ■ Al menos un carácter especial ■ Al menos cinco caracteres distintos ■ Sin palabras del diccionario ■ Sin palíndromos ■ No se admiten más de cuatro secuencias de caracteres monotónicos. <p>El nombre de usuario de la CLI está establecido como admin.</p>

Opción	Descripción
Contraseña raíz y confirmación de contraseña	<p>Establezca la contraseña raíz y la confirmación de contraseña para el nuevo nodo. Su contraseña debe cumplir las restricciones de seguridad para contraseñas.</p> <ul style="list-style-type: none"> ■ Al menos 12 caracteres ■ Al menos una letra en minúsculas ■ Al menos una letra en mayúsculas ■ Al menos un dígito ■ Al menos un carácter especial ■ Al menos cinco caracteres distintos ■ Sin palabras del diccionario ■ Sin palíndromos ■ No se admiten más de cuatro secuencias de caracteres monotónicos.
Servidores DNS	Introduzca la dirección IP del servidor DNS disponible en vCenter Server.
Servidores NTP	Introduzca la dirección IP del servidor NTP.

4 Introduzca los detalles del nodo de NSX Manager.

Opción	Descripción
Nombre	Introduzca un nombre para el nodo de NSX Manager.
Clúster	Designa el clúster al que se va a unir el nodo en el menú desplegable.
Grupo de recursos o host	Asigne un grupo de recursos o un host al nodo en el menú desplegable.
Almacén de datos	Seleccione un almacén de datos para los archivos del nodo en el menú desplegable.
Red	Asigne la red en el menú desplegable.
Máscara de red o IP de administración	Introduzca la dirección IP y la máscara de red.
Puerta de enlace de administración	Introduzca la dirección IP de la puerta de enlace.

5 (opcional) Haga clic en **Nuevo nodo** y configure otro nodo.

Repita los pasos 3 y 4.

6 Haga clic en **Finalizar**.

Se implementarán los nuevos nodos. Puede realizar un seguimiento del proceso de implementación en la página **Sistema > Dispositivos > Información general** o en vCenter Server.

7 Espere de 10 a 15 minutos para que finalicen la implementación, la creación del clúster y la sincronización del repositorio.

Los detalles de repositorio y la contraseña del primer nodo de NSX Manager implementado se sincronizan con los nodos recién implementados en el clúster.

8 Una vez que NSX Manager arranque, inicie sesión en la interfaz de línea de comandos y ejecute el comando `get interface eth0` para comprobar que la dirección IP se aplicó según lo previsto.

- 9 Introduzca el comando `get services` para comprobar que todos los servicios se están ejecutando.

Si los servicios no se están ejecutando, espere a que todos los servicios empiecen a ejecutarse.

Nota Los siguientes servicios no se ejecutan de forma predeterminada: `liagent`, `migration-coordinator` y `snmp`. Puede iniciarlos de la siguiente forma:

- `start service liagent`
- `start service migration-coordinator`
- Para SNMP:

```
set snmp community <community-string>
start service snmp
```

- 10 Inicie sesión en el primer nodo de NSX Manager implementado e introduzca el comando `get cluster status` para comprobar que los nodos se hayan agregado correctamente al clúster.

- 11 Compruebe que NSX Manager tenga la conectividad necesaria.

Asegúrese de que puede realizar las siguientes tareas.

- Haga ping a NSX Manager desde otro equipo.
- NSX Manager puede hacer ping a la puerta de enlace predeterminada.
- NSX Manager puede hacer ping a los hosts del hipervisor que están en la misma red que NSX Manager con la interfaz de administración.
- NSX Manager puede hacer ping al servidor DNS y al servidor NTP.
- Si habilitó SSH, asegúrese de que puede utilizarlo con su NSX Manager.

Si no se estableció la conectividad, asegúrese de que el adaptador de red del dispositivo virtual esté en la VLAN o red adecuada.

Pasos siguientes

Configure NSX Edge. Consulte [Instalar una instancia de NSX Edge en ESXi utilizando una GUI de vSphere](#).

Implementar nodos de NSX Manager para formar un clúster mediante la CLI

Unir NSX Manager para formar un clúster mediante la CLI garantiza que todos los nodos de NSX Manager del clúster puedan comunicarse entre sí.

Requisitos previos

Se debe haber completado la instalación de los componentes de NSX-T Data Center.

Procedimiento

- 1 Abra una sesión SSH en el primer nodo de NSX Manager implementado.
- 2 Inicie sesión con las credenciales del administrador.

- 3 En el nodo de NSX Manager, ejecute el comando `get certificate api thumbprint`.
La salida de comandos es una cadena de números única para este NSX Manager.
- 4 Ejecute el comando `get cluster config` para obtener el primer identificador de clúster de NSX Manager implementado.
- 5 Agregue un nodo de NSX Manager al clúster.

Nota Debe ejecutar el comando `join` en el nodo de NSX Manager recién implementado.

Proporcione la siguiente información de NSX Manager:

- Nodo de nombre de host o dirección IP al que desea unirse
- ID de clúster (Cluster ID)
- Nombre de usuario (User name)
- Contraseña
- Huella digital de certificado

Puede utilizar el comando de la CLI o la llamada API.

- Comando de la CLI

```
host> join <NSX-Manager-IP> cluster-id <cluster-id> username<NSX-Manager-username>
password<NSX-Manager-password> thumbprint <NSX-Manager1's-thumbprint>
```

- POST `https://<nsx-mgr>/api/v1/cluster?action=join_cluster` de llamada de API

El proceso de unión y estabilización del clúster puede tardar entre 10 y 15 minutos.

- 6 Agregue el tercer nodo de NSX Manager al clúster.
Repita el paso 5.
- 7 Compruebe el estado del clúster ejecutando el comando `get cluster status` en sus hosts.
- 8 Seleccione **Sistema > Dispositivos > Información general** y compruebe la conectividad del clúster.

Pasos siguientes

Cree una zona de transporte. Consulte [Crear un host independiente o un nodo de transporte sin sistema operativo](#).

Configurar una dirección IP virtual (VIP) para un clúster

Para proporcionar tolerancia a errores y alta disponibilidad a nodos de NSX Manager, asigne una dirección IP virtual (VIP) a un miembro del clúster de NSX-T.

Las instancias de NSX Manager de un clúster pasan a formar parte de un grupo HTTPS para atender las solicitudes de IU y API. El nodo principal del clúster asume la propiedad de la VIP establecida del clúster para atender cualquier solicitud de IU y API. Cualquier solicitud de IU y API procedente de los clientes se dirige al nodo principal.

Nota Al asignar la IP virtual, todas las máquinas virtuales de NSX Manager incluidas en el clúster deben configurarse en la misma subred.

Si el nodo principal que es propietario de la VIP deja de estar disponible, NSX-T elegirá un nuevo nodo principal. El nuevo nodo principal es el propietario de la VIP. Envía un paquete ARP gratuito para anunciar la nueva VIP a la asignación de direcciones MAC. Después de seleccionar un nuevo nodo principal, las nuevas solicitudes de IU y API se enviarán a él.

La conmutación por error de la VIP a un nuevo nodo principal del clúster puede tardar unos minutos en funcionar. Si la VIP conmuta por error a un nuevo nodo principal porque el anterior dejó de estar disponible, vuelva a autenticar las credenciales para que las solicitudes de API se dirijan al nuevo nodo principal.

Nota La VIP no está diseñada para funcionar como equilibrador de carga y no se puede utilizar si se habilita la **integración del equilibrador de carga externo** de vIDM en **Sistema > Usuarios > Configuración**. No configure una VIP si desea utilizar el equilibrador de carga externo de vIDM. Consulte la sección [Configurar la integración de VMware Identity Manager](#) de la guía *Guía de administración de NSX-T Data Center* para obtener más información.

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión con privilegios de administrador en NSX Manager.
- 2 Vaya a **Sistema > Información general**.
- 3 En el campo IP virtual, haga clic en **Editar**.
- 4 Introduzca la VIP del clúster. Asegúrese de que la VIP forme parte de la misma subred que los demás nodos de administración.
- 5 Haga clic en **Guardar**.
- 6 Para comprobar el estado del clúster y el nodo principal de API del grupo HTTPS, introduzca el NSX Manager comando de la CLI `get cluster status verbose` en la consola de NSX Manager o a través de SSH.

A continuación se muestra un ejemplo de resultado en el que el nodo principal está marcado en negrita.

```
Group Type: HTTPS
Group Status: STABLE
```

```
Members:
```

UUID	FQDN	IP
STATUS		

	cdb93642-ccba-fdf4-8819-90bf018cd727	nsx-manager	192.196.197.84
UP			
	51a13642-929b-8dfc-3455-109e6cc2a7ae	nsx-manager	192.196.198.156
UP			
	d0de3642-d03f-c909-9cca-312fd22e486b	nsx-manager	192.196.198.54
UP			
Leaders:			
SERVICE		LEADER	LEASE
VERSION			
api	cdb93642-ccba-fdf4-8819-90bf018cd727		8

- 7 Para solucionar problemas relacionados con las VIP, compruebe en la CLI de NSX Manager los registros del proxy inverso en `/var/log/proxy/reverse-proxy.log` y los registros del administrador del clúster en `/var/log/cbm/cbm.log`.

Resultados

Cualquier solicitud de API a NSX-T se redireccionará a la dirección IP virtual del clúster, que pertenece al nodo principal. A continuación, el nodo principal redirecciona la solicitud a los otros componentes del dispositivo.

Instalar una instancia de NSX Edgeen ESXi utilizando una GUI de vSphere

Si prefiere una instalación interactiva de NSX Edge, puede utilizar al cliente web de vSphere.

Importante En NSX-T, la máquina virtual de NSX Edge no admite vMotion.

Requisitos previos

Consulte requisitos de red de NSX Edge en [Instalación de NSX Edge](#).

Procedimiento

- 1 Busque el archivo OVA del dispositivo de NSX Edge en el portal de descargas de VMware.
Puede copiar la URL de descarga, o bien descargar el archivo OVA en el equipo.
- 2 En vSphere Client, seleccione el host en el que desee instalar en dispositivo de NSX Edge.
- 3 Haga clic en el botón secundario y seleccione **Implementar plantilla OVF** para iniciar el Asistente de instalación.
- 4 Introduzca la URL de descarga del archivo OVA, o desplácese hasta el archivo OVA guardado.
- 5 Introduzca un nombre para la máquina virtual de NSX Edge.
El nombre que escriba aparece en el inventario.
- 6 Seleccione un recurso informático para el dispositivo de NSX Edge.

- 7 Para que el rendimiento sea óptimo, reserve memoria para el dispositivo de NSX Edge.
Establezca la reserva para garantizar que NSX Edge tenga suficiente memoria como para ejecutarse de forma eficiente. Consulte [Requisitos del sistema de máquinas virtuales de NSX Edge](#).
- 8 Compruebe los detalles de la plantilla de OVF.
- 9 Seleccione un almacén de datos para almacenar los archivos de dispositivos de NSX Edge.
- 10 Acepte la interfaz de red de origen y destino predeterminada.
Puede aceptar el destino de red predeterminado para el resto de redes y cambiar la configuración de red después de implementar NSX Edge.
- 11 Seleccione la asignación IP en el menú desplegable.
- 12 Especifique la raíz del sistema de NSX Edge, el administrador de la CLI y las contraseñas de auditoría.
Sus contraseñas deben cumplir las restricciones de seguridad para contraseñas.
 - Al menos 12 caracteres
 - Al menos una letra en minúsculas
 - Al menos una letra en mayúsculas
 - Al menos un dígito
 - Al menos un carácter especial
 - Al menos cinco caracteres distintos
 - Sin palabras del diccionario
 - Sin palíndromos
 - No se admiten más de cuatro secuencias de caracteres monotónicos.
- 13 Introduzca la puerta de enlace predeterminada, la IPv4 de la red de administración, la máscara de red de administración, el DNS y la dirección IP de NTP.
- 14 (opcional) Registre NSX Edge en el plano de administración si hay una instancia de NSX Manager disponible.
 - a Introduzca la dirección IP y la huella digital del nodo principal de NSX Manager.
 - b Ejecute la llamada de API POST `https://<nsx-manager>/api/v1/aaa/registration-token` para recuperar el token de NSX Manager.
- 15 Escriba el nombre de host de la máquina virtual de NSX Edge.
- 16 Habilite SSH y permita el inicio de sesión SSH raíz a la línea de comandos de NSX Edge.
De forma predeterminada, estas opciones están deshabilitadas por motivos de seguridad.
- 17 Compruebe que las especificaciones de la plantilla OVA personalizada sean precisas y haga clic en **Finalizar** para iniciar la instalación.
La instalación puede durar entre 7 y 8 minutos.

- 18 Abra la consola de NSX Edge para hacer un seguimiento del proceso de arranque.

Si no se abre la ventana de la consola, asegúrese de que no estén bloqueadas las ventanas emergentes.

- 19 Después de iniciar NSX Edge, inicie sesión en la CLI con credenciales de administrador.

Nota Una vez iniciado NSX Edge, si no inicia sesión con las credenciales de administrador por primera vez, el servicio de plano de datos no se inicia automáticamente en NSX Edge.

- 20 Ejecute el comando `get interface eth0.<vlan_ID>` para comprobar que la dirección IP se aplicó según lo esperado.

```
nsx-edge-1> get interface eth0.100

Interface: eth0.100
Address: 192.168.110.37/24
MAC address: 00:50:56:86:62:4d
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

Nota Al activar las máquinas virtuales de NSX Edge en un host no administrado por NSX, compruebe que el valor de la opción MTU sea 1600 (y no 1500) en el conmutador de host físico de la NIC de datos.

- 21 Ejecute el comando `get managers` para comprobar que se haya registrado NSX Edge.

```
- 10.29.14.136 Standby
- 10.29.14.135 Standby
- 10.29.14.134 Connected
```

- 22 Compruebe que el dispositivo de NSX Edge tiene la conectividad necesaria.

Si habilitó SSH, asegúrese de que puede utilizarlo con su NSX Edge.

- Puede hacer ping a NSX Edge.
- NSX Edge puede hacer ping a su puerta de enlace predeterminada.
- NSX Edge puede hacer ping a los hosts del hipervisor que están en la misma red que NSX Edge.
- NSX Edge puede hacer ping al servidor DNS y al servidor NTP.

- 23 Solucione los problemas de conectividad.

Nota Si no se estableció la conectividad, asegúrese de que el adaptador de red de la máquina virtual esté en la VLAN o red adecuada.

De forma predeterminada, la ruta de acceso a datos de NSX Edge reclama todas las NIC de máquinas virtuales a excepción de la NIC de administración (la que tiene una dirección IP y una ruta predeterminada). Si asigna una NIC de forma incorrecta como interfaz de administración, siga estos pasos para asignar la dirección IP de administración a la NIC correcta utilizando DHCP.

- a Inicie sesión en la CLI y escriba el comando **stop service dataplane**.
- b Escriba el comando **set interface *interfaz* dhcp plane mgmt**.
- c Coloque la *interfaz* en la red DHCP y espere a que se asigne una dirección IP a esa *interfaz*.
- d Escriba el comando **start service dataplane**.

Los puertos fp-ethX de la ruta de datos utilizados para el vínculo superior VLAN y la superposición de túnel se muestran en los comandos **get interfaces** y **get physical-port** en NSX Edge.

Pasos siguientes

Una NSX Edge al plano de administración. Consulte [Unir NSX Edge al plano de administración](#).

Instalar NSX Edge en ESXi utilizando la herramienta OVF de la línea de comandos

Si prefiere automatizar la instalación de NSX Edge, puede utilizar la herramienta OVF de VMware, que es una utilidad de línea de comandos.

Requisitos previos

- Compruebe que se cumplan los requisitos del sistema. Consulte [Requisitos del sistema](#).
- Compruebe que estén abiertos los puertos necesarios. Consulte [Puertos y protocolos](#).
- Compruebe que haya un almacén de datos configurado y accesible en el host ESXi.
- Compruebe que tenga 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.
- Si aún no tiene una, cree la red del grupo de puertos de máquinas virtuales de destino. Coloque los dispositivos de NSX-T Data Center en una red de máquinas virtuales de administración.

Si tiene varias redes de administración, puede agregar rutas estáticas a las otras redes desde el dispositivo NSX-T Data Center.

- Planifique su esquema de direcciones IP IPv4 o IPv6 de NSX Manager.
- Consulte requisitos de red de NSX Edge en [Instalación de NSX Edge](#).
- Compruebe que tenga privilegios adecuados para implementar una plantilla OVF en el host ESXi.
- Compruebe que los nombres de host no incluyan guiones bajos. De lo contrario, el nombre de host se establece en *localhost*.
- Herramienta OVF, versión 4.3 o posterior.

Procedimiento

- ◆ En un host independiente, ejecute el comando `ovftool` con los parámetros adecuados.

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-edge-1
--deploymentOption=medium
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--net:"Network 0=Mgmt"
--net:"Network 1=nsx-tunnel"
--net:"Network 2=vlan-uplink"
--net:"Network 3=vlan-uplink"
--acceptAllEulas
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.37
--prop:nsx_netmask_0=255.255.255.0
--prop:nsx_gateway_0=192.168.110.1
--prop:nsx_dns1_0=192.168.110.10
--prop:nsx_domain_0=corp.local
--prop:nsx_ntp_0=192.168.110.10
--prop:nsx_isSSHEnabled=True
--prop:nsx_allowSSHRootLogin=True
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-edge
<path/url to nsx component ova>
vi://root:<password>@192.168.110.51
```

```
Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://root@192.168.110.24
Deploying to VI: vi://root@192.168.110.24
Transfer Completed
Powering on VM: nsx-edge-1
Task Completed
Completed successfully
```

- ◆ En un host administrado por vCenter Server, ejecute el comando `ovftool` con los parámetros adecuados.

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-edge-1
--deploymentOption=medium
--X:injectOvfEnv
```

```
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--net:"Network 0=Mgmt"
--net:"Network 1=nsx-tunnel"
--net:"Network 2=vlan-uplink"
--net:"Network 3=vlan-uplink"
--acceptAllEulas
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.37
--prop:nsx_netmask_0=255.255.255.0
--prop:nsx_gateway_0=192.168.110.1
--prop:nsx_dns1_0=192.168.110.10
--prop:nsx_domain_0=corp.local
--prop:nsx_ntp_0=192.168.110.10
--prop:nsx_isSSHEnabled=True
--prop:nsx_allowSSHRootLogin=True
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-edge
<path/url to nsx component ova>
vi://administrator@vsphere.local:<password>@192.168.110.24/?ip=192.168.210.53
```

```
Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://administrator@vsphere.local@192.168.110.24:443/
Deploying to VI: vi://administrator@vsphere.local@192.168.110.24:443/
Transfer Completed
Powering on VM: nsx-edge-1
Task Completed
Completed successfully
```

- ◆ Para que el rendimiento sea óptimo, reserve memoria para el dispositivo de NSX Manager.
Establezca la reserva para garantizar que NSX Manager tenga suficiente memoria como para ejecutarse de forma eficiente. Consulte [Requisitos del sistema de máquinas virtuales de NSX Manager](#).
- ◆ Abra la consola de NSX Edge para hacer un seguimiento del proceso de arranque.
- ◆ Después de iniciar NSX Edge, inicie sesión en la CLI con credenciales de administrador.
- ◆ Ejecute el comando `get interface eth0.<vlan_ID>` para comprobar que la dirección IP se aplicó según lo esperado.

```
nsx-edge-1> get interface eth0.100

Interface: eth0.100
```

```
Address: 192.168.110.37/24
MAC address: 00:50:56:86:62:4d
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

Nota Al activar las máquinas virtuales de NSX Edge en un host no administrado por NSX, compruebe que el valor de la opción MTU sea 1600 (y no 1500) en el conmutador de host físico de la NIC de datos.

- ◆ Compruebe que el dispositivo de NSX Edge tiene la conectividad necesaria.

Si habilitó SSH, asegúrese de que puede utilizarlo con su NSX Edge.

- Puede hacer ping a NSX Edge.
- NSX Edge puede hacer ping a su puerta de enlace predeterminada.
- NSX Edge puede hacer ping a los hosts del hipervisor que están en la misma red que NSX Edge.
- NSX Edge puede hacer ping al servidor DNS y al servidor NTP.

- ◆ Solucione los problemas de conectividad.

Nota Si no se estableció la conectividad, asegúrese de que el adaptador de red de la máquina virtual esté en la VLAN o red adecuada.

De forma predeterminada, la ruta de acceso a datos de NSX Edge reclama todas las NIC de máquinas virtuales a excepción de la NIC de administración (la que tiene una dirección IP y una ruta predeterminada). Si asigna una NIC de forma incorrecta como interfaz de administración, siga estos pasos para asignar la dirección IP de administración a la NIC correcta utilizando DHCP.

- a Inicie sesión en la CLI y escriba el comando **stop service dataplane**.
- b Escriba el comando **set interface *interfaz* dhcp plane mgmt**.
- c Coloque la *interfaz* en la red DHCP y espere a que se asigne una dirección IP a esa *interfaz*.
- d Escriba el comando **start service dataplane**.

Los puertos fp-ethX de la ruta de datos utilizados para el vínculo superior VLAN y la superposición de túnel se muestran en los comandos **get interfaces** y **get physical-port** en NSX Edge.

Pasos siguientes

Una NSX Edge al plano de administración. Consulte [Unir NSX Edge al plano de administración](#).

Instalar NSX-T Data Center en KVM

5

NSX-T Data Center es compatible con KVM de dos maneras: como nodo de transporte de host, y como host de NSX Manager.

Asegúrese de que tiene las versiones compatibles de KVM. Consulte [Requisitos del sistema de máquinas virtuales de NSX Manager](#).

Este capítulo incluye los siguientes temas:

- [Configurar KVM](#)
- [Administrar sus VM invitadas en la CLI de KVM](#)
- [Instalar NSX Manager en KVM](#)
- [Iniciar sesión en la instancia de NSX Manager recién creada](#)
- [Instalar paquetes de terceros en un host de KVM](#)
- [Comprobar la versión de Open vSwitch en los hosts de KVM de RHEL](#)
- [Implementar nodos de NSX Manager para formar un clúster mediante la CLI](#)
- [Instalar NSX Edge mediante un archivo ISO o con PXE](#)

Configurar KVM

Si planea utilizar KVM como nodo de transporte o como host para máquinas virtuales invitadas de NSX Manager, pero aún no configuró KVM, puede utilizar el procedimiento descrito aquí.

Nota El Protocolo de encapsulación Geneve usa el puerto UDP 6081. Debe permitir que este puerto acceda al firewall del host de KVM.

Procedimiento

- 1 (Solo RHEL) Abra el archivo `/etc/yum.conf`.
- 2 Busque la línea `excl`.

- 3 Agregue la línea "kernel* redhat-release*" para configurar YUM con el fin de evitar cualquier actualización de RHEL no compatible.

```
exclude=[existing list] kernel* redhat-release*
```

Si tiene pensado ejecutar NSX-T Data Center Container Plug-in, que tiene requisitos específicos de compatibilidad, excluya también los módulos relacionados con contenedores.

```
exclude=[existing list] kernel* redhat-release* kubelet-* kubeadm-* kubectl-* docker-*
```

Las versiones de RHEL compatibles son la 7.4 y la 7.5.

- 4 Instale las utilidades de puente y KVM.

Distribución de Linux	Comandos
Ubuntu	<pre>apt-get install -y qemu-kvm libvirt-bin ubuntu-vm-builder bridge-utils virtinst virt-manager virt-viewer libguestfs-tools</pre>
RHEL o CentOS Linux	<pre>yum groupinstall "Virtualization Hypervisor" yum groupinstall "Virtualization Client" yum groupinstall "Virtualization Platform" yum groupinstall "Virtualization Tools"</pre>
SUSE Linux Enterprise Server	Inicie YaSt y seleccione Virtualización > Instalar hipervisor y herramientas . YaSt permite habilitar y configurar automáticamente el puente de red.

- 5 Compruebe la capacidad de virtualización del hardware.

```
cat /proc/cpuinfo | egrep "vmx|svm"
```

La salida debe contener vmx.

- 6 Verifique que el módulo KVM esté instalado.

Distribución de Linux	Comandos
Ubuntu	<pre>kvm-ok INFO: /dev/kvm exists KVM acceleration can be used</pre>
RHEL o CentOS Linux	<pre>lsmod grep kvm kvm_intel 53484 6 kvm 316506 1 kvm_intel</pre>
SUSE Linux Enterprise Server	

- 7 Para que KVM se utilice como un host en NSX Manager, prepare la red de puente, la interfaz de administración y las interfaces de NIC.

En el siguiente ejemplo, la primera interfaz de Ethernet (eth0 o ens32) se utiliza para conectarse a la propia máquina Linux. Dependiendo de su entorno de implementación, esta interfaz puede utilizar

una configuración de IP estática o DHCP. Antes de asignar las interfaces de vínculo superior a los hosts NSX-T Data Center, asegúrese de que ya se hayan configurado los scripts de las interfaces que utilizan estos vínculos superiores. Sin estos archivos de la interfaz en el sistema, no se puede crear correctamente un nodo de transporte de host.

Nota Los nombres de la interfaz pueden variar en función del entorno.

Distribución de Linux

Configuración de red

Ubuntu

Edite /etc/network/interfaces:

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet manual

auto br0
iface br0 inet static
    address 192.168.110.51
    netmask 255.255.255.0
    network 192.168.110.0
    broadcast 192.168.110.255
    gateway 192.168.110.1
    dns-nameservers 192.168.3.45
    dns-search example.com
    bridge_ports eth0
    bridge_stp off
    bridge_fd 0
    bridge_maxwait 0
```

Cree un archivo XML de definiciones de redes para el puente. Por ejemplo, cree /tmp/bridge.xml con las siguientes líneas:

```
<network>
  <name>bridge</name>
  <forward mode='bridge' />
  <bridge name='br0' />
</network>
```

Defina e inicie la red de puente con los siguientes comandos:

```
virsh net-define
bridge.xml
virsh net-start bridge
virsh net-autostart bridge
```

Compruebe el estado de la red de puente con el siguiente comando:

```
virsh net-list --all
```

Name	State	Autostart	Persistent
bridge	active	yes	yes
default	active	yes	yes

RHEL o CentOS Linux

Edite /etcetera/sysconfig/red-scripts/ifcfg-*interfaz_administración*:

```
DEVICE="ens32"
TYPE="Ethernet"
NAME="ens32"
UUID="<UUID>"
BOOTPROTO="none"
HWADDR="<HWADDR>"
```

Distribución de Linux

Configuración de red

```
ONBOOT="yes"
NM_CONTROLLED="no"
BRIDGE="br0"
```

Edite /etc/sysconfig/network-scripts/ifcfg-eth1:

```
DEVICE="eth1"
TYPE="Ethernet"
NAME="eth1"
UUID="<UUID>"
BOOTPROTO="none"
HWADDR="<HWADDR>"
ONBOOT="yes"
NM_CONTROLLED="no"
```

Edite /etc/sysconfig/network-scripts/ifcfg-eth2:

```
DEVICE="eth2"
TYPE="Ethernet"
NAME="eth2"
UUID="<UUID>"
BOOTPROTO="none"
HWADDR="<HWADDR>"
ONBOOT="yes"
NM_CONTROLLED="no"
```

Edite /etc/sysconfig/network-scripts/ifcfg-br0:

```
DEVICE="br0"
BOOTPROTO="dhcp"
NM_CONTROLLED="no"
ONBOOT="yes"
TYPE="Bridge"
```

SUSE Linux
Enterprise Server

- 8 Para que KVM se utilice como nodo de transporte, prepare el puente de red.

En el siguiente ejemplo, la primera interfaz de Ethernet (eth0 o ens32) se utiliza para conectarse a la propia máquina Linux. Dependiendo de su entorno de implementación, esta interfaz puede utilizar una configuración de IP estática o DHCP.

Nota Los nombres de la interfaz pueden variar en función del entorno.

Distribución de Linux	Configuración de red
Ubuntu	<p>Edite /etc/network/interfaces:</p> <pre> auto lo iface lo inet loopback auto eth0 iface eth0 inet manual auto eth1 iface eth1 inet manual auto br0 iface br0 inet dhcp bridge_ports eth0 </pre>
RHEL o CentOS Linux	<p>Edite /etc/sysconfig/network-scripts/ifcfg-ens32:</p> <pre> DEVICE="ens32" TYPE="Ethernet" NAME="ens32" UUID="<something>" BOOTPROTO="none" HWADDR="<something>" ONBOOT="yes" NM_CONTROLLED="no" BRIDGE="br0" </pre> <p>Edite /etc/sysconfig/network-scripts/ifcfg-ens33:</p> <pre> DEVICE="ens33" TYPE="Ethernet" NAME="ens33" UUID="<something>" BOOTPROTO="none" HWADDR="<something>" ONBOOT="yes" NM_CONTROLLED="no" </pre> <p>Edite /etc/sysconfig/network-scripts/ifcfg-br0:</p> <pre> DEVICE="br0" BOOTPROTO="dhcp" NM_CONTROLLED="no" ONBOOT="yes" TYPE="Bridge" </pre>
SUSE Linux Enterprise Server	

Importante Para Ubuntu, todas las configuraciones de red deben especificarse en `/etc/network/interfaces`. No cree archivos de configuración de red individual, como `/etc/network/ifcfg-eth1`, que pueden dar lugar a errores en la creación de nodos de transporte.

Una vez que el host de KVM esté configurado como nodo de transporte, se creará la interfaz de puente "nsx-vtep0.0". En Ubuntu, `/etc/network/interfaces` tiene entradas como la siguiente:

```
iface nsx-vtep0.0 inet static
pre-up ip addr flush dev nsx-vtep0.0
address <IP_pool_address>
netmask <subnet_mask>
mtu 1600
down ifconfig nsx-vtep0.0 down
up ifconfig nsx-vtep0.0 up
```

En RHEL, el agente NSX de host (nsxa) crea un archivo de configuración denominado "ifcfg-nsx-vtep0.0", que tiene entradas como la siguiente:

```
DEVICE=nsx-vtep0.0
BOOTPROTO=static
NETMASK=<IP address>
IPADDR=<subnet mask>
MTU=1600
ONBOOT=yes
USERCTL=no
NM_CONTROLLED=no
```

En SUSE,

- 9 Reinicie el servicio de red, `systemctl restart network`, o reinicie el servidor de Linux para que los cambios de la red surtan efecto.

Administrar sus VM invitadas en la CLI de KVM

NSX Manager se puede instalar como máquinas virtuales de KVM. Además, KVM puede utilizarse como hipervisor para los nodos de transporte de NSX-T Data Center.

La administración de VM invitadas de KVM no entra dentro del alcance de esta guía. No obstante, aquí se muestran algunos comandos sencillos de la CLI de KVM con los que podrá ponerse en marcha.

Para administrar sus máquinas virtuales invitadas en la CLI de KVM, puede utilizar los comandos `virsh`. A continuación se muestran algunos comandos de `virsh` comunes. Si desea obtener información adicional, consulte la documentación de KVM.

```
# List running
virsh list

# List all
virsh list --all
```

```
# Control instances
virsh start <instance>
virsh shutdown <instance>
virsh destroy <instance>
virsh undefine <instance>
virsh suspend <instance>
virsh resume <instance>

# Access an instance's CLI
virsh console <instance>
```

En la CLI de Linux, el comando `ifconfig` muestra la interfaz `vnetX`, que representa la interfaz creada para la VM invitada. Si agrega VM invitadas adicionales, se agregan interfaces `vnetX` adicionales.

```
ifconfig
...

vnet0    Link encap:Ethernet  HWaddr fe:54:00:b0:a0:6d
         inet6 addr: fe80::fc54:ff:feb0:a06d/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:13183 errors:0 dropped:0 overruns:0 frame:0
         TX packets:181524 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:500
         RX bytes:4984832 (4.9 MB)  TX bytes:29498709 (29.4 MB)
```

Instalar NSX Manager en KVM

NSX Manager se puede instalar como dispositivo virtual en un host de KVM.

El procedimiento de instalación de QCOW2 utiliza `guestfish`, una herramienta de línea de comandos de Linux para escribir la configuración de máquina virtual en el archivo QCOW2.

Requisitos previos

- Configuración de KVM. Consulte [Configurar KVM](#).
- Privilegios para implementar una imagen QCOW2 en el host de KVM.
- Compruebe que la contraseña en `guestinfo` cumpla con los requisitos de complejidad de contraseña para que pueda iniciar sesión después de la instalación. Consulte [Instalación de NSX Manager](#).
- Familiarícese con los requisitos de recursos de NSX Manager. Consulte [Requisitos del sistema de máquinas virtuales de NSX Manager](#).
- Si quiere instalar el sistema operativo Ubuntu, se recomienda instalar la versión 18.04 antes de instalar NSX Manager en el host de KVM.

Procedimiento

- 1 Descargue la imagen QCOW2 de NSX Manager de la carpeta **nsx-unified-appliance > exports > kvm**.

- 2 Cópielo en la máquina KVM que va a ejecutar NSX Manager mediante SCP o realice una sincronización.
- 3 (Solo para Ubuntu) Agregue el usuario que tiene iniciada la sesión actualmente como un usuario libvirt:


```
adduser $USER libvirt
```

- 4 En el mismo directorio en el que guardó la imagen QCOW2, cree un archivo llamado guestinfo.xml y rellénelo con las propiedades de la máquina virtual de NSX Manager.

Propiedad	Descripción
<ul style="list-style-type: none"> ■ nsx_cli_passwd_0 ■ nsx_cli_audit_passwd_0 ■ nsx_passwd_0 	Sus contraseñas deben cumplir las restricciones de seguridad para contraseñas. <ul style="list-style-type: none"> ■ Al menos 12 caracteres ■ Al menos una letra en minúsculas ■ Al menos una letra en mayúsculas ■ Al menos un dígito ■ Al menos un carácter especial ■ Al menos cinco caracteres distintos ■ Sin palabras del diccionario ■ Sin palíndromos ■ No se admiten más de cuatro secuencias de caracteres monotónicos.
nsx_hostname	Introduzca el nombre de host de NSX Manager. El nombre de host debe ser un nombre de dominio válido. Asegúrese de que cada parte del nombre de host (dominio y subdominio) que esté separada por el punto empiece por un carácter alfabético.
nsx_role	<ul style="list-style-type: none"> ■ <i>nsx-manager</i>: obligatorio. Este nombre de función instala el dispositivo de NSX Manager. ■ <i>nsx-cloud-service-manager</i>: opcional. Después de instalar NSX Manager, utilice este nombre de función para instalar el dispositivo de Cloud Service Manager para NSX Cloud.
nsx_isSSHEnabled	Puede habilitar o deshabilitar esta propiedad. Si se habilita, puede iniciar sesión en NSX Manager mediante SSH.
nsx_allowSSHRootLogin	Puede habilitar o deshabilitar esta propiedad. Si se habilita, puede iniciar sesión en NSX Manager mediante SSH como usuario raíz. Para poder utilizar esta propiedad, se debe habilitar <i>nsx_isSSHEnabled</i> .
<ul style="list-style-type: none"> ■ nsx_dns1_0 ■ nsx_ntp_0 ■ nsx_domain_0 ■ nsx_gateway_0 ■ nsx_netmask_0 ■ nsx_ip_0 	Introduzca las direcciones IP de la puerta de enlace predeterminada, la IPv4 de la red de administración, la máscara de red de administración, el DNS y la dirección IP de NTP.

Por ejemplo:

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<Environment
  xmlns="http://schemas.dmtf.org/ovf/environment/1"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:oe="http://schemas.dmtf.org/ovf/environment/1">
  <PropertySection>
    <Property oe:key="nsx_cli_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_cli_audit_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_hostname" oe:value="nsx-manager1"/>
    <Property oe:key="nsx_role" oe:value="nsx-manager"/>
    <Property oe:key="nsx_isSSHEnabled" oe:value="True"/>
    <Property oe:key="nsx_allowSSHRootLogin" oe:value="True"/>
    <Property oe:key="nsx_dns1_0" oe:value="10.168.110.10"/>
    <Property oe:key="nsx_ntp_0" oe:value="10.168.110.10"/>
    <Property oe:key="nsx_domain_0" oe:value="corp.local"/>
    <Property oe:key="nsx_gateway_0" oe:value="10.168.110.83"/>
    <Property oe:key="nsx_netmask_0" oe:value="255.255.252.0"/>
    <Property oe:key="nsx_ip_0" oe:value="10.168.110.19"/>
  </PropertySection>
</Environment>
```

Nota En el ejemplo, `nsx_isSSHEnabled` y `nsx_allowSSHRootLogin` están habilitados. Cuando están deshabilitados, no puede utilizar SSH ni iniciar sesión en la línea de comandos de NSX Manager. Si habilita `nsx_isSSHEnabled` pero no habilita `nsx_allowSSHRootLogin`, podrá utilizar SSH con NSX Manager, pero no podrá iniciar sesión como raíz.

- 5 Use `guestfish` para escribir el archivo `guestinfo.xml` en la imagen QCOW2.

Nota Una vez que la información de `guestinfo` esté escrita en una imagen QCOW2, no se podrá sobrescribir la información.

```
sudo guestfish --rw -i -a nsx-unified-appliance-<BuildNumber>.qcow2 upload guestinfo /config/
guestinfo
```

- 6 Implemente la imagen QCOW2 con el comando `virt-install`.

Los valores de vCPU y RAM son adecuados para una máquina virtual de gran tamaño. Los nombres de la red y el grupo de puertos son específicos de su entorno. El modelo debe ser `virtio`.

```
sudo virt-install \
--import \
--ram 48000 \
--vcpus 12 \
--name <manager-name> \
--disk path=<manager-qcow2-file-path>,bus=virtio,cache=none \
--network network=<network-name>,portgroup=<portgroup-name>,model=virtio \
--noautoconsole \
```



```
--cpu mode=host-passthrough,cache.mode=passthrough

Starting install...
Domain installation still in progress. Waiting for installation to complete.
```

7 Compruebe que NSX Manager esté implementado.

```
virsh list --all
```

Id	Name	State
18	nsx-manager1	running

8 Abra la consola de NSX Manager e inicie sesión.

```
virsh console 18
Connected to domain nsx-manager1
Escape character is ^]

nsx-manager1 login: admin
Password:
```

9 Una vez que NSX Manager arranque, inicie sesión en la interfaz de línea de comandos y ejecute el comando `get interface eth0` para comprobar que la dirección IP se aplicó según lo previsto.

10 Ejecute `get services` para comprobar que los servicios se están ejecutando.

11 Compruebe que NSX Manager tenga la conectividad necesaria.

Asegúrese de que puede realizar las siguientes tareas.

- Haga ping a NSX Manager desde otro equipo.
- NSX Manager puede hacer ping a la puerta de enlace predeterminada.
- NSX Manager puede hacer ping a los hosts del hipervisor que están en la misma red que NSX Manager con la interfaz de administración.
- NSX Manager puede hacer ping al servidor DNS y al servidor NTP.
- Si habilitó SSH, asegúrese de que puede utilizarlo con su NSX Manager.

Si no se estableció la conectividad, asegúrese de que el adaptador de red del dispositivo virtual esté en la VLAN o red adecuada.

12 Cierre la consola de KVM.

```
control-]
```

13 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión con privilegios de administrador en NSX Manager.

Iniciar sesión en la instancia de NSX Manager recién creada

Después de instalar NSX Manager, puede utilizar la interfaz de usuario para realizar otras tareas de instalación.

Después de instalar NSX Manager, puede unirse al Programa de mejora de la experiencia de cliente (Customer Experience Improvement Program, CEIP) de NSX-T Data Center. Consulte el Programa de mejora de la experiencia de cliente en *Guía de administración de NSX-T Data Center* para obtener más información acerca del programa, incluyendo cómo unirse o salir de él más adelante.

Requisitos previos

Compruebe que esté instalado NSX Manager. Consulte [Instalar NSX Manager y los dispositivos disponibles](#).

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión con privilegios de administrador en NSX Manager.
Se muestra el CLUF.
- 2 Lea y acepte las condiciones del CLUF.
- 3 Seleccione si desea unirse al programa CEIP de VMware.
- 4 Haga clic en **Guardar**

Instalar paquetes de terceros en un host de KVM

Para preparar un host de KVM para que se convierta en un nodo de tejido, debe instalar algunos paquetes de terceros.

Requisitos previos

- (RHEL y CentOS) Antes de instalar los paquetes de terceros, ejecute los siguientes comandos para instalar los paquetes de virtualización.

```
yum groupinstall "Virtualization Hypervisor"  
yum groupinstall "Virtualization Client"  
yum groupinstall "Virtualization Platform"  
yum groupinstall "Virtualization Tools"
```

Si no puede instalar los paquetes, puede hacerlo manualmente con el comando `yum install glibc.i686 nspr` en una nueva instalación.

- (Ubuntu) Antes de instalar los paquetes de terceros, ejecute los siguientes comandos para instalar los paquetes de virtualización.

```
apt install -y \
qemu-kvm \
libvirt-bin \
virtinst \
virt-manager \
virt-viewer \
ubuntu-vm-builder \
bridge-utils
```

- (SUSE Linux Enterprise Server) Antes de instalar los paquetes de terceros, ejecute los siguientes comandos para instalar los paquetes de virtualización.

```
libcap-progs
```

Procedimiento

- ◆ En Ubuntu, ejecute `apt-get install <package_name>` para instalar los paquetes de terceros de forma manual.

Paquetes de Ubuntu 18.04	Paquetes de Ubuntu 16.04
tracertoute python-mako python-netaddr python-simplejson python-unittest2 python-yaml python-openssl dkms make	libboost-chrono1.58.0 libboost-filesystem1.58.0 libgoogle-glog0v5 libgoogle-perftools4 libprotobuf9v5 tracertoute python-mako python-netaddr python-simplejson python-unittest2 python-yaml python-openssl libboost-date-time1.58.0 libleveldb1v5 python-gevent python-protobuf libboost-program-options1.58.0 dkms

- ◆ En RHEL y CentOS Linux, ejecute `yum install <package_name>` para instalar los paquetes de terceros de forma manual.

Si prepara manualmente el host que ya está registrado en RHEL o CentOS, no es necesario instalar los paquetes de terceros en el host.

RHEL 7.6, 7.5 y 7.4	CentOS Linux 7.5 y 7.4
wget PyYAML libunwind python-gevent python-mako python-netaddr redhat-lsb-core tcpdump	wget PyYAML libunwind python-gevent python-mako python-netaddr redhat-lsb-core tcpdump

- ◆ En SUSE, ejecute `zypper install <package_name>` para instalar los paquetes de terceros de forma manual.

SUSE Linux Enterprise Server 12.0
python-simplejson python-PyYAML python-netaddr lsb-release

Comprobar la versión de Open vSwitch en los hosts de KVM de RHEL

Si hay paquetes de OVS en el host RHEL, debe eliminarlos e instalar los paquetes compatibles.

La versión Open vSwitch compatible es la 2.9.1.8614397-1.

Procedimiento

- 1 Compruebe la versión actual de la instancia de Open vSwitch instalada en el host.
`ovs-vswitchd --version`
Si tiene una versión más antigua o más reciente de Open vSwitch, debe reemplazar dicha versión por la que es compatible.
- 2 Abra la carpeta de Open vSwitch.
- 3 Elimine los siguientes paquetes de Open vSwitch.
 - `kmod-openvswitch`
 - `openvswitch`
 - `openvswitch-selinux-policy`
- 4 Como alternativa, agregue los paquetes de Open vSwitch requeridos por NSX-T Data Center.
 - a Inicie sesión en el host como administrador.
 - b Descargue y copie el archivo `nsx-lcp` en el directorio `/tmp`.
 - c Descomprima el paquete.
`tar -zxvf nsx-lcp-<release>-rhel75_x86_64.tar.gz`

- d Desplácese hasta el directorio del paquete.

```
cd nsx-lcp-rhel75_x86_64/
```

- e Reemplace la versión existente de Open vSwitch por la versión compatible.

- Para la versión más reciente de Open vSwitch, utilice el comando `--nodeps`.

Por ejemplo, `rpm -Uvh kmod-openvswitch-<nueva versión>.e17.x86_64.rpm --nodeps`

```
rpm -Uvh openvswitch-*.rpm --nodeps
```

- Para una versión anterior de Open vSwitch, utilice el comando `--force`.

Por ejemplo, `rpm -Uvh kmod-openvswitch-<nueva versión>.e17.x86_64.rpm --nodeps --force`

```
rpm -Uvh openvswitch-*.rpm --nodeps --force
```

Implementar nodos de NSX Manager para formar un clúster mediante la CLI

Unir NSX Manager para formar un clúster mediante la CLI garantiza que todos los nodos de NSX Manager del clúster puedan comunicarse entre sí.

Requisitos previos

Se debe haber completado la instalación de los componentes de NSX-T Data Center.

Procedimiento

- 1 Abra una sesión SSH en el primer nodo de NSX Manager implementado.
- 2 Inicie sesión con las credenciales del administrador.
- 3 En el nodo de NSX Manager, ejecute el comando `get certificate api thumbprint`.
La salida de comandos es una cadena de números única para este NSX Manager.
- 4 Ejecute el comando `get cluster config` para obtener el primer identificador de clúster de NSX Manager implementado.
- 5 Agregue un nodo de NSX Manager al clúster.

Nota Debe ejecutar el comando `join` en el nodo de NSX Manager recién implementado.

Proporcione la siguiente información de NSX Manager:

- Nodo de nombre de host o dirección IP al que desea unirse
- ID de clúster (Cluster ID)
- Nombre de usuario (User name)
- Contraseña
- Huella digital de certificado

Puede utilizar el comando de la CLI o la llamada API.

- Comando de la CLI

```
host> join <NSX-Manager-IP> cluster-id <cluster-id> username<NSX-Manager-username>
password<NSX-Manager-password> thumbprint <NSX-Manager1's-thumbprint>
```

- POST https://<nsx-mgr>/api/v1/cluster?action=join_cluster de llamada de API

El proceso de unión y estabilización del clúster puede tardar entre 10 y 15 minutos.

6 Agregue el tercer nodo de NSX Manager al clúster.

Repita el paso 5.

7 Compruebe el estado del clúster ejecutando el comando `get cluster status` en sus hosts.

8 Seleccione **Sistema > Dispositivos > Información general** y compruebe la conectividad del clúster.

Pasos siguientes

Cree una zona de transporte. Consulte [Crear un host independiente o un nodo de transporte sin sistema operativo](#).

Instalar NSX Edge mediante un archivo ISO o con PXE

Puede instalar dispositivos de NSX Edge de forma automatizada en un sistema sin sistema operativo o como una VM utilizando PXE.

Nota La instalación de arranque de PXE no es compatible con NSX Manager. Tampoco se pueden configurar ajustes de red como, por ejemplo, la dirección IP, la puerta de enlace, la máscara de red, NTP o DNS.

Instalar NSX Edge mediante un archivo ISO como un dispositivo virtual

Puede instalar máquinas virtuales de NSX Edge de forma manual utilizando un archivo ISO.

Importante Las instalaciones de máquina virtual del componente NSX-T Data Center incluyen VMware Tools. No se permite la eliminación ni la actualización de VMware Tools para dispositivos NSX-T Data Center.

Requisitos previos

- Consulte requisitos de red de NSX Edge en [Instalación de NSX Edge](#).

Procedimiento

- 1** Vaya a su cuenta de MyVMware (myvmware.com) y acceda a **VMware NSX-T Data Center > Descargas**.
- 2** Busque y descargue el archivo ISO correspondiente a NSX Edge.

- 3 EnvSphere Client, seleccione el almacén de datos del host.
- 4 Seleccione **Archivos > Cargar archivos > Cargar un archivo en un almacén de datos**, desplácese hasta el archivo ISO y cárguelo.

Si utiliza un certificado autofirmado, abra la dirección IP en un navegador y acepte el certificado. Después, vuelva a cargar el archivo ISO.
- 5 En el inventario de vSphere Client, seleccione el host donde cargó el archivo ISO. o en vSphere Client,
- 6 Haga clic con el botón derecho y seleccione **Nueva máquina virtual**.
- 7 Seleccione un recurso informático para el dispositivo de NSX Edge.
- 8 Seleccione un almacén de datos para almacenar los archivos de dispositivos de NSX Edge.
- 9 Acepte la compatibilidad predeterminada para la máquina virtual de NSX Edge.
- 10 Seleccione los sistemas operativos de ESXi compatibles para la máquina virtual de NSX Edge.
- 11 Configure el hardware virtual.
 - Disco duro nuevo: **200 GB**
 - Nueva red: **red de máquina virtual**
 - Nueva unidad de CD/DVD: **archivo ISO de almacén de datos**Debe hacer clic en **Conectar** para enlazar el archivo ISO de NSX Edge con la máquina virtual.
- 12 Encienda la máquina virtual de NSX Edge nueva.
- 13 Durante el arranque ISO, abra la consola de VM y seleccione **Instalación automatizada**.

Después de pulsar la tecla Intro, podría haber una pausa de 10 segundos.

Durante la instalación, se le solicitará que introduzca un identificador de VLAN para la interfaz de administración. Seleccione **Sí** (Yes) e introduzca un identificador de VLAN para crear una subinterfaz VLAN para la interfaz de red. Seleccione **No** si no desea configurar el etiquetado de VLAN en el paquete.

Durante el encendido, la VM solicita una configuración de red mediante DHCP. Si DHCP no está disponible en su entorno, el instalador le pide la configuración de IP.

De forma predeterminada, la contraseña raíz de inicio de sesión es **vmware** y la contraseña de inicio de sesión de administración es **default**.

Cuando inicie sesión por primera vez, se le pide que cambie la contraseña. Este método de cambio de contraseña tiene reglas estrictas de complejidad, incluyendo las siguientes:
 - Al menos 12 caracteres
 - Al menos una letra en minúsculas
 - Al menos una letra en mayúsculas
 - Al menos un dígito

- Al menos un carácter especial
- Al menos cinco caracteres distintos
- Sin palabras del diccionario
- Sin palíndromos
- No se admiten más de cuatro secuencias de caracteres monotónicos.

Importante Los servicios principales del dispositivo no se inician hasta que se establezca una contraseña con un nivel de complejidad suficiente.

- 14** Para que el rendimiento sea óptimo, reserve memoria para el dispositivo de NSX Edge.

Establezca la reserva para garantizar que NSX Edge tenga suficiente memoria como para ejecutarse de forma eficiente. Consulte [Requisitos del sistema de máquinas virtuales de NSX Edge](#).

- 15** Después de iniciar NSX Edge, inicie sesión en la CLI con credenciales de administrador.

Nota Una vez iniciado NSX Edge, si no inicia sesión con las credenciales de administrador por primera vez, el servicio de plano de datos no se inicia automáticamente en NSX Edge.

- 16** Hay tres formas de configurar una interfaz de administración.

- Interfaz sin etiquetas. Este tipo de interfaz crea una interfaz de administración fuera de banda.

(DHCP) `set interface eth0 dhcp plane mgmt`

(Estática) `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt`

- Interfaz con etiquetas.

`set interface eth0 vlan <vlan_ID> plane mgmt`

(DHCP) `set interface eth0.<vlan_ID> dhcp plane mgmt`

(Estática) `set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt`

- Interfaz en banda.

`set interface mac <mac_address> vlan <vlan_ID> in-band plane mgmt`

(DHCP) `set interface eth0.<vlan_ID> dhcp plane mgmt`

(Estática) `set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt`

- 17** (Opcional) Inicie el servicio SSH. Ejecute `start service ssh`.

- 18** Ejecute el comando `get interface eth0.<vlan_ID>` para comprobar que la dirección IP se aplicó según lo esperado.

```
nsx-edge-1> get interface eth0.100
```

```
Interface: eth0.100
```

```
Address: 192.168.110.37/24
```



```
MAC address: 00:50:56:86:62:4d
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

Nota Al activar las máquinas virtuales de NSX Edge en un host no administrado por NSX, compruebe que el valor de la opción MTU sea 1600 (y no 1500) en el conmutador de host físico de la NIC de datos.

- 19 (Interfaz con etiqueta e interfaz en banda) Se debe borrar cualquier interfaz de administración de VLAN existente antes de crear una nueva.

```
Clear interface eth0.<vlan_ID>
```

Para establecer una nueva interfaz, consulte el paso 15.

- 20 Compruebe que el dispositivo de NSX Edge tiene la conectividad necesaria.

Si habilitó SSH, asegúrese de que puede utilizarlo con su NSX Edge.

- Puede hacer ping a NSX Edge.
- NSX Edge puede hacer ping a su puerta de enlace predeterminada.
- NSX Edge puede hacer ping a los hosts del hipervisor que están en la misma red que NSX Edge.
- NSX Edge puede hacer ping al servidor DNS y al servidor NTP.

- 21 Solucione los problemas de conectividad.

Nota Si no se estableció la conectividad, asegúrese de que el adaptador de red de la máquina virtual esté en la VLAN o red adecuada.

De forma predeterminada, la ruta de acceso a datos de NSX Edge reclama todas las NIC de máquinas virtuales a excepción de la NIC de administración (la que tiene una dirección IP y una ruta predeterminada). Si asigna una NIC de forma incorrecta como interfaz de administración, siga estos pasos para asignar la dirección IP de administración a la NIC correcta utilizando DHCP.

- a Inicie sesión en la CLI y escriba el comando **stop service dataplane**.
- b Escriba el comando **set interface *interfaz* dhcp plane mgmt**.
- c Coloque la *interfaz* en la red DHCP y espere a que se asigne una dirección IP a esa *interfaz*.
- d Escriba el comando **start service dataplane**.

Los puertos fp-ethX de la ruta de datos utilizados para el vínculo superior VLAN y la superposición de túnel se muestran en los comandos **get interfaces** y **get physical-port** en NSX Edge.

Pasos siguientes

Si no se unió a NSX Edge con el plano de administración, consulte [Unir NSX Edge al plano de administración](#).

Instalar NSX Edge mediante un archivo ISO sin sistema operativo

Puede instalar dispositivos de NSX Edge de forma manual en un equipo sin sistema operativo utilizando un archivo ISO. Esto incluye el ajuste de la configuración de red, como dirección IP, puerta de enlace, máscara de red, NTP y DNS.

Requisitos previos

- Compruebe que el modo de BIOS del sistema está establecido en el BIOS heredado.
- Consulte requisitos de red de NSX Edge en [Instalación de NSX Edge](#).

Procedimiento

- 1 Busque el archivo ISO de dispositivo de NSX Edge en la carpeta **nsx-edgenode > publish > xenial_amd64**.

Descargue el archivo ISO en el equipo.

- 2 Inicie sesión en el ILO sin sistema operativo.
- 3 Haga clic en **Iniciar** en la vista previa de la consola virtual.
- 4 Seleccione **Medios virtuales > Conectar medios virtuales**.

Espere unos segundos a que se conecte el medio virtual.

- 5 Seleccione **Medios virtuales > Asignar CD/DVD** y desplácese hasta el archivo ISO.
- 6 Seleccione **Siguiente arranque > CD/DVD/ISO virtual**.
- 7 Seleccione **Alimentación > Restablecer sistema (inicio en caliente)**.

La duración de la instalación dependerá del entorno sin sistema operativo.

- 8 Seleccione **Instalación automatizada** (Automated installation).

Después de pulsar la tecla Intro, podría haber una pausa de 10 segundos.

- 9 Seleccione la interfaz de red principal aplicable.

Durante el encendido, el instalador solicita una configuración de red mediante DHCP. Si DHCP no está disponible en su entorno, el instalador le pide la configuración de IP.

De forma predeterminada, la contraseña raíz de inicio de sesión es **vmware** y la contraseña de inicio de sesión de administración es **default**.

- 10 Abra la consola de NSX Edge para hacer un seguimiento del proceso de arranque.

Si no se abre la ventana de la consola, asegúrese de que no estén bloqueadas las ventanas emergentes.

- 11 Después de iniciar NSX Edge, inicie sesión en la CLI con credenciales de administrador.

Nota Una vez iniciado NSX Edge, si no inicia sesión con las credenciales de administrador por primera vez, el servicio de plano de datos no se inicia automáticamente en NSX Edge.

12 Después del reinicio, puede iniciar sesión con las credenciales de administrador o raíz. La contraseña raíz predeterminada es **vmware**.

13 Hay tres formas de configurar una interfaz de administración.

- Interfaz sin etiquetas. Este tipo de interfaz crea una interfaz de administración fuera de banda.

(DHCP) `set interface eth0 dhcp plane mgmt`

(Estática) `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt`

- Interfaz con etiquetas.

`set interface eth0 vlan <vlan_ID> plane mgmt`

(DHCP) `set interface eth0.<vlan_ID> dhcp plane mgmt`

(Estática) `set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt`

- Interfaz en banda.

`set interface mac <mac_address> vlan <vlan_ID> in-band plane mgmt`

(DHCP) `set interface eth0.<vlan_ID> dhcp plane mgmt`

(Estática) `set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt`

14 Ejecute el comando `get interface eth0.<vlan_ID>` para comprobar que la dirección IP se aplicó según lo esperado.

```
nsx-edge-1> get interface eth0.100

Interface: eth0.100
Address: 192.168.110.37/24
MAC address: 00:50:56:86:62:4d
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

Nota Al activar las máquinas virtuales de NSX Edge en un host no administrado por NSX, compruebe que el valor de la opción MTU sea 1600 (y no 1500) en el conmutador de host físico de la NIC de datos.

15 (Interfaz con etiqueta e interfaz en banda) Se debe borrar cualquier interfaz de administración de VLAN existente antes de crear una nueva.

`clear interface eth0.<vlan_ID>`

Para establecer una nueva interfaz, consulte el paso 13.

16 Compruebe que el dispositivo de NSX Edge tiene la conectividad necesaria.

Si habilitó SSH, asegúrese de que puede utilizarlo con su NSX Edge.

- Puede hacer ping a NSX Edge.
- NSX Edge puede hacer ping a su puerta de enlace predeterminada.
- NSX Edge puede hacer ping a los hosts del hipervisor que están en la misma red que NSX Edge.
- NSX Edge puede hacer ping al servidor DNS y al servidor NTP.

17 Solucione los problemas de conectividad.

Nota Si no se estableció la conectividad, asegúrese de que el adaptador de red de la máquina virtual esté en la VLAN o red adecuada.

De forma predeterminada, la ruta de acceso a datos de NSX Edge reclama todas las NIC de máquinas virtuales a excepción de la NIC de administración (la que tiene una dirección IP y una ruta predeterminada). Si asigna una NIC de forma incorrecta como interfaz de administración, siga estos pasos para asignar la dirección IP de administración a la NIC correcta utilizando DHCP.

- a Inicie sesión en la CLI y escriba el comando **stop service dataplane**.
- b Escriba el comando **set interface *interfaz* dhcp plane mgmt**.
- c Coloque la *interfaz* en la red DHCP y espere a que se asigne una dirección IP a esa *interfaz*.
- d Escriba el comando **start service dataplane**.

Los puertos fp-ethX de la ruta de datos utilizados para el vínculo superior VLAN y la superposición de túnel se muestran en los comandos **get interfaces** y **get physical-port** en NSX Edge.

Pasos siguientes

Una NSX Edge al plano de administración. Consulte [Unir NSX Edge al plano de administración](#).

Instalar NSX Edge en el servidor PXE

PXE está formado por varios componentes: DHCP, HTTP y TFTP. Este procedimiento demuestra cómo configurar un servidor PXE en Ubuntu.

DHCP distribuye dinámicamente ajustes de IP a componentes de NSX-T Data Center, como NSX Edge. En un entorno PXE, el servidor DHCP permite a NSX Edge solicitar y recibir automáticamente una dirección IP.

TFTP es un protocolo de transferencia de archivos. El servidor TFTP siempre está escuchando en busca de clientes de PXE en la red. Si detecta que hay algún cliente PXE de la red solicitando servicios PXE, proporciona el archivo ISO del componente NSX-T Data Center y la configuración de instalación contenida en un archivo de preconfiguración.

Requisitos previos

- Un servidor PXE debe estar disponible en su entorno de implementación. El servidor PXE se puede establecer en cualquier distribución de Linux. El servidor PXE debe tener dos interfaces, una para las comunicaciones externas y otra para suministrar los servicios TFTP y DHCP IP.

Si tiene varias redes de administración, puede agregar rutas estáticas a las otras redes desde el dispositivo NSX-T Data Center.

- Compruebe que el archivo de configuración preconfigurado tenga los parámetros `net.ifnames=0` y `biosdevname = 0` establecidos tras `--` para que persistan después de reiniciar.
- Consulte requisitos de red de NSX Edge en [Instalación de NSX Edge](#).

Procedimiento

- 1 (opcional) Use un archivo inicial para configurar nuevos servicios TFTP o DHCP en un servidor Ubuntu.

Un archivo inicial es un archivo de texto que contiene comandos CLI que ejecuta en el dispositivo tras el primer arranque.

Asigne un nombre al archivo inicial según el servidor PXE al que se dirige. Por ejemplo:

```
nsxcli.install
```

El archivo debe copiarse en su servidor web, por ejemplo en `/var/www/html/nsx-edge/nsxcli.install`.

En el archivo inicial, puede agregar los comandos CLI. Por ejemplo, para configurar la dirección IP de la interfaz de administración:

```
stop dataplane
set interface eth0 <ip-cidr-format> plane mgmt
start dataplane
```

Para cambiar la contraseña del usuario administrador:

```
set user admin password <new_password> old-password <old-password>
```

Si especifica una contraseña en el archivo `preseed.cfg`, debe utilizar la misma contraseña en el archivo inicial. De lo contrario, utilice la contraseña predeterminada, que es "default".

Para unir el NSX Edge al plano de administración:

```
join management-plane <manager-ip> thumbprint <manager-thumbprint> username <manager-username>
password <manager password>
```

- 2 Cree dos interfaces, una para administración y otra para servicios DHCP y TFTP.

Asegúrese de que la interfaz DHCP/TFTP esté en la misma subred en la que reside el NSX Edge.

Por ejemplo, si las interfaces de administración del NSX Edge van a estar en la subred 192.168.210.0/24, coloque eth1 en esa misma subred.

```
# The loopback network interface
auto lo
iface lo inet loopback

# PXE server's management interface
auto eth0
iface eth0 inet static
    address 192.168.110.81
    gateway 192.168.110.1
    netmask 255.255.255.0
    dns-nameservers 192.168.110.10

# PXE server's DHCP/TFTP interface
auto eth1
iface eth1 inet static
    address 192.168.210.82
    gateway 192.168.210.1
    netmask 255.255.255.0
    dns-nameservers 192.168.110.10
```

3 Instale el software de servidor DHCP.

```
sudo apt-get install isc-dhcp-server -y
```

4 Edite el archivo /etc/default/isc-dhcp-server y agregue la interfaz que suministra el servicio DHCP.

```
INTERFACES="eth1"
```

5 (opcional) Si quiere que este servidor DHCP sea el servidor DHCP oficial de la red local, quite la marca de comentario de la línea **authoritative**; del archivo /etc/dhcp/dhcpd.conf.

```
...
authoritative;
...
```

6 En el archivo /etc/dhcp/dhcpd.conf, defina la configuración de DHCP para la red PXE.

Por ejemplo:

```
subnet 192.168.210.0 netmask 255.255.255.0 {
    range 192.168.210.90 192.168.210.95;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 192.168.110.10;
    option routers 192.168.210.1;
    option broadcast-address 192.168.210.255;
    default-lease-time 600;
    max-lease-time 7200;
}
```

7 Inicie el servicio DHCP.

```
sudo service isc-dhcp-server start
```

8 Compruebe que se está ejecutando el servicio DHCP.

```
service --status-all | grep dhcp
```

9 Instale Apache, TFTP y el resto de componentes necesarios requeridos para el arranque de PXE.

```
sudo apt-get install apache2 tftpd-hpa inetutils-inetd
```

10 Verifique que el servidor TFTP y Apache se estén ejecutando.

```
service --status-all | grep tftpd-hpa
service --status-all | grep apache2
```

11 Agregue las siguientes líneas al archivo /etc/default/tftpd-hpa.

```
RUN_DAEMON="yes"
OPTIONS="-l -s /var/lib/tftpboot"
```

12 Agregue la siguiente línea al archivo /etc/inetd.conf.

```
tftp    dgram    udp    wait    root    /usr/sbin/in.tftpd /usr/sbin/in.tftpd -s /var/lib/tftpboot
```

13 Reinicie el servicio TFTP.

```
sudo /etc/init.d/tftpd-hpa restart
```

14 Copie o descargue el archivo ISO del instalador de NSX Edge en una carpeta temporal.

15 Monte el archivo ISO y copie los componentes de instalación en el servidor TFTP y el servidor Apache.

```
sudo mount -o loop ~/nsx-edge.<build>.iso /mnt
cd /mnt
sudo cp -fr install/netboot/* /var/lib/tftpboot/
sudo mkdir /var/www/html/nsx-edge
sudo cp -fr /mnt/* /var/www/html/nsx-edge/
```

- 16** (opcional) Edite el archivo `/var/www/html/nsx-edge/preseed.cfg` para modificar las contraseñas cifradas.

Puede utilizar una herramienta Linux como `mkpasswd` para crear un hash de contraseña.

```
sudo apt-get install whois sudo mkpasswd -m sha-512
```

```
Password:
$6$SUFGqs[...]FcoHLiJ0uFD
```

- a Modifique la contraseña raíz, edite el archivo `/var/www/html/nsx-edge/preseed.cfg` y busque la siguiente línea:

```
d-i passwd/root-password-crypted password $6$tgmlNLmp$9BuAHhN...
```

- b Reemplace la cadena hash.

No es necesario escapar ningún carácter especial, como `$`, `'`, `"` o `\`.

- c Agregue el comando `usermod` al archivo `preseed.cfg` para establecer la contraseña del usuario raíz, del administrador o de ambos.

Por ejemplo, busque la línea `echo 'VMware NSX Edge'` y agregue el siguiente comando.

```
usermod --password '\$6\$VS3exId0aKmzW\$U3g0V7BF0DXlmRI.LR0v/VgloxVotEDp00b02hUF8u/' root; \
usermod --password '\$6\$VS3exId0aKmzW\$U3g0V7BF0DXlmRI.LR0v/VgloxVotEDp00b02hUF8u/' admin; \
```

La cadena hash es un ejemplo. Debe escapar todos los caracteres especiales. La contraseña raíz del primer comando `usermod` reemplaza a la contraseña establecida en `d-i passwd/root-password-crypted password 6tgml...`

Si utiliza el comando `usermod` para establecer la contraseña, no se pide al usuario que cambie la contraseña tras iniciar sesión por primera vez. De lo contrario, el usuario deberá cambiar la contraseña al iniciar sesión por primera vez.

- 17** Agregue las siguientes líneas al archivo `/var/lib/tftpboot/pxelinux.cfg/default`.

Reemplace `192.168.210.82` con la dirección IP de su servidor TFTP.

```
label nsxedge
    kernel ubuntu-installer/amd64/linux
    ipappend 2
    append netcfg/dhcp_timeout=60 auto=true priority=critical vga=normal partman-lvm/
device_remove_lvm=true netcfg/choose_interface=auto debian-installer/allow_unauthenticated=true
preseed/url=http://192.168.210.82/nsx-edge/preseed.cfg mirror/country=manual mirror/http/
hostname=192.168.210.82 nsx-kickstart/url=http://192.168.210.82/nsx-edge/nsxcli.install mirror/
http/directory=/nsx-edge initrd=ubuntu-installer/amd64/initrd.gz mirror/suite=xenial --
```


18 Agregue las siguientes líneas al archivo `/etc/dhcp/dhcpd.conf`.

Reemplace 192.168.210.82 con la dirección IP de su servidor DHCP.

```
allow booting;
allow bootp;

next-server 192.168.210.82; #Replace this IP address
filename "pxelinux.0";
```

19 Reinicie el servicio DHCP.

```
sudo service isc-dhcp-server restart
```

Nota Si se devuelve un error, por ejemplo: "parada: Instancia desconocida: inicio: No se pudo iniciar el trabajo" (stop: Unknown instance: start: Job failed to start), ejecute `sudo /etc/init.d/isc-dhcp-server stop` y, a continuación, `sudo /etc/init.d/isc-dhcp-server start`. El comando `sudo /etc/init.d/isc-dhcp-server start` devuelve información sobre el origen del error.

Pasos siguientes

Instale NSX Edge sin sistema operativo utilizando un archivo ISO. Consulte [Instalar NSX Edge mediante un archivo ISO sin sistema operativo](#) o [Instalar NSX Edge mediante un archivo ISO como un dispositivo virtual](#).

Configurar el servidor sin sistema operativo para usar NSX-T Data Center

6

Para usar NSX-T Data Center en un servidor sin sistema operativo, debe instalar paquetes de terceros compatibles.

NSX-T Data Center es compatible con el servidor sin sistema operativo de dos maneras: como nodo de transporte de host, y como host para NSX Manager.

Asegúrese de que dispone de las versiones compatibles del servidor sin sistema operativo. Consulte [Requisitos del sistema del servidor sin sistema operativo](#).

Nota Si las instancias de NSX Edge están en el factor de forma de máquina virtual y desea usar el servicio DHCP de NSX (implementado en un conmutador lógico basado en VLAN), debe establecer la opción de transmisiones falsificadas en Aceptar en los hosts sin sistema operativo en los se haya implementado NSX Edge. Consulte la sección de transmisiones falsificadas en la documentación de vSphere.

Este capítulo incluye los siguientes temas:

- [Instalar paquetes de terceros en un servidor sin sistema operativo](#)
- [Crear una interfaz de aplicación para cargas de trabajo de servidor nativo](#)

Instalar paquetes de terceros en un servidor sin sistema operativo

Para preparar un servidor sin sistema operativo para que se convierta en un nodo de tejido, debe instalar algunos paquetes de terceros.

Requisitos previos

- Compruebe que el usuario que realiza la instalación tenga permisos administrativos para realizar las siguientes acciones, algunas de las cuales pueden requerir permisos `sudo`:
 - Descargue y descomprima el paquete.
 - Ejecute los comandos `dpkg` o `rpm` para instalar/desinstalar los componentes de NSX.
 - Ejecute el comando `nsxcli` para ejecutar los comandos de unión del plano de administración.

- Compruebe que se hayan instalado los paquetes de virtualización.
 - Red Hat o CentOS: `yum install libvirt-libs`
 - Ubuntu: `apt-get install libvirt0`
 - SUSE: `zypper install libvirt-libs`

Procedimiento

- ◆ En Ubuntu, ejecute `apt-get install <package_name>` para instalar los paquetes de terceros.

Ubuntu18.04	Ubuntu16.04
traceroute python-mako python-netaddr python-simplejson python-unittest2 python-yaml python-openssl dkms libvirt0	libunwind8 libgflags2v5 libgoogle-perftools4 traceroute python-mako python-simplejson python-unittest2 python-yaml python-netaddr libboost-filesystem1.58.0 libboost-chrono1.58.0 libgoogle-glog0v5 dkms libboost-date-time1.58.0 python-protobuf python-gevent libsnappy1v5 libleveldb1v5 libboost-program-options1.58.0 libboost-thread1.58.0 libboost-iostreams1.58.0 libvirt0

- ◆ En RHEL o CentOS, ejecute `yum install` para instalar los paquetes de terceros.

RHEL 7.4, 7.5 y 7.6	CentOS 7.4, 7.5 y 7.6
tcpdump	tcpdump
boost-filesystem	boost-filesystem
PyYAML	PyYAML
boost-iostreams	boost-iostreams
boost-chrono	boost-chrono
python-mako	python-mako
python-netaddr	python-netaddr
python-six	python-six
gperftools-libs	gperftools-libs
libunwind	libunwind
snappy	snappy
boost-date-time	boost-date-time
c-ares	c-ares
redhat-lsb-core	redhat-lsb-core
wget	wget
net-tools	net-tools
yum-utils	yum-utils
lsof	lsof
python-gevent	python-gevent
libev	libev
python-greenlet	python-greenlet
libvirt-libs	libvirt-libs

- ◆ En SUSE, ejecute `zypper install <package_name>` para instalar los paquetes de terceros de forma manual.

SUSE 12.0
net-tools
tcpdump
python-simplejson
python-netaddr
python-PyYAML
python-six
libunwind
wget
lsof
libcap-progs
libvirt-libs

Crear una interfaz de aplicación para cargas de trabajo de servidor nativo

Debe configurar NSX-T Data Center e instalar paquetes de terceros de Linux antes de crear o migrar una interfaz de aplicación para cargas de trabajo de servidor nativo.

NSX-T Data Center no admite la unión de interfaces del sistema operativo Linux. Debe usar el conmutador virtual Open vSwitch (OVS) para los nodos de transporte de servidor sin sistema operativo.

Consulte el artículo 67835 de la base de conocimientos [El servidor sin sistema operativo admite el conmutador virtual OVS para la configuración de nodos de transporte en NSX-T](#) .

Procedimiento

- 1 Instale los paquetes de terceros que se requieren.
Consulte [Instalar paquetes de terceros en un servidor sin sistema operativo](#).
- 2 Configure los puertos TCP y UDP.
Consulte [Puertos TCP y UDP utilizados por ESXi, hosts de KVM y servidor nativo](#).
- 3 Agregue un servidor sin sistema operativo al tejido de NSX-T Data Center y cree un nodo de transporte.
Consulte [Crear un host independiente o un nodo de transporte sin sistema operativo](#).
- 4 Utilice el playbook de Ansible para crear una interfaz de aplicación.
Consulte <https://github.com/vmware/bare-metal-server-integration-with-nsxt>.

Configurar el clúster de NSX Manager

7

En las siguientes subsecciones se describe cómo configurar el clúster de NSX Manager, se detallan los requisitos de dicho clúster y se proporcionan recomendaciones para implementaciones de sitios específicos. También se describe cómo usar vSphere HA con NSX-T Data Center para habilitar la recuperación rápida si falla el host en el que se ejecuta el nodo de NSX Manager.

Este capítulo incluye los siguientes temas:

- [Requisitos del clúster de NSX Manager](#)
- [Requisitos del clúster de NSX Manager para sitios únicos, dobles y múltiples](#)

Requisitos del clúster de NSX Manager

A continuación, se indican los requisitos que se aplican a la configuración del clúster de NSX Manager:

- En un entorno de producción, el clúster de NSX Manager debe tener tres miembros para evitar una interrupción en los planos de administración y control.

Cada miembro del clúster debe estar en un host de hipervisor único con tres hosts de hipervisor físicos en total. Esto es necesario para evitar un error de host de hipervisor físico único que afecte al plano de control de NSX. Se recomienda aplicar reglas de antiafinidad para garantizar que los tres miembros del clúster se ejecuten en hosts diferentes.

El estado de funcionamiento normal de producción es un clúster de NSX Manager de tres nodos. Sin embargo, puede agregar nodos de NSX Manager adicionales y temporales para permitir cambios en la dirección IP.

Importante A partir de NSX-T Data Center 2.4, NSX Manager contiene el proceso del plano de control de NSX central. Este servicio es fundamental para el funcionamiento de NSX. Si se produce una pérdida completa de instancias de NSX Manager o si el clúster se reduce de tres instancias de NSX Manager a una instancia de NSX Manager, no podrá realizar cambios de topología en el entorno y se producirá un error en vMotion de las máquinas que dependen de NSX.

- Para las implementaciones de prueba de concepto y laboratorio donde no hay cargas de trabajo de producción, puede ejecutar una única instancia de NSX Manager para ahorrar recursos. Se pueden implementar nodos de NSX Manager tanto en ESXi como en KVM. Sin embargo, no se admiten implementaciones mixtas de administradores ni en ESXi ni en KVM.

Importante El número de sitios que se utilicen en una implementación de NSX-T Data Center puede afectar a los requisitos. Consulte [Requisitos del clúster de NSX Manager para sitios únicos, dobles y múltiples](#).

Requisitos del clúster de NSX Manager para sitios únicos, dobles y múltiples

La configuración del clúster de NSX Manager cambiará en función de si la implementación es para un sitio único, doble o múltiple.

Puede usar vSphere HA con NSX-T Data Center para habilitar la recuperación rápida si falla el host en el que se ejecuta el nodo de NSX Manager.

Nota Consulte *Crear y usar clústeres de vSphere HA* en la documentación de vSphere.

Requisitos y recomendaciones para un sitio único

Las siguientes recomendaciones se aplican a las implementaciones de NSX-T Data Center en un único sitio.

- Se recomienda colocar las instancias de NSX Manager en distintos hosts para evitar que un error de host único afecte a varios administradores.
- La latencia máxima entre las instancias de NSX Manager es de 10 ms.
- Puede colocar instancias de NSX Manager en distintos clústeres de vSphere, o bien, en un clúster de vSphere común.
- Se recomienda colocar las instancias de NSX Manager en distintas subredes de administración o en una subred de administración compartida. Si utiliza vSphere HA, se recomienda utilizar una subred de administración compartida para que las instancias de NSX Manager que vSphere recupere puedan conservar su dirección IP.
- Se recomienda colocar las instancias de NSX Manager también en el almacenamiento compartido. Para vSphere HA, revise los requisitos de dicha solución.

También puede usar vSphere HA con NSX-T para proporcionar la recuperación de una instancia de NSX Manager perdida cuando falla el host en el que se ejecuta NSX Manager.

Ejemplo de escenario:

- Un clúster de vSphere en el que están implementadas las tres instancias de NSX Manager.
- El clúster de vSphere consta de cuatro hosts como mínimo:
 - Host-01 con nsxmgr-01 implementado

- Host-02 con nsxmgr-02 implementado
- Host-03 con nsxmgr-03 implementado
- Host-04 sin NSX Manager implementado
- vSphere HA está configurado para recuperar la pérdida de cualquier instancia de NSX Manager (por ejemplo, nsxmgr-01) de cualquier host (por ejemplo, el Host-01) en el Host-04.

Por lo tanto, tras la pérdida de cualquier host en el que se esté ejecutando NSX Manager, vSphere recuperará la instancia perdida de NSX Manager en el host-04.

Requisitos y recomendaciones para un sitio doble

A continuación, se indican las recomendaciones que se aplican a las implementaciones de NSX-T Data Center en un sitio doble (sitio A/sitio B).

- No se recomienda implementar instancias de NSX Manager en un escenario de dos sitios sin vSphere HA. En este escenario, un sitio requiere la implementación de dos instancias de NSX Manager y la pérdida de dicho sitio afectará al funcionamiento de NSX-T Data Center.
- La implementación de NSX Manager en un escenario de sitio doble con vSphere HA se puede realizar teniendo en cuenta lo siguiente:
 - Un clúster único de vSphere ampliado contiene todos los hosts de las instancias de NSX Manager.
 - Las tres instancias de NSX Manager se implementan en una VLAN o subred de administración común para permitir que la dirección IP se conserve tras recuperar una instancia perdida de NSX Manager.
 - Para obtener información sobre la latencia entre sitios, consulte los requisitos del producto de almacenamiento.

Ejemplo de escenario:

- Un clúster de vSphere en el que están implementadas las tres instancias de NSX Manager.
- El clúster de vSphere consta de seis o más hosts, con tres hosts en el sitio A y tres hosts en el sitio B.
- Las tres instancias de NSX Manager se implementan en hosts distintos con hosts adicionales para colocar las instancias de NSX Manager recuperadas.

Sitio A:

- Host-01 con nsxmgr-01 implementado
- Host-02 con nsxmgr-02 implementado
- Host-03 con nsxmgr-03 implementado

Sitio B:

- Host-04 sin NSX Manager implementado
- Host-05 sin NSX Manager implementado

- Host-06 sin NSX Manager implementado
- vSphere HA está configurado para recuperar cualquier instancia perdida de NSX Manager (por ejemplo, nsxmgr-01) de cualquier host (por ejemplo, host-01) en el sitio A en uno de los hosts del sitio B.

Por lo tanto, tras un error en el sitio A, vSphere HA recuperará todas las instancias de NSX Manager en los hosts del sitio B.

Importante Debe configurar correctamente las reglas de antiafinidad para evitar que las instancias de NSX Manager se recuperen en el mismo host común.

Recomendaciones y requisitos para sitios múltiples (tres o más)

A continuación, se indican las recomendaciones que se aplican a las implementaciones de NSX-T Data Center en sitios múltiples (sitio A/sitio B/sitio C).

En un escenario con tres sitios o más, puede implementar instancias de NSX Manager con o sin vSphere HA.

Si las implementa sin vSphere HA:

- Se recomienda utilizar VLAN o subredes de administración independientes en cada sitio.
- La latencia máxima entre las instancias de NSX Manager es de 10 ms.

Ejemplo de escenario (tres sitios):

- Tres clústeres independientes de vSphere, uno por sitio.
- Al menos un host por cada sitio que ejecute NSX Manager:
 - Host-01 con nsxmgr-01 implementado
 - Host-02 con nsxmgr-02 implementado
 - Host-03 con nsxmgr-03 implementado

Escenarios de error:

- Error de sitio único: siguen funcionando dos instancias de NSX Manager que quedan en otros sitios. NSX-T Data Center está en estado degradado, pero continúa funcionando. Se recomienda implementar manualmente una tercera instancia de NSX Manager para reemplazar el miembro del clúster perdido.
- Error de dos sitios: pérdida de cuórum y, por lo tanto, impacto en el funcionamiento de NSX-T Data Center.

La recuperación de las instancias de NSX Manager puede tardar hasta 20 minutos según ciertas condiciones del entorno, tales como la velocidad de la CPU, el rendimiento del disco y otros factores de implementación.

Zonas de transporte y nodos de transporte

8

Las zonas de transporte y los nodos de transporte son conceptos importantes en NSX-T Data Center.

Este capítulo incluye los siguientes temas:

- [Crear zonas de transporte](#)
- [Crear un grupo de direcciones IP para direcciones IP de endpoints de túneles](#)
- [Ruta de datos mejorada](#)
- [Configurar perfiles](#)
- [Crear un host independiente o un nodo de transporte sin sistema operativo](#)
- [Instalación manual de módulos kernel NSX-T Data Center](#)
- [Configuración de red de NSX Edge](#)
- [Crear un nodo de transporte de NSX Edge](#)
- [Crear un clúster de NSX Edge](#)

Crear zonas de transporte

Las zonas de transporte establecen qué hosts y, por lo tanto, qué máquinas virtuales pueden participar en el uso de una red determinada. Una zona de transporte hace esto limitando los hosts que pueden "ver" un conmutador lógico y, por tanto, qué VM pueden conectarse al conmutador lógico. Una zona de transporte puede abarcar a uno o varios clústeres de host.

Un entorno de NSX-T Data Center puede contener una o más zonas de transporte según los requisitos del usuario. Un host puede corresponder a varias zonas de transporte. Un conmutador lógico puede corresponder a una sola zona de transporte.

NSX-T Data Center no permite la conexión de máquinas virtuales que se encuentran en zonas de transporte diferentes de la red de Capa 2. La expansión de un conmutador lógico se limita a una zona de transporte, de modo que las máquinas virtuales de diferentes zonas de transporte no pueden estar en la misma red de Capa 2.

La zona de transporte superpuesta la utilizan tanto nodos de transporte de host como NSX Edge. Cuando un host o nodo de transporte de NSX Edge se agrega a una zona de transporte superpuesta, se instala un N-VDS en el host o NSX Edge.

NSX Edge y los nodos de transporte de host utilizan la zona de transporte de VLAN para sus vínculos superiores de VLAN. Cuando se agrega un NSX Edge a una zona de transporte de VLAN, se instala un N-VDS de VLAN en NSX Edge.

Los N-VDS permiten el flujo de paquetes virtuales a físicos al asociar vínculos superiores y descendentes de enrutador lógico con NIC físicas.

Cuando cree una zona de transporte, debe proporcionar un nombre para el N-VDS que se instalará en los nodos de transporte cuando se agreguen más adelante a esta zona de transporte. Puede asignar al N-VDS el nombre que desee.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión con privilegios de administrador en NSX Manager.
- 2 Seleccione **Sistema > Tejido > Zonas de transporte > Agregar**.
- 3 Introduzca un nombre para la zona de transporte y, opcionalmente, una descripción.
- 4 Introduzca un nombre para el N-VDS.
- 5 Seleccione un modo de N-VDS.
 - El modo **Estándar** se aplica a todos los hosts compatibles.
 - **Ruta de datos mejorada** es un modo de pila de red que solo se aplica a los nodos de transporte del tipo de versión de host ESXi 6.7 y versiones posteriores que puede pertenecer a una zona de transporte.
- 6 Si el modo de N-VDS se establece como Estándar, seleccione un tipo de tráfico.
Las opciones son **Superposición (Overlay)** y **VLAN**.
- 7 Si el modo de N-VDS se establece como Ruta de datos mejorada, seleccione un tipo de tráfico.
Las opciones son **Superposición (Overlay)** y **VLAN**.

Nota En el modo de ruta de datos mejorada, se admiten solo configuraciones específicas de NIC. Asegúrese de configurar las NIC admitidas.

- 8 Introduzca uno o varios nombres de directivas de formación de equipos de vínculos superiores. Conmutadores lógicos asociados a la zona de transporte pueden utilizar estas directivas de formación de equipos con nombre. Si los conmutadores lógicos no encuentran una directiva de formación de equipos con nombre que coincida, se utiliza la directiva de formación de equipos de vínculo superior predeterminada.
- 9 Puede ver la nueva zona de transporte en la página **Zonas de transporte (Transport Zones)**.

- 10** (opcional) También puede ver la nueva zona de transporte con la llamada API GET <https://<nsx-mgr>/api/v1/transport-zones>.

```
{
  "cursor": "00369b661aed-1eaa-4567-9408-ccbcfe50b416tz-vlan",
  "result_count": 2,
  "results": [
    {
      "resource_type": "TransportZone",
      "description": "comp overlay transport zone",
      "id": "efd7f38f-c5da-437d-af03-ac598f82a9ec",
      "display_name": "tz-overlay",
      "host_switch_name": "overlay-hostswitch",
      "transport_type": "OVERLAY",
      "transport_zone_profile_ids": [
        {
          "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
          "resource_type": "BfdHealthMonitoringProfile"
        }
      ],
      "_create_time": 1459547126454,
      "_last_modified_user": "admin",
      "_system_owned": false,
      "_last_modified_time": 1459547126454,
      "_create_user": "admin",
      "_revision": 0,
      "_schema": "/v1/schema/TransportZone"
    },
    {
      "resource_type": "TransportZone",
      "description": "comp vlan transport zone",
      "id": "9b661aed-1eaa-4567-9408-ccbcfe50b416",
      "display_name": "tz-vlan",
      "host_switch_name": "vlan-uplink-hostswitch",
      "transport_type": "VLAN",
      "transport_zone_profile_ids": [
        {
          "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
          "resource_type": "BfdHealthMonitoringProfile"
        }
      ],
      "_create_time": 1459547126505,
      "_last_modified_user": "admin",
      "_system_owned": false,
      "_last_modified_time": 1459547126505,
      "_create_user": "admin",
      "_revision": 0,
      "_schema": "/v1/schema/TransportZone"
    }
  ]
}
```

Pasos siguientes

De forma opcional, cree un perfil de zona de transporte personalizado y asócielo a la zona de transporte. Puede crear perfiles personalizados de zona de transporte mediante la API POST `/api/v1/transportzone-profiles`. No existe flujo de trabajo de IU para crear un perfil de zona de transporte. Una vez que se creó el perfil de la zona de transporte, podrá encontrarlo en la zona de transporte mediante la API PUT `/api/v1/transport-zones/<transport-zone-id>`.

Crear un nodo de transporte. Consulte [Crear un host independiente o un nodo de transporte sin sistema operativo](#).

Crear un grupo de direcciones IP para direcciones IP de endpoints de túneles

Puede utilizar un grupo de direcciones IP para los endpoints de túneles. Los endpoints de túneles son las direcciones IP de origen y destino que se utilizan en el encabezado IP externo para identificar a los hosts del hipervisor que originan y finalizan la encapsulación de tramas superpuestas de NSX-T Data Center. Para las direcciones IP de endpoint de túnel, también puede utilizar DHCP o grupos de direcciones IP configuradas manualmente.

Si está utilizando tanto hosts ESXi como hosts de KVM, una opción de diseño sería utilizar dos subredes diferentes para el grupo de direcciones IP de endpoint de túneles de ESXi (sub_a) y el grupo de direcciones IP de endpoint de túneles de KVM (sub_b). En este caso, en los hosts de KVM se debe agregar una ruta estática a sub_a con una puerta de enlace predeterminada dedicada.

Un ejemplo de la tabla de enrutamiento resultante en un host de Ubuntu donde sub_a = 192.168.140.0 y sub_b = 192.168.150.0. (La subred de administración, por ejemplo, podría ser 192.168.130.0).

Tabla de enrutamiento de direcciones IP de kernel:

Destination	Gateway	Genmask	Iface
0.0.0.0	192.168.130.1	0.0.0.0	eth0
192.168.122.0	0.0.0.0	255.255.255.0	virbr0
192.168.130.0	0.0.0.0	255.255.255.0	eth0
192.168.140.0	192.168.150.1	255.255.255.0	nsx-vtep0.0
192.168.150.0	0.0.0.0	255.255.255.0	nsx-vtep0.0

La ruta se puede agregar al menos de dos formas diferentes. De estos dos métodos, la ruta se conserva después de reiniciar el host solo si se la agrega mediante la edición de la interfaz. La acción de agregar una ruta mediante el comando para agregar rutas no continúa después de reiniciar un host.

```
route add -net 192.168.140.0 netmask 255.255.255.0 gw 192.168.150.1 dev nsx-vtep0.0
```

En `/etc/network/interfaces`, antes de "up ifconfig nsx-vtep0.0 up" agregue esta ruta estática:

```
post-up route add -net 192.168.140.0 netmask 255.255.255.0 gw 192.168.150.1
```

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión con privilegios de administrador en NSX Manager.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Inventario > Grupos > Grupos de direcciones IP > Agregar**.
- 3 Introduzca los detalles del grupo de direcciones IP.

Opción	Ejemplo de parámetro
Nombre y descripción	Introduzca el grupo de direcciones IP y una descripción opcional.
Rangos de IP	Rangos de asignación IP 192.168.200.100 - 192.168.200.115
Puerta de enlace	192.168.200.1
CIDR	Dirección de red en notación CIDR 192.168.200.0/24
Servidores DNS	Lista separada por comas de servidores DNS 192.168.66.10
Sufijo DNS	corp.local

Resultados

El grupo de direcciones IPv4 o IPv6 se enumera en la página Grupo de IP.

También puede utilizar la llamada de API de GET `https://<nsx-mgr>/api/v1/pools/ip-pools` para ver la lista de los grupos de direcciones IP.

Pasos siguientes

Cree un perfil de vínculo superior. Consulte [Crear un perfil de vínculo superior](#).

Ruta de datos mejorada

La ruta de datos mejorada es un modo de pila de red que, cuando está configurado, proporciona un rendimiento superior de red. Está dirigido principalmente a cargas de trabajo NFV, que requieren las ventajas de rendimiento que ofrece este modo.

El conmutador de N-VDS solo se puede configurar en el modo de ruta de datos mejorada en un host ESXi. ENS también admite el tráfico que fluye a través de las máquinas virtuales de Edge.

En el modo de ruta de datos mejorada, puede configurar:

- Tráfico de superposición
- Tráfico de VLAN

NIC de VMkernel admitidas

Con NSX-T Data Center, que admite varios conmutadores de host de ENS, el número máximo de NIC de VMkernel admitidas por host es 32.

Proceso de alto nivel para configurar la ruta de datos mejorada

Como administrador de red, antes de crear las zonas de transporte que admiten N-VDS en el modo de ruta de datos mejorada, debe preparar la red con las tarjetas NIC y los controladores admitidos. Para mejorar el rendimiento de la red, puede habilitar la directiva de formación de equipos de origen de carga equilibrada para que reconozca los nodos de NUMA.

Los pasos de alto nivel son los siguientes:

- 1 Use tarjetas NIC que admitan la ruta de datos mejorada.

Consulte la [Guía de compatibilidad de VMware](#) para saber qué tarjetas NIC admiten la ruta de datos mejorada.

En la página de la Guía de compatibilidad de VMware, en la categoría **Dispositivos de E/S**, seleccione **ESXi 6.7**, el tipo de dispositivo de E/S como **Red**, y la función como **Ruta de datos mejorada de N-VDS**.

- 2 Descargue e instale los controladores actualizados de NIC en la [página My VMware](#).

- a Vaya a **Controladores y herramientas > CD de controladores**.

- b Descarga controladores de NIC:

Controlador de NIC VMware ESXi 6.7 ixgbe-ens 1.1.3 para la familia de controladores Ethernet de Intel 82599, x520, x540, x550 y x552

Controlador de NIC VMware ESXi 6.7 i40en-ens 1.1.3 para la familia de controladores Ethernet de Intel X710, XL710, XXV710 y X722

- 3 Cree una directiva de vínculo superior.

Consulte [Crear un perfil de vínculo superior](#).

- 4 Cree una zona de transporte con N-VDS en el modo de ruta de datos mejorada.

Consulte [Crear zonas de transporte](#).

Nota Zonas de transporte de ENS configuradas para el tráfico de superposición: para las máquinas virtuales de Microsoft Windows que ejecuten la versión de VMware Tools anterior a la 11.0.0 y el tipo de vNIC VMXNET3, asegúrese de que el valor de MTU sea 1500. Para las máquinas virtuales de Microsoft Windows que ejecuten vSphere 6.7 U1 y la versión 11.0.0 de VMware Tools o posteriores, asegúrese de que el valor de MTU sea inferior a 8900. Para las máquinas virtuales que ejecutan otros sistemas operativos compatibles, asegúrese de que el valor de MTU de la máquina virtual sea inferior a 8900.

- 5 Cree un nodo de transporte de host, Configure N-VDS con ruta de datos mejorada con núcleos lógicos y nodos de NUMA.

Consulte [Crear un host independiente o un nodo de transporte sin sistema operativo](#).

Modo de directiva de formación de equipos de origen de equilibrio de carga con reconocimiento de NUMA

El modo de directiva de formación de equipos de origen de equilibrio de carga definido para un N-VDS con ruta de datos mejorada deja de reconocer NUMA cuando se cumplen las siguientes condiciones:

- La **Sensibilidad de latencia** en las máquinas virtuales es **Alta**.
- El tipo de adaptador de red utilizado es VMXNET3.

Si la ubicación del nodo de NUMA de la máquina virtual o la NIC física no está disponible, la directiva de formación de equipos de origen de equilibrio de carga no tiene en cuenta el reconocimiento de NUMA para alinear la NIC y las máquinas virtuales.

La directiva funciona sin reconocimiento de NUMA en las siguientes condiciones:

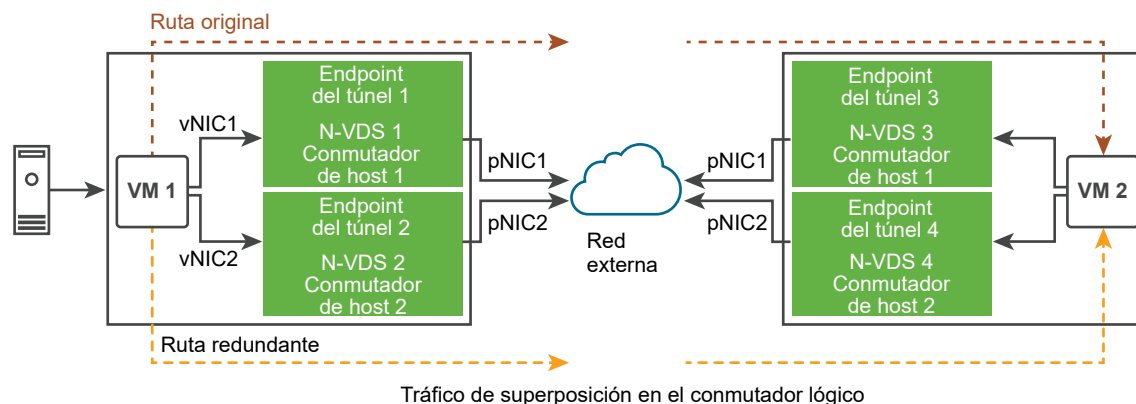
- El vínculo superior de LAG está configurado con enlaces físicos de varios nodos de NUMA.
- La máquina virtual tiene afinidad con varios nodos de NUMA.
- El host ESXi no pudo definir la información de NUMA para la máquina virtual o los enlaces físicos.

Compatibilidad con ENS de las aplicaciones de SCTP

En entornos de SCTP, las cargas de trabajo de NFV usan funciones de hospedaje múltiple y redundancia para aumentar la resistencia y la fiabilidad del tráfico que se ejecuta en las aplicaciones. El hospedaje múltiple es la capacidad para admitir rutas redundantes de una máquina virtual de origen a una máquina virtual de destino.

Según el número de NIC físicas disponibles para su uso como vínculos superiores de una red VLAN o de superposición, muchas de esas rutas de red redundantes estarán disponibles para que una máquina virtual envíe tráfico a través de la máquina virtual de destino. Las rutas redundantes se utilizan cuando se produce un error en la pNIC anclada a un conmutador lógico. Por lo tanto, el N-VDS de ruta de datos mejorada proporciona rutas de red redundantes al tráfico enrutado a través del protocolo SCTP.

Figura 8-1. Tráfico de ENS que se ejecutan en aplicaciones de SCTP



Estas son las tareas de alto nivel:

- 1 Preparar el host como nodo de transporte de NSX-T Data Center.
- 2 Preparar la zona de transporte de VLAN o de superposición con dos conmutadores de N-VDS en el modo de ruta de datos mejorada.
- 3 En el N-VDS 1, asigne la primera NIC física al conmutador.
- 4 En el N-VDS 2, asigne la segunda NIC física al conmutador.

El N-VDS en el modo de ruta de datos mejorada garantiza que si pNIC1 deja de estar disponible, el tráfico de VM 1 se enrutará a través de la ruta redundante - vNIC 1 → Endpoint de túnel 2 → pNIC 2 → VM 2. Tenga en cuenta que la vNIC1 de VM 1 y VM 2 están en una subred. De forma similar, vNIC2 de VM 1 y VM 2 están en otra subred.

Configurar perfiles

Los perfiles le permiten configurar de manera coherente capacidades idénticas para adaptadores de red en varios hosts o nodos.

Los perfiles son contenedores para las propiedades o capacidades que quiera que tengan sus adaptadores de red. En lugar de configurar propiedades o capacidades individuales para cada adaptador de red, puede especificar las capacidades en los perfiles, que después puede aplicar a varios hosts o nodos.

Crear un perfil de vínculo superior

Un vínculo superior es un vínculo de los nodos de NSX Edge a los conmutadores de la parte superior del rack o a los conmutadores lógicos de NSX-T Data Center. Un vínculo va de una interfaz de red física en un nodo de NSX Edge a un conmutador.

Un perfil de vínculo superior define las directivas de los vínculos superiores. La configuración definida por los perfiles de vínculo superior podría incluir políticas de formación de equipos, vínculos activos o en espera, el ID de la red VLAN de transporte y la configuración de MTU.

Cómo configurar los vínculos superiores para dispositivos basados en dispositivo de la máquina virtual NSX Edge y nodos de transporte de host:

- Si la directiva de formación de equipos de conmutación por error está configurada para un perfil de vínculo superior, solo podrá configurar un único vínculo superior activo en la directiva de formación de equipos. Los vínculos superiores en espera no son compatibles y no deben configurarse en la directiva de formación de equipos de conmutación por error. Cuando instale NSX Edge como dispositivo virtual o nodo de transporte de host, utilice el perfil de vínculo superior predeterminado.
- Si la directiva de formación de equipos de origen de equilibrio de carga está configurada para un perfil de vínculo superior, puede configurar varios vínculos superiores activos en el mismo N-VDS. Cada vínculo superior se asocia a una NIC física con un nombre y una dirección IP distintos. La dirección IP asignada a un endpoint de vínculo superior se puede configurar mediante Asignación de IP para el N-VDS.

Debe usar la directiva de formación de equipos de **origen de equilibrio de carga** para el equilibrio de carga del tráfico.

Requisitos previos

- Consulte requisitos de red de NSX Edge en [Instalación de NSX Edge](#).
- Cada vínculo superior en el perfil de vínculos superiores debe corresponder a un vínculo físico activo y disponible del host de hipervisor o del nodo de NSX Edge.

Por ejemplo, suponga que el host de hipervisor tiene dos vínculos físicos activos, vmnic0 y vmnic1, y que vmnic0 se usa para redes de almacenamiento y administración, mientras que vmnic1 no se usa. Esto podría significar que vmnic1 se puede utilizar como vínculo superior de NSX-T Data Center, pero no vmnic0. Para formar equipos de vínculos, debe tener dos vínculos físicos disponibles que no se estén utilizando, como vmnic1 y vmnic2.

Para un NSX Edge, el endpoint del túnel y los vínculos superiores de VLAN pueden utilizar el mismo vínculo físico. Por ejemplo, vmnic0/eth0/em0 podría utilizarse en la red de administración y vmnic1/eth1/em1, en los vínculos fp-ethX.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión con privilegios de administrador en NSX Manager.
- 2 Seleccione **Sistema > Tejido > Perfiles > Perfiles de vínculo superior > Agregar**.

3 Complete los detalles del perfil de vínculo superior.

Opción	Descripción
Nombre y descripción	<p>Introduzca un nombre de perfil de vínculo superior.</p> <p>Agregue una descripción de perfil de vínculo superior opcional.</p>
LAG	<p>(Opcional) En la sección LAG, haga clic en Agregar para grupos de agregación de vínculos (LAG) usando el Protocolo de control de adición de enlaces (LACP) para la red de transporte.</p> <p>Nota Para LACP, no se admiten múltiples LAG en los hosts de KVM.</p> <p>Los nombres de vínculos superiores activos y en espera que cree pueden ser cualquier texto que represente vínculos físicos. Más adelante, cuando cree nodos de transporte, se hace referencia a estos nombres de vínculos superiores. La IU/API del nodo de transporte le permite especificar qué vínculo físico se corresponde a cada vínculo superior con nombre.</p> <p>Posibles opciones del mecanismo de hash de LAG:</p> <ul style="list-style-type: none"> ■ Dirección MAC de origen ■ Dirección MAC de destino ■ Dirección MAC de origen y destino ■ Dirección IP y VLAN de origen y destino ■ Dirección MAC, dirección IP y puerto TCP/UDP de origen y destino
Formaciones de equipos	<p>En la sección Formación de equipos, puede introducir una directiva de formación de equipos predeterminada o introducir una directiva de formación de equipos con nombre. Haga clic en Agregar para agregar una directiva de formación de equipos. Una directiva de formación de equipos define cómo utiliza N-VDS su vínculo superior para la redundancia y el equilibrio de carga de tráfico. Puede configurar una directiva de formación de equipos en los siguientes modos:</p> <ul style="list-style-type: none"> ■ Orden de conmutación por error: se especifica un vínculo superior activo junto con una lista opcional de vínculos superiores en espera. Si se produce un error en el vínculo superior activo, es reemplazado por el próximo vínculo superior de la lista en espera. No se realiza ningún equilibrio de carga mediante esta opción. ■ Origen con equilibrio de carga: se especifica una lista de vínculos superiores activos y cada interfaz en el nodo de transporte está fijada a un vínculo superior activo. Esta configuración permite emplear varios vínculos superiores activos al mismo tiempo. <p>Nota</p> <ul style="list-style-type: none"> ■ En hosts de KVM: solo se admite la directiva de formación de equipos de orden de conmutación por error, mientras no se admiten las directivas de formación de equipos MAC de origen de equilibrio de carga y de equilibrio de carga. ■ En NSX Edge: para la directiva de formación de equipos predeterminada, se admiten las directivas de origen de equilibrio de carga y formación de equipos de orden de conmutación por error. Para la directiva de formación de equipos con nombre, solo se admite la directiva de orden de conmutación por error. ■ En los hosts ESXi: se admiten las directivas MAC de origen de equilibrio de carga, de origen de equilibrio de carga y formación de equipos de orden de conmutación por error.

Opción	Descripción
	<p>(Hosts ESXi y NSX Edge) Puede definir las siguientes directivas en una zona de transporte:</p> <ul style="list-style-type: none"> ■ Una directiva de formación de equipos con nombre para cada segmento o conmutador lógico basados en VLAN. ■ Una directiva de formación de equipos predeterminada para todo el N-VDS. <p>Directiva de formación de equipos con nombre: una directiva de formación de equipos con nombre significa que puede definir nombres de modos de directiva de formación de equipos y vínculos superiores específicos para cada segmento o cada conmutador lógico basado en VLAN. Este tipo de directiva le ofrece flexibilidad para seleccionar vínculos superiores específicos según la directiva de dirección de tráfico, por ejemplo, en función del requisito de ancho de banda.</p> <ul style="list-style-type: none"> ■ Si define una directiva de formación de equipos con nombre, N-VDS la utilizará si se asocia a la zona de transporte basada en VLAN y si, por último, se selecciona el conmutador lógico basado en VLAN o el segmento del host específicos. ■ Si no se define ninguna directiva de formación de equipos con nombre, N-VDS usa la directiva predeterminada.

- 4 Introduzca un valor de VLAN de transporte. La VLAN de transporte establecida en las etiquetas de perfil de vínculo superior solo superponen el tráfico, y el TEP utiliza el identificador de VLAN.

- 5 Introduzca el valor de MTU.

El valor predeterminado de MTU del perfil de vínculo superior es 1600.

La MTU de vínculo superior físico global configura el valor de MTU para todas las instancias de N-VDS del dominio NSX-T Data Center. Si no se especifica el valor de MTU de vínculo superior físico global, se usará el valor de la MTU del perfil de vínculo superior si está configurado. En caso contrario, se utilizará el valor predeterminado (1600). La MTU del perfil de vínculo superior puede reemplazar la MTU del vínculo superior físico global en un host específico.

La MTU de la interfaz lógica global configura el valor de MTU de todas las interfaces de enrutador lógico. Si no se especifica el valor de MTU de la interfaz lógica global, se usará el valor de MTU del enrutador lógico de nivel 0. El valor de MTU del vínculo superior del enrutador lógico puede anular el valor de MTU de la interfaz lógica global en un puerto específico.

Resultados

Además de la interfaz de usuario, también puede ver los perfiles de vínculo superior con la llamada API GET /api/v1/host-switch-profiles.

Pasos siguientes

Cree una zona de transporte. Consulte [Crear zonas de transporte](#).

Configurar perfiles de Network I/O Control

Utilice el perfil de Network I/O Control (NIOC) para asignar el ancho de banda de la red a las aplicaciones fundamentales para el negocio y con el fin de resolver situaciones en las que varios tipos de tráfico compiten por recursos en común.

El perfil de NIOC incorpora un mecanismo que permite reservar ancho de banda para el tráfico del sistema en función de la capacidad de los adaptadores físicos de un host. La versión 3 de la función Network I/O Control ofrece un proceso mejorado de reserva y asignación de recursos de red en todo el conmutador.

La versión 3 de Network I/O Control para NSX-T Data Center admite la administración de recursos del tráfico del sistema relacionado con las máquinas virtuales y los servicios de infraestructura, como vSphere Fault Tolerance. El tráfico del sistema está asociado estrictamente con un host ESXi.

Garantía de ancho de banda para el tráfico del sistema

La versión 3 de Network I/O Control suministra ancho de banda a los adaptadores de red de las máquinas virtuales a través de restricciones de recursos compartidos, reservas y límites. Estas restricciones pueden definirse en la interfaz de usuario de NSX-T Data Center Manager. La reserva de ancho de banda para el tráfico de máquina virtual también se usa en el control de admisiones. Cuando se enciende una máquina virtual, la utilidad de control de admisiones comprueba que haya suficiente ancho de banda disponible antes de colocar una máquina virtual en un host que puede proporcionar la capacidad de recursos.

Asignación de ancho de banda para el tráfico del sistema

Puede configurar Network I/O Control para asignar cierta cantidad de ancho de banda al tráfico generado por vSphere Fault Tolerance, vSphere vMotion, máquinas virtuales, etc.

- Tráfico de administración: es el tráfico de administración de un host.
- Tráfico de Fault Tolerance (FT): es el tráfico para conmutación por error y recuperación.
- Tráfico de NFS: es el tráfico relacionado con una transferencia de archivos en el sistema de archivos de red.
- Tráfico de vSAN: es el tráfico que genera la red de área de almacenamiento virtual.
- Tráfico de vMotion: es el tráfico para el cálculo de migración de recursos.
- Tráfico de vSphere Replication: es el tráfico para replicación.
- Tráfico de copia de seguridad de vSphere Data Protection: es el tráfico generado por la copia de seguridad de datos.
- Tráfico de máquina virtual: es el tráfico que generan las máquinas virtuales.
- Tráfico de iSCSI: es el tráfico de la interfaz de sistema de equipos pequeños de Internet.

vCenter Server propaga la asignación desde el conmutador distribuido hasta cada adaptador físico en los hosts que están conectados al conmutador.

Parámetros de asignación de ancho de banda para el tráfico del sistema

Mediante varios parámetros de configuración, el servicio Network I/O Control asigna ancho de banda al tráfico desde las funciones básicas del sistema vSphere. Parámetros de asignación para el tráfico del sistema.

Parámetros de asignación para el tráfico del sistema.

- Recursos compartidos: de 1 a 100, reflejan la prioridad relativa de un tipo de tráfico de sistema con respecto a los demás tipos de tráfico de sistema activos en el mismo adaptador físico. Los recursos compartidos relativos asignados a un tipo de tráfico del sistema y la cantidad de datos transmitidos por otras funciones del sistema determinan el ancho de banda disponible para ese tipo de tráfico del sistema.
- Reserva: el ancho de banda mínimo, en Mbps, que se debe garantizar en un único adaptador físico. El total de ancho de banda reservado entre todos los tipos de tráfico de sistema no puede superar el 75 % del ancho de banda que puede proporcionar el adaptador de red física de menor capacidad. El ancho de banda reservado que no se usa queda disponible para los demás tipos de tráfico del sistema. Sin embargo, Network I/O Control no redistribuye la capacidad que el tráfico del sistema no utiliza para la selección de máquinas virtuales.
- Límite: el ancho de banda máximo, en Mbps o Gbps, que puede consumir un tipo de tráfico del sistema en un único adaptador físico.

Nota No puede reservar más de un 75 % del ancho de banda de un adaptador de red física.

Por ejemplo, si los adaptadores de red conectados a un host ESXi son de 10 GbE, solo puede asignar un ancho de banda de 7,5 Gbps a los distintos tipos de tráfico. Se puede dejar más capacidad sin reservar. El host puede asignar dinámicamente el ancho de banda sin reservar según los recursos compartidos, los límites y el uso. El host solo reserva el ancho de banda que es suficiente para el funcionamiento de una función del sistema.

Configurar Network I/O Control y la asignación de ancho de banda para el tráfico del sistema en un N-VDS

Si quiere garantizar el ancho de banda mínimo para el tráfico del sistema que se ejecuta en hosts NSX-T Data Center, habilite y configure la administración de recursos de red en un N-VDS.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión con privilegios de administrador en NSX Manager.
- 2 Seleccione **Sistema > Tejido > Perfiles > Perfiles de NIOC > Agregar**.

3 Introduzca los detalles del perfil de NIOC.

Opción	Descripción
Nombre y descripción	Introduzca un nombre de perfil de NIOC. Si lo desea, también puede introducir los detalles del perfil, como los tipos de tráfico habilitados.
Estado	Actívelo para habilitar las asignaciones de ancho de banda que aparecen en los recursos del tráfico.
Recurso de tráfico de infraestructura de host	Puede aceptar los recursos de tráfico predeterminados que se enumeran. Haga clic en Agregar e introduzca su recurso de tráfico para personalizar el perfil de NIOC. (Opcional) Seleccione un tipo de tráfico existente y haga clic en Eliminar para quitar el recurso del perfil de NIOC.

El nuevo perfil de NIOC se agregará a la lista de perfiles de NIOC.

Configurar asignación de ancho de banda y Network I/O Control para el tráfico del sistema en un N-VDS mediante API

Puede usar las API de NSX-T Data Center para configurar la red y el ancho de banda de las aplicaciones que se ejecutan en el host.

Procedimiento

- 1 Realice una consulta en el host para que muestre los dos perfiles de conmutador de host, tanto el definido por el sistema como el definido por el usuario.
- 2 GET `https://<nsx-mgr>/api/v1/host-switch-profiles?include_system_owned=true`.

La respuesta de ejemplo muestra el perfil de NIOC aplicado al host.

```
{
  "description": "This profile is created for Network I/O Control (NIOC).",
  "extends": {
    "$ref": "BaseHostSwitchProfile"+
  },
  "id": "NiocProfile",
  "module_id": "NiocProfile",
  "polymorphic-type-descriptor": {
    "type-identifier": "NiocProfile"
  },
  "properties": {
    "_create_time": {
      "$ref": "EpochMsTimestamp"+,
      "can_sort": true,
      "description": "Timestamp of resource creation",
      "readonly": true
    },
    "_create_user": {
      "description": "ID of the user who created this resource",
      "readonly": true,
      "type": "string"
    }
  }
}
```

```

    },
    "_last_modified_time": {
      "$ref": "EpochMsTimestamp"+,
      "can_sort": true,
      "description": "Timestamp of last modification",
      "readonly": true
    },

    "_last_modified_user": {
      "description": "ID of the user who last modified this resource",
      "readonly": true,
      "type": "string"
    },

    "_links": {
      "description": "The server will populate this field when returning the resource. Ignored on PUT
and POST.",
      "items": {
        "$ref": "ResourceLink"+
      },

      "readonly": true,
      "title": "References related to this resource",
      "type": "array"
    },

    "_protection": {
      "description": "Protection status is one of the following:
        PROTECTED – the client who retrieved the entity is not allowed to modify it.
        NOT_PROTECTED – the client who retrieved the entity is allowed to modify it
        REQUIRE_OVERRIDE – the client who retrieved the entity is a super user and can modify it,
        but only when providing the request header X-Allow-Overwrite=true.
        UNKNOWN – the _protection field could not be determined for this entity.",
      "readonly": true,
      "title": "Indicates protection status of this resource",
      "type": "string"
    },

    "_revision": {
      "description": "The _revision property describes the current revision of the resource.
        To prevent clients from overwriting each other's changes, PUT operations must include the
        current _revision of the resource,
        which clients should obtain by issuing a GET operation.
        If the _revision provided in a PUT request is missing or stale, the operation
will be rejected.",
      "readonly": true,
      "title": "Generation of this resource config",
      "type": "int"
    },

    "_schema": {
      "readonly": true,
      "title": "Schema for this resource",
      "type": "string"
    },

```



```

    "_self": {
      "$ref": "SelfResourceLink"+,
      "readonly": true,
      "title": "Link to this resource"
    },

    "_system_owned": {
      "description": "Indicates system owned resource",
      "readonly": true,
      "type": "boolean"
    },

    "description": {
      "can_sort": true,
      "maxLength": 1024,
      "title": "Description of this resource",
      "type": "string"
    },

    "display_name": {
      "can_sort": true,
      "description": "Defaults to ID if not set",
      "maxLength": 255,
      "title": "Identifier to use when displaying entity in logs or GUI",
      "type": "string"
    },

    "enabled": {
      "default": true,
      "description": "The enabled property specifies the status of NIOC feature.

```

When enabled is set to true, NIOC feature is turned on and the bandwidth allocations specified for the traffic resources are enforced.

When enabled is set to false, NIOC feature is turned off and no bandwidth allocation is guaranteed.

By default, enabled will be set to true."

```

    "nsx_feature": "Nioc",
    "required": false,
    "title": "Enabled status of NIOC feature",
    "type": "boolean"
  },

  "host_infra_traffic_res": {
    "description": "host_infra_traffic_res specifies bandwidth allocation for various traffic resources.",
    "items": {
      "$ref": "ResourceAllocation"+
    },
    "nsx_feature": "Nioc",
    "required": false,
    "title": "Resource allocation associated with NiocProfile",
    "type": "array"
  },

```

```

    "id": {
      "can_sort": true,
      "readonly": true,
      "title": "Unique identifier of this resource",
      "type": "string"
    },

    "required_capabilities": {
      "help_summary":
        "List of capabilities required on the fabric node if this profile is
        used.
        The required capabilities is determined by whether specific features are enabled in the
        profile.",
      "items": {
        "type": "string"
      },
      "readonly": true,
      "required": false,
      "type": "array"
    },

    "resource_type": {
      "$ref": "HostSwitchProfileType",
      "required": true
    },

    "tags": {
      "items": {
        "$ref": "Tag"
      },
      "maxItems": 30,
      "title": "Opaque identifiers meaningful to the API user",
      "type": "array"
    },
    "title": "Profile for NIOC",
    "type": "object"
  }

```

3 Si no existe un perfil de NIOC, créelo.

POST <https://<nsx-mgr>/api/v1/host-switch-profiles>

```

{
  "description": "Specify limit, shares and reservation for all kinds of traffic.
  Values for limit and reservation are expressed in percentage. And for shares,
  the value is expressed as a number between 1-100.\n\nThe overall reservation among all traffic
  types should not exceed 75%.
  Otherwise, the API request will be rejected.",
  "id": "ResourceAllocation",
  "module_id": "NiocProfile",
  "nsx_feature": "Nioc",

```

```

"properties": {
  "limit": {
    "default": -1.0,
    "description": "The limit property specifies the maximum bandwidth allocation for a given
traffic type and is expressed in percentage. The default value for this
field is set to -1 which means the traffic is unbounded for the traffic
type. All other negative values for this property is not supported\nand will be rejected by
the API.",
    "maximum": 100,
    "minimum": -1,
    "required": true,
    "title": "Maximum bandwidth percentage",
    "type": "number"
  },
  "reservation": {
    "default": 0.0,
    "maximum": 75,
    "minimum": 0,
    "required": true,
    "title": "Minimum guaranteed bandwidth percentage",
    "type": "number"
  },
  "shares": {
    "default": 50,
    "maximum": 100,
    "minimum": 1,
    "required": true,
    "title": "Shares",
    "type": "int"
  },
  "traffic_type": {
    "$ref": "HostInfraTrafficType+",
    "required": true,
    "title": "Resource allocation traffic type"
  }
},
"title": "Resource allocation information for a host infrastructure traffic type",
"type": "object"

```

- 4 Actualice la configuración del nodo de transporte con el ID de perfil de NIOC del perfil de NIOC recién creado.

PUT <https://<nsx-mgr>/api/v1/transport-nodes/<TN-id>>

```

{
  "resource_type": "TransportNode",
  "description": "Updated NSX configured Test Transport Node",
  "id": "77816de2-39c3-436c-b891-54d31f580961",
  "display_name": "NSX Configured TN",
  "host_switch_spec": {

```

```

"resource_type": "StandardHostSwitchSpec",
"host_switches": [
  {
    "host_switch_profile_ids": [
      {
        "value": "e331116d-f59e-4004-8cfd-c577ae563a",
        "key": "UplinkHostSwitchProfile"
      },
      {
        "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
        "key": "LldpHostSwitchProfile"
      }
    ],
    "host_switch_name": "nsxvswitch",
    "pnics": [
      {
        "device_name": "vmnic1",
        "uplink_name": "uplink1"
      }
    ],
    "ip_assignment_spec": {
      "resource_type": "StaticIpPoolSpec",
      "ip_pool_id": "ecddcdde-4dc5-4026-ad4f-8857995d4c92"
    }
  }
],
"transport_zone_endpoints": [
  {
    "transport_zone_id": "e14c6b8a-9edd-489f-b624-f9ef12afbd8f",
    "transport_zone_profile_ids": [
      {
        "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
        "resource_type": "BfdHealthMonitoringProfile"
      }
    ]
  }
]
],

"host_switches": [
  {
    "host_switch_profile_ids": [
      {
        "value": "e331116d-f59e-4004-8cfd-c577ae563a",
        "key": "UplinkHostSwitchProfile"
      },
      {
        "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
        "key": "LldpHostSwitchProfile"
      }
    ],
  }
],

```

```

    "host_switch_name": "nsxvswitch",
    "pnics": [
    {
        "device_name": "vmnic1",
        "uplink_name": "uplink1"
    }
    ],
    "static_ip_pool_id": "ecddcdde-4dc5-4026-ad4f-8857995d4c92"
}
],
"node_id": "41a4eebd-d6b9-11e6-b722-875041b9955d",
"_revision": 0
}

```

- 5 Confirme que los parámetros del perfil de NIOC están actualizados en el archivo `com.vmware.common.respools.cfg`.

```
# [root@ host:] net-dvs -l
```

```

        switch 1d 73 f5 58 99 7a 46 6a-9c cc d0 93 17 bb 2a 48 (vswitch)
max ports: 2560
global properties:

com.vmware.common.opaqueDvs = true ,      propType = CONFIG
com.vmware.nsx.kcp.enable = true ,        propType = CONFIG
com.vmware.common.alias = nsxvswitch ,    propType = CONFIG
com.vmware.common.uplinkPorts: uplink1    propType = CONFIG
com.vmware.common.portset.mtu = 1600, propType = CONFIG
com.vmware.etherswitch.cdp = LLDP, listen propType = CONFIG
com.vmware.common.respools.version = version3, propType = CONFIG
com.vmware.common.respools.cfg:
netsched.pools.persist.ft:0:50:-1:255
netsched.pools.persist.hbr:0:50:-1:255
netsched.pools.persist.vmotion:0:50:-1:255
netsched.pools.persist.vm:0:100:-1:255
netsched.pools.persist.iscsi:0:50:-1:255
netsched.pools.persist.nfs:0:50:-1:255
netsched.pools.persist.mgmt:0:50:-1:255
netsched.pools.persist.vdp:0:50:-1:255
netsched.pools.persist.vsan:0:50:-1:255
propType = CONFIG

```

- 6 Compruebe los perfiles de NIOC en el kernel del host.

```
# [root@ host:] /get /net/portsets/DvsPortset-1/ports/50335755/nioCvnicInfo
```

```

Vnic NIOC Info
{
    Uplink reserved on:vmnic4
    Reservation in Mbps:200
    Shares:50
    Limit in Mbps:4294967295
    World ID:1001400726
}

```

```
vNIC Index:0
Respool Tag:0
NIOC Version:3
Active Uplink Bit Map:15
Parent Respool ID:netsched.pools.persist.vm
}
```

7 Compruebe la información del perfil de NIOC.

```
# [root@ host:] /get /net/portsets/DvsPortset-1/uplinks/vmnic4/nioInfo
```

```
Uplink NIOC Info
{
  Uplink device:vmnic4
  Link Capacity in Mbps:750
  vm respool reservation:275
  link status:1
  NetSched Ready:1
  Infrastructure reservation:0
  Total VM reservation:200
  Total vnics on this uplink:1
  NIOC Version:3
  Uplink index in BitMap:0
}
```

Resultados

El perfil de NIOC está configurado con la asignación de ancho de banda predefinido para las aplicaciones que se ejecutan en los hosts NSX-T Data Center.

Agregar un perfil de clúster de NSX Edge

El perfil de clúster de NSX Edge define las directivas del nodo de transporte NSX Edge.

Requisitos previos

Compruebe que el clúster de NSX Edge esté disponible.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión con privilegios de administrador en NSX Manager.
- 2 Seleccione **Sistema > Tejido > Perfiles > Perfiles de clústeres de Edge > Agregar**.

3 Introduzca los detalles del perfil de clúster de NSX Edge.

Opción	Descripción
Nombre y descripción	<p>Escriba un nombre de perfil para el clúster de NSX Edge.</p> <p>Opcionalmente, puede introducir otros detalles del perfil, como la configuración de detección de reenvío bidireccional (BFD).</p>
Intervalo de sondeo de BFD	<p>Acepte la configuración predeterminada.</p> <p>BFD es el protocolo de detección que se utiliza para identificar fallos de ruta de reenvío. Puede establecer el tiempo de intervalo de BFD para detectar fallos de ruta de reenvío.</p>
Saltos permitidos de BFD	<p>Acepte la configuración predeterminada.</p> <p>Puede establecer el número de sesiones de BFD de salto admitidas para el perfil.</p>
Varias declaraciones de inactividad de BFD	<p>Acepte la configuración predeterminada.</p> <p>Puede establecer la cantidad de veces que no se recibe el paquete de BFD antes de indicar que la sesión está inactiva.</p>
Umbral de reubicación en espera	Acepte la configuración predeterminada.

Agregar un perfil de puente de NSX Edge

El perfil de puente de NSX Edge define las directivas del clúster de puente de ESXi.

Un clúster de puente es una colección de nodos de transporte de host de ESXi.

Requisitos previos

- Compruebe que el clúster de NSX Edge esté disponible.
- Compruebe que el clúster de puente de ESXi esté disponible.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión con privilegios de administrador en NSX Manager.
- 2 Seleccione **Sistema > Tejido > Perfiles > Perfiles de puente de Edge > Agregar**.
- 3 Introduzca los detalles del perfil de clúster de NSX Edge.

Opción	Descripción
Nombre y descripción	<p>Introduzca un nombre para el perfil de clúster de puente de NSX Edge.</p> <p>Opcionalmente, puede introducir otros detalles del perfil, como los detalles del nodo principal y del nodo de copia de seguridad.</p>
Clúster de Edge	Seleccione el clúster de NSX Edge que desea utilizar.
Nodo principal	Designa el nodo de NSX Edge preferido del clúster.

Opción	Descripción
Nodo de copia de seguridad	Designa un nodo de copia de seguridad de NSX Edge en caso de error del nodo principal.
Modo de conmutación por error	<p>Seleccione el modo Preferente o No preferente.</p> <p>El modo de alta disponibilidad predeterminado es preferente, lo que puede ralentizar el tráfico cuando el nodo preferido NSX Edge se vuelve a conectar. El modo no preferente no ralentiza el tráfico.</p>

Agregar perfil de nodo de transporte

Un perfil de nodo de transporte captura la configuración necesaria para crear un nodo de transporte. El perfil de nodo de transporte puede aplicarse a un clúster de vCenter Server existente para crear nodos de transporte para los hosts miembro. Los perfiles de nodo de transporte definen las zonas de transporte, los hosts miembros y la configuración de conmutador N-VDS, incluido el perfil de vínculo superior, la asignación de direcciones IP, la asignación de NIC físicas al vínculo superior virtual interfaces, etc.

La creación de nodos de transporte comienza cuando se aplica un perfil de nodo de transporte a un clúster de vCenter Server. NSX Manager prepara los hosts del clúster e instala los componentes de NSX-T Data Center en todos los hosts. Los nodos de transporte de los hosts se crean en función de la configuración especificada en el perfil de nodo de transporte.

Para eliminar un perfil de nodo de transporte, primero debe desasociar el perfil del clúster asociado. Los nodos de transporte existentes no se verán afectados. Los nuevos hosts agregados al clúster ya no se convierten automáticamente en nodos de transporte.

Consideraciones para la creación del perfil de nodo de transporte:

- Puede agregar un máximo de cuatro conmutadores de N-VDS para cada configuración: N-VDS mejorado creado para la zona de transporte de VLAN, N-VDS estándar creado para la zona de transporte de superposición y N-VDS mejorado creado para la zona de transporte de superposición.
- No hay límite en la cantidad de conmutadores de N-VDS estándar creados para la zona de transporte de VLAN.
- En una topología de clúster de host único que ejecuta varios conmutadores de N-VDS estándar de superposición y una máquina virtual de Edge en el mismo host, NSX-T Data Center proporciona aislamiento de tráfico de modo que el tráfico que pasa a través del primer N-VDS esté aislado del tráfico que pasa a través del segundo N-VDS, y así sucesivamente. Las NIC físicas de cada N-VDS deben asignarse a la máquina virtual de Edge en el host para permitir la conectividad del tráfico de norte a sur con el mundo externo. Los paquetes que salen de una máquina virtual en la primera zona de transporte deben redirigirse a través de un enrutador externo o una máquina virtual externa a la máquina virtual en la segunda zona de transporte.
- Cada nombre de conmutador de N-VDS debe ser único. NSX-T Data Center no admite el uso de nombres de conmutador duplicados.
- Cada identificador de zona de transporte debe ser único. NSX-T Data Center no admite el uso de nombres de identificadores duplicados.

- Puede agregar un máximo de 1000 zonas de transporte al perfil de nodo de transporte.
- Para agregar una zona de transporte, se debe haber realizado con cualquiera de los N-VDS presentes en el perfil de nodo de transporte.

Requisitos previos

- Compruebe que los hosts formen parte de un clúster de vCenter Server.
vCenter Server debe tener al menos un clúster.
- Compruebe que esté configurada una zona de transporte. Consulte [Crear zonas de transporte](#).
- Compruebe que haya un clúster disponible. Consulte [Implementar nodos de NSX Manager para formar un clúster mediante la interfaz de usuario](#).
- Compruebe que se haya configurado un grupo de direcciones IP, o que DHCP esté disponible en la implementación de red. Consulte [Crear un grupo de direcciones IP para direcciones IP de endpoints de túneles](#).
- Compruebe que se haya configurado un administrador de equipos. Consulte [Agregar un administrador de equipos](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión con privilegios de administrador en NSX Manager.
- 2 Seleccione **Sistema > Tejido > Perfiles > Perfiles de nodo de transporte > Agregar**.
- 3 Introduzca un nombre para introducir el perfil de nodo de transporte.
También puede agregar una descripción sobre el perfil de nodo de transporte.
- 4 Seleccione las zonas de transporte disponibles y haga clic en el botón > para incluir las zonas de transporte en el perfil de nodo de transporte.

Nota Puede agregar varias zonas de transporte.

- 5 Haga clic en la pestaña **N-VDS** y proporcione la información del conmutador.

Opción	Descripción
Nombre del N-VDS	Si el nodo de transporte está asociado a una zona de transporte, asegúrese de que el nombre que introdujo para el N-VDS sea el mismo que el nombre del N-VDS especificado en la zona de transporte. Un nodo de transporte puede crearse sin asociarlo a una zona de transporte.
Zonas de transporte asociadas	Muestra las zonas de transporte que se han realizado con conmutadores de host asociados. No se puede agregar una zona de transporte si no se ha realizado con cualquier N-VDS del perfil de nodo de transporte.
Perfil NIOC	Seleccione el perfil NIOC en el menú desplegable. Se aplican las asignaciones de ancho de banda especificadas en el perfil para los recursos de tráfico.

Opción	Descripción
Perfil de vínculo superior	<p>Seleccione un perfil de enlace ascendente en el menú desplegable o cree un perfil personalizado.</p> <p>Nota Los hosts del clúster deben tener el mismo perfil de enlace ascendente.</p> <p>También puede utilizar el perfil de enlace ascendente predeterminado.</p>
Perfil de LLDP	<p>De forma predeterminada, NSX-T solo recibe paquetes LLDP de un vecino LLDP. Sin embargo, NSX-T se puede configurar para enviar paquetes LLDP a un vecino LLDP y recibirlos de él.</p>
Asignación de IP	<p>Seleccione Usar DHCP, Usar grupo de direcciones IP o Usar lista de direcciones IP estáticas para asignar una dirección IP a los endpoints de túnel virtual (VTEP) del nodo de transporte.</p> <p>Si selecciona Usar lista de direcciones IP estáticas (Use Static IP List), debe especificar una lista de direcciones IP separadas por comas, una puerta de enlace y una máscara de subred. Todos los VTEP del nodo de transporte deben estar en la misma subred, de lo contrario no se establecerá la sesión de flujo bidireccional (BFD).</p>
Grupo de direcciones IP	<p>Si seleccionó Usar grupo de direcciones IP para la asignación de direcciones IP, especifique el nombre del grupo de direcciones IP.</p>
NIC físicas	<p>Agregue NIC físicas al nodo de transporte. Puede usar el enlace ascendente o asignar uno existente en el menú desplegable.</p> <p>Haga clic en Agregar PNIC para configurar NIC físicas adicionales en el nodo de transporte.</p> <p>Nota La migración de las NIC físicas que se agreguen en este campo dependerá de cómo se configuren Migración solamente de PNIC, Asignaciones de red para instalación y Asignaciones de red para desinstalación.</p> <ul style="list-style-type: none"> ■ Para migrar una NIC física utilizada (por ejemplo, mediante un vSwitch estándar o un conmutador distribuido de vSphere) sin una asignación de VMkernel asociada, asegúrese de que la opción Migración solamente de PNIC esté habilitada. De lo contrario, el nodo de transporte sigue en estado parcialmente correcto y no se puede establecer la conectividad del LCP del nodo de tejido. ■ Para migrar una NIC física utilizada con una asignación de red de VMkernel asociada, deshabilite la opción Migrar solamente de PNIC y configure la asignación de red de VMkernel. ■ Para migrar una NIC física libre, habilite la opción Migrar solamente de PNIC.

Opción	Descripción
Migración solamente de PNIC	<p>Antes de establecer este campo, tenga en cuenta los siguientes puntos:</p> <ul style="list-style-type: none"> ■ Sepa si la NIC física definida es una NIC utilizada o una NIC libre. ■ Determine si las interfaces de VMkernel de un host se deben migrar junto con las NIC físicas. <p>Configure el campo:</p> <ul style="list-style-type: none"> ■ Habilite la opción Migración solamente de PNIC solo si desea migrar las NIC físicas de un conmutador VSS o DVS a un conmutador de N-VDS. ■ Deshabilite la opción Migración solamente de PNIC si va a migrar una NIC física utilizada y su asignación de interfaz de VMkernel asociada. Una NIC física disponible o libre se asocia al conmutador de N-VDS cuando se especifica la asignación de migración de interfaz de VMkernel. <p>En un host con varios conmutadores de host:</p> <ul style="list-style-type: none"> ■ Si todos los conmutadores de host se van a migrar solo a PNIC, puede migrar las PNIC en una sola operación. ■ Si algunos conmutadores de hosts se van a migrar a interfaces de VMkernel y el resto de conmutadores de host se van a migrar solo a PNIC: <ol style="list-style-type: none"> 1 En la primera operación, migre solo las PNIC. 2 En la segunda operación, migre las interfaces de VMkernel. Asegúrese de que la opción Migración solamente de PNIC esté deshabilitada. <p>Las opciones Migración solamente de PNIC y Migración de interfaces de VMkernel no se admiten al mismo tiempo en varios hosts.</p> <hr/> <p>Nota Para migrar una NIC de la red de administración, configure su asignación de red de VMkernel asociado y mantenga la opción Migración solamente de PNIC deshabilitada. Si solo va a migrar la NIC de administración, el host perderá conectividad.</p> <hr/> <p>Para obtener más información, consulte Migrar VMkernel a un conmutador de N-VDS.</p>

Opción	Descripción
Asignaciones de red para instalación	<p>Para migrar VMkernel al conmutador de N-VDS durante la instalación, se asignan VMkernel a un conmutador lógico existente. NSX Manager migra el VMkernel al conmutador lógico asignado en N-VDS.</p> <p>Precaución Asegúrese de que la NIC de administración y la interfaz de VMkernel se migran a un conmutador lógico conectado a la misma VLAN a la que estaba conectada la NIC de administración antes de la migración. Si vmnic<n> y VMkernel<n> se migran a una VLAN distinta, se perderá la conectividad con el host.</p> <p>Precaución Para las NIC físicas asignadas, asegúrese de que la asignación de conmutador de host de la NIC física con la interfaz de VMkernel coincide con la configuración especificada en el perfil de nodo de transporte. Como parte del proceso de validación, NSX-T Data Center comprueba la asignación, y si la validación es correcta, la migración de las interfaces de VMkernel a un conmutador de N-VDS es correcta. También es obligatorio configurar la asignación de red para la desinstalación porque NSX-T Data Center no almacena la configuración de asignación del conmutador del host después de migrar las interfaces de VMkernel al conmutador de N-VDS. Si la asignación no está configurada, se puede perder la conectividad con los servicios, como vSAN, después de volver a migrar al conmutador de VSS o VDS.</p> <p>Para obtener más información, consulte Migrar VMkernel a un conmutador de N-VDS.</p>
Asignaciones de red para desinstalación	<p>Para revertir la migración de VMkernel durante la desinstalación, asigne VMkernel a los grupos de puertos de VSS o DVS, para que NSX Manager sepa a qué grupo de puertos se debe volver a migrar el VMkernel en el VSS o DVS. Para un conmutador de DVS, asegúrese de que el grupo de puertos sea del tipo Efímero.</p> <p>Precaución Para las NIC físicas asignadas, asegúrese de que la asignación de perfil de nodo de transporte de la NIC física con la interfaz de VMkernel coincide con la configuración especificada en el conmutador de host. Es obligatorio configurar la asignación de red para la desinstalación porque NSX-T Data Center no almacena la configuración de asignación del conmutador del host después de migrar las interfaces de VMkernel al conmutador de N-VDS. Si la asignación no está configurada, se puede perder la conectividad con los servicios, como vSAN, después de volver a migrar al conmutador de VSS o VDS.</p> <p>Para obtener más información, consulte Migrar VMkernel a un conmutador de N-VDS.</p>

6 Para agregar otro conmutador de N-VDS, haga clic en **+ AGREGAR N-VDS**.

7 Haga clic en **Guardar** para finalizar la configuración.

Pasos siguientes

Aplique el perfil de nodo de transporte a un clúster de vSphere existente. Consulte [Configurar un nodo de transporte de host administrado](#).

Migrar VMkernel a un conmutador de N-VDS

Para migrar las interfaces de VMkernel desde un conmutador de VSS o DVS a un conmutador de N-VDS en un nivel de clúster, configure el perfil del nodo de transporte con los detalles de asignación de red que

se necesitan para la migración (asignar las interfaces de VMkernel a conmutadores lógicos). De forma similar, para migrar las interfaces de VMkernel en un nodo de host, establezca la configuración del nodo de transporte. Para revertir la migración de las interfaces de VMkernel a un conmutador de VSS o DVS, configure la desinstalación de asignación de red (asignar puertos lógicos a una interfaz de VMkernel) en el perfil del nodo de transporte para que se realice durante la desinstalación.

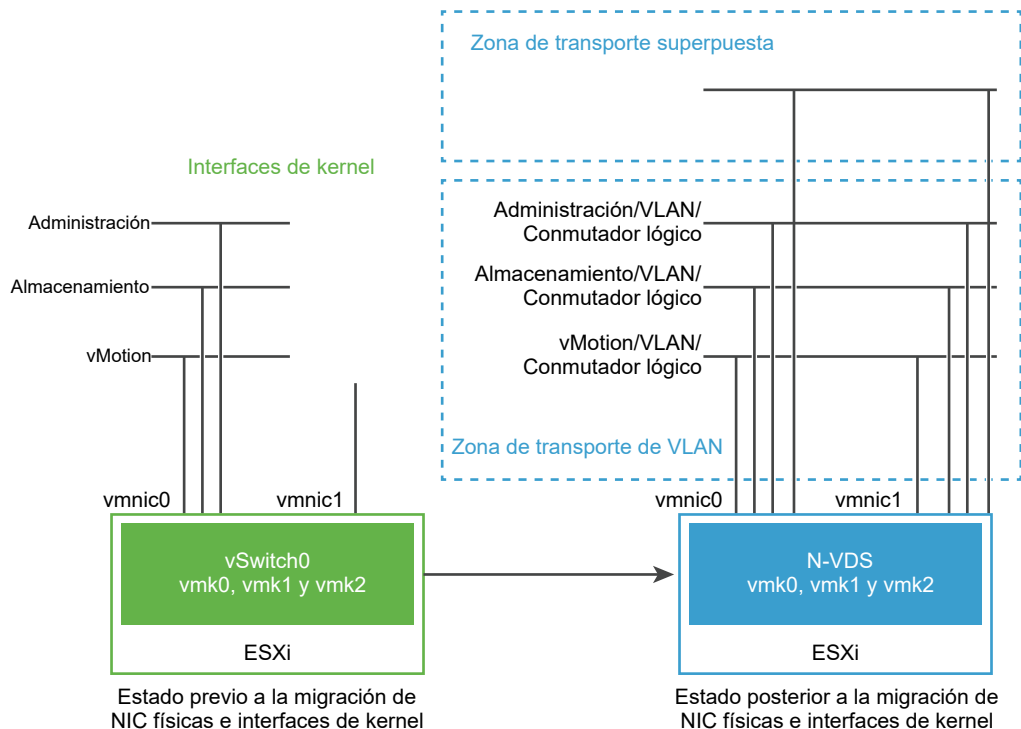
Durante la migración, se migran las NIC físicas que se están usando en ese momento a un conmutador de N-VDS, mientras que las NIC físicas que están disponibles o libres se asocian al conmutador de N-VDS después de la migración.

Nota Los perfiles del nodo de transporte se aplican a todos los hosts miembros de un clúster. Sin embargo, si desea limitar la migración de interfaces de VMkernel en hosts específicos, puede configurar el host directamente. Después de la migración, N-VDS controlará el tráfico en la VLAN y la red de superposición en aquellas interfaces que se asocien al conmutador de N-VDS.

Importante Las configuraciones que se realizan en hosts individuales se marcan como Anuladas. Cualquier otra actualización que se realice en el perfil del nodo de transporte no se aplicará a estos hosts anulados. Estos hosts permanecerán en estado anulado hasta que se desinstale NSX-T Data Center.

En la siguiente figura, si un host solo tiene dos NIC físicas, es posible que desee asignar ambas NIC al N-VDS para la redundancia y sus interfaces de VMkernel asociadas, de manera que las interfaces no pierdan la conectividad con el host.

Figura 8-2. Migración previa y posterior de las interfaces de red a un N-VDS



Antes de la migración, el host ESXi tiene dos vínculos superiores derivados de los dos puertos físicos: vmnic0 y vmnic1. Aquí, vmnic0 está configurado para estar en un estado activo, conectado a un VSS, mientras que vmnic1 no se utiliza. Adicionalmente, existen tres interfaces de VMkernel: vmk0, vmk1 y vmk2.

Las interfaces de VMkernel se pueden migrar mediante la interfaz de usuario de NSX-T Data Center Manager o las API de NSX-T Data Center. Consulte *Guía de la API de NSX-T Data Center*.

Después de la migración, vmnic0, vmnic1 y sus interfaces de VMkernel se migran al conmutador de N-VDS. Tanto vmnic0 como vmnic1 se conectan a través de VLAN y las zonas de transporte superpuestas.

Consideraciones para la migración de VMkernel

- Migración de PNIC y VMkernel: antes de migrar las NIC físicas ancladas y las interfaces de VMkernel asociadas a un conmutador de N-VDS, anote la asignación de red (asignación de NIC físicas a un grupo de puertos) en el conmutador de host.
- Migración solo de PNIC: si tiene pensado migrar solo las PNIC, compruebe que no se ha migrado la NIC física de administración conectada a la interfaz de administración de VMkernel. Provoca la pérdida de conectividad con el host. Para obtener más detalles, consulte el campo **Migración solo de PNIC** en [Agregar perfil de nodo de transporte](#).
- Revertir la migración: antes de plantearse revertir la migración de las interfaces de VMkernel al conmutador de host VSS o DVS para las dos NIC físicas ancladas, compruebe que ha anotado la asignación de red (asignación de NIC físicas a un grupo de puertos) en el conmutador de host. Es obligatorio configurar el perfil del nodo de transporte con la asignación del conmutador de host en el campo **Asignación de red para la desinstalación**. Sin esta asignación, NSX-T Data Center no sabe a qué grupos de puertos se deben migrar de nuevo las interfaces de VMkernel. Esta situación puede provocar la pérdida de conectividad con la red de vSAN.
- Registro de vCenter Server antes de la migración: si tiene pensado migrar una VMkernel o PNIC conectada a un conmutador de DVS, compruebe que vCenter Server está protegido con NSX Manager.
- Coincidencia del identificador de VLAN: después de la migración, la interfaz de VMkernel de administración y la NIC de administración deben estar en la misma VLAN en la que la NIC estaba conectada antes de la migración. Si vmnic0 y vmk0 están conectados a la red de administración y se migran a una VLAN distinta, se perderá la conectividad con el host.
- Migración al conmutador de VSS: no se pueden volver a migrar las dos interfaces de VMkernel al mismo grupo de puertos de un conmutador de VSS.
- vMotion: Ejecute vMotion para mover cargas de trabajo de máquinas virtuales a otro host antes de la migración a PNIC y/o VMkernel. Si se produce un error en la migración, las máquinas virtuales de la carga de trabajo no se ven afectadas.
- vSAN: Si el tráfico de vSAN se ejecuta en el host, ponga el host en modo de mantenimiento mediante vCenter Server y mueva las máquinas virtuales del host mediante la función vMotion antes de la migración de PNIC y/o VMkernel.

- **Migración:** Si un VMkernel ya está conectado a un conmutador de destino, aún se puede seleccionar para migrarlo al mismo conmutador. Esta propiedad hace que la operación de migración de PNIC y/o VMK sean idempotente. Esto resulta útil cuando se migra solo PNICs a un conmutador de destino. Debido a que la migración siempre requiere al menos un VMkernel y una PNIC, debe seleccionar un VMkernel que ya se haya migrado a un conmutador de destino cuando migre solo PNICs a un conmutador de destino. Si no es necesario migrar ningún VMkernel, cree un VMkernel temporal mediante una instancia de vCenter Server en el conmutador de origen o en el de destino. A continuación, mígrelo junto con las PNIC y elimine el VMkernel temporal mediante vCenter Server una vez que haya finalizado la migración.
- **Uso compartido de direcciones MAC:** Si una interfaz de VMkernel y una PNIC comparten la misma dirección MAC y se encuentran en el mismo conmutador, se deberán migrar conjuntamente al mismo conmutador de destino si se usan después de la migración. Mantenga siempre vmk0 y vmnic0 en el mismo conmutador.

Compruebe los equipos Mac utilizados por todos los VMK y PNIC en el host. Para ello, ejecute los siguientes comandos:

```
esxcfg-vmknics -l
```

```
esxcfg-nics -l
```

- **Puertos lógicos de VIF creados después de la migración:** después de migrar el VMkernel de un conmutador VSS o DVS a otro N-VDS, se crea un puerto de conmutador lógico del tipo VIF en NSX Manager. No debe crear reglas de firewall distribuido en estos puertos de conmutadores lógicos de VIF.

Migrar interfaces de VMkernel a un conmutador de N-VDS

El flujo de trabajo de alto nivel para migrar Interfaces de VMkernel a un conmutador de N-VDS:

- 1 Si es necesario, cree un conmutador lógico.
- 2 Apague las máquinas virtuales en el host desde el cual se migran las interfaces de VMkernel y las PNICs a un conmutador de N-VDS.
- 3 Configure un perfil de nodo de transporte con una asignación de red que se utilice para migrar las interfaces de VMkernel durante la creación de los nodos de transporte. La asignación de red implica la asignación de una interfaz de VMkernel a un conmutador lógico.

Para obtener más información, consulte [Agregar perfil de nodo de transporte](#).
- 4 Compruebe que las asignaciones de adaptador de red en vCenter Server reflejan una nueva asociación del conmutador de VMkernel con un conmutador de N-VDS. En el caso de las NIC físicas ancladas, compruebe que la asignación en NSX-T Data Center refleja cualquier VMkernel anclada en una NIC física en vCenter Server.
- 5 En NSX Manager, vaya a **Opciones avanzadas de redes y seguridad > Redes > Conmutación**. En la página de **conmutadores**, compruebe que la interfaz de VMkernel está asociada al conmutador lógico a través de un puerto lógico creado recientemente.

- 6 Vaya a **Sistema > Nodos > Nodo de transporte de host**. Para cada nodo de transporte, compruebe que el estado en la columna **Estado del nodo** es **Correcto** para confirmar que la configuración del nodo de transporte se ha validado correctamente.
- 7 En la página **Nodo de transporte de host**, compruebe que el estado en **Estado de configuración** es **Correcto** para confirmar que el host se ha realizado correctamente con la configuración especificada.

Después de migrar interfaces de VMkernel y PNIC de un conmutador VDS a un N-VDS mediante la interfaz de usuario de NSX-T o la API del nodo de transporte, vCenter Server mostrará advertencias para el VDS. Si es necesario que el host esté conectado al VDS, quite el host del VDS. La instancia de vCenter Server dejará de mostrar advertencias para VDS.

Para obtener detalles sobre los errores que pueden surgir durante la migración, consulte [Errores de migración de VMkernel](#).

Revertir la migración de las interfaces de VMkernel a un conmutador de VSS o DVS

El flujo de trabajo de alto nivel para revertir la migración de las interfaces de VMkernel desde un conmutador de N-VDS a un conmutador de VSS o DVS durante la desinstalación de NSX-T Data Center:

- 1 En el host de ESXi, apague las máquinas virtuales conectadas a los puertos lógicos que aloja la interfaz de VMkernel después de la migración.
- 2 Configure un perfil de nodo de transporte con una asignación de red que se utilice para migrar las interfaces de VMkernel durante el proceso de desinstalación. La asignación de red durante la desinstalación asigna las interfaces de VMkernel a un grupo de puertos en el conmutador de VSS o DVS en el host de ESXi.

Nota Para revertir la migración de una interfaz de VMkernel a un grupo de puertos en un conmutador de DVS, compruebe que el tipo de grupo de puertos está establecido en **Efímero**.

Para obtener más información, consulte [Agregar perfil de nodo de transporte](#).

- 3 Compruebe que las asignaciones de adaptador de red en vCenter Server reflejan una nueva asociación del conmutador de VMkernel con un grupo de puertos del conmutador de VSS o DVS.
- 4 En NSX Manager, vaya a **Opciones avanzadas de redes y seguridad > Redes > Conmutación**. En la página **Conmutadores**, compruebe que se elimina el conmutador lógico que contiene las interfaces de VMkernel.

Para obtener detalles sobre los errores que pueden surgir durante la migración, consulte [Errores de migración de VMkernel](#).

Actualizar la asignación del conmutador de host

Importante

- Hosts con estado: se admiten las operaciones de agregar y actualizar. Para actualizar una asignación existente, puede agregar una nueva entrada de la interfaz de VMkernel a la configuración de asignación de red. Si actualiza la configuración de asignación de red de una interfaz de VMkernel que ya se ha migrado al conmutador de N-VDS, no se realiza la asignación de red actualizada en el host.
- Hosts sin estado: se admiten las operaciones de agregar, actualizar y eliminar. Los cambios que se realicen en la configuración de asignación de red se harán efectivos una vez que se reinicie el host.

Para actualizar las interfaces de VMkernel a un nuevo conmutador lógico, puede editar el perfil de nodo de transporte para aplicar las asignaciones de red en un nivel de clúster. Si prefiere que las actualizaciones se apliquen únicamente a un host, configure el nodo de transporte mediante las API de nivel de host.

Nota Después de actualizar la configuración del nodo de transporte para un host individual, las nuevas actualizaciones que se apliquen mediante el perfil de nodo de transporte no se aplicarán a ese host. El estado de ese host pasa a ser anulado.

- 1 Para actualizar todos los hosts de un clúster, edite el campo **Asignación de red durante la instalación** para actualizar la asignación de VMkernel a conmutadores lógicos.
Para obtener más información, consulte [Agregar perfil de nodo de transporte](#).
- 2 Guarde los cambios. Los cambios que se realizan en un perfil de nodo de transporte se aplican automáticamente a todos los hosts miembros del clúster, a excepción de los hosts que están marcados con el estado se anulado.
- 3 Del mismo modo, para actualizar un host individual, edite la asignación de VMkernel en la configuración del nodo de transporte.

Nota Si actualiza el campo **Asignación de red durante la instalación** con una nueva asignación de VMkernel, tendrá que agregar la misma interfaz de VMkernel al campo **Asignación de red durante la desinstalación**.

Para obtener detalles sobre los errores que pueden surgir durante la migración, consulte [Errores de migración de VMkernel](#).

Migrar interfaces de VMkernel en un clúster sin estado

- 1 Prepare y configure un host como un host de referencia mediante las API de nodo de transporte.
- 2 Extraiga el perfil de host del host de referencia.
- 3 En vCenter Server, aplique el perfil de host al clúster sin estado.
- 4 En NSX-T Data Center, aplique el perfil de nodo de transporte al clúster sin estado.
- 5 Reinicie cada host del clúster.

Los hosts del clúster pueden tardar varios minutos en aplicar los estados actualizados.

Escenarios de errores en la migración

- Si se produce un error en la migración por algún motivo, el host intentará migrar las NIC físicas y las interfaces de VMkernel tres veces.
- Si se sigue generando un error en la migración, el host realiza una reversión a la configuración anterior mediante la conversación de la conectividad de VMkernel con la NIC física de administración, vmnic0.
- En caso de que se produzca también un error en la reversión (por ejemplo, que se pierda el VMkernel configurado en la NIC física de administración), tendrá que restablecer el host.

Escenarios de migración no compatible

No se admiten los siguientes escenarios:

- Las interfaces de VMkernel de dos conmutadores de VSS o DVS distintos se migran al mismo tiempo.
- En hosts con estado, la asignación de red se actualiza para asignar la interfaz de VMkernel a otro conmutador lógico. Por ejemplo, antes de la migración, el VMkernel se asigna al conmutador lógico 1 y la interfaz de VMkernel se asigna al conmutador lógico 2.

Errores de migración de VMkernel

Es posible que se produzcan errores al migrar interfaces de VMkernel y NIC físicas de un conmutador VSS o DVS a un conmutador N-VDS o al revertir las interfaces de migración a un conmutador de host VSS o DVS.

Tabla 8-1. Errores de migración de VMkernel

Código de error	Problema	Motivo	Resolución
8224	No se ha encontrado el conmutador de host especificado por la configuración del nodo de transporte.	No se ha encontrado el identificador de conmutador de host.	<ul style="list-style-type: none"> ■ Asegúrese de que la zona de transporte se haya creado con el nombre del conmutador de host y, a continuación, cree el nodo de transporte. ■ Asegúrese de utilizar un conmutador de host válido en la configuración del nodo de transporte.
8225	La migración de VMkernel está en curso.	La migración está en curso.	Espere a que la migración finalice antes de realizar otra acción.
8226	La migración de VMkernel solo se admite en hosts de ESXi.	La migración solo es válida para los hosts de ESXi.	Asegúrese de que el host sea un host de ESXi antes de iniciar la migración.

Tabla 8-1. Errores de migración de VMkernel (continuación)

Código de error	Problema	Motivo	Resolución
8227	La interfaz de VMkernel no se anexa al nombre del conmutador de host.	En un host con varios conmutadores de host, NSX-T Data Center no puede identificar la asociación de cada interfaz de VMkernel con su conmutador de host.	<p>Si el host tiene varios conmutadores de host de N-VDS, asegúrese de que la interfaz de VMkernel se anexe al nombre del conmutador de N-VDS al que esté conectado el host.</p> <p>Por ejemplo, la asignación de red para la desinstalación de un host con el nombre de conmutador de host de N-VDS nsxvswitch1 y VMkernel1 y otro nombre de conmutador de host de N-VDS nsxvswitch2 y VMkernel2 deben definirse tal como se indica a continuación: <code>device_name: VMkernel1@nsxvswitch1</code>, <code>destination_network: DPortGroup</code>.</p>
8228	El conmutador de host que se usa en el campo <code>device_name</code> no se encuentra en el host.	El nombre del conmutador de host no es correcto.	Introduzca el nombre de conmutador de host correcto.
8229	El nodo de transporte no ha especificado la zona de transporte del conmutador lógico.	No se ha agregado la zona de transporte.	Agregue la zona de transporte a la configuración del nodo de transporte.
8230	No hay ninguna NIC física en el conmutador de host.	Debe haber al menos una NIC física en el conmutador de host.	Especifique al menos una NIC física para un perfil de vínculo superior, y la configuración de asignación de red de VMkernel a un conmutador lógico.
8231	El nombre del conmutador de host no coincide.	Si el nombre del conmutador de host utilizado en <code>vmk1@host_switch</code> no coincide con el nombre del conmutador de host utilizado por el conmutador lógico de destino de la interfaz.	Asegúrese de que el nombre del conmutador de host especificado en la configuración de asignación de red coincida con el nombre utilizado por el conmutador lógico de la interfaz.
8232	El conmutador lógico no se ha realizado en el host.	La realización del conmutador lógico en el host no se ha realizado correctamente.	Sincronice el host con NSX Manager.
8233	Hay un conmutador lógico inesperado en la asignación de interfaz de red.	La asignación de interfaz de red para la instalación y la desinstalación muestra los conmutadores lógicos y los grupos de puertos.	La asignación de red de la instalación solo debe contener conmutadores lógicos como destinos de destino. De forma similar, la asignación de red de la desinstalación solo debe contener grupos de puertos como destinos.

Tabla 8-1. Errores de migración de VMkernel (continuación)

Código de error	Problema	Motivo	Resolución
8294	El conmutador lógico no existe en la asignación de interfaz de red.	No se han especificado conmutadores lógicos.	Asegúrese de que los conmutadores lógicos se hayan especificado en la configuración de asignación de interfaz de red.
8296	Error de coincidencia del conmutador de host.	La asignación de interfaz de red de la desinstalación se ha configurado con el nombre del conmutador de host incorrecto.	Asegúrese de que el nombre del conmutador de host utilizado en la configuración de asignación coincida con el nombre introducido en el conmutador de host donde se encuentran las interfaces de VMkernel.
8297	VMkernel duplicado.	Se han especificado VMkernel duplicados para la migración.	Asegúrese de que no haya interfaces de VMkernel duplicadas en la configuración de asignación de la instalación o la desinstalación.
8298	Error de coincidencia entre el número de interfaces de VMkernel y los destinos.	Configuración incorrecta.	Asegúrese de que cada interfaz VMkernel tenga un destino especificado correspondiente en la configuración.
8299	No se puede eliminar el nodo de transporte debido a que la interfaz de VMkernel está utilizando los puertos en N-VDS.	Las interfaces de VMkernel están usando puertos del conmutador de N-VDS.	Revierta la migración de todas las interfaces de VMkernel del conmutador de N-VDS a un conmutador VSS/DVS. A continuación, intente eliminar el nodo de transporte.
9412	No se pueden migrar VMkernel de un N-VDS a otro.	Acción no admitida.	Revierta la migración de la interfaz de VMkernel a un conmutador VSS o DVS. A continuación, podrá migrar la interfaz de VMkernel a otro conmutador de N-VDS.
9413	No se pueden migrar las interfaces de VMkernel a otro conmutador lógico.	En los hosts con estado, un VMkernel conectado a un conmutador lógico no puede migrarse a otro conmutador lógico.	Revierta la migración del VMkernel del conmutador lógico a un conmutador VSS/DVS. A continuación, migre el VMkernel a otro conmutador lógico del N-VDS.
9414	Interfaces de VMkernel duplicadas.	Se han asignado interfaces de VMkernel duplicadas a la configuración de asignación de la instalación y la desinstalación.	Asegúrese de que las interfaces de VMkernel sean únicas en las asignaciones de la instalación y la desinstalación.
9415	Hay máquinas virtuales encendidas en el host.	Con máquinas virtuales encendidas, la migración no puede continuar.	Apague las máquinas virtuales en el host antes de iniciar la migración de las interfaces de VMkernel.
9416	No se encuentra el VMkernel en el host.	No se ha especificado un VMkernel existente en el host de la configuración de asignación de red.	Especifique un VMkernel que exista en la configuración de asignación de red.

Tabla 8-1. Errores de migración de VMkernel (continuación)

Código de error	Problema	Motivo	Resolución
9417	No se encontró el grupo de puertos.	No se ha especificado un grupo de puertos existente en el host de la configuración de asignación de red.	Especifique un grupo de puertos que exista en la configuración de asignación de red.
9419	No se ha encontrado el conmutador lógico durante la migración.	No se ha encontrado el conmutador lógico definido en la configuración de asignación de interfaz de red.	Especifique un conmutador lógico que exista en la configuración de asignación de interfaz de red.
9420	No se ha encontrado el puerto lógico durante la migración.	Durante la migración, NSX-T Data Center no ha encontrado los puertos creados en el conmutador lógico.	Para que la migración se realice correctamente, asegúrese de que no se hayan eliminado puertos lógicos del conmutador lógico.
9421	Falta la información del host para validar el proceso de migración.	No se puede recuperar la información del host del inventario.	Reintente el proceso de migración.
9423	Las NIC físicas asignadas a una interfaz de VMkernel no se han migrado al conmutador de host correcto.	Se ha encontrado una NIC física asignada en el entorno, pero el VMkernel y la NIC física no se han migrado al mismo conmutador de host.	Una NIC física asignada a la interfaz de VMkernel debe tener una configuración de nodo de transporte que asigne la NIC física al VMkernel en el mismo conmutador de host.
600	No se encuentra el objeto.	La zona de transporte especificada utilizada por el conmutador lógico no existe. No se encuentra el conmutador lógico que se encuentra en el destino de la asignación de VMK.	<ul style="list-style-type: none"> ■ Especifique una zona de transporte que exista en el entorno. ■ Cree el conmutador lógico deseado o utilice un conmutador lógico de VLAN existente.
8310	El tipo de conmutador lógico es incorrecto.	El tipo de conmutador lógico es Superposición.	Cree un conmutador lógico VLAN.
9424	Si las opciones Migración solamente de PNIC y Asignación de red de la instalación o la desinstalación se configuran al mismo tiempo, no se puede realizar la migración.	La migración solo progresa cuando se configura una de esas opciones.	Asegúrese de que solo se haya configurado una de las opciones Migración solamente de PNIC o Asignación de red para la instalación o la desinstalación.

Crear un host independiente o un nodo de transporte sin sistema operativo

Primero, agregue el host de ESXi, el host de KVM o el servidor sin sistema operativo al tejido de NSX-T Data Center y, a continuación, configure el nodo de transporte.

Un nodo de tejido es un nodo que se registró con el plano de administración de NSX-T Data Center y que tiene módulos de NSX-T Data Center instalados. Para que un host o un servidor sin sistema operativo formen parte de la superposición de NSX-T Data Center, deben agregarse primero al tejido de NSX-T Data Center.

Un nodo de transporte es un nodo que participa en una superposición de NSX-T Data Center o redes VLAN de NSX-T Data Center.

Para un host o un servidor sin sistema operativo de KVM, puede preconfigurar el N-VDS o puede hacer que NSX Manager realice la configuración. Para un host ESXi, NSX Manager siempre configura el N-VDS.

Nota Si planea crear nodos de transporte desde una VM de plantilla, asegúrese de que no haya certificados en el host en `/etc/vmware/nsx/`. El agente netcpa no crea ningún certificado si existe uno.

El servidor sin sistema operativo admite superposición y zona de transporte de VLAN. Puede utilizar la interfaz de administración para administrar el servidor sin sistema operativo. La interfaz de la aplicación permite acceder a las aplicaciones del servidor sin sistema operativo.

Las NIC físicas únicas proporcionan una dirección IP a las interfaces IP de administración y aplicación.

Las NIC físicas dobles proporcionan una NIC física y una dirección IP única a la interfaz de administración. Las NIC físicas dobles también proporcionan una NIC física y una dirección IP única a la interfaz de aplicación.

Varias NIC físicas en una configuración asociada proporcionan NIC físicas dobles y una dirección IP única a la interfaz de administración. Varias NIC físicas en una configuración asociada también proporcionan NIC físicas dobles y una dirección IP única a la interfaz de aplicación.

Puede agregar un máximo de cuatro conmutadores de N-VDS para cada configuración: N-VDS estándar creado para la zona de transporte de VLAN, N-VDS mejorado creado para la zona de transporte de VLAN, N-VDS estándar creado para la zona de transporte de superposición y N-VDS mejorado creado para la zona de transporte de superposición.

En una topología de clúster de host único que ejecuta varios conmutadores de N-VDS estándar de superposición y una máquina virtual de Edge en el mismo host, NSX-T Data Center proporciona aislamiento de tráfico de modo que el tráfico que pasa a través del primer N-VDS esté aislado del tráfico que pasa a través del segundo N-VDS, y así sucesivamente. Las NIC físicas de cada N-VDS deben asignarse a la máquina virtual de Edge en el host para permitir la conectividad del tráfico de norte a sur con el mundo externo. Los paquetes que salen de una máquina virtual en la primera zona de transporte deben redirigirse a través de un enrutador externo o una máquina virtual externa a la máquina virtual en la segunda zona de transporte.

Requisitos previos

- El host debe estar conectado al plano de administración y la conectividad debe estar activa.
- Debe haber una zona de transporte configurada.
- Se debe configurar un perfil de enlace ascendente, o puede utilizar el perfil de enlace ascendente predeterminado.
- Se debe configurar un grupo de direcciones IP o debe estar disponible el protocolo DHCP en la implementación de la red.
- Debe haber disponible al menos una tarjeta NIC física no utilizada en el nodo host.

- Nombre de host
- Dirección IP de administración
- Nombre de usuario
- Contraseña
- (Opcional) (KVM) Huella digital SHA-256 SSL
- (Opcional) (ESXi) Huella digital SHA-256 SSL
- Compruebe que estén instalados los paquetes de terceros requeridos. Consulte [Instalar paquetes de terceros en un host de KVM](#).

Procedimiento

- 1 (opcional) Recupere la huella digital del hipervisor para que pueda proporcionarlo al agregar el host al tejido.

- a Recopile la información de la huella digital del hipervisor.

Utilice un shell de Linux.

```
# echo -n | openssl s_client -connect <esxi-ip-address>:443 2>/dev/null | openssl x509 -noout -fingerprint -sha256
```

Utilice la CLI de ESXi en el host.

```
[root@host:~] openssl x509 -in /etc/vmware/ssl/rui.crt -fingerprint -sha256 -noout
SHA256
Fingerprint=49:73:F9:A6:0B:EA:51:2A:15:57:90:DE:C0:89:CA:7F:46:8E:30:15:CA:4D:5C:95:28:0A:9E:A
2:4E:3C:C4:F4
```

- b Recupere la huella digital SHA-256 de un hipervisor de KVM, ejecute el comando en el host de KVM:

```
# awk '{print $2}' /etc/ssh/ssh_host_rsa_key.pub | base64 -d | sha256sum -b | sed 's/ .*$//' | xxd -r -p | base64
```

- 2 Seleccione **Sistema > Tejido > Nodos > Nodos de transporte de host**.
- 3 En el campo Administrado por, seleccione **Hosts independientes** y haga clic en **+ Agregar**.
- 4 Introduzca los detalles del host independiente o del servidor sin sistema operativo que se agregará al tejido.

Opción	Descripción
Nombre y descripción	<p>Escriba un nombre para identificar el host independiente o el servidor sin sistema operativo.</p> <p>También puede agregar una descripción del sistema operativo utilizado para el host o el servidor sin sistema operativo.</p>
Direcciones IP	Escriba la dirección IP del host o el servidor sin sistema operativo.

Opción	Descripción
Sistema operativo	<p>Seleccione el sistema operativo en el menú desplegable.</p> <p>En función del host o el servidor sin sistema operativo, podrá seleccionar uno de los sistemas operativos compatibles. Consulte Requisitos del sistema.</p>
Nombre de usuario y contraseña	<p>Escriba el nombre de usuario y la contraseña del host.</p>
Huella digital de SHA-256	<p>Introduzca el valor de la huella digital del host para la autenticación.</p> <p>Si deja el valor de huella digital en blanco, se le solicitará que acepte el valor que proporciona el servidor. NSX-T Data Center tarda unos segundos en detectar y autenticar el host.</p>

- 5 (Requerido) Para un host de KVM o un servidor sin sistema operativo, seleccione el tipo de N-VDS.

Opción	Descripción
NSX creado	<p>NSX Manager crea el N-VDS.</p> <p>Esta opción está seleccionada de manera predeterminada.</p>
Preconfigurado	<p>Ya se configuró el N-VDS.</p>

Para un host de ESXi, el tipo de N-VDS siempre se establece como **NSX creado**.

- 6 Introduzca los detalles de N-VDS estándar. Se pueden configurar varios conmutadores de N-VDS en un único host.

Opción	Descripción
Zona de transporte	<p>Seleccione la zona de transporte a la que corresponde este nodo de transporte en el menú desplegable.</p>
Nombre del N-VDS	<p>Debe ser igual al nombre del N-VDS de la zona de transporte a la que pertenece este nodo.</p>
Perfil NIOC	<p>Para un host ESXi, seleccione el perfil NIOC en el menú desplegable.</p>
Perfil de vínculo superior	<p>Seleccione un perfil de enlace ascendente en el menú desplegable o cree un perfil personalizado.</p> <p>También puede utilizar el perfil de enlace ascendente predeterminado.</p>
Perfil de LLDP	<p>De forma predeterminada, NSX-T solo recibe paquetes LLDP de un vecino LLDP. Sin embargo, NSX-T se puede configurar para enviar paquetes LLDP a un vecino LLDP y recibirlos de él.</p>
Asignación de IP	<p>Seleccione Usar DHCP (Use DHCP), Usar grupo de direcciones IP (Use IP Pool) o Usar lista de direcciones IP estáticas (Use Static IP List).</p> <p>Si selecciona Usar lista de direcciones IP estáticas (Use Static IP List), debe especificar una lista de direcciones IP separadas por comas, una puerta de enlace y una máscara de subred.</p>
Grupo de direcciones IP	<p>Si seleccionó Usar grupo de direcciones IP (Use IP Pool) para la asignación de direcciones IP, especifique el nombre del grupo de direcciones IP.</p>

Opción	Descripción
NIC físicas	<p>Agregue NIC físicas al nodo de transporte. Puede usar el enlace ascendente o asignar uno existente en el menú desplegable.</p> <p>Haga clic en Agregar PNIC para configurar NIC físicas adicionales en el nodo de transporte.</p> <hr/> <p>Nota La migración de las NIC físicas que se agreguen en este campo dependerá de cómo se configuren Migración solamente de PNIC, Asignaciones de red para instalación y Asignaciones de red para desinstalación.</p> <hr/> <ul style="list-style-type: none"> ■ Para migrar una NIC física utilizada (por ejemplo, mediante un vSwitch estándar o un conmutador distribuido de vSphere) sin una asignación de VMkernel asociada, asegúrese de que la opción Migración solamente de PNIC esté habilitada. De lo contrario, el nodo de transporte sigue en estado parcialmente correcto y no se puede establecer la conectividad del LCP del nodo de tejido. ■ Para migrar una NIC física utilizada con una asignación de red de VMkernel asociada, deshabilite la opción Migrar solamente de PNIC y configure la asignación de red de VMkernel. ■ Para migrar una NIC física libre, habilite la opción Migrar solamente de PNIC.
Migración solamente de PNIC	<p>Antes de establecer este campo, tenga en cuenta los siguientes puntos:</p> <ul style="list-style-type: none"> ■ Sepa si la NIC física definida es una NIC utilizada o una NIC libre. ■ Determine si las interfaces de VMkernel de un host se deben migrar junto con las NIC físicas. <p>Configure el campo:</p> <ul style="list-style-type: none"> ■ Habilite la opción Migración solamente de PNIC solo si desea migrar las NIC físicas de un conmutador VSS o DVS a un conmutador de N-VDS. ■ Deshabilite la opción Migración solamente de PNIC si va a migrar una NIC física utilizada y su asignación de interfaz de VMkernel asociada. Una NIC física disponible o libre se asocia al conmutador de N-VDS cuando se especifica la asignación de migración de interfaz de VMkernel. <p>En un host con varios conmutadores de host:</p> <ul style="list-style-type: none"> ■ Si todos los conmutadores de host se van a migrar solo a PNIC, puede migrar las PNIC en una sola operación. ■ Si algunos conmutadores de hosts se van a migrar a interfaces de VMkernel y el resto de conmutadores de host se van a migrar solo a PNIC: <ol style="list-style-type: none"> 1 En la primera operación, migre solo las PNIC. 2 En la segunda operación, migre las interfaces de VMkernel. Asegúrese de que la opción Migración solamente de PNIC esté deshabilitada. <p>Las opciones Migración solamente de PNIC y Migración de interfaces de VMkernel no se admiten al mismo tiempo en varios hosts.</p> <hr/> <p>Nota Para migrar una NIC de la red de administración, configure su asignación de red de VMkernel asociado y mantenga la opción Migración solamente de PNIC deshabilitada. Si solo va a migrar la NIC de administración, el host perderá conectividad.</p> <hr/> <p>Para obtener más información, consulte Migrar VMkernel a un conmutador de N-VDS.</p>

Opción	Descripción
Asignaciones de red para instalación	<p>Para migrar VMkernel al conmutador de N-VDS durante la instalación, se asignan VMkernel a un conmutador lógico existente. NSX Manager migra el VMkernel al conmutador lógico asignado en N-VDS.</p> <p>Precaución Asegúrese de que la NIC de administración y la interfaz de VMkernel se migran a un conmutador lógico conectado a la misma VLAN a la que estaba conectada la NIC de administración antes de la migración. Si vmnic<n> y VMkernel<n> se migran a una VLAN distinta, se perderá la conectividad con el host.</p> <p>Precaución Para las NIC físicas asignadas, asegúrese de que la asignación de conmutador de host de la NIC física con la interfaz de VMkernel coincide con la configuración especificada en el perfil de nodo de transporte. Como parte del proceso de validación, NSX-T Data Center comprueba la asignación, y si la validación es correcta, la migración de las interfaces de VMkernel a un conmutador de N-VDS es correcta. Al mismo tiempo, es obligatorio configurar la asignación de red para la desinstalación porque NSX-T Data Center no almacena la configuración de asignación del conmutador del host después de migrar las interfaces de VMkernel al conmutador de N-VDS. Si la asignación no está configurada, se puede perder la conectividad con los servicios, como vSAN, después de volver a migrar al conmutador de VSS o VDS.</p> <p>Para obtener más información, consulte Migrar VMkernel a un conmutador de N-VDS.</p>
Asignaciones de red para desinstalación	<p>Para revertir la migración de VMkernel durante la desinstalación, asigne VMkernel a los grupos de puertos de VSS o DVS, para que NSX Manager sepa a qué grupo de puertos se debe volver a migrar el VMkernel en el VSS o DVS. Para un conmutador de DVS, asegúrese de que el grupo de puertos sea del tipo Efímero.</p> <p>Precaución Para las NIC físicas asignadas, asegúrese de que la asignación de perfil de nodo de transporte de la NIC física con la interfaz de VMkernel coincide con la configuración especificada en el conmutador de host. Es obligatorio configurar la asignación de red para la desinstalación porque NSX-T Data Center no almacena la configuración de asignación del conmutador del host después de migrar las interfaces de VMkernel al conmutador de N-VDS. Si la asignación no está configurada, se puede perder la conectividad con los servicios, como vSAN, después de volver a migrar al conmutador de VSS o VDS.</p> <p>Para obtener más información, consulte Migrar VMkernel a un conmutador de N-VDS.</p>

- 7 Introduzca los detalles de N-VDS de ruta de datos mejorada. Se pueden configurar varios conmutadores de N-VDS en un único host.

Opción	Descripción
Nombre del N-VDS	Debe ser igual al nombre del N-VDS de la zona de transporte a la que pertenece este nodo.
Asignación de IP	<p>Seleccione Usar DHCP (Use DHCP), Usar grupo de direcciones IP (Use IP Pool) o Usar lista de direcciones IP estáticas (Use Static IP List).</p> <p>Si selecciona Usar lista de direcciones IP estáticas (Use Static IP List), debe especificar una lista de direcciones IP separadas por comas, una puerta de enlace y una máscara de subred.</p>

Opción	Descripción
Grupo de direcciones IP	Si seleccionó Usar grupo de direcciones IP para la asignación de direcciones IP, especifique el nombre del grupo de direcciones IP.
NIC físicas	<p>Agregue NIC físicas al nodo de transporte. Puede usar el enlace ascendente o asignar uno existente en el menú desplegable.</p> <p>Haga clic en Agregar PNIC para configurar NIC físicas adicionales en el nodo de transporte.</p> <p>Nota La migración de las NIC físicas que se agreguen en este campo dependerá de cómo se configuren Migración solamente de PNIC, Asignaciones de red para instalación y Asignaciones de red para desinstalación.</p> <ul style="list-style-type: none"> ■ Para migrar una NIC física utilizada (por ejemplo, mediante un vSwitch estándar o un conmutador distribuido de vSphere) sin una asignación de VMkernel asociada, asegúrese de que la opción Migración solamente de PNIC esté habilitada. De lo contrario, el nodo de transporte sigue en estado parcialmente correcto y no se puede establecer la conectividad del LCP del nodo de tejido. ■ Para migrar una NIC física utilizada con una asignación de red de VMkernel asociada, deshabilite la opción Migrar solamente de PNIC y configure la asignación de red de VMkernel. ■ Para migrar una NIC física libre, habilite la opción Migrar solamente de PNIC.
Vínculo superior	Seleccione el perfil de enlace ascendente en el menú desplegable.
Configuración de CPU	<p>En el menú desplegable Índice de nodos de NUMA, seleccione el nodo de NUMA que desea asignar a un conmutador N-VDS. El primer nodo de NUMA incluido en el nodo se representa con el valor 0.</p> <p>Para averiguar el número de nodos de NUMA en el host, ejecute el comando <code>esxcli hardware memory get</code>.</p> <p>Nota Si desea cambiar el número de nodos de NUMA que tienen afinidad con un conmutador N-VDS, puede actualizar el valor de índice de nodos de NUMA.</p> <p>En el menú desplegable Lcore por nodo de NUMA, seleccione el número de núcleos lógicos que debe utilizar la ruta de datos mejorada.</p> <p>Para averiguar el número máximo de núcleos lógicos que pueden crearse en el nodo de NUMA, ejecute el comando <code>esxcli network ens maxLcores get</code>.</p> <p>Nota Si se agotaron los nodos de NUMA y los núcleos lógicos disponibles, no podrá habilitarse para el tráfico de ENS ningún conmutador nuevo que se agregue al nodo de transporte.</p>

8 Para un N-VDS preconfigurado, proporcione los siguientes detalles.

Opción	Descripción
ID externo del N-VDS	Debe ser igual al nombre del N-VDS de la zona de transporte a la que pertenece este nodo.
VTEP	Nombre del endpoint del túnel virtual.

9 Puede ver el estado de conexión en la página **Nodos de transporte de host**.

Después de agregar el host o el servidor sin sistema operativo como nodo de transporte, la conexión con NSX Manager cambia al estado activo en 3-4 minutos.

10 Como alternativa, puede ver el estado de conexión mediante los comandos de la CLI.

- ◆ Para ESXi, escriba el comando `esxcli network ip connection list | grep 1234`.

```
# esxcli network ip connection list | grep 1234
tcp    0    0 192.168.210.53:20514 192.168.110.34:1234 ESTABLECIDO (ESTABLISHED)
1000144459 newreno netcpa
```

- ◆ Para KVM, escriba el comando `netstat -anp --tcp | grep 1234`.

```
user@host:~$ netstat -anp --tcp | grep 1234
tcp    0    0 192.168.210.54:57794 192.168.110.34:1234 ESTABLECIDO -
```

11 Compruebe que los módulos de NSX-T Data Center estén instalados en el host o el servidor sin sistema operativo.

Como resultado de agregar un host o un servidor sin sistema operativo al tejido de NSX-T Data Center, se instala una colección de módulos de NSX-T Data Center en el host o el servidor sin sistema operativo.

Los módulos de los diferentes hosts se empaquetan como se indica a continuación:

- KVM en RHEL o CentOS: RPM
- KVM en Ubuntu: DEB
- En ESXi, escriba el comando `esxcli software vib list | grep nsx`.

La fecha es el día en que se realizó la instalación.

- En RHEL o CentOS, escriba el comando `yum list installed o rpm -qa`.
- En Ubuntu, escriba el comando `dpkg --get-selections`.

- 12** (opcional) Cambie los intervalos de sondeo de determinados procesos si hay 500 hipervisores o más.

Es posible que NSX Manager experimente problemas de rendimiento y un alto uso de CPU si hay más de 500 hipervisores.

- a Utilice el comando `copy file` de la CLI de NSX-T Data Center o la API `POST /api/v1/node/file-store/<file-name>?action=copy_to_remote_file` para copiar el script `aggsvc_change_intervals.py` en un host.
- b Ejecute el script, que se encuentra en el almacén de archivos de NSX-T Data Center.

```
python aggsvc_change_intervals.py -m '<NSX ManagerIPAddress>' -u 'admin' -p '<password>' -i 900
```

- c (opcional) Restablezca los valores predeterminados de los intervalos de sondeo.

```
python aggsvc_change_intervals.py -m '<NSX ManagerIPAddress>' -u 'admin' -p '<password>' -r
```

Resultados

Nota Para un N-VDS creado con NSX-T Data Center, si desea cambiar la configuración, como la asignación de direcciones IP al endpoint de túnel, después de crear el nodo de transporte, debe hacerlo a través de la GUI de NSX Manager y no a través de la CLI en el host.

Pasos siguientes

Migre las interfaces de red de un conmutador estándar de vSphere a un N-VDS. Consulte [Migrar VMkernel a un conmutador de N-VDS](#).

Configurar un nodo de transporte de host administrado

Si tiene una instancia de vCenter Server, podrá automatizar la instalación y la creación de nodos de transporte de todos los hosts de NSX-T Data Center en lugar de realizar la configuración de forma manual.

Si el nodo de transporte ya está configurado, la creación automática del nodo de transporte no se aplica a dicho nodo.

Requisitos previos

- Compruebe que todos los hosts de vCenter Server estén encendidos.
- Compruebe que se cumplan los requisitos del sistema. Consulte [Requisitos del sistema](#).
- Compruebe que haya zona de transporte disponible. Consulte [Crear zonas de transporte](#).
- Compruebe que se haya configurado un perfil de nodo de transporte. Consulte [Agregar perfil de nodo de transporte](#).

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión con privilegios de administrador en NSX Manager.
- 2 Seleccione **Sistema > Tejido > Nodos > Nodos de transporte de host**.
- 3 En el menú desplegable Administrado por, seleccione una instancia de vCenter Server existente.
La página mostrará los clústeres de vSphere y los hosts ESXi de la instancia de vCenter Server seleccionada. Es posible que necesite expandir un clúster para ver los hosts ESXi.
- 4 Seleccione un único host de la lista y haga clic en **Configurar NSX**.
Se abrirá el cuadro de diálogo Configurar NSX.
 - a Compruebe el nombre del host en el panel Detalles del host. De forma opcional, puede agregar una descripción.
 - b Haga clic en **Siguiente** para pasar al panel **Configurar NSX**.
 - c Seleccione las zonas de transporte disponibles y haga clic en el botón **>** para incluir las zonas de transporte en el perfil de nodo de transporte.
- 5 Verifique el nombre del host en el panel Detalles del host y haga clic en **Siguiente**.
De forma opcional, puede agregar una descripción.
- 6 En el panel **Configurar NSX**, seleccione las zonas de transporte deseadas.
Puede seleccionar más de una zona de transporte.
- 7 (opcional) Consulte el estado de conexión de ESXi.

```
# esxcli network ip connection list | grep 1235
tcp    0    0 192.168.210.53:20514 192.168.110.34:1234 ESTABLECIDO 1000144459 newreno netcpa
```

- 8 En la página Nodo de transporte de host, compruebe que el estado de conectividad de NSX Manager de los hosts del clúster sea Activo, y que el estado de configuración de NSX-T Data Center sea Correcto.
También puede comprobar que la zona de transporte se haya aplicado a los hosts del clúster.
- 9 (opcional) Quite una instalación de NSX-T Data Center y un nodo de transporte de un host de la zona de transporte.
 - a Seleccione uno o varios hosts y haga clic en **Acciones > Quitar NSX**.

La desinstalación puede tardar hasta tres minutos. Al desinstalar NSX-T Data Center, se quitará la configuración del nodo de transporte de los hosts, y el host se desasociará de las zonas de transporte y el conmutador de N-VDS. Los nuevos hosts que se agreguen al clúster vCenter Server no se configurarán automáticamente hasta que se vuelva a aplicar el perfil de nodo de transporte al clúster.

10 (opcional) Quite un nodo de transporte de la zona de transporte.

- a Seleccione un único nodo de transporte y haga clic en **Acciones > Quitar de la zona de transporte**.

Pasos siguientes

Cree un conmutador lógico y asígnele puertos lógicos. Consulte la sección Conmutación avanzada de la *Guía de administración de NSX-T Data Center*.

Configurar un nodo de transporte de host ESXi con agregado de enlaces

Con este procedimiento se explica cómo crear un perfil de vínculo superior que tiene configurado un grupo de agregado de vínculos y cómo configurar un nodo de transporte de host ESXi para que use ese perfil de vínculo superior.

Requisitos previos

- Familiarícese con los pasos para crear un perfil de vínculo superior. Consulte [Crear un perfil de vínculo superior](#).
- Familiarícese con los pasos para crear un nodo de transporte de host. Consulte [Crear un host independiente o un nodo de transporte sin sistema operativo](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión con privilegios de administrador en NSX Manager.
- 2 Seleccione **Sistema > Tejido > Perfiles > Perfiles de vínculo superior > Agregar**.
- 3 Introduzca un nombre y, si lo desea, una descripción.
Por ejemplo, el nombre **uplink-profile1**.
- 4 En **LAG**, haga clic en **Agregar** para añadir un grupo de agregado de vínculos.
Por ejemplo, un LAG llamado **lag1** con dos vínculos superiores.
- 5 En **Formación de equipos** (Teamings), seleccione **Formación de equipos predeterminada** (Default Teaming).
- 6 En el campo **Vínculos superiores activos**, introduzca el nombre del LAG que agregó en el paso 4.
En este ejemplo, el nombre es **lag1**.
- 7 Introduzca un valor de **VLAN de transporte** y **MTU**.
- 8 Haga clic en **Agregar** en la parte inferior del cuadro de diálogo.
- 9 En **Formaciones de equipos**, haga clic en **Agregar** para añadir una entrada de agregado de vínculos.
- 10 Seleccione **Tejido > Nodos > Nodos de transporte de host > Agregar** (Fabric > Nodes > Host Transport Nodes > Add).

- 11 En la pestaña **Detalles del host** (Host Details), introduzca la dirección IP, el nombre del sistema operativo, las credenciales de administración y la huella digital SHA-256 del host.
- 12 En la pestaña **N-VDS**, seleccione el perfil de vínculo superior **uplink-profile1** que creó en el paso 3.
- 13 En el campo **NIC físicas** (Physical NICs), la lista desplegable de NIC físicas y vínculos superiores refleja las nuevas NIC y el nuevo perfil de vínculo superior. En concreto, los vínculos superiores **lag1-0** y **lag1-1**, que se corresponden con el LAG **lag1** que creó en el paso 4. Seleccione una NIC física para **lag1-0** y otra para **lag1-1**.
- 14 Introduzca la información que corresponda en el resto de campos.

Implementación de clúster de vSphere totalmente contraído en NSX-T

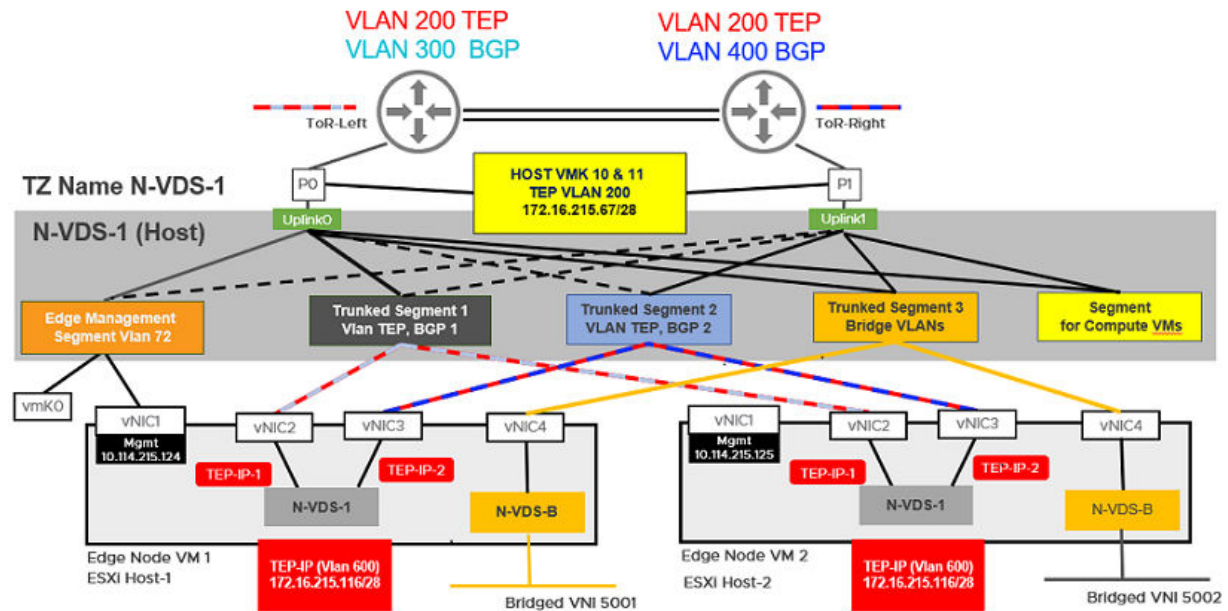
Configure NSX Manager, los nodos de transporte de hosts para que ejecuten máquinas virtuales de carga de trabajo y máquinas virtuales de NSX Edge en un solo clúster. Cada host del clúster proporciona dos NIC físicas configuradas para NSX-T.

Importante Implemente la topología de clúster único de vSphere totalmente contraído a partir de la versión 2.4.2 y 2.5 de NSX-T.

La topología a la que se hace referencia en este proceso utiliza:

- vSAN configurado con los hosts del clúster.
- Un mínimo de dos NIC físicas por host
- Interfaces de VMkernel de administración y vMotion.

Figura 8-3. Topología: conmutador N-VDS único que gestiona la comunicación del host con NSX Edge y las máquinas virtuales invitadas



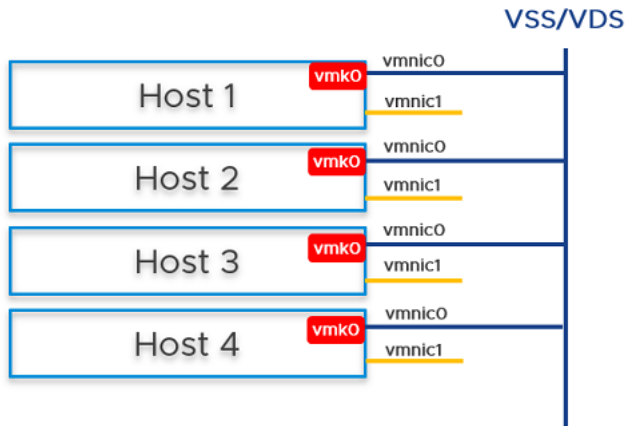
Nota Aunque el host tenga cuatro NIC físicas, solo se pueden utilizar dos para implementar la topología totalmente contraída. Este procedimiento hace referencia a las NIC físicas del host como vmnic0 y vmnic1.

Requisitos previos

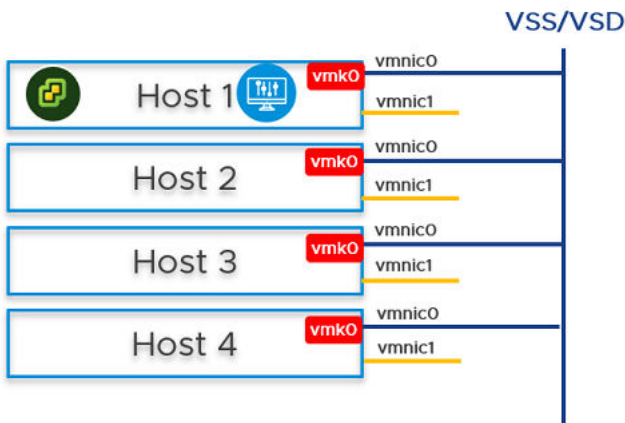
- Todos los hosts deben formar parte de un clúster de vSphere.
- Cada host tiene habilitadas dos NIC físicas.
- Registre todos los hosts en un vCenter Server.
- Compruebe que los hosts puedan utilizar el almacenamiento compartido en vCenter Server.
- Asegúrese de que el identificador de VLAN usado para el TEP y el TEP del host sean diferentes de NSX Edge.

Procedimiento

- 1 Prepare cuatro hosts ESXi con vmnic0 en VSS o VDS; vmnic1 está libre.



- 2 En el host 1, instale vCenter Server, configure un grupo de puertos de VSS o VDS e instale NSX Manager en el grupo de puertos creado en el host.

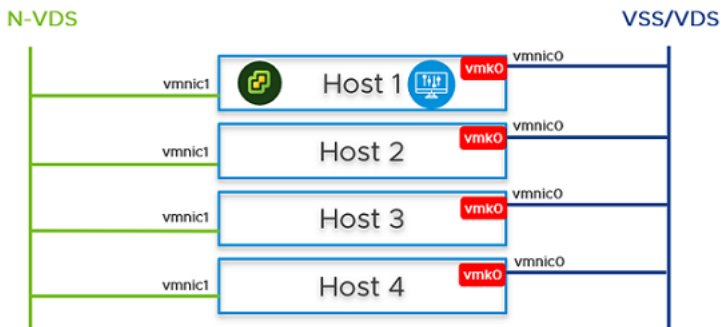


- 3 Prepare los host ESXi 1, 2, 3 y 4 para que actúen como nodos de transporte.
 - a Cree zonas de transporte de VLAN con una directiva de formación de equipos con nombre. Consulte [Crear zonas de transporte](#).
 - b Cree un grupo de direcciones IP o DHCP para las direcciones IP del endpoint del túnel de los hosts. Consulte [Crear un grupo de direcciones IP para direcciones IP de endpoints de túneles](#).
 - c Cree un grupo de direcciones IP o DHCP para las direcciones IP del endpoint del túnel del nodo de Edge. Consulte [Crear un grupo de direcciones IP para direcciones IP de endpoints de túneles](#).
 - d Cree un perfil de vínculo superior con una directiva de formación de equipos con nombre. Consulte [Crear un perfil de vínculo superior](#).

- e Configure los hosts como nodos de transporte mediante la aplicación del perfil de nodo de transporte. En este paso, el perfil de nodo de transporte solo migra vmnic1, la NIC física no utilizada, al conmutador N-VDS. Después de aplicar el perfil de nodo de transporte a los hosts del clúster, se crea el conmutador N-VDS y vmnic1 se conecta al conmutador N-VDS. Consulte [Agregar perfil de nodo de transporte](#).

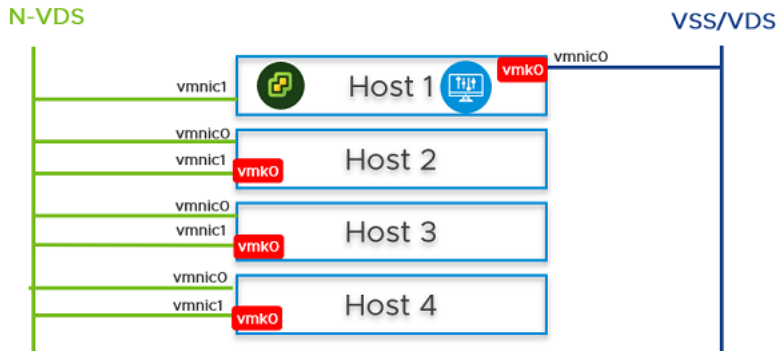
Editar perfil de nodo de transporte: TNP-host ?

Nombre del N-VDS *	vds-1	▼
Zonas de transporte tz asociadas		
Perfil de NIOC *	nsx-default-nioc-hostswitch-profile	▼
O crear nuevo perfil de NIOC		
Perfil de vínculo superior *	hostnodeprofile	▼
O crear nuevo perfil de vínculo superior		
Perfil de LLDP *	LLDP [Send Packet Enabled]	▼
Asignación de IP *	Usar grupo de direcciones IP	▼
Grupo de direcciones IP *	ippoolhostnode	▼
O crear y usar un nuevo grupo de direcciones IP		
NIC físicas	vmnic1	activeuplinkhost ▼
Agregar PNIC		
Migración solamente de PNIC	<input checked="" type="checkbox"/> Sí	
Habilite esta opción si no hay VMK en PNIC seleccionados para la migración		
Asignaciones de red para instalación	Agregar asignación	
Asignaciones de red para desinstalación	Agregar asignación	



Las vmnic1 de todos los hosts se migran al conmutador N-VDS. Por lo tanto, de las dos NIC físicas, una se migra al conmutador de N-VDS. La interfaz de vmnic0 sigue conectada al conmutador VSS o de VDS, lo que garantiza que haya conectividad con el host.

- 4 En la interfaz de usuario de NSX Manager, cree segmentos respaldados por VLAN para NSX Manager, vCenter Server y NSX Edge. Asegúrese de seleccionar la directiva de formación de equipos correcta para cada uno de los segmentos respaldados por VLAN.
- 5 En el host 2, el host 3 y el host 4, debe migrar los adaptadores de vmk0 y vmnic0 de forma conjunta desde VSS o VDS al conmutador N-VDS. Actualice la configuración de NSX-T en cada host. Al migrar, asegúrese de que vmnic0 esté asignado a un vínculo superior activo.



Asignaciones de red para instalación



La conectividad del host puede perderse cuando se migran vmnic0 y vmk0.

Si se cambia el conmutador lógico para el host con estado (independiente o en clúster), no tendrá ningún efecto y no se podrá realizar la operación.

+ AGREGAR ELIMINAR

<input type="checkbox"/> Adaptador de VMkernel *	Segmento de VLAN/Conmutador lógico *
<input type="checkbox"/> vmk0	Seg-Vlan2200-ESXi-MGT

CANCELAR

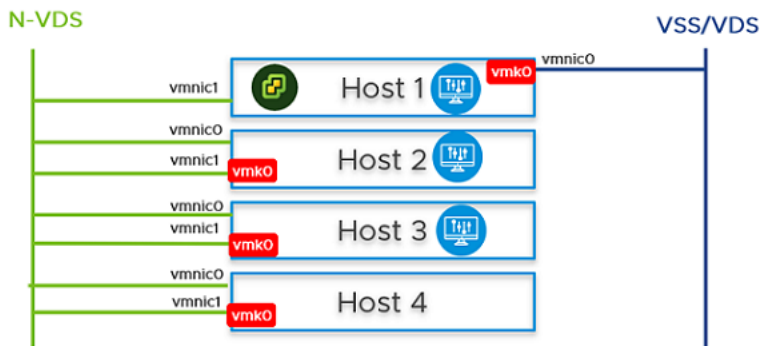
AGREGAR



- 6 En vCenter Server, acceda al host 2, al host 3 y al host 4, y compruebe que el adaptador de vmk0 esté conectado a la NIC física de vmnic0 en el conmutador N-VDS y que sea accesible.
- 7 En la interfaz de usuario de NSX Manager, acceda al host 2, al host 3 y al host 4, y compruebe que ambas pNIC estén en el conmutador N-VDS.

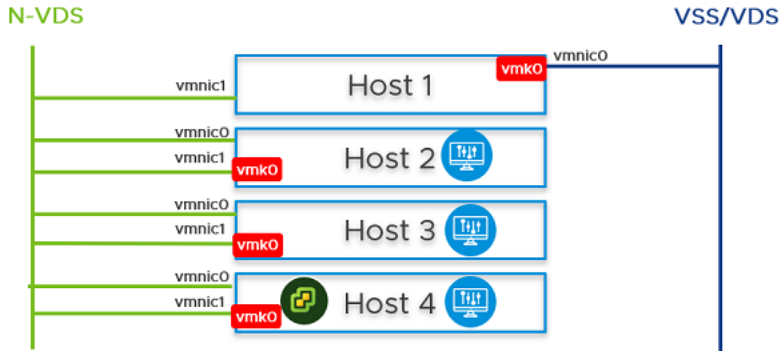


- 8 Cree un segmento lógico y asocie la instancia de NSX Manager al segmento lógico. Espere unos 10 minutos a que el clúster se forme y compruebe que el clúster se haya formado.
- 9 En el host 2 y el host 3, en la interfaz de usuario de NSX Manager, instale NSX Manager.



- 10 Apague el primer nodo de NSX Manager. Espere aproximadamente 10 minutos.
- 11 Vuelva a asociar la instancia de NSX Manager y vCenter Server al conmutador lógico creado anteriormente. En el host 4, encienda la instancia de NSX Manager. Espere aproximadamente 10 minutos para comprobar que el clúster se encuentra en un estado estable. Con la primera instancia de NSX Manager apagada, ejecute vMotion en frío para migrar NSX Manager y vCenter Server del host 1 al host 4.

Para consultar las limitaciones de vMotion, consulte <https://kb.vmware.com/s/article/56991>.



- 12 Desde la interfaz de usuario de NSX Manager, vaya al host 1, migre vmk0 y vmnic0 de forma conjunta desde VSS al conmutador N-VDS.
- 13 En el campo **Asignaciones de red para instalación**, asegúrese de que el adaptador de vmk0 esté asignado al segmento lógico de administración en el conmutador N-VDS.

Configurar NSX

- 1 Detalles del host
- 2 Configurar NSX

Configurar NSX

Asignación de IP *

Usar lista de direcciones IP estáticas

Lista de direcciones IP estáticas *

172.16.228.36 x

Puerta de enlace *

172.16.228.33

Máscara de subred *

255.255.255.240

NIC físicas

vmnic1	▼	uplink-1	▼	🗑️
vmnic2	▼	uplink-2	▼	🗑️

Migración solamente de PNIC

☐ No

Habilite esta opción si no hay VMK en PNIC seleccionados para la migración

Asignaciones de red para instalación

Agregar asignación

Asignaciones de red para desinstalación

Agregar asignación

CANCELAR

ANTERIOR

FINALIZAR

Asignaciones de red para instalación



La conectividad del host puede perderse cuando se migran vmnic0 y vmk0.

Si se cambia el conmutador lógico para el host con estado (independiente o en clúster), no tendrá ningún efecto y no se podrá realizar la operación.

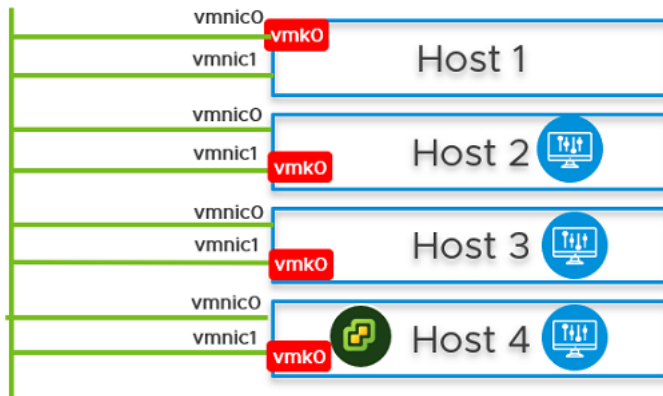
+ AGREGAR ELIMINAR

<input type="checkbox"/> Adaptador de VMkernel *	Segmento de VLAN/Conmutador lógico
<input type="checkbox"/> vmk0	Seg-Vlan2200-ESXi-MGT

CANCELAR

AGREGAR

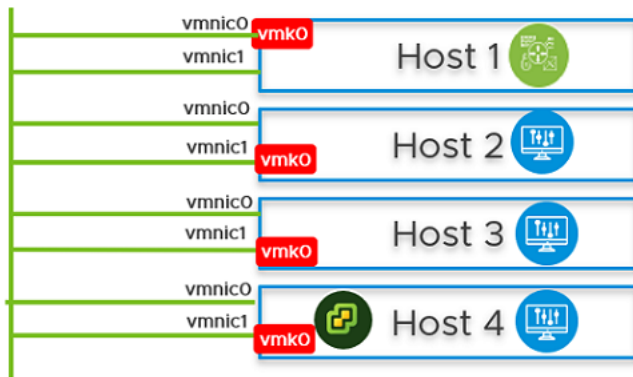
N-VDS



- 14 En el host 1, instale la máquina virtual de NSX Edge desde la interfaz de usuario de NSX Manager.

Consulte [Crear un nodo de transporte de NSX Edge](#).

N-VDS



- 15 Una la máquina virtual de NSX Edge al plano de administración.
Consulte [Unir NSX Edge al plano de administración](#).
- 16 Para establecer la conectividad del tráfico de norte a sur, configure la máquina virtual de NSX Edge con un enrutador externo.
- 17 Compruebe la conectividad del tráfico de norte a sur entre la máquina virtual de NSX Edge y el enrutador externo.
- 18 Configure y compruebe la conectividad de BFD entre NSX Manager y la máquina virtual de NSX Edge.
- 19 Si se produce un fallo de alimentación en el que se reinicie todo el clúster, es posible que el componente de administración de NSX-T no aparezca y se comuniquen con N-VDS. Para resolver este problema, siga estos pasos:

Precaución Cualquier comando de API que se ejecute de forma incorrecta provocará una pérdida de conectividad con NSX Manager.

Nota En una configuración de clúster único, los componentes de administración se alojan en un conmutador N-VDS como máquinas virtuales. El puerto de N-VDS al que se conecta el componente de administración de forma predeterminada se inicializa como un puerto bloqueado por motivos de seguridad. Si se produce un fallo de alimentación por el que sea necesario reiniciar los cuatro hosts (mínimo recomendado), el estado de reinicio predeterminado del puerto de la máquina virtual de administración será bloqueado. Para evitar dependencias circulares, se recomienda crear un puerto desbloqueado en N-VDS. Los puertos desbloqueados permiten que el componente de administración de NSX-T se comuniquen con N-VDS para recuperar su funcionamiento normal cuando se reinicia el clúster.

Al final de la subtarea, el comando de migración toma el:

- UUID del nodo de host en el que reside NSX Manager.
- UUID de la máquina virtual de NSX Manager y la migra al puerto lógico estático que está en estado desbloqueado.

Si todos los hosts se apagan o se encienden, o si una máquina virtual de NSX Manager se traslada a otro host, se podrá conectar al puerto desbloqueado cuando se haga una copia de seguridad de NSX Manager. De este modo, se evita la pérdida de conectividad con el componente de administración de NSX-T.

- a Acceda a **Opciones avanzadas de redes y seguridad** → **Conmutación** y seleccione MGMT-VLAN-Segment. En la pestaña **Información general**, busque y copie el UUID. El UUID utilizado en este ejemplo es *c3fd8e1b-5b89-478e-abb5-d55603f04452*.
- b Para crear puertos lógicos que se inicializan en el estado **UNBLOCKED_VLAN**, cree cuatro archivos JSON: tres para NSX Manager y otro para vCenter Server Appliance (VCSA). Reemplace el valor de `logical_switch_id` por el UUID del segmento MGMT-VLAN-Segment creado anteriormente.

```
mgrhost.json
{
  "admin_state": "UP",
  "attachment": {
    "attachment_type": "VIF",
    "id": "nsxmgr-port-147"
  },
  "display_name": "NSX Manager Node 147 Port",
  "init_state": "UNBLOCKED_VLAN",
  "logical_switch_id": "c3fd8e1b-5b89-478e-abb5-d55603f04452"
}
```

- c Cree el puerto lógico para Manager con un cliente de API o con el comando curl.

```
root@nsx-mgr-147:/var/CollapsedCluster# curl -X POST -k -u
'<username>:<password>' -H 'Content-Type:application/json' -d @mgr.json https://
localhost/api/v1/logical-ports
{
  "logical_switch_id" : "c3fd8e1b-5b89-478e-abb5-d55603f04452",
  "attachment" : {
    "attachment_type" : "VIF",
    "id" : "nsxmgr-port-147"
  },
  "admin_state" : "UP",
  "address_bindings" : [ ],
  "switching_profile_ids" : [ {
    "key" : "SwitchSecuritySwitchingProfile",
    "value" : "fbc4fb17-83d9-4b53-a286-ccd0f4301888"
  }, {
    "key" : "SpoofGuardSwitchingProfile",
    "value" : "fad98876-d7ff-11e4-b9d6-1681e6b88ec1"
  }, {
    "key" : "IpDiscoverySwitchingProfile",
    "value" : "0c403bc9-7773-4680-a5cc-847ed0f9f52e"
  }, {
    "key" : "MacManagementSwitchingProfile",
    "value" : "1e7101c8-cfef-415a-9c8c-ce3d8dd078fb"
  }, {
    "key" : "PortMirroringSwitchingProfile",
    "value" : "93b4b7e8-f116-415d-a50c-3364611b5d09"
  }, {
    "key" : "QosSwitchingProfile",
    "value" : "f313290b-eba8-4262-bd93-fab5026e9495"
  } ],
  "init_state" : "UNBLOCKED_VLAN",
  "ignore_address_bindings" : [ ],
  "resource_type" : "LogicalPort",
  "id" : "02e0d76f-83fa-4839-a525-855b47ecb647",
  "display_name" : "NSX Manager Node 147 Port",
  "_create_user" : "admin",
  "_create_time" : 1574716624192,
  "_last_modified_user" : "admin",
  "_last_modified_time" : 1574716624192,
  "_system_owned" : false,
  "_protection" : "NOT_PROTECTED",
  "_revision" : 0
}
```

Commutadores Puertos Perfiles De Conmutación							
<div> + AGREGAR EDITAR ELIMINAR ACCIONES </div> <div> <input type="text" value="Buscar"/> </div>							
<input type="checkbox"/>	Puerto lógico	Identificador	Estado de admin	Estado operativo	Perfiles de conmutación	Asociación	Commutador lógico
<input type="checkbox"/>	1356a49d-dc33-42be-9e83-4c6...	1356...d0ee	Activo	Activo	nsx-default-switch-security-non...	LR:80fb...2662	Is3
<input type="checkbox"/>	61d5708b-a4ff-4954-b217-8338...	61d5...b43a	Activo	Activo	nsx-default-switch-security-non...	LR:42ac...ad24	Is1
<input type="checkbox"/>	NSX Manager Node 147 Port	58ad...a1cb	Activo	Inactivo	nsx-default-switch-security-vif...	VM:nsx-mgr-147	Is1
<input type="checkbox"/>	ubuntu12.04.1-2G-LAMP/ubuntu...	3fb2...f698	Activo	Activo	nsx-default-switch-security-vif...	Máquina virtual/vml	Is1
<input type="checkbox"/>	vmknic@n-vds-1@94b323e6-1ee...	2021...4d76	Activo	Activo	nsx-default-switch-security-vif...	VIF:abf2...0495	Seg-Vlan2200-ESXi-MGT
<input type="checkbox"/>	worker/worker.vmx@94b323e6-...	50b7...9b4c	Activo	Activo	nsx-default-switch-security-vif...	Máquina virtual/vm3	Is3

- d Traslade NSX Manager al puerto lógico estático.
- e Para copiar el identificador de la instancia de máquina virtual de NSX Manager, vaya a Opciones avanzadas de redes y seguridad → Inventario → Máquinas virtuales. Seleccione la máquina virtual de NSX Manager. En la pestaña **Información general**, busque y copie el ID. El identificador que utilizamos en este ejemplo es *5028d756-d36f-719e-3db5-7ae24aa1d6f3*.
- f Para encontrar el identificador de host en el que está instalado NSX Manager, vaya a **Sistema -> Tejido -> Nodos -> Nodo de transporte de host**. Seleccione el host y haga clic en la pestaña **Información general**. Busque y copie el ID de host. El identificador utilizado en este ejemplo es *11161331-11f8-45c7-8747-34e7218b687f*.
- g Migre NSX Manager de la red de la máquina virtual al puerto lógico creado anteriormente en MGMT-VLAN-Segment. El valor `vnic_migration_dest` es el identificador de conexión de los puertos creados anteriormente para NSX Manager.

```
root@nsx-mgr-147:/var/CollapsedCluster# curl -k -X PUT -u 'username:<password>' -H
'Content-Type:application/json' -d @mgrhost.json
'https://localhost/api/v1/transport-nodes/11161331-11f8-45c7-8747-34e7218b687f?
vnic_migration_dest=nsxmgr-port-147'
```

- h En la interfaz de usuario de NSX Manager, asegúrese de que el puerto lógico creado de forma estática esté activo.

Commutadores **Puertos** Perfiles De Conmutación

+ AGREGAR EDITAR ELIMINAR ACCIONES

Buscar

<input type="checkbox"/>	Puerto lógico	Identificador	Estado de admin	Estado operativo	Perfiles de conmutación	Asociación	Commutador lógico
<input type="checkbox"/>	1356a49d-dc33-42be-9e83-4c6...	1356...d0ee	Activo	Activo	nsx-default-switch-security-non...	LR:80fb...2662	Is3
<input type="checkbox"/>	61d5708b-a4ff-4954-b217-8338...	61d5...b43a	Activo	Activo	nsx-default-switch-security-non...	LR:42ac...ad24	Is1
<input type="checkbox"/>	NSX Manager Node 147 Port	58ad...a1cb	Activo	Activo	nsx-default-switch-security-vif...	VM:nsx-mgr-147	Is1
<input type="checkbox"/>	ubuntu2.04.1-2G-LAMP/ubuntuL...	3fb2...f698	Activo	Activo	nsx-default-switch-security-vif...	Máquina virtual/vm1	Is1
<input type="checkbox"/>	vmknic@n-vds-1@94b323e6-1ee...	2021...4d76	Activo	Activo	nsx-default-switch-security-vif...	VIF:abf2...0495	Seg-Vlan2200-ESXi-MGT
<input type="checkbox"/>	worker/worker.vmx@94b323e6-...	50b7...9b4c	Activo	Activo	nsx-default-switch-security-vif...	Máquina virtual/vm3	Is3

- i Repita los pasos anteriores en cada instancia de NSX Manager del clúster.

Comprobar el estado de nodos de transporte

Asegúrese de que el proceso de creación de nodos de transporte esté funcionando correctamente.

Tras crear un nodo de transporte de host, el N-VDS se instala en el host.

Procedimiento

- 1 Inicie sesión en NSX-T Data Center.
- 2 Vaya a la página **Nodo de transporte** y consulte el estado de N-VDS.

- 3 Como alternativa, puede ver el N-VDS en ESXi con el comando `esxcli network ip interface list`.

En ESXi, la salida de comandos debería incluir una interfaz vmk (como vmk10) con un nombre de VDS que coincida con el nombre que utilizó al configurar la zona de transporte y el nodo de transporte.

```
# esxcli network ip interface list
...

vmk10
  Name: vmk10
  MAC Address: 00:50:56:64:63:4c
  Enabled: true
  Portset: DvsPortset-1
  Portgroup: N/A
  Netstack Instance: vxlan
  VDS Name: overlay-hostswitch
  VDS UUID: 18 ae 54 04 2c 6f 46 21-b8 ae ef ff 01 0c aa c2
  VDS Port: 10
  VDS Connection: 10
  Opaque Network ID: N/A
  Opaque Network Type: N/A
  External ID: N/A
  MTU: 1600
  TSO MSS: 65535
  Port ID: 67108895
...
```

Si utiliza vSphere Client, puede ver el N-VDS instalado en la interfaz de usuario seleccionando **Configuración > Adaptadores de red** del host.

El comando de KVM para comprobar la instalación del N-VDS es `ovs-vsctl show`. Tenga en cuenta que en KVM, el nombre del N-VDS es `nsx-switch.0`. No coincide con el nombre en la configuración del nodo de transporte. Esto es así por diseño.

```
# ovs-vsctl show
...
  Bridge "nsx-switch.0"
    Port "nsx-uplink.0"
      Interface "em2"
    Port "nsx-vtep0.0"
      tag: 0
      Interface "nsx-vtep0.0"
        type: internal
    Port "nsx-switch.0"
```

```
Interface "nsx-switch.0"
  type: internal
  ovs_version: "2.4.1.3340774"
```

- 4 Compruebe la dirección del endpoint del túnel asignado del nodo de transporte.

La interfaz vmk10 recibe una dirección IP desde DHCP o el grupo de direcciones IP de NSX-T Data Center, tal como se muestra aquí:

```
# esxcli network ip interface ipv4 get
Name    IPv4 Address    IPv4 Netmask    IPv4 Broadcast    Address Type    DHCP DNS
-----
vmk0    192.168.210.53  255.255.255.0   192.168.210.255   STATIC          false
vmk1    10.20.20.53    255.255.255.0   10.20.20.255     STATIC          false
vmk10  192.168.250.3  255.255.255.0   192.168.250.255   STATIC          false
```

En KVM, puede verificar la asignación de direcciones IP y el endpoint de túnel mediante el comando `ifconfig`.

```
# ifconfig
...
nsx-vtep0.0 Link encap:Ethernet HWaddr ba:30:ae:aa:26:53
    inet addr:192.168.250.4 Bcast:192.168.250.255 Mask:255.255.255.0
    ...
```

- 5 Compruebe la API para obtener la información sobre el estado del nodo de transporte.

Utilice la llamada API GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/state`. Por ejemplo:

```
{
  "state": "success",
  "host_switch_states": [
    {
      "endpoints": [
        {
          "default_gateway": "192.168.250.1",
          "device_name": "vmk10",
          "ip": "192.168.250.104",
          "subnet_mask": "255.255.255.0",
          "label": 69633
        }
      ],
      "transport_zone_ids": [
        "efd7f38f-c5da-437d-af03-ac598f82a9ec"
      ],
      "host_switch_name": "overlay-hostswitch",
      "host_switch_id": "18 ae 54 04 2c 6f 46 21-b8 ae ef ff 01 0c aa c2"
    }
  ]
}
```

```

    }
  ],
  "transport_node_id": "2d030569-5769-4a13-8918-0c309c63fdb9"
}

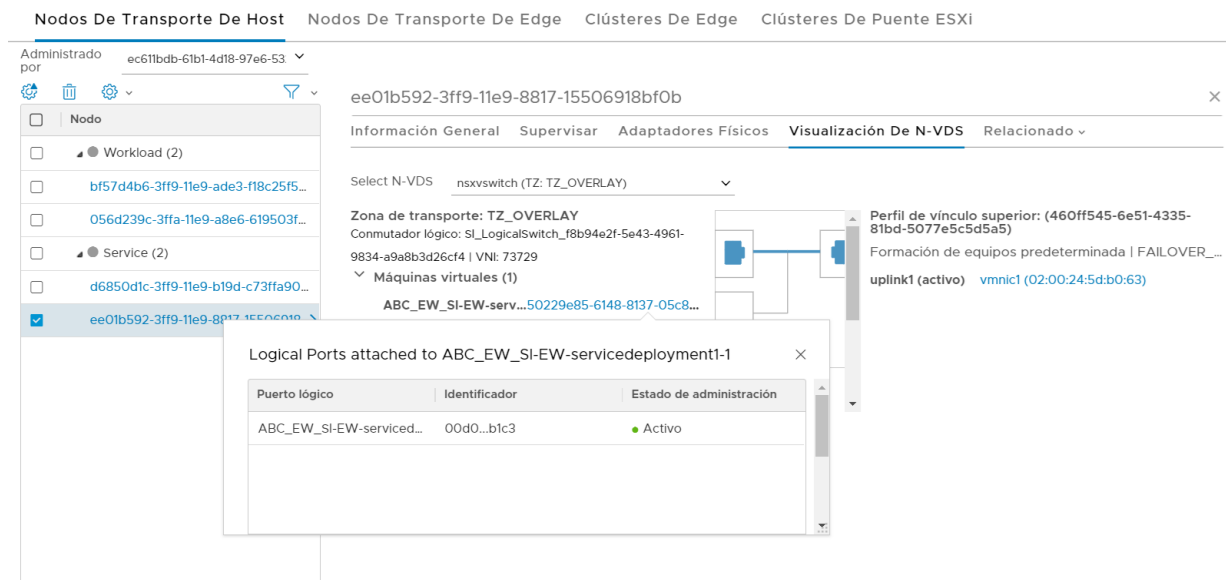
```

Representación visual de N-VDS

A nivel de host individual, se obtiene una vista granular de N-VDS. NSX-T Data Center ofrece una representación visual del estado de conectividad entre el vínculo superior del N-VDS y las máquinas virtuales asociadas a una zona de transporte. Los objetos representados visualmente incluyen la directiva de formación de equipos: el vínculo superior y la NIC física que proporcionan conectividad a las máquinas virtuales. El otro conjunto de objetos representados visualmente son las máquinas virtuales, los puertos y conmutadores lógicos asociados y el estado de las máquinas virtuales. La representación visual facilita la administración del N-VDS.

Nota Solo los hosts de ESXi admiten la visualización del objeto N-VDS.

Figura 8-4. Visualización de N-VDS



Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión con privilegios de administrador en NSX Manager.
- 2 Seleccione **Sistema > Tejido > Nodos > Nodos de transporte de host**.
- 3 En el campo Administrado por, seleccione un **host independiente** o un *administrador de equipos*.
- 4 Seleccione el host.
- 5 Haga clic en la pestaña **Visualización de N-VDS**.

6 Seleccione un N-VDS.

NSX-T representa visualmente los perfiles de vínculo superior conectados a las máquinas virtuales, los puertos lógicos asociados a las máquinas virtuales y los conmutadores lógicos conectados a una zona de transporte.

7 Para ver los perfiles de vínculo superior conectados a una máquina virtual y el puerto lógico al que está conectada una máquina virtual, seleccione dicha máquina virtual.

NSX-T representa visualmente la conectividad entre una máquina virtual y un perfil de vínculo superior.

8 Para ver las máquinas virtuales conectadas a un perfil de vínculo superior, seleccione dicho perfil de vínculo superior.

9 Para ver los puertos lógicos asociados a una máquina virtual, amplíe el conmutador lógico y, a continuación, haga clic en la máquina virtual.

La información del puerto lógico se muestra en un cuadro de diálogo independiente.

Nota El estado de administración de un puerto lógico se muestra en el cuadro de diálogo. Si el estado operativo es inactivo, no se muestra en el cuadro de diálogo.

Instalación manual de módulos kernel NSX-T Data Center

Como alternativa al uso de la IU **Tejido > Nodos > Hosts > Agregar** de NSX-T Data Center o la API `POST /api/v1/fabric/nodes`, puede instalar manualmente módulos kernel de NSX-T Data Center desde la línea de comandos del hipervisor.

Nota No se pueden instalar manualmente módulos kernel de NSX-T Data Center en un servidor nativo.

Instalar manualmente módulos kernel de NSX-T Data Center en hipervisores de ESXi

Para preparar hosts para que participen en NSX-T Data Center, debe instalar módulos kernel de NSX-T Data Center en hosts de ESXi. Esto le permite crear el tejido del plano de administración y del panel de control de NSX-T Data Center. Los módulos de kernel de NSX-T Data Center empaquetados en archivos VIB se ejecutan dentro del kernel del hipervisor y ofrecen servicios, como enrutamiento distribuido, firewall distribuido y capacidades de puente.

Puede descargar los VIB de NSX-T Data Center manualmente y hacer que formen parte de la imagen del host. Las rutas de descarga pueden variar en cada versión de NSX-T Data Center. Compruebe siempre la página de descargas de NSX-T Data Center para obtener los VIB apropiados.

Procedimiento

1 Inicie sesión en el host como raíz o usuario con privilegios administrativos.

- 2 Desplácese hasta el directorio /tmp.

```
[root@host:~]: cd /tmp
```

- 3 Descargue y copie el archivo nsx-lcp en el directorio /tmp.

- 4 Ejecute el comando de instalación.

```
[root@host:/tmp]: esxcli software vib install -d /tmp/nsx-lcp-<release>.zip
Installation Result
  Message: Operation finished successfully.
  Reboot Required: false
  VIBs Installed: VMware_bootbank_nsx-aggsservice-<release>, VMware_bootbank_nsx-da-<release>,
VMware_bootbank_nsx-esx-datapath-<release>, VMware_bootbank_nsx-exporter-<release>,
VMware_bootbank_nsx-host-<release>, VMware_bootbank_nsx-lldp-<release>, VMware_bootbank_nsx-
mpa-<release>, VMware_bootbank_nsx-netcpa-<release>, VMware_bootbank_nsx-python-
protobuf-<release>, VMware_bootbank_nsx-sfhc-<release>, VMware_bootbank_nsxa-<release>,
VMware_bootbank_nsxcli-<release>
  VIBs Removed:
  VIBs Skipped:
```

Dependiendo de lo que ya esté instalado en el host, podrían instalarse, eliminarse u omitirse determinados VIB. No es necesario reiniciar el equipo salvo que la salida de comandos diga Reboot Required: true.

Resultados

Como resultado de agregar un host ESXi al tejido de NSX-T Data Center, se instalan en el host los siguientes VIB.

nsx-adf	(Marco de diagnóstico automatizado) Recopila y analiza los datos de rendimiento para generar diagnósticos locales (en el host) y centrales (entre centros de datos) de problemas de rendimiento.
nsx-aggsservice	proporciona bibliotecas en el lado de host para el servicio de agregación de NSX-T Data Center. El servicio de agregación de NSX-T Data Center se ejecuta en los nodos del plano de administración y captura el estado de los componentes de NSX-T Data Center.
nsx-cli-libs	proporciona la CLI de NSX-T Data Center en hosts del hipervisor.
nsx-common-libs	proporciona algunas clases de utilidades, como AES, SHA-1, UUID, mapa de bits y otras.
nsx-context-mux	Proporciona la funcionalidad de retransmisión de NSX Guest Introspection. Permite que VMware Tools agentes invitados retransmitan el contexto invitado a dispositivos asociados de terceros registrados.
nsx-esx-datapath	Proporciona la funcionalidad de procesamiento de paquetes de plano de datos de NSX-T Data Center.

nsx-exporter	proporciona agentes de host que comunican el estado en tiempo de ejecución al servicio de agregación que se ejecuta en el plano de administración.
nsx-host	proporciona metadatos para el paquete de VIB que está instalado en el host.
nsx-metrics-libs	Proporciona clases de utilidades de métricas para recopilar métricas de daemon.
nsx-mpa	proporciona comunicación entre NSX Manager y los hosts de hipervisor.
nsx-nestdb-libs	NestDB es una base de datos que almacena configuraciones de NSX relacionadas con el host (estado de tiempo de ejecución/deseado, etc.).
nsx-netcpa	proporciona comunicación entre el plano de control central y los hipervisores. Recibe el estado de red lógica del plano de control central y programa este estado en el plano de datos.
nsx-opsagent	Comunica las ejecuciones de los agentes de operaciones (realización de nodos de transporte, protocolo de detección de nivel de vínculo-LLDP, Traceflow, captura de paquetes, etc.) con el plano de administración.
nsx-platform-client	Proporciona un agente de ejecución de CLI común para la recopilación centralizada de la CLI y el registro de auditoría.
nsx-profiling-libs	Proporciona la funcionalidad de generación de perfiles basada en gpeftool utilizada para la generación de perfiles de procesos de daemon.
nsx-proxy	Proporciona el único agente de punto de contacto en dirección norte, que se comunica con el plano de control central y el plano de administración.
nsx-python-gevent	Contiene Python Gevent.
nsx-python-greenlet	Contiene la biblioteca Python Greenlet (bibliotecas de terceros).
nsx-python-logging	Contiene los registros de Python.
nsx-python-protobuf	Proporciona enlaces de Python para búferes de protocolo.
nsx-rpc-libs	Esta biblioteca proporciona la funcionalidad NSX-RPC.
nsx-sfhc	Componente de host de tejido del servicio (SFHC). Proporciona un agente de host para administrar el ciclo de vida del hipervisor como un host de tejido en el inventario del plano de administración. Esto proporciona un canal para operaciones como las de actualización y desinstalación de NSX-T Data Center y la de supervisión de módulos de NSX-T Data Center en hipervisores.
nsx-shared-libs	Contiene las bibliotecas compartidas de NSX.

nsx-upm-libs	Proporciona funcionalidad de administración de perfiles unificada para acoplar la configuración del lado del cliente y evitar la transmisión de datos duplicada.
nsx-vdpi	Proporciona la capacidades de inspección de paquetes en profundidad para el firewall distribuido de NSX-T Data Center.
nsxcli	proporciona la CLI de NSX-T Data Center en hosts del hipervisor.
vsipfwlib	Proporciona funcionalidad de firewall distribuido.

Para comprobarlo, puede ejecutar los comandos `esxcli software vib list | grep nsx` y `esxcli software vib list | grep vsipfwlib` en el host ESXi. También puede ejecutar el comando `esxcli software vib list | grep <yyyy-mm-dd>`, donde la fecha es el día que realizó la instalación.

Pasos siguientes

Agregue el host al plano de administración de NSX-T Data Center. Consulte [Implementar nodos de NSX Manager para formar un clúster mediante la CLI](#).

Instalar manualmente módulos kernel de NSX-T Data Center en hipervisores de KVM en Ubuntu

Para preparar los hosts que participen en NSX-T Data Center, puede instalar de forma manual módulos kernel de NSX-T Data Center en hosts de KVM de Ubuntu. Esto le permite crear el tejido del plano de administración y del panel de control de NSX-T Data Center. Los módulos de kernel de NSX-T Data Center empaquetados en archivos DEB se ejecutan dentro del kernel del hipervisor y ofrecen servicios, como enrutamiento distribuido, firewall distribuido y capacidades de puente.

Puede descargar los DEB de NSX-T Data Center manualmente y hacer que formen parte de la imagen del host. Tenga en cuenta que las rutas de descarga pueden variar en cada versión de NSX-T Data Center. Compruebe siempre la página de descargas de NSX-T Data Center para obtener los DEB apropiados.

Requisitos previos

- Compruebe que estén instalados los paquetes de terceros requeridos. Consulte [Instalar paquetes de terceros en un host de KVM](#).

Procedimiento

- 1 Inicie sesión en el host como usuario con privilegios de administrador.
- 2 (opcional) Desplácese hasta el directorio /tmp.

```
cd /tmp
```

- 3 Descargue y copie el archivo nsx-lcp en el directorio /tmp.

4 Descomprima el paquete.

```
tar -xvf nsx-lcp-<release>-ubuntu-trusty-amd64.tar.gz
```

5 Desplácese hasta el directorio del paquete.

```
cd nsx-lcp-trusty-amd64/
```

6 Instale los paquetes.

```
sudo dpkg -i *.deb
```

7 Vuelva a cargar el módulo kernel de OVS.

```
/etc/init.d/openvswitch-switch force-reload-kmod
```

Si el hipervisor utiliza DHCP en las interfaces de OVS, reinicie la interfaz de red en la que está configurado DHCP. Puede detener manualmente el proceso de dhclient anterior en la interfaz de red y reiniciar un nuevo proceso dhclient en esa interfaz.

8 Para comprobar, puede ejecutar el comando `dpkg -l | grep nsx`.

```
user@host:~$ dpkg -l | grep nsx
```

ii	nsx-agent	<release>	amd64	NSX Agent
ii	nsx-aggservice	<release>	all	NSX Aggregation Service Lib
ii	nsx-cli	<release>	all	NSX CLI
ii	nsx-da	<release>	amd64	NSX Inventory Discovery Agent
ii	nsx-host	<release>	all	NSX host meta package
ii	nsx-host-node-status-reporter	<release>	amd64	NSX Host Status Reporter for
	Aggregation Service			
ii	nsx-lldp	<release>	amd64	NSX LLDP Daemon
ii	nsx-logical-exporter	<release>	amd64	NSX Logical Exporter
ii	nsx-mpa	<release>	amd64	NSX Management Plane Agent Core
ii	nsx-netcpa	<release>	amd64	NSX Netcpa
ii	nsx-sfhc	<release>	amd64	NSX Service Fabric Host
	Component			
ii	nsx-transport-node-status-reporter	<release>	amd64	NSX Transport Node Status
	Reporter			
ii	nsxa	<release>	amd64	NSX L2 Agent

Lo más probable es que los errores se deban a la existencia de dependencias incompletas. El comando `apt-get install -f` puede intentar resolver las dependencias y volver a ejecutar la instalación de NSX-T Data Center.

Pasos siguientes

Agregue el host al plano de administración de NSX-T Data Center. Consulte [Implementar nodos de NSX Manager para formar un clúster mediante la CLI](#).

Instalar manualmente módulos kernel de NSX-T Data Center en hipervisores de KVM en RHEL y CentOS

Para preparar los hosts que participan en NSX-T Data Center, puede instalar manualmente módulos kernel de NSX-T Data Center en hosts de KVM de RHEL o CentOS.

Esto le permite crear el tejido del plano de administración y del panel de control de NSX-T Data Center. Los módulos de kernel de NSX-T Data Center empaquetados en archivos RPM se ejecutan dentro del kernel del hipervisor y ofrecen servicios, como enrutamiento distribuido, firewall distribuido y capacidades de puente.

Puede descargar los RPM de NSX-T Data Center manualmente y hacer que formen parte de la imagen del host. Tenga en cuenta que las rutas de descarga pueden variar en cada versión de NSX-T Data Center. Compruebe siempre la página de descargas de NSX-T Data Center para obtener los RPM apropiados.

Requisitos previos

Capacidad para acceder a un repositorio de RHEL o CentOS.

Procedimiento

- 1 Inicie sesión en el host como administrador.
- 2 Descargue y copie el archivo nsx-lcp en el directorio /tmp.
- 3 Descomprima el paquete.

```
tar -zxvf nsx-lcp-<release>-rhel7.4_x86_64.tar.gz
```

- 4 Desplácese hasta el directorio del paquete.

```
cd nsx-lcp-rhel74_x86_64/
```

- 5 Instale los paquetes.

```
sudo yum install *.rpm
```

Al ejecutar el comando de instalación yum, se resuelve cualquier dependencia de NSX-T Data Center, siempre y cuando los hosts de RHEL o CentOS puedan comunicarse con sus respectivos repositorios.

- 6 Vuelva a cargar el módulo kernel de OVS.

```
/etc/init.d/openvswitch force-reload-kmod
```

Si el hipervisor utiliza DHCP en las interfaces de OVS, reinicie la interfaz de red en la que está configurado DHCP. Puede detener manualmente el proceso de dhclient anterior en la interfaz de red y reiniciar un nuevo proceso dhclient en esa interfaz.

- 7 Para comprobar, puede ejecutar el comando `rpm -qa | egrep 'nsx|openvswitch|nicira'`.

Los paquetes instalados en la salida deben coincidir con los paquetes en el directorio nsx-rhel74 o nsx-centos74.

Pasos siguientes

Agregue el host al plano de administración de NSX-T Data Center. Consulte [Implementar nodos de NSX Manager para formar un clúster mediante la CLI](#).

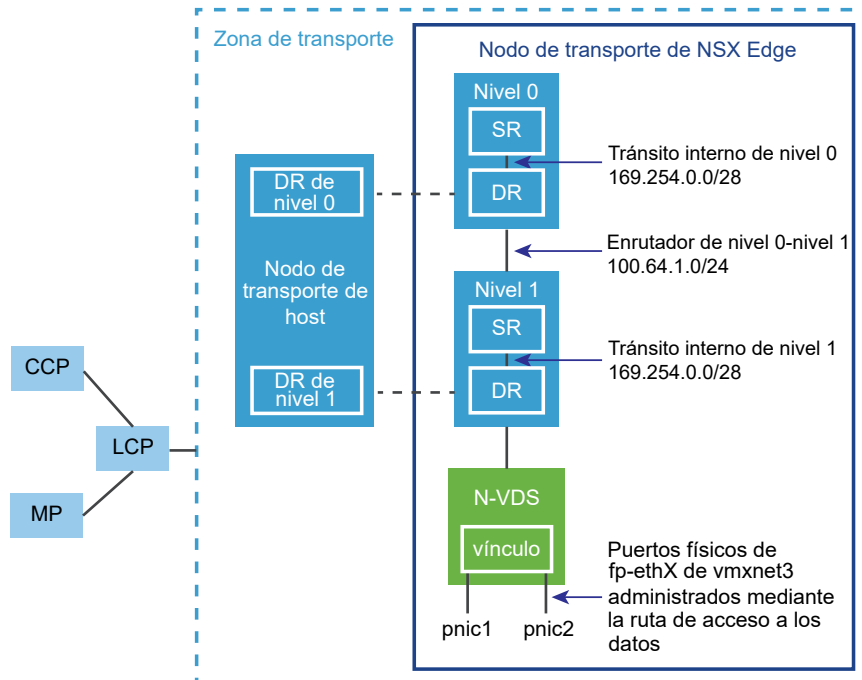
Configuración de red de NSX Edge

NSX Edge se puede instalar mediante inicio ISO, OVA/OVF o PXE. Independientemente del método de instalación, asegúrese de que la red del host esté preparada antes de instalar NSX Edge.

Vista de alto nivel de NSX Edge dentro de una zona de transporte

La vista de alto nivel de NSX-T Data Center muestra dos nodos de transporte en una zona de transporte. Un nodo de transporte es un host. El otro es un NSX Edge.

Figura 8-5. Descripción general de alto nivel de NSX Edge



Cuando implementa NSX Edge por primera vez, puede verlo como un contenedor vacío. NSX Edge no hace nada hasta que usted crea los enrutadores lógicos. NSX Edge proporciona respaldo de proceso para enrutadores lógicos de nivel 0 y 1. Cada enrutador lógico contiene un enrutador de servicios (SR) y un enrutador distribuido (DR). Cuando decimos que un enrutador es distribuido, queremos decir que está replicado en todos los nodos de transporte que pertenecen a la misma zona de transporte. En la figura, el nodo de transporte del host contiene los mismos enrutadores distribuidos (DR) contenidos en los enrutadores de nivel 0 y 1. Se requiere un enrutador de servicios si el enrutador lógico se va a configurar para realizar servicios, como NAT. Todos los enrutadores lógicos de nivel 0 tienen un enrutador de servicios. Un enrutador de nivel 1 puede tener un enrutador de servicios si fuese necesario teniendo en cuenta sus consideraciones de diseño.

De manera predeterminada, los vínculos entre el SR y el DR utilizan la subred 169.254.0.0/28. Estos vínculos de tránsito entre enrutadores se crean automáticamente al implementar un enrutador lógico de nivel 0 o 1. No tiene que configurar ni modificar la configuración de vínculo salvo que ya se esté utilizando la subred 169.254.0.0/28 en su implementación. En un enrutador lógico de nivel 1, el SR solo está presente si selecciona un clúster de NSX Edge al crear el enrutador lógico de nivel 1.

El espacio de dirección predeterminado asignado a las conexiones de nivel 0 a nivel 1 es 100.64.0.0/10. A cada conexión del mismo nivel de nivel 0 a nivel 1 se le proporciona una subred /31 dentro del espacio de direcciones 100.64.0.0/10. Este vínculo se crea de forma automática al crear un enrutador de nivel 1 y conectarlo a un enrutador de nivel 0. No tiene que configurar ni modificar las interfaces de este vínculo salvo que ya se esté utilizando la subred 100.64.0.0/10 en su implementación.

Todas las implementaciones de NSX-T Data Center tienen un clúster de plano de administración (MP) y un clúster de plano de control (CCP). El MP y el CCP insertan configuraciones en el plano de control local (LCP) de cada zona de transporte. Cuando un host o NSX Edge se une al plano de administración, el agente del plano de administración (MPA) establece la conectividad con el host o NSX Edge, y el host o NSX Edge se convierten en un nodo de tejido de NSX-T Data Center. Cuando el nodo de tejido se agrega a continuación como un nodo de transporte, se establece la conectividad del LCP con el host o NSX Edge.

Por último, la figura muestra un ejemplo de dos NIC físicas (pNIC1 y pNIC2) que se conectan para proporcionar una alta disponibilidad. La ruta de datos administra las NIC físicas. Pueden servir como vínculos superiores de VLAN a una red externa o como vínculos de endpoints de túnel a redes de máquinas virtuales (VM) internas administradas por NSX-T Data Center.

Una práctica recomendada es asignar al menos dos vínculos físicos a cada NSX Edge que se implementa como una máquina virtual. De forma opcional, puede solapar los grupos de puertos en la misma pNIC utilizando distintos ID de VLAN. El primer vínculo de red se utiliza para la administración. Por ejemplo, en una VM de NSX Edge, el primer vínculo hallado podría ser vnic1. En una instalación sin sistema operativo, el primer vínculo hallado podría ser eth0 o em0. Los vínculos restantes se utilizan para los vínculos superiores y túneles. Por ejemplo, uno podría ser para un endpoint de túnel utilizado por las VM administradas por NSX-T Data Center. El otro podría utilizarse para un vínculo superior de NSX Edge a TOR externo.

Puede ver la información del vínculo físico de NSX Edge si inicia sesión en la CLI como administrador y ejecuta los comandos `get interfaces` y `get physical-ports`. En la API, puede utilizar la llamada API `GET fabric/nodes/<edge-node-id>/network/interfaces`. En la siguiente sección se habla sobre los vínculos físicos en mayor profundidad.

Independientemente de que instale NSX Edge como un dispositivo de VM o sin sistema operativo, dispone de varias opciones para configurar la red en función de la implementación que lleve a cabo.

Zonas de transporte y N-VDS

Para comprender las redes de NSX Edge, debe conocer algo sobre zonas de transporte y N-VDS. Las zonas de transporte controlan el alcance de las redes de Capa 2 en NSX-T Data Center. N-VDS es un conmutador de software que se crea en un nodo de transporte. El propósito de un N-VDS es asociar enlaces ascendentes y descendentes de enrutador lógico con NIC físicas. Para cada zona de transporte a la que pertenece un NSX Edge, se instala un N-VDS individual en NSX Edge.

Hay dos tipos de zonas de transporte:

- Superposición para tunelización interna de NSX-T Data Center entre los nodos de transporte.
- VLAN para vínculos superiores externos a NSX-T Data Center.

Un NSX Edge puede pertenecer a cero zonas de transporte VLAN o a muchas. En el caso de cero zonas de transporte VLAN, NSX Edge sigue pudiendo tener vínculos superiores, porque los vínculos superiores de NSX Edge pueden utilizar el mismo N-VDS instalado para la zona de transporte superpuesta. Puede hacer esto si quiere que cada NSX Edge tenga solamente un N-VDS. Otra opción de diseño consiste en que el NSX Edge pertenezca a varias zonas de transporte VLAN, una para cada vínculo superior.

La opción de diseño más común está compuesta por tres zonas de transporte: una zona de transporte superpuesta y dos zonas de transporte VLAN para vínculos superiores redundantes.

Para utilizar el mismo ID de VLAN para una red de transporte de tráfico superpuesto y otra para el tráfico VLAN, como un vínculo superior de VLAN, configure el ID en dos N-VDS diferentes, uno para VLAN y otro para superposición.

Redes de NSX Edge de dispositivos virtuales/VM

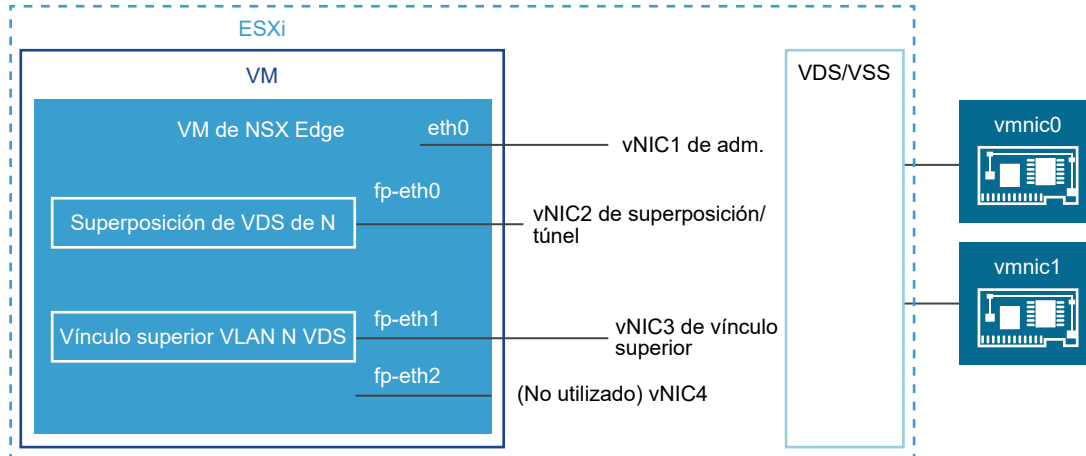
Cuando instala NSX Edge como un dispositivo virtual o VM, se crean interfaces internas, llamadas `fp-ethX`, donde X es 0, 1, 2 y 3. Estas interfaces se asignan para vínculos superiores a conmutadores para parte superior del rack (TOR) y para la tunelización superpuesta de NSX-T Data Center.

Cuando cree el nodo de transporte de NSX Edge, puede seleccionar interfaces `fp-ethX` para asociarlas a los vínculos superiores y al túnel superpuesto. Puede decidir cómo utilizar las interfaces `fp-ethX`.

En el conmutador distribuido o estándar de vSphere, debe asignar al menos dos `vmnics` al NSX Edge: uno para la administración de NSX Edge y otro para vínculos superiores y túneles.

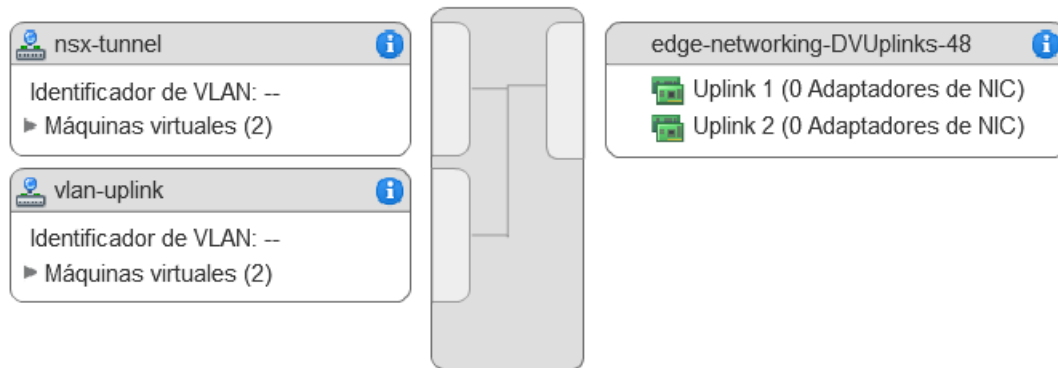
En la siguiente topología física de ejemplo, se utiliza `fp-eth0` para el túnel superpuesto de NSX-T Data Center. `fp-eth1` se utiliza para el vínculo superior de VLAN. `fp-eth2` y `fp-eth3` no se utilizan. Se asigna `vNIC1` a la red de administración.

Figura 8-6. Una configuración recomendada de vínculo para redes de VM de NSX Edge



El NSX Edge que se muestra en este ejemplo pertenece a dos zonas de transporte (una de superposición y otra de VLAN) y, por lo tanto, tiene dos N-VDS, uno para el túnel y otro para el tráfico de enlaces ascendentes.

Esta captura de pantalla muestra los grupos de puertos de máquinas virtuales, el túnel de NSX y el vínculo superior de VLAN.



Durante la implementación debe especificar los nombres de red que se corresponden con los nombres configurados en sus grupos de puertos de VM. Por ejemplo, para que se correspondan con los grupos de puertos de VM del ejemplo, su configuración de ovftool de red puede ser tal como se indica a continuación si utilizase la ovftool para implementar NSX Edge:

```
--net:"Network 0-Mgmt" --net:"Network 1-nsx-tunnel" --net:"Network 2=vlan-uplink"
```

El ejemplo mostrado aquí utiliza los nombres de grupos de puertos de VM Mgmt, nsx-tunnel y vlan-uplink. Puede utilizar el nombre que quiera para sus grupos de puertos de VM.

Los grupos de puertos de VM de vínculos superiores y túnel configurados para el NSX Edge no tienen que asociarse a puertos VMkernel ni a direcciones IP proporcionadas. Esto se debe a que solo se utilizan en la Capa 2. Si su implementación utiliza DHCP para proporcionar una dirección a la interfaz de administración, asegúrese de que solo se asigne la NIC a la red de administración.

Tenga en cuenta que los grupos de puertos de túnel y VLAN se configuran como puertos troncales. Esto es obligatorio. Por ejemplo, en un vSwitch estándar, los puertos troncales se configuran de la siguiente manera: **Host > Configuración > Redes > Agregar redes > Máquina virtual > ID VLAN todos (4095)**.

Si está utilizando un NSX Edge de VM o basado en dispositivo, puede utilizar conmutadores vSwitch o conmutadores distribuidos vSphere.

La VM de NSX Edge puede instalarse en un host preparado para NSX-T Data Center y configurado como un nodo de transporte. Existen dos tipos de implementación:

- La VM de NSX Edge puede implementarse mediante grupos de puertos VSS/VDS donde VSS/VDS consumen pNIC independiente en el host. El nodo de transporte del host consume pNIC independientes para los N-VDS instalados en el host. El N-VDS del nodo de transporte del host coexiste con un VSS o VDS, que consumen ambos pNIC independientes. El TEP (endpoint de túnel) del host y el TEP de NSX Edge pueden estar en la misma subred o en subredes diferentes.
- La VM de NSX Edge puede implementarse mediante conmutadores lógicos respaldados por VLAN en el N-VDS del nodo de transporte del host. El TEP del host y el TEP de NSX Edge deben estar en subredes diferentes.

De forma opcional, puede instalar varios dispositivos/VM de NSX Edge en un mismo host, y todos los NSX Edge instalados pueden utilizar los grupos de puertos de endpoint de túnel.

Una vez que estén configurados los grupos de puertos de VM y los vínculos físicos subyacentes activos, puede instalar el NSX Edge.

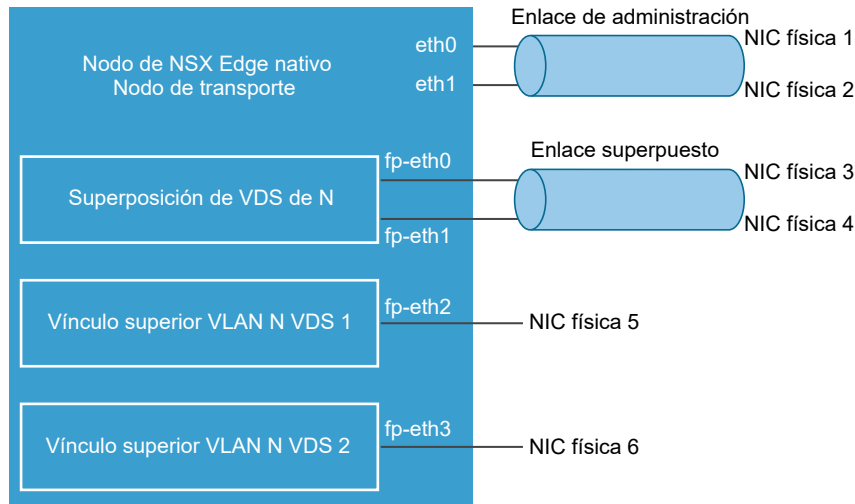
Redes de NSX Edge sin sistema operativo

El NSX Edge sin sistema operativo contiene interfaces denominadas fp-ethX, donde X es 0, 1, 2, 3 o 4. El número de interfaces fp-ethX creado depende de cuántas NIC físicas tenga su NSX Edge sin sistema operativo. Se pueden asignar hasta cuatro de estas interfaces para vínculos superiores de conmutadores para parte superior de bastidor rack (ToR) y tunelización superpuesta de NSX-T Data Center.

Cuando cree el nodo de transporte de NSX Edge, puede seleccionar interfaces fp-ethX para asociarlas a los vínculos superiores y al túnel superpuesto.

Puede decidir cómo utilizar las interfaces fp-ethX. En la siguiente topología física de ejemplo, se asocian y utilizan fp-eth0 y fp-eth1 para el túnel superpuesto de NSX-T Data Center. fp-eth2 y fp-eth3 se utilizan como vínculos superiores de VLAN a las TOR.

Figura 8-7. Una configuración recomendada de vínculo para redes de NSX Edge sin sistema operativo



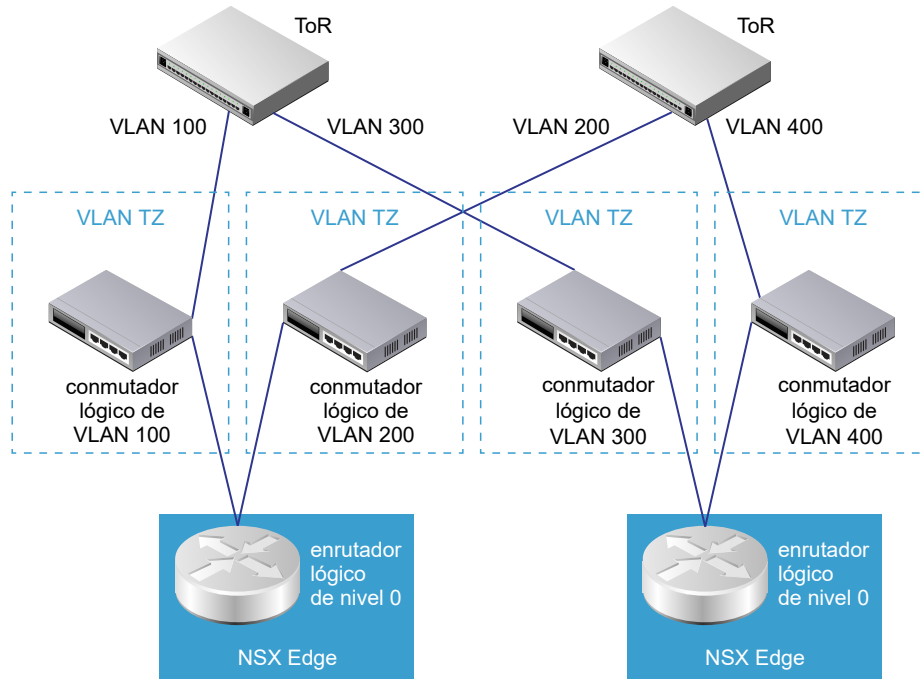
Redundancia de vínculos superiores de NSX Edge

La redundancia de vínculos superiores de NSX Edge permite utilizar dos vínculos superiores Multipath de igual coste (ECMP) en la conexión de red de NSX Edge a TOR externa.

Si tiene dos vínculos superiores de VLAN ECMP, también debe tener dos conmutadores TOR para disfrutar de una alta disponibilidad y una conectividad totalmente de malla. Cada conmutador lógico de VLAN tienen asociado un ID de VLAN.

Cuando agregue un NSX Edge a una zona de transporte de VLAN, se instalará un nuevo N-VDS. Por ejemplo, si agrega un nodo de NSX Edge a cuatro zonas de transporte VLAN, tal como se muestra en la figura, se instalarán cuatro N-VDS en NSX Edge.

Figura 8-8. Una configuración recomendada de VLAN ECMP para NSX Edge a TOR.



Nota Para una máquina virtual Edge implementada en un host ESXi con vSphere Distributed Switch (vDS) y sin N-VDS, debe hacer lo siguiente:

- Habilitar la transmisión manipulada para que DHCP funcione.
- Habilitar el modo promiscuo para que la máquina virtual de Edge reciba paquetes de unidifusión desconocidos porque el aprendizaje de direcciones MAC está deshabilitado de forma predeterminada. Esto no es necesario para vDS 6.6 y versiones posteriores, ya que tienen el aprendizaje de direcciones MAC habilitado de forma predeterminada.

Crear un nodo de transporte de NSX Edge

Puede agregar una instancia de NSX Edge al tejido de NSX-T Data Center y configurar la instancia de NSX Edge como un nodo de transporte.

Un nodo de transporte es un nodo que es capaz de participar en una superposición de NSX-T Data Center o redes VLAN de NSX-T Data Center. Cualquier nodo puede servir como nodo de transporte si contiene un N-VDS. Este tipo de nodos incluye NSX Edge, entre otros.

Un NSX Edge puede pertenecer a una zona de transporte superpuesta y a múltiples zonas de transporte de VLAN. Si una VM requiere acceso al mundo exterior, el NSX Edge debe pertenecer a la misma zona de transporte a la que pertenece el conmutador lógico de la VM. Por lo general, el NSX Edge pertenece al menos a una zona de transporte de VLAN para proporcionar el acceso al vínculo superior.

Nota Si planea crear nodos de transporte desde una VM de plantilla, asegúrese de que no haya certificados en el host en `/etc/vmware/nsx/`. El agente netcpa no crea ningún certificado si ya existe uno.

Requisitos previos

- Se deben configurar las zonas de transporte.
- Compruebe que se haya configurado el administrador de equipos. Consulte [Agregar un administrador de equipos](#).
- Debe haber un perfil de vínculo superior configurado, o bien puede utilizar el perfil de vínculo superior predeterminado para nodos de NSX Edge nativos.
- Debe haber un grupo de direcciones IP configurado o disponible en la implementación de la red.
- Debe haber disponible al menos una tarjeta NIC física no utilizada en el host o nodo de NSX Edge.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión con privilegios de administrador en NSX Manager.
- 2 Seleccione **Sistema > Tejido > Nodos > Nodos de transporte de Edge > Agregar máquina virtual de Edge**.
- 3 Introduzca un nombre para NSX Edge.
- 4 Escriba el nombre de host o el FQDN de vCenter Server.
- 5 Para que el rendimiento sea óptimo, reserve memoria para el dispositivo de NSX Edge.
 Establezca la reserva para garantizar que NSX Edge tenga suficiente memoria como para ejecutarse de forma eficiente. Consulte [Requisitos del sistema de máquinas virtuales de NSX Edge](#).
- 6 Especifique la CLI y las contraseñas raíz de NSX Edge.

Sus contraseñas deben cumplir las restricciones de seguridad para contraseñas.

- Al menos 12 caracteres
- Al menos una letra en minúsculas
- Al menos una letra en mayúsculas
- Al menos un dígito
- Al menos un carácter especial
- Al menos cinco caracteres distintos
- Sin palabras del diccionario
- Sin palíndromos
- No se admiten más de cuatro secuencias de caracteres monotónicos.

7 Introduzca los detalles de NSX Edge.

Opción	Descripción
Administrador de equipo	Seleccione el administrador de equipos en el menú desplegable. El administrador de equipos es el vCenter Server registrado en el Plano de administración.
Clúster	Designa el clúster al que se va a unir NSX Edge en el menú desplegable.
Grupo de recursos o host	Asigne un grupo de recursos o un host específico a NSX Edge en el menú desplegable.
Almacén de datos	Seleccione un almacén de datos para los archivos de NSX Edge en el menú desplegable.

8 Introduzca los detalles de la interfaz de NSX Edge.

Opción	Descripción
Asignación de IP	Seleccione DHCP o IP estática . Si selecciona Estática , debe especificar una lista de direcciones IP separadas por comas, una puerta de enlace y una máscara de subred.
Interfaz de administración	Seleccione la interfaz de red de máquinas virtuales en el menú desplegable.

9 Seleccione las zonas de transporte a las que corresponde este nodo de transporte.

Un nodo de transporte de NSX Edge corresponde al menos a dos zonas de transporte, una superposición para la conectividad de NSX-T Data Center y una red VLAN para la conectividad de vínculo superior.

Nota Se deben configurar varios VTEP en una zona de transporte en el mismo segmento de red. Si los VTEP de una zona de transporte se configuran en segmentos de red diferentes, no se podrán establecer sesiones de BFD entre los VTEP.

10 Introduzca la información del N-VDS.

Opción	Descripción
Nombre del conmutador de Edge	Seleccione el conmutador de superposición en el menú desplegable.
Perfil de vínculo superior	Seleccione el perfil de vínculo superior en el menú desplegable. Los vínculos superiores disponibles dependen de la configuración del perfil de vínculo superior seleccionado.
Asignación de IP	Seleccione Usar grupo de direcciones IP o Usar lista de direcciones IP estáticas para el N-VDS superpuesto. Si selecciona Usar lista de direcciones IP estáticas (Use Static IP List), debe especificar una lista de direcciones IP separadas por comas, una puerta de enlace y una máscara de subred.

Opción	Descripción
Grupo de direcciones IP	Si seleccionó Usar grupo de direcciones IP (Use IP Pool) para la asignación de direcciones IP, especifique el nombre del grupo de direcciones IP.
Interfaces de la ruta de datos	Seleccione el nombre de la interfaz de ruta de datos para la interfaz de vínculo superior.

Nota No se admite el perfil de LLDP en un dispositivo de máquina virtual de NSX Edge.

11 Puede ver el estado de conexión en la página **Nodos de transporte (Transport Nodes)**.

Después de agregar NSX Edge como nodo de transporte, el estado de conexión cambiará a Activo en unos 10-12 minutos.

12 (opcional) Consulte el nodo de transporte con la llamada API GET `https://<nsx-manager>/api/v1/transport-nodes/<transport-node-id>`:

13 (opcional) Para obtener información sobre el estado, utilice la llamada API GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/status`.

Pasos siguientes

Agregue el nodo de NSX Edge a un clúster de NSX Edge. Consulte [Crear un clúster de NSX Edge](#).

Crear un clúster de NSX Edge

Tener un clúster multinodo de NSX Edge ayuda a garantizar que siempre haya disponible al menos un NSX Edge.

Para crear un enrutador lógico de nivel 0 o un enrutador de nivel 1 con servicios con estado, como NAT, equilibrador de carga, entre otros, debe asociarlo a un clúster de NSX Edge. Por tanto, aunque solo tenga un NSX Edge, debe pertenecer a un clúster de NSX Edge para que sea útil.

Un nodo de transporte de NSX Edge solo se puede agregar a un único clúster de NSX Edge.

Un clúster de NSX Edge se puede utilizar para respaldar varios enrutadores lógicos.

Tras crear el clúster de NSX Edge, puede editarlo para agregar NSX Edge adicionales.

Requisitos previos

- Instale al menos un nodo de NSX Edge.
- Una los NSX Edge al plano de administración.
- Agregue los NSX Edge como nodos de transporte.
- Opcionalmente, puede crear un perfil de clúster de NSX Edge para la alta disponibilidad (HA). También puede utilizar el perfil de clústeres de NSX Edge predeterminado.

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión con privilegios de administrador en NSX Manager.

2 Seleccione **Sistema > Tejido > Nodos > Clústeres de Edge > Agregar**.

3 Introduzca un nombre para el clúster de NSX Edge.

4 Seleccione un perfil de clúster de NSX Edge en el menú desplegable.

5 Seleccione Nodo de NSX Edge en el menú desplegable Tipo de miembro.

Si la máquina virtual se implementa en un entorno de nube pública, seleccione Nodo de puerta de enlace de nube pública. De lo contrario, seleccione nodo de NSX Edge.

6 Desde la columna **Disponible**, seleccione los NSX Edge y haga clic en la flecha derecha para moverlos a la columna **Seleccionados**.

Pasos siguientes

Ahora puede crear topologías de redes lógicas y configurar servicios. Consulte la *Guía de administración de NSX-T Data Center*.

Clúster sin estado con Auto Deploy

9

La configuración no se aplica a los hosts sin estado, por lo que necesitan un servidor Auto Deploy para obtener los archivos de inicio requeridos cuando se encienden los hosts.

En esta sección, se explica cómo configurar un clúster sin estado con vSphere Auto Deploy y un perfil de nodo de transporte de NSX-T para volver a aprovisionar un host con una imagen de perfil nueva que contenga una versión diferente de ESXi y NSX-T. Los hosts que se configuran con vSphere Auto Deploy utilizan un servidor de Auto Deploy y perfiles de host de vSphere para personalizar los hosts. Estos hosts también se pueden configurar con un perfil de nodo de transporte de NSX-T para implementar NSX-T en los hosts.

Por lo tanto, un host sin estado se puede configurar con vSphere Auto Deploy y un perfil de nodo de transporte de NSX-T para volver a aprovisionar un host con una versión personalizada de ESXi y NSX-T.

Este capítulo incluye los siguientes temas:

- [Tareas de alto nivel para un clúster sin estado con Auto Deploy](#)
- [Requisitos previos y versiones admitidas](#)
- [Crear un perfil de imagen personalizada para hosts sin estado](#)
- [Asociar la imagen personalizada con el host de referencia y los hosts de destino](#)
- [Establecer la configuración de red en el host de referencia](#)
- [Configurar el host de referencia como un nodo de transporte en NSX-T](#)
- [Extraer el perfil de host y verificarlo](#)
- [Verificar la asociación del perfil de host con el clúster sin estado](#)
- [Actualizar las personalizaciones de host](#)
- [Activar la implementación automática en los hosts de destino](#)
- [Solucionar problemas del perfil de host y el perfil de nodo de transporte](#)

Tareas de alto nivel para un clúster sin estado con Auto Deploy

A continuación, se indican las tareas de alto nivel para un clúster sin estado con Auto Deploy.

Las tareas de alto nivel para configurar un clúster sin estado con Auto Deploy son las siguientes:

- 1 Requisitos previos y versiones admitidas. Consulte [Requisitos previos y versiones admitidas](#).
- 2 (Host de referencia) Cree un perfil de imagen personalizada. Consulte [Crear un perfil de imagen personalizada para hosts sin estado](#).
- 3 (Hosts de referencia y de destino) Asocie el perfil de imagen personalizada. Consulte [Asociar la imagen personalizada con el host de referencia y los hosts de destino](#).
- 4 (Host de referencia) Establezca la configuración de red en ESXi. Consulte [Establecer la configuración de red en el host de referencia](#).
- 5 (Host de referencia) Configúrelo como un nodo de transporte en NSX. Consulte [Configurar el host de referencia como un nodo de transporte en NSX-T](#).
- 6 (Host de referencia) Extraiga y compruebe el perfil de host. Consulte [Extraer el perfil de host y verificarlo](#).
- 7 (Hosts de referencia y de destino) Compruebe la asociación del perfil de host con el clúster sin estado. Consulte [Verificar la asociación del perfil de host con el clúster sin estado](#).
- 8 (Host de referencia) Actualice la personalización del host. Consulte [Actualizar las personalizaciones de host](#).
- 9 (Hosts de destino) Active el servicio Auto Deploy. Consulte [Activar la implementación automática en los hosts de destino](#).
 - a Antes de aplicar el perfil de nodo de transporte. Consulte [Reiniciar hosts antes de aplicar el TNP](#).
 - b Aplique el perfil de nodo de transporte. Consulte [Aplicar un TNP a un clúster sin estado](#).
 - c Después de aplicar el perfil de nodo de transporte. Consulte [Reiniciar hosts después de aplicar el TNP](#).
- 10 Solucione los problemas del perfil de host y el perfil de nodo de transporte. Consulte [Solucionar problemas del perfil de host y el perfil de nodo de transporte](#).

Requisitos previos y versiones admitidas

Requisitos previos y versiones de ESXi y NSX-T admitidas.

Flujos de trabajo admitidos

- Con el perfil de imagen y HostProfile

Requisitos previos

- Solo se admiten clústeres homogéneos (todos los hosts de un clúster debe ser sin estado o con estado).
- El servicio Image Builder debe estar habilitado.
- El servicio Auto Deploy debe estar habilitado.

Versiones compatibles de NSX y ESXi

Versión de ESXi compatible	ESXi 67ep6	ESXi 67u2	ESXi 67u3	ESXi 67ep7
NSX-T Data Center 2.4	Sí	Sí	No	No
NSX-T Data Center 2.4.1	Sí	Sí	No	No
NSX-T Data Center 2.4.2	Sí	Sí	No	No
NSX-T Data Center 2.4.3	Sí	Sí	No	No
NSX-T Data Center 2.5	Sí	Sí	Sí	Sí

Crear un perfil de imagen personalizada para hosts sin estado

En el centro de datos, identifique el host que se deba preparar como host de referencia.

La primera vez que se inicia el host de referencia, ESXi asocia la regla predeterminada al host de referencia. En este procedimiento, añadirá un perfil de imagen personalizada (ESXi y los VIB de NSX) y asociará el host de referencia a la nueva imagen personalizada. Un perfil de imagen con la imagen de NSX-T reduce significativamente el tiempo de instalación. La misma imagen personalizada se asocia a los hosts de destino del clúster sin estado.

Nota También puede agregar solo un perfil de imagen de ESXi al clúster de referencia y de destino sin estado. Los VIB de NSX-T se descargan al aplicar el perfil de nodo de transporte en el clúster sin estado. Consulte [Agregar un almacén de software](#).

Requisitos previos

Asegúrese de que los servicios de Image Builder y Auto Deploy estén habilitados. Consulte [Usar vSphere Auto Deploy para reprovisionar hosts](#).

Procedimiento

- 1 Para importar paquetes de NSX-T, cree un almacén de software.
- 2 Descargue los paquetes nsx-lcp.
 - a Inicie sesión en <https://my.vmware.com>.
 - b En la página Descargar VMware NSX-T Data Center, seleccione la versión de NSX-T.
 - c En la página Descargas de productos, busque los módulos de kernel de NSX-T para obtener la versión específica de VMware ESXi.
 - d Haga clic en **Descargar ahora** para iniciar la descarga del paquete nsx-lcp.
 - e Importe los paquetes nsx-lcp al almacén de software.

NSX Kernel Module for VMware ESXi 6.7
File size: 32.48 MB
File type: zip

Download Now

Name: nsx-lcp-2.4.10.0.13716576-esx67.zip
Release Date: 2019-05-21
Build Number: 13716575

NSX Kernel Module for VMware ESXi 6.7

This package includes the required kernel modules to enable NSX on ESXi 6.7 if needed for a manual installation. Use esxcli to install manually or include as part of an automated deployment system of the ESXi hosts.

MD5SUM: dff46ee2f452aa5719f2e5a2fdf55909

SHA1SUM: 7b86170aafc3ce2b9c12a130cd31483f2cb50134

SHA256SUM:

1425de96f01310cd54d2b5f1d4b0b612cd3eb13aa7bc8dde26ed7d7
55e646c0d

- 3 Cree otro almacén de software para importar los paquetes de ESXi.
vSphere Web Client mostrará los dos almacenados creados en el host de referencia.
- 4 Cree un almacén de software personalizado para clonar la imagen de ESXi y los paquetes nsx-lcp importados previamente.
 - a Seleccione el perfil de imagen de ESXi en el almacén de software de ESXi que creó en el paso anterior.
 - b Haga clic en **Clonar**.
 - c En el asistente Clonar perfil de imagen, introduzca un nombre para que se cree la imagen personalizada.
 - d Seleccione el almacén de software personalizado en el que deba estar disponible la imagen clonada (ESXi).
 - e En la ventana Seleccionar paquetes de software, seleccione **Certificado por VMware** para Nivel de aceptación. Los VIB de ESXi están preseleccionados.
 - f Identifique los paquetes de NSX-T manualmente en la lista de paquetes y selecciónelos. A continuación, haga clic en **Siguiente**.
 - g En la pantalla Listo para completar, compruebe la información y haga clic en **Finalizar** para crear la imagen clonada que contiene los paquetes de ESXi y NSX-T en el almacén de software personalizado.

Edit Image Profile

- 1 Name and details
- 2 Select software packages
- 3 Ready to complete

Select software packages

Acceptance level

VMware certified

<input type="checkbox"/>	Name	Version	Acceptance Level	Vendor	Depot
<input checked="" type="checkbox"/>	nsx-esx-datapath	2.5.0.0-6.7.14215647	VMware certified	VMware	NSXLCP
<input checked="" type="checkbox"/>	nsx-exporter	2.5.0.0-6.7.14215860	VMware certified	VMware	NSXLCP
<input checked="" type="checkbox"/>	nsx-host	2.5.0.0-6.7.14215622	VMware certified	VMware	NSXLCP
<input checked="" type="checkbox"/>	nsx-metrics-libs	2.5.0.0-6.7.14215788	VMware certified	VMware	NSXLCP
<input checked="" type="checkbox"/>	nsx-mpa	2.5.0.0-6.7.14215860	VMware certified	VMware	NSXLCP
<input checked="" type="checkbox"/>	nsx-nestdb	2.5.0.0-6.7.14215763	VMware certified	VMware	NSXLCP

172 selected of 184 items

CANCEL

BACK

NEXT

Pasos siguientes

Asocie la imagen personalizada con el host de referencia y los hosts de destino. Consulte [Asociar la imagen personalizada con el host de referencia y los hosts de destino](#).

Asociar la imagen personalizada con el host de referencia y los hosts de destino

Para iniciar el host de referencia y los hosts de destino con la nueva imagen personalizada que contiene paquetes de NSX y ESXi, asocie el perfil de la imagen personalizada.

En este punto del procedimiento, la imagen personalizada solo se asocia al host de referencia y los hosts de destino, pero no se instala NSX.

Importante Asocie la imagen personalizada en el host de referencia y los hosts de destino.

Requisitos previos

Procedimiento

- 1 En el host ESXi, desplácese hasta **Menú > Auto Deploy > Hosts implementados**.
- 2 Para asociar el perfil de la imagen personalizada con un host, selecciona la imagen personalizada.
- 3 Haga clic en **Editar asociación de perfil de imagen**.
- 4 En el asistente de Editar asociación de perfil de imagen, haga clic en **Examinar**, seleccione un almacén personalizado y, a continuación, el perfil de la imagen personalizada.
- 5 Habilite **Omitir comprobación de firma de perfil de imagen**.
- 6 Haga clic en **Aceptar** (OK).

Almacenes de software	Reglas de implementación	Hosts implementados	Hosts detectados	Paquetes de scripts	Configuración
<p>ⓘ El perfil de imagen, perfil de host y ubicación que Auto Deploy asoció con los hosts se indican a continuación. Las asociaciones podrían diferir del estado actual del host.</p> <p>COMPROBAR CUMPLIMIENTO DE ASOCIACIONES DE HOSTS... CORREGIR ASOCIACIONES DE HOSTS EDITAR ASOCIACIÓN DE PERFIL DE IMAGEN</p>					
<input type="checkbox"/>	Host	Perfil de imagen asociado	Perfil de host asociado	Ubicación asociada	Paquete de scripts asociado
<input type="checkbox"/>	10.144.139.147	CustomDepot(ESXi and NSX)		1-datacenter-1964	
<input type="checkbox"/>	10.144.137.225	CustomDepot(ESXi and NSX)		Statless-Cluster	

Resultados

Pasos siguientes

Establezca la configuración de red en el host de referencia. Consulte [Establecer la configuración de red en el host de referencia](#).

Establecer la configuración de red en el host de referencia

En el host de referencia, se crea un conmutador estándar con un adaptador de VMkernel para establecer la configuración de red en ESXi.

Esta configuración de red procede del perfil de host que se extrae del host de referencia. Durante una implementación sin estado, el perfil de host replica esta configuración de red en cada host de destino.

Procedimiento

- 1 En el host ESXi, configure un conmutador estándar de vSphere (vSphere Standard Switch, VSS) o un conmutador virtual distribuido (Distributed Virtual switch, DVS). Para ello, agregue un adaptador de VMkernel.
- 2 Compruebe que el conmutador VSS o DVS que acaba de agregar aparezca en la página adaptadores de VMkernel.

Dispositivo	Etiqueta de red	Conmutador	Dirección IP	Pila de TCP/IP	VM
vmk0	Management N...	vSwitch0	10.192.193.193	Predeterminado	D
vmk1	VMkernel	vSwitch2	192.163.242.185	Predeterminado	D

Pasos siguientes

Configure el host de referencia como un nodo de transporte en NSX-T. Consulte [Configurar el host de referencia como un nodo de transporte en NSX-T](#).

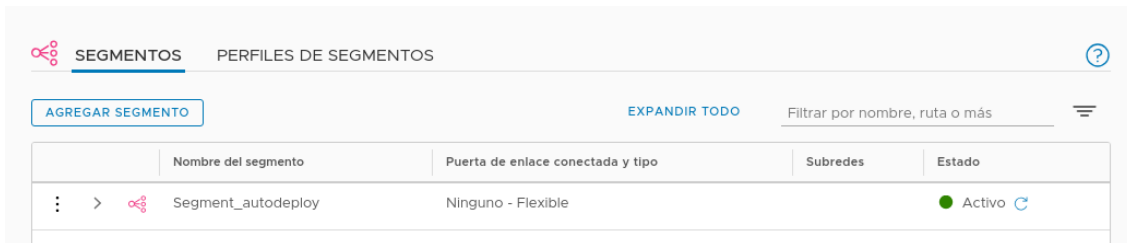
Configurar el host de referencia como un nodo de transporte en NSX-T

Una vez haya asociado el host de referencia con el perfil de la imagen personalizada y lo haya configurado con un conmutador de VSS, configure el host de referencia como un nodo de transporte en NSX-T.

Procedimiento

- 1 En el navegador, inicie sesión en NSX-T <https://<dirección-ip-nsx-manager>>.
- 2 Para localizar el host de referencia, desplácese hasta **Sistema -> Nodos -> Nodo de transporte de host**.

- 3 Cree una zona de transporte de VLAN para establecer la expansión de la red virtual. Para definir este valor, adjunte conmutadores de N-VDS a la zona de transporte. Gracias a que adjunta estos conmutadores, N-VDS puede acceder a los segmentos definidos dentro de la zona de transporte. Consulte [Crear una zona de transporte](#).
- 4 Cree un segmento de VLAN en la zona de transporte. Aparecerá como un conmutador lógico.
 - a Desplácese hasta **Redes -> Segmentos**.
 - b Seleccione la zona de transporte a la que desea asignar el segmento.
 - c Introduzca el identificador de VLAN.
 - d Haga clic en **Guardar**.



- 5 Cree un perfil de vínculo superior para el host de referencia que determine el modo en que un N-VDS se conecta a la red física. Consulte [Crear un perfil de vínculo superior](#).



- 6 Configure el host de referencia como un nodo de transporte. Consulte [Configurar un nodo de transporte de host administrado](#).
 - a En la página Nodo de transporte de host, seleccione el host de referencia.
 - b Haga clic en Configurar NSX y seleccione el perfil de vínculo superior, N-VDS y zona de transporte que creó anteriormente.

- 7 En la sección Asignaciones de red para instalación, haga clic en **Agregar asignación** para agregar la asignación de VMkernel a un segmento o conmutador lógico.

Asignaciones de red para instalación



La conectividad del host puede perderse cuando se migran vmnic0 y vmk0.

Si se cambia el conmutador lógico para el host con estado (independiente o en clúster), no tendrá ningún efecto y no se podrá realizar la operación.

+ AGREGAR ELIMINAR

<input checked="" type="checkbox"/> Adaptador de VMkernel *	Segmento de VLAN/Conmutador lógico
<input checked="" type="checkbox"/> vmk0	segment-autodeploy

- 8 Haga clic en **Finalizar** para empezar a instalar NSX-T en el host de referencia.

Durante la instalación, los adaptadores de VMkernel y las NCI físicas se migran desde un conmutador de VSS o DVS hasta un conmutador de N-VDS. Tras la instalación, la configuración del host de referencia tendrá el estado Correcto.

Nota El host de referencia aparecerá en Otros hosts.

Nodos De Transporte De Host

Nodos De Transporte De Edge

Clústeres De Edge

Clústeres De Puente ESXi

Administrado por

vc

CONFIGURAR NSX

QUITAR NSX

ACCIONES

Ver

Todo

<input type="checkbox"/>	Nodo	Identificad	Direcciones IP	Tipo de sistem	Configuración d	Estado de confi	Estado del nodo	Túneles	Zonas de transp	Versión de NSX	N-VDS
<input type="checkbox"/>	Other Hosts (2)	Identific...					1 host degrad...				
<input type="checkbox"/>	10.192.193.193	42ea...8...	10.192.193.1...	ESXi 6.7.0	Configurado	Correcto	Degradado ⓘ	No disp...	tz	2.5.0.0.0.14...	1
<input checked="" type="checkbox"/>	hostnode	6d4c...f...	10.160.169.8...	ESXi 6.7.0	Configurado	Correcto	Activo ⓘ	↑ 1	tz	2.5.0.0.0.14...	1

- En vCenter Server, verifique que los adaptadores de VMkernel y los PNIC del conmutador de VSS se migren y conecten al conmutador de N-VDS.

Adaptadores de VMkernel				
Agregar redes... Actualizar Editar... Quitar				
Dispositivo	Etiqueta de red	Conmutador	Dirección IP	Pila de TCP/IP
vmk0	Management Network	vSwitch0	10.160.169.87	Predeterminado
vmk1	Segment_autodeploy	vds-1	169.254.171.95	Predeterminado

Pasos siguientes

Extraiga el perfil de host y verifíquelo. Consulte [Extraer el perfil de host y verificarlo](#).

Extraer el perfil de host y verificarlo

Después de extraer el perfil de host del host de referencia, compruebe la configuración de NSX-T extraída en el perfil de host. Se compone de la configuración de ESXi y NSX-T que se aplica a los hosts de destino.

Procedimiento

- Para extraer el perfil de host, consulte [Extraer y configurar un perfil de host a partir de un host de referencia](#).

2 Compruebe la configuración de NSX en el perfil de host extraído.

FAVORITOS TODO

Q Filtrar

> Configuración de almacenamiento

> Configuración de redes

> Conmutador estándar

> Grupo de puertos de máquina virtual

> Grupo de puertos del host

> Configuración de NIC física

vSphere Distributed Switch

NIC virtual de host

> vNIC de host de NSX:

> vNIC de host de NSX : Segment_autodeploy

> Instancia de Netstack

Configuración de volcados de núcleos de red

> Configuración general del sistema

> Opciones de configuración avanzadas

> Otro

> Seguridad y servicios

vNIC de host de NSX : Segment_autodeploy

Determinar la instancia de LogicSwitch a la que debe conectarse esta NIC virtual

Elija que un LogicSwitch se conecte con

*Nombre de LogicSwitch

Segment_autodeploy

Determinar cuándo se creará la NIC virtual en LogicSwitch

Crear siempre el objeto

Propiedades de arranque sin estado para NIC virtual en LogicSwitch

Parámetros de configuración de arranque sin estado (consultar el documento antes de hacer cambios)

*VLAN (consultar el documento antes de hacer cambios)	0
*Directiva de formación (consultar el documento antes de hacer cambios)	first uplink
Vínculos superiores activos que se utilizaron (consultar el documento antes de hacer cambios).	vmnic1
Vínculos superiores en espera que se utilizaron (consultar el documento antes de hacer cambios).	--
*Nombre de OpaqueSwitch utilizado (consultar el documento antes de hacer cambios)	vds-1

> Configuración de redes

> Conmutador estándar

> Grupo de puertos de máquina virtual

> Grupo de puertos del host

> Configuración de NIC física

vSphere Distributed Switch

NIC virtual de host

> vNIC de host de NSX:

> vNIC de host de NSX : Segment_autodeploy

> Instancia de Netstack

Configuración de volcados de núcleos de red

> Configuración general del sistema

> Opciones de configuración avanzadas

> Otro

> Seguridad y servicios

Determinar de qué manera se debe decidir la dirección MAC para vmknic

Solicitarle al usuario la dirección MAC si no hay un valor predeterminado disponible

Directiva de nomenclatura del adaptador de red de VMkernel

Nombre de interfaz asignado

Adaptador de red de VMkernel

vmk1

Directiva de MTU

Asignar la MTU especificada

*MTU

1500

Pila de TCP/IP:

Instancia de Netstack donde se conectará vmknic

*Nombre

defaultTcpipStack

Resultados

El perfil de host contiene la configuración relativa a ESXi y NSX cuando se preparó el host para los dos entornos.

Pasos siguientes

Verifique la asociación del perfil de host con el clúster sin estado. Consulte [Verificar la asociación del perfil de host con el clúster sin estado](#).

Verificar la asociación del perfil de host con el clúster sin estado

Para preparar el clúster sin estado de destino con la configuración de ESXi y NSX, asocie el perfil de host extraído del host de referencia con el clúster sin estado de destino.

Sin el perfil de host asociado al clúster sin estado, los nodos nuevos que se unen al clúster no se podrán implementar automáticamente con los VIB de ESXi y NSX.

Procedimiento

- 1 Asocie el perfil de host al clúster sin estado o sepárelo. Consulte [Asociar o separar entidades de un perfil de host](#).
- 2 En la pestaña Hosts implementados, compruebe que el host sin estado existente esté asociado con la imagen correcta y el perfil de host.
- 3 Si falta la asociación del perfil de host, seleccione el host de destino y haga clic en Corregir asociaciones de hosts para forzar la actualización de la imagen y el perfil de host en el host de destino.

Almacenes de software	Reglas de implementación	Hosts implementados	Hosts detectados	Paquetes de scripts	Configuración
<p>El perfil de imagen, perfil de host y ubicación que Auto Deploy asoció con los hosts se indican a continuación. Las asociaciones podrían diferir del estado actual del host.</p> <p>COMPROBAR CUMPLIMIENTO DE ASOCIACIONES DE HOSTS... CORREGIR ASOCIACIONES DE HOSTS EDITAR ASOCIACIÓN DE PERFIL DE IMAGEN</p>					
<input type="checkbox"/>	Host	Perfil de imagen asociado	Perfil de host asociado	Ubicación asociada	Paquete de scripts asociado
<input type="checkbox"/>	10.144.139.147	CustomDepot(ESXi and NSX)		1-datacenter-1964	
<input type="checkbox"/>	10.144.137.225	CustomDepot(ESXi and NSX)	Host Profile_ReferenceHost	Statless-Cluster	

Pasos siguientes

Actualice las personalizaciones de host. Consulte [Actualizar las personalizaciones de host](#).

Actualizar las personalizaciones de host

Después de asociar el perfil de host con el clúster de destino, es posible que el host necesite entradas personalizadas adicionales para poder implementar de forma automática y correcta los paquetes de ESXi y NSX-T.

Procedimiento

- 1 Después de asociar el perfil de host con el clúster de destino, si los hosts no se actualizan con los valores personalizados, el sistema mostrará el mensaje que se incluye a continuación.

Host Profile


ACCIONES

Resumen

Supervisar

Configurar

Hosts



Nombre: Host Profile

Descripción:

Creado el: 07-nov-2019 14:36

Última modificación: 07-nov-2019 14:36

Versión: 6.7.0

El host 10.160.183.211 requiere personalización adicional.

El host 10.160.170.243 requiere personalización adicional.

- 2 Para actualizar las personalizaciones de host, desplácese hasta el perfil de host y haga clic en **Acciones -> Editar personalizaciones de host**.

- Para las versiones 67ep6, 67ep7 y 67u2 de ESXi, introduzca la contraseña de usuario de MUX.

Customize hosts

Enter host customizations.

IMPORT HOST CUSTOMIZATIONS ⓘ

Required	Property Name	Path	Value
No	MAC Address	Networking configu...	02:00:0c:23:e9:9a
Yes	Adapter MA...	Storage configurati...	02:00:0c:23:e9:9a
Yes	Activate	Storage configurati...	false
Yes	Password	Security and...	Security and Services > Security Settings > Security > User Configuration > mux_user > Pass...

- Compruebe que todos los campos obligatorios se actualicen con los valores correspondientes.

Pasos siguientes

Active la implementación automática en los hosts de destino. Consulte [Activar la implementación automática en los hosts de destino](#).

Activar la implementación automática en los hosts de destino

Cuando se agrega un nodo nuevo al clúster, necesita reiniciarlo manualmente para que los VIB de ESXi y NSX-T se configuren.

Nota Solo se aplica a los hosts sin estado.

Puede utilizar dos métodos para preparar los hosts con fin de activar la implementación automática de los VIB ESXi y NSX-T para que se configuren.

- Reinicie los hosts antes de aplicar el TNP al clúster sin estado.
- Reinicie los hosts después de aplicar el TNP al clúster sin estado.

Si quiere migrar adaptadores de VMkernel cuando instale NSX-T en los hosts, consulte:

- [Escenarios en los que el host sin estado está dentro del clúster de destino](#)
- [Escenarios en los que el host sin estado está fuera del clúster de destino](#)

Pasos siguientes

Reinicie los hosts antes de aplicar el TNP al clúster sin estado. Consulte [Reiniciar hosts antes de aplicar el TNP](#).

Reiniciar hosts antes de aplicar el TNP

Solo se aplica a los hosts sin estado. En este escenario, el perfil de nodo de transporte no se aplica al clúster sin estado, lo que significa que NSX-T no está instalado ni configurado en el host de destino.

Procedimiento

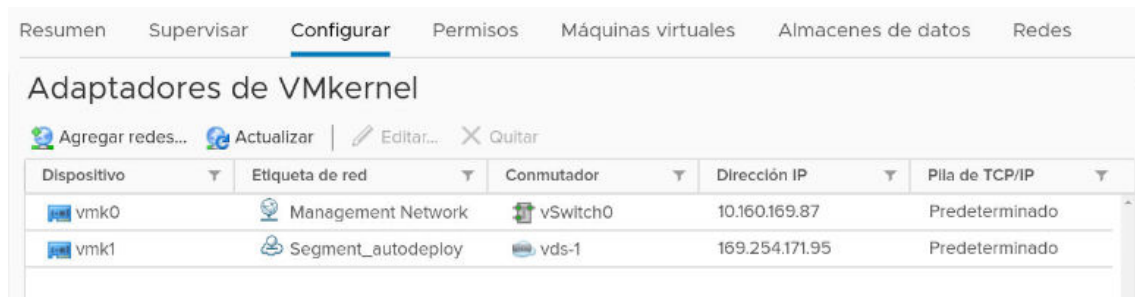
1 Reinicie los hosts.

El host de destino se inicia con la imagen de ESXi. Después de iniciarse, el host de destino permanece en modo de mantenimiento hasta que el perfil de TNP se aplica al host de destino y se completa la instalación de NSX-T. Los perfiles se aplican a los hosts en el siguiente orden:

Los perfiles se aplican a los hosts en el orden que se indica a continuación.

- El perfil de imagen se aplica al host.
- La configuración del perfil de imagen se aplica al host.
- La configuración de NSX-T se aplica al host.

2 En el host ESXi, el adaptador de VMkernel se asocia a un segmento temporal denominado <N-LogicalSegment> porque el host todavía no es un nodo de transporte. Después de instalar NSX-T, el conmutador temporal se sustituye por el conmutador N-VDS real y el segmento lógico.



Dispositivo	Etiqueta de red	Conmutador	Dirección IP	Pila de TCP/IP
vmk0	Management Network	vSwitch0	10.160.169.87	Predeterminado
vmk1	Segment_autodeploy	vds-1	169.254.171.95	Predeterminado

Los VIB de ESXi se aplican a todos los hosts reiniciados. Un conmutador de NSX temporal en un host ESXi. Cuando el TNP se aplica a los hosts, el conmutador temporal se sustituye por el conmutador de NSX-T real.

Pasos siguientes

Aplique el TNP al clúster sin estado. Consulte [Aplicar un TNP a un clúster sin estado](#).

Aplicar un TNP a un clúster sin estado

NSX-T solo se configura e instala en los hosts de destino cuando se aplica un perfil de nodo de transporte (Transport Node Profile, TNP) al clúster.

Procedimiento

- 1 Anote los ajustes extraídos del host de referencia en el perfil de host. Las entidades correspondientes del TNP deben tener el mismo valor. Por ejemplo, el nombre del N-VDS debe ser igual en el perfil de host y el TNP.

Para obtener más información sobre los ajustes del perfil de host extraído, consulte [Extraer el perfil de host y verificarlo](#).

- 2 Agregue un TNP. Consulte [Agregar perfil de nodo de transporte](#).
- 3 Asegúrese de que los valores de los siguientes parámetros coincidan tanto en el TNP nuevo como en el perfil de host existente.
 - Nombre del N-VDS: verifique que el nombre del N-VDS al que se hace referencia en el perfil de host sea igual que el del TNP.
 - Perfil de vínculo superior: asegúrese de que el perfil de vínculo superior incluido en el perfil de host sea igual que el del TNP.
 - PNIC: al asignar una NIC física a un perfil de vínculo superior, primero verifique la NIC usada en el perfil de host y, a continuación, asigne esa NIC física al perfil de vínculo superior.
 - Asignaciones de red para instalación: al asignar una red durante la instalación, primero verifique qué VMkernel se asigna a cada segmento en el perfil de host y agregue la misma asignación al TNP.
 - Asignaciones de red para desinstalación: al asignar una red durante la desinstalación, primero verifique qué VMkernel se asigna a cada conmutador VSS o DVS en el perfil de host y agregue la misma asignación al TNP.

- 4 Para agregar un TNP, introduzca todos los campos requeridos. Consulte [Agregar perfil de nodo de transporte](#).

Asegúrese de que los valores de los siguientes parámetros coincidan tanto en el TNP nuevo como en el perfil de host existente.

- Zona de transporte: asegúrese de que la zona de transporte incluida en el perfil de host coincida con la del TNP.
- Nombre del N-VDS: verifique que el nombre del N-VDS al que se hace referencia en el perfil de host sea igual que el del TNP.
- Perfil de vínculo superior: compruebe que el perfil de vínculo superior incluido en el perfil de host sea igual que el del TNP.
- PNIC: al asignar una NIC física a un perfil de vínculo superior, primero verifique la NIC usada en el perfil de host y, a continuación, asigne esa NIC física al perfil de vínculo superior.
- Asignaciones de red para instalación: al asignar una red durante la instalación, primero verifique qué VMkernel se asigna a cada conmutador lógico en el perfil de host y agregue la misma asignación al TNP.

- Asignaciones de red para desinstalación: al asignar una red durante la desinstalación, primero verifique qué VMkernel se asigna a cada conmutador VSS/DVS en el perfil de host y agregue la misma asignación al TNP.

Nombre del N-VDS * vds-tzvlan

Zonas de transporte asociadas tz-33

Perfil de NIOC * nsx-default-nioc-hostswitch-profile

[O crear nuevo perfil de NIOC](#)

Perfil de vínculo superior * nsx-default-uplink-hostswitch-profile

[O crear nuevo perfil de vínculo superior](#)

Perfil de LLDP * LLDP [Send Packet Enabled]

Asignación de IP *

NIC físicas vmnic1 uplink-1

[Agregar PNIC](#)

Migración solamente de PNIC ☐ No

Habilite esta opción si no hay VMK en PNIC seleccionados para la migración

Asignaciones de red para instalación 1 asignación

Asignaciones de red para desinstalación [Agregar asignación](#)

Después de aplicar el TNP a los nodos de destino, si la configuración del TNP no coincide con la configuración del perfil de host, el nodo podría no aparecer por errores de conformidad.

- 5 Compruebe que el perfil de TNP se cree correctamente.

- 6 Aplique el TNP al clúster de destino y haga clic en **Guardar**.



- 7 Compruebe que el TNP se aplique correctamente al clúster de destino. Esto significa que NSX se configuró correctamente en todos los nodos del clúster.
- 8 En vSphere, verifique que las NIC físicas o los adaptadores de VMkernel estén adjuntos al conmutador de N-VDS.

Agregar redes... Actualizar Editar... Quitar				
Dispositivo	Etiqueta de red	Conmutador	Dirección IP	Pila de TCP/IP
vmk0	Management Network	vSwitch0	10.160.169.87	Predeterminado
vmk1	Segment_autodeploy	vds-1	169.254.171.95	Predeterminado

- 9 En NSX, verifique que el host ESXi esté configurado correctamente como nodo transporte.

Pasos siguientes

También puede reiniciar un host de destino después de aplicar el TNP al clúster. Consulte [Reiniciar hosts después de aplicar el TNP](#).

Reiniciar hosts después de aplicar el TNP

Solo se aplica a los hosts sin estado. Cuando agregue un nodo nuevo al clúster, reinicie manualmente el nodo para que los paquetes de ESXi y NSX-T se configuren en él.

Procedimiento

- 1 Aplique el TNP al clúster sin estado que ya esté preparado con el perfil de host. Consulte [Crear y aplicar un TNP a un clúster sin estado](#).
- 2 Reinicie los hosts.

Después de aplicar el perfil de TNP al clúster sin estado, al reiniciar cualquier nodo nuevo que se una al clúster, se configurará automáticamente con NSX-T en el host.

Pasos siguientes

Asegúrese de reiniciar todos los nodos nuevos que se unan al clúster para que ESXi y NSX-T se implementen y configuren automáticamente en el nodo reiniciado.

Para solucionar problemas relacionados con los perfiles de host y de nodo de transporte al configurar la implementación automática, consulte [Solucionar problemas del perfil de host y el perfil de nodo de transporte](#).

Escenarios en los que el host sin estado está dentro del clúster de destino

En esta sección, se analizan casos prácticos en los que hay un host sin estado dentro del clúster de destino.

Importante En un host de destino sin estado:

- No puede migrar el adaptador de vmk0 desde VSS o DVS hasta N-DVS en NSX-T 2.4 y NSX-T 2.4.1.
 - Se puede migrar el adaptador de vmk0 desde VSS o DVS hasta N-VDS en NSX-T 2.5.
-

Host de destino	Configuración del host de referencia	Pasos para activar el servicio Auto Deploy en los hosts de destino
El host de destino tiene el adaptador de vmk0 configurado.	El perfil de host extraído del host de referencia tiene vmk0 configurado en un conmutador N-VDS. En NSX-T, TNP solo tiene configurada la asignación de migraciones de vmk0.	<ol style="list-style-type: none"> 1 Asocie el perfil de host al host de destino. El adaptador de vmk0 se asocia a un conmutador vSwitch. 2 Actualice las personalizaciones del host, si fuera necesario. 3 Reinicie el host. El perfil de host se aplica al host. vmk0 se asocia a un conmutador temporal. 4 Aplique el TNP. El adaptador de vmk0 se migra a N-VDS. El host de destino se implementó correctamente con los VIB de ESXi y NSX-T.
El host de destino tiene el adaptador de vmk0 configurado.	El perfil de host extraído del host de referencia tiene vmk0 en vSwitch y vmk1 en un conmutador N-VDS. En NSX-T, TNP solo tiene configurada la asignación de migraciones de vmk1.	<ol style="list-style-type: none"> 1 Asocie el perfil de host al host de destino. El adaptador de vmk0 se asocia a un conmutador vSwitch, pero vmk1 no aplica a ningún conmutador. 2 Actualice las personalizaciones del host, si fuera necesario. 3 Reinicie el host. vmk0 se asocia a un conmutador vSwitch y vmk1 se asocia a un conmutador de NSX temporal. 4 Aplique TNP. El adaptador de vmk1 se migra a N-VDS. 5 (Opcional) Si el host continúa no siendo conforme con el perfil de host, reinicie el host para que sea compatible. El host de destino se implementó correctamente con los VIB de ESXi y NSX-T.
El host de destino tiene el adaptador de vmk0 configurado.	El perfil de host extraído del host de referencia tiene vmk0 configurado en un conmutador vSwitch y vmk1 en un conmutador N-VDS. En NSX-T, el TNP tiene configuradas las asignaciones de migraciones de vmk0 y vmk1.	<ol style="list-style-type: none"> 1 Asocie el perfil de host al host de destino. El adaptador de vmk0 se asocia a un conmutador vSwitch, pero vmk1 no aplica a ningún conmutador. 2 Actualice las personalizaciones del host, si fuera necesario. 3 Reinicie el host. El adaptador de vmk0 se asocia a un conmutador vSwitch y vmk1 se asocia a un conmutador de NSX temporal. 4 Aplique TNP. 5 (Opcional) Si el host continúa no siendo conforme con el perfil de host, reinicie el host para que sea compatible. El host de destino se implementó correctamente con los VIB de ESXi y NSX-T.

Host de destino	Configuración del host de referencia	Pasos para activar el servicio Auto Deploy en los hosts de destino
El host de destino tiene adaptadores de vmk0 y vmk1 configurados.	El perfil de host extraído del host de referencia tiene configurado vmk0 en vSwitch y vmk1 en un conmutador N-VDS. En NSX-T, TNP tiene configurada la asignación de migraciones de vmk1.	<ol style="list-style-type: none"> 1 Asocie el perfil de host al host de destino. Los adaptadores de vmk0 y vmk1 se asocian a un conmutador vSwitch. 2 Actualice las personalizaciones del host, si fuera necesario. 3 Reinicie el host. 4 Aplique TNP. El adaptador de vmk0 se asocia a un conmutador vSwitch y vmk1 se asocia a un conmutador N-VDS. 5 (Opcional) Si el host continúa no siendo conforme con el perfil de host, reinicie el host para que sea compatible. El host de destino se implementó correctamente con los VIB de ESXi y NSX-T.
El host de destino tiene adaptadores de vmk0 y vmk1 configurados.	El perfil de host extraído del host de referencia tiene configurados vmk0 y vmk1 en un conmutador N-VDS. En NSX-T, el TNP tiene configuradas las asignaciones de migraciones de vmk0 y vmk1.	<ol style="list-style-type: none"> 1 Asocie el perfil de host al host de destino. Los adaptadores de vmk0 y vmk1 se asocian a un conmutador vSwitch. 2 Actualice las personalizaciones del host, si fuera necesario. 3 Reinicie el host. 4 Aplique TNP. vmk0 y vmk1 se migran a un conmutador N-VDS. El host de destino se implementó correctamente con los VIB de ESXi y NSX-T.

Escenarios en los que el host sin estado está fuera del clúster de destino

En esta sección, se analizan casos prácticos en los que hay un host sin estado fuera del clúster de destino.

Importante En los hosts sin estado:

- No puede migrar el adaptador de vmk0 desde VSS o DVS hasta N-DVS en NSX-T 2.4 y NSX-T 2.4.1.
- Se puede migrar el adaptador de vmk0 desde VSS o DVS hasta N-VDS en NSX-T 2.5.

Estado del host de destino	Configuración del host de referencia	Pasos para activar el servicio Auto Deploy en los hosts de destino
<p>El host está en estado apagado (primera vez que se inicia). Posteriormente, se agrega al clúster.</p> <p>Se configura la regla de Auto Deploy predeterminada para el clúster de destino y se asocia con el perfil de host.</p> <p>El TNP se aplica en el clúster.</p>	<p>El perfil de host extraído del host de referencia tiene configurado el adaptador de VMkernel 0 (vmk0) en vSwitch y el adaptador de VMkernel 1 (vmk1) en un conmutador N-VDS.</p> <p>En NSX-T, TNP solo tiene configurada la asignación de migraciones de vmk1.</p>	<ol style="list-style-type: none"> 1 Encienda el host. <p>Después de encenderlo:</p> <ul style="list-style-type: none"> ■ El host se agrega al clúster. ■ El perfil de host se aplica al host de destino. ■ El adaptador de vmk0 se encuentra en vSwitch y el adaptador de vmk1 en un conmutador temporal. ■ Se activa el TNP. ■ Una vez que se aplica el TNP al clúster, el adaptador de vmk0 se encuentra en vSwitch y vmk1 se migra al conmutador N-VDS. <ol style="list-style-type: none"> 2 (Opcional) Si el host continúa no siendo conforme con el perfil de host, reinicie el host para que sea compatible. <p>El host se implementó correctamente con los VIB de ESXi y NSX-T.</p>
<p>El host está en estado apagado (primera vez que se inicia). Posteriormente, se agrega al clúster.</p> <p>Se configura la regla de Auto Deploy predeterminada para el clúster de destino y se asocia con el perfil de host.</p> <p>El TNP se aplica en el clúster.</p>	<p>El perfil de host extraído del host de referencia tiene configurados el adaptador de VMkernel 0 (vmk0) y el adaptador de VMkernel 1 (vmk1) en un conmutador N-VDS.</p> <p>En NSX-T, TNP tiene configuradas las migraciones de vmk0 y vmk1.</p>	<ol style="list-style-type: none"> 1 Encienda el host. <p>Después de encenderlo:</p> <ul style="list-style-type: none"> ■ El host se agrega al clúster. ■ El perfil de host se aplica al host de destino. ■ Los adaptadores de vmk0 y vmk1 se encuentran en un conmutador temporal. ■ Se activa el TNP. ■ Una vez que se aplica el TNP al clúster, el adaptador de vmk0 y vmk1 se migran al conmutador N-VDS. <p>El host se implementó correctamente con los VIB de ESXi y NSX-T.</p>
<p>El host está en estado encendido. Posteriormente, se agrega al clúster.</p> <p>Se configura la regla de Auto Deploy predeterminada para el clúster de destino y se asocia con el perfil de host.</p> <p>El host de destino solo tiene un adaptador de vmk0 configurado.</p>	<p>El perfil de host extraído del host de referencia tiene configurado el adaptador de VMkernel 0 (vmk0) en vSwitch y el adaptador de VMkernel 1 (vmk1) en un conmutador N-VDS.</p> <p>En NSX-T, el TNP tiene configurada la asignación de migraciones de vmk1.</p>	<ol style="list-style-type: none"> 1 Traslade el host al clúster. 2 Reinicie el host. <p>Una vez que se reinicia el host, el perfil de host se aplica al host de destino.</p> <ul style="list-style-type: none"> ■ El adaptador de vmk0 se asocia a un conmutador vSwitch, mientras que el adaptador de vmk1 se asocia a un conmutador de NSX temporal. ■ Se activa el TNP. ■ vmk1 se migra al conmutador N-VDS. <ol style="list-style-type: none"> 3 (Opcional) Si el host continúa no siendo conforme con el perfil de host, reinicie el host para que sea compatible. <p>El host se implementó correctamente con los VIB de ESXi y NSX-T.</p>

Estado del host de destino	Configuración del host de referencia	Pasos para activar el servicio Auto Deploy en los hosts de destino
<p>El host está en estado encendido. Posteriormente, se agrega al clúster.</p> <p>Se configura la regla de Auto Deploy predeterminada para el clúster de destino y se asocia con el perfil de host.</p> <p>El host de destino solo tiene un adaptador de vmk0 configurado.</p>	<p>El perfil de host extraído del host de referencia tiene configurados el adaptador de VMkernel 0 (vmk0) y el adaptador de VMkernel 1 (vmk1) en un conmutador N-VDS.</p> <p>En NSX-T, el TNP tiene configuradas las migraciones de vmk0 y vmk1.</p>	<ol style="list-style-type: none"> 1 Traslade el host al clúster. 2 Reinicie el host. <p>Una vez que se reinicia el host, el perfil de host se aplica al host de destino.</p> <ul style="list-style-type: none"> ■ Los adaptadores de vmk0 y vmk1 se asocian a un conmutador de NSX temporal. ■ Se activa el TNP. ■ vmk0 y vmk1 se asocian a un conmutador N-VDS. <p>El host se implementó correctamente con los VIB de ESXi y NSX-T.</p>
<p>El host está en estado encendido. Posteriormente, se agrega al clúster.</p> <p>Se configura la regla de Auto Deploy predeterminada para el clúster de destino y se asocia con el perfil de host.</p> <p>El host de destino tiene configuradas las asignaciones de red de vmk0 y vmk1.</p>	<p>El perfil de host extraído del host de referencia tiene configurado el adaptador de VMkernel 0 (vmk0) en vSwitch y el adaptador de VMkernel 1 (vmk1) en un conmutador N-VDS.</p> <p>En NSX-T, el TNP tiene configurada la migración de vmk1.</p>	<ol style="list-style-type: none"> 1 Traslade el host al clúster. 2 Reinicie el host. <p>Una vez que se reinicia el host, el perfil de host se aplica al host de destino.</p> <ul style="list-style-type: none"> ■ El adaptador de vmk0 se asocia a un conmutador vSwitch, mientras que el adaptador de vmk1 se asocia a un conmutador de NSX temporal. ■ Se activa el TNP. ■ vmk1 se migra al conmutador N-VDS. <ol style="list-style-type: none"> 3 (Opcional) Si el host continúa no siendo conforme con el perfil de host, reinicie el host para que sea compatible. <p>El host se implementó correctamente con los VIB de ESXi y NSX-T.</p>
<p>El host está en estado encendido. Posteriormente, se agrega al clúster.</p> <p>Se configura la regla de Auto Deploy predeterminada para el clúster de destino y se asocia con el perfil de host.</p> <p>El host tiene configuradas las asignaciones de red de vmk0 y vmk1.</p>	<p>En el host de referencia, el perfil de host tiene configurados el adaptador de VMkernel 0 (vmk0) y el adaptador de VMkernel 1 (vmk1) en un conmutador N-VDS.</p> <p>En NSX-T, el TNP tiene configuradas las migraciones de vmk0 y vmk1.</p>	<ol style="list-style-type: none"> 1 Traslade el host al clúster. 2 Reinicie el host. <p>Una vez que se reinicia el host, el perfil de host se aplica al host de destino.</p> <ul style="list-style-type: none"> ■ Los adaptadores de vmk0 y vmk1 se asocian a un conmutador de NSX temporal. ■ Se activa el TNP. ■ Los adaptadores de vmk0 y vmk1 se migran a un conmutador N-VDS. <p>El host se implementó correctamente con los VIB de ESXi y NSX-T.</p>

Solucionar problemas del perfil de host y el perfil de nodo de transporte

Solucione los problemas relacionados con los perfiles de host y los TNP cuando se utilizan con clústeres sin estado con Auto Deploy.

Escenario	Descripción
El perfil de host no es portátil.	<p>Problema: ninguno de los vCenter Server puede utilizar el perfil de host que incluye la configuración de NSX-T.</p> <p>Solución alternativa: ninguna.</p>
Motor de reglas de Auto Deploy	<p>Problema: no se puede utilizar el perfil de host en las reglas de Auto Deploy para implementar clústeres nuevos. Si se implementan clústeres nuevos, los hosts se implementarán con redes básicas y permanecerán en modo de mantenimiento.</p> <p>Solución alternativa: prepare cada clúster a partir de la interfaz gráfica de usuario de NSX-T. Consulte Aplicar un TNP a un clúster sin estado.</p>
Compruebe si existen errores de conformidad.	<p>Problema: la solución para el perfil de host no puede corregir los errores de conformidad relacionados con la configuración de NSX-T.</p> <ul style="list-style-type: none"> ■ Las NIC físicas configuradas en el perfil de host y el TNP son diferentes. ■ En la asignación de vNIC y conmutadores lógicos, el perfil de host encuentra una falta de coincidencia con respecto al perfil de TNP. ■ El VMkernel conectado a N-VDS no coincide en el perfil de host y el TNP. ■ El conmutador opaco no coincide en el perfil de host y el TNP. <p>Solución alternativa: asegúrese de que la configuración de NSX-T sea la misma en el perfil de host y el TNP. Reinicie el host para aplicar los cambios de configuración. El host se encenderá.</p>
Corrección	<p>Problema: si hay algún error de conformidad específico de NSX-T, la solución para el perfil de host de ese clúster se bloquea.</p> <p>Configuración incorrecta:</p> <ul style="list-style-type: none"> ■ Asignación de vNIC y conmutadores lógicos ■ Asignación de NIC físicas <p>Solución alternativa: asegúrese de que la configuración de NSX-T sea la misma en el perfil de host y el TNP. Reinicie el host para aplicar los cambios de configuración. El host se encenderá.</p>
Asociar	<p>Problema: en un clúster configurado con NSX-T, el perfil de host no se puede asociar a un host.</p> <p>Solución alternativa: ninguna.</p>
Desasociar	<p>Problema: al desasociar y asociar un perfil de host nuevo en un clúster configurado con NSX-T no se elimina la configuración de NSX-T. Aunque el clúster sea conforme con el perfil de host que se acaba de asociar, sigue teniendo la configuración de NSX-T de un perfil anterior.</p> <p>Solución alternativa: ninguna.</p>
Actualizar	<p>Problema: si el usuario cambió la configuración de NSX-T en el clúster, extraiga un perfil de host nuevo. Actualice todos los ajustes del perfil de host que se hayan perdido manualmente.</p> <p>Solución alternativa: ninguna.</p>
Configuración de nodo de transporte en el host	<p>Problema: después de implementar automáticamente el nodo anportsport, se comporta como una entidad independiente. Puede que las actualizaciones de ese nodo de transporte no coincidan con el TNP.</p> <p>Solución alternativa: actualice el clúster. Ninguna actualización de un nodo de transporte independiente puede persistir en su especificación de migración. Es posible que la migración no pueda compartir el reinicio.</p>

Escenario	Descripción
No se puede aplicar el perfil de host porque no se restableció la contraseña y la directiva de contraseñas de mux_user.	<p>Problema: solo en hosts que ejecutan versiones anteriores a vSphere 6.7 U3. Es posible que la solución para el host y la aplicación de perfil de host de los hosts produzcan errores a menos restablezca la contraseña de mux_user.</p> <p>Solución alternativa: en Directivas y perfiles, edite el perfil de host para modificar la directiva de contraseñas de mux_user password policy y restablezca la contraseña de mux_user.</p>
No se admite la configuración de PeerDNS en el adaptador de VMkernel seleccionado para la migración al conmutador N-VDS.	<p>Problema: si el adaptador de VMkernel seleccionado para la migración a N-VDS está habilitado para DNS del mismo nivel, la aplicación del perfil de host no funcionará correctamente.</p> <p>Solución alternativa: edite el perfil de host extraído. Para ello, deshabilite la configuración de DNS del mismo nivel en el adaptador de VMkernel que debe migrarse a un conmutador N-VDS. También puede asegurarse de que no se migren los adaptadores de VMkernel habilitados para DNS del mismo nivel a un conmutador N-VDS.</p>
No se guarda la dirección DHCP de la dirección de la NIC de VMkernel	<p>Problema: si el host de referencia tiene estado, los hosts sin estado que utilizan el perfil extraído del host de referencia con estado no pueden guardar la dirección MAC de administración de VMkernel derivada de la dirección MAC desde la que se arrancó el sistema con PXE. Esto genera problemas relacionados con las direcciones DHCP.</p> <p>Solución alternativa: edite el perfil de host extraído del host con estado y cambie la opción "Determinar de qué manera se debe decidir la dirección MAC para vmknic" a "Utilizar la dirección MAC desde la cual el sistema se arrancó con PXE".</p>
El error de la aplicación del perfil de host en vCenter puede provocar problemas con la configuración de NSX en el host.	<p>Problema: si la aplicación del perfil de host no funciona correctamente en vCenter, la configuración de NSX también puede fallar.</p> <p>Solución alternativa: en vCenter, compruebe que el perfil de host se aplicó correctamente. Corrija los errores e inténtelo de nuevo.</p>
No se admiten los LAG en los hosts ESXi sin estado.	<p>Problema: el perfil de vínculo superior configurado como LAG en NSX no se admite en un host ESXi sin estado administrado por un vCenter Server o en NSX.</p> <p>Solución alternativa: ninguna.</p>

Desinstalar NSX-T Data Center de un nodo de transporte de host

10

Los pasos para desinstalar NSX-T Data Center de un nodo de transporte de host varían según el tipo de host y según la forma en la que está configurado.

- [Comprobar las asignaciones de red de host para la desinstalación](#)

Antes de desinstalar NSX-T Data Center de un host ESXi, compruebe que dispone de las asignaciones de red adecuadas para la desinstalación configurada. Las asignaciones son obligatorias si el host ESXi tiene interfaces de VMkernel conectadas a N-VDS.

- [Desinstalar NSX-T Data Center de un clúster de vSphere](#)

Si instaló NSX-T Data Center en un clúster de vSphere mediante perfiles de nodo de transporte, puede seguir estas instrucciones para desinstalar NSX-T Data Center de todos los hosts del clúster.

- [Desinstalar NSX-T Data Center de un host en un clúster de vSphere](#)

Puede desinstalar NSX-T Data Center de un único host administrado por vCenter Server. Los otros hosts del clúster no se ven afectados.

- [Desinstalar NSX-T Data Center de un host independiente](#)

Puede desinstalar NSX-T Data Center de un host independiente. Los hosts independientes pueden ser ESXi o KVM.

Comprobar las asignaciones de red de host para la desinstalación

Antes de desinstalar NSX-T Data Center de un host ESXi, compruebe que dispone de las asignaciones de red adecuadas para la desinstalación configurada. Las asignaciones son obligatorias si el host ESXi tiene interfaces de VMkernel conectadas a N-VDS.

La asignación de desinstalación determina dónde se conectan las interfaces después de la desinstalación. Hay asignaciones de desinstalación para las interfaces físicas (vmnicX) y las interfaces de VMkernel (vmkX). Al realizar la desinstalación, las interfaces de VMkernel se mueven de sus conexiones actuales a los grupos de puertos especificados en la asignación de desinstalación. Si se incluye una interfaz física en la asignación de desinstalación, la interfaz física se conecta a vSphere Distributed Switch o vSphere Standard Switch según el grupo de puertos de destino de las interfaces de VMkernel.

Precaución Desinstalar NSX-T Data Center de un host ESXi resulta disruptivo si las interfaces físicas o las interfaces de VMkernel están conectadas a N-VDS. Si el host o el clúster participan en otras aplicaciones, como vSAN, es posible que estas aplicaciones se vean afectadas por la desinstalación.

Hay dos lugares en los que puede configurar asignaciones de red para desinstalar.

- En la configuración del nodo de transporte, que se aplica a ese host.
- En una configuración de perfil de nodo de transporte, que se puede aplicar a un clúster.

Nota Debe tener un administrador de equipos configurado para aplicar un perfil de nodo de transporte a un clúster.

Si se configura un administrador de equipo, un host puede tener una configuración de nodo de transporte y una configuración de perfil de nodo de transporte. Si ambas existen, la configuración de nodo de transporte está activa. Compruebe que las asignaciones de red para la desinstalación estén configuradas correctamente en la configuración activa.

En este ejemplo, se aplicó el perfil de nodo de transporte TNP-1 al clúster cluster-1. El host tn-1 muestra un "Error de coincidencia de configuración". Este mensaje de falta de coincidencia indica que se ha aplicado una configuración diferente a tn-1. La falta de coincidencia se conserva hasta que la configuración del nodo de transporte coincide con la configuración del perfil de nodo de transporte. El nodo de transporte tn-2 utiliza las asignaciones de red del perfil de nodo de transporte, mientras que el nodo de transporte tn-1 utiliza su propia configuración.

 CONFIGURAR NSX  QUITAR NSX  ACCIONES ▾					
<input type="checkbox"/>	Nodo	Identific	Direccion	Tipo de si	Configuración de NSX
<input type="checkbox"/>	 New Cluster (2)	MoR...			 TNP-1
<input type="checkbox"/>	tn-1	926...	10....	ESXi ...	 Error de coincidencia de configuración
<input type="checkbox"/>	tn-2	901f....	10....	ESXi ...	Configurado

Requisitos previos

- Compruebe que tiene los grupos de puertos adecuados configurados para usarlos en la asignación de desinstalación. Debe utilizar grupos de puertos efímeros de vSphere Distributed Switch o grupos de puertos de vSphere Standard Switch.

- Configure un administrador de equipos si desea utilizar un grupo de puertos de vSphere Distributed Switch en las asignaciones de desinstalación de un host ESXi independiente. Consulte [Agregar un administrador de equipos](#). Si no hay ningún administrador de equipos configurado, debe utilizar un grupo de puertos de vSphere Standard Switch.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión con privilegios de administrador en NSX Manager.
- 2 Seleccione **Sistema > Tejido > Nodos > Nodos de transporte de host**.
- 3 Para cada host que desee desinstalar, compruebe que la asignación de red para la desinstalación incluya un grupo de puertos para cada interfaz de VMkernel que se encuentre en N-VDS. Agregue las asignaciones que falten.

Importante El grupo de puertos de la asignación de red para la desinstalación debe ser un grupo de puertos efímeros de vSphere Distributed Switch o un grupo de puertos de vSphere Standard Switch.

- a Para ver las interfaces de VMkernel, inicie sesión en vCenter Server, seleccione el host y haga clic en **Configurar > Adaptadores de VMkernel**.
- b Si la configuración del nodo de transporte es la configuración activa, seleccione el host y haga clic en **Editar** (para los hosts independientes) o en **Configurar NSX** (para los hosts administrados). Haga clic en **Siguiente** y, a continuación, en **Asignaciones de red para desinstalación**. Consulte las asignaciones en las pestañas **Asignaciones de VMKNic** y **Asignaciones de NIC física**.
- c Si el perfil del nodo de transporte es la configuración activa, haga clic en el nombre del perfil del nodo de transporte del clúster en la columna **Configuración de NSX** y, a continuación, en **Editar**. En la pestaña **N-VDS**, haga clic en **Asignaciones de red para desinstalación**. Consulte las asignaciones en las pestañas **Asignaciones de VMKNic** y **Asignaciones de NIC física**.

Desinstalar NSX-T Data Center de un clúster de vSphere

Si instaló NSX-T Data Center en un clúster de vSphere mediante perfiles de nodo de transporte, puede seguir estas instrucciones para desinstalar NSX-T Data Center de todos los hosts del clúster.

Para obtener más información sobre los perfiles de nodo de transporte, consulte [Agregar perfil de nodo de transporte](#).

Precaución Desinstalar NSX-T Data Center de un host ESXi resulta disruptivo si las interfaces físicas o las interfaces de VMkernel están conectadas a N-VDS. Si el host o el clúster participan en otras aplicaciones, como vSAN, es posible que estas aplicaciones se vean afectadas por la desinstalación.

Si no utilizó un perfil de nodo de transporte para instalar NSX-T Data Center, o si desea quitar NSX-T Data Center de un subconjunto de los hosts del clúster, consulte [Desinstalar NSX-T Data Center de un host en un clúster de vSphere](#).

Nota Al quitar un host de un clúster no se desinstala NSX-T Data Center. Siga estas instrucciones para desinstalar NSX-T Data Center de un host de un clúster: [Desinstalar NSX-T Data Center de un host en un clúster de vSphere](#).

Requisitos previos

- Compruebe que los hosts que desea desinstalar tengan configuradas asignaciones de desinstalación de red. Consulte [Comprobar las asignaciones de red de host para la desinstalación](#).
- Compruebe que los hosts que desea desinstalar estén en modo de mantenimiento en vSphere.

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión con privilegios de administrador en NSX Manager.
- 2 Seleccione **Sistema > Tejido > Nodos > Nodos de transporte de host**.
- 3 En el menú desplegable **Administrado por**, seleccione la instancia de vCenter Server.
- 4 Seleccione el clúster que desea desinstalar y haga clic en **Quitar NSX**.
- 5 Compruebe que el software NSX-T Data Center se haya desinstalado del host.
 - a Inicie sesión en la interfaz de línea de comandos del host como usuario raíz.
 - b Ejecute este comando para comprobar si hay algún VIB de NSX-T Data Center

```
esxcli software vib list | grep -E 'nsx|vsipfwlib'
```

Si el software NSX-T Data Center se desinstaló correctamente, no se mostrará ningún VIB. Si queda algún VIB de NSX en el host, póngase en contacto con el servicio de soporte de VMware.

Desinstalar NSX-T Data Center de un host en un clúster de vSphere

Puede desinstalar NSX-T Data Center de un único host administrado por vCenter Server. Los otros hosts del clúster no se ven afectados.

Precaución Desinstalar NSX-T Data Center de un host ESXi resulta disruptivo si las interfaces físicas o las interfaces de VMkernel están conectadas a N-VDS. Si el host o el clúster participan en otras aplicaciones, como vSAN, es posible que estas aplicaciones se vean afectadas por la desinstalación.

Requisitos previos

- Compruebe que los hosts que desea desinstalar tengan configuradas asignaciones de desinstalación de red. Consulte [Comprobar las asignaciones de red de host para la desinstalación](#).

- Compruebe que los hosts que desea desinstalar estén en modo de mantenimiento en vSphere.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión con privilegios de administrador en NSX Manager.
- 2 Seleccione **Sistema > Tejido > Nodos > Nodos de transporte de host**.
- 3 En el menú desplegable **Administrado por**, seleccione la instancia de vCenter Server.
- 4 Si el clúster tiene un perfil de nodo de transporte aplicado, seleccione el clúster y haga clic en **Acciones > Separar perfil de TN**.

Si el clúster tiene un perfil de nodo de transporte aplicado, la columna **Configuración de NSX** del clúster muestra el nombre del perfil.

- 5 Seleccione el host y haga clic en **Quitar NSX**.
- 6 Compruebe que el software NSX-T Data Center se haya desinstalado del host.
 - a Inicie sesión en la interfaz de línea de comandos del host como usuario raíz.
 - b Ejecute este comando para comprobar si hay algún VIB de NSX-T Data Center

```
esxcli software vib list | grep -E 'nsx|vsipfwlib'
```

Si el software NSX-T Data Center se desinstaló correctamente, no se mostrará ningún VIB. Si queda algún VIB de NSX en el host, póngase en contacto con el servicio de soporte de VMware.

- 7 Si se aplicó un perfil de nodo de transporte al clúster y desea volver a aplicarlo, seleccione el clúster, haga clic en **Configurar NSX** y seleccione el perfil en el menú desplegable **Seleccionar perfil de implementación**.

Desinstalar NSX-T Data Center de un host independiente

Puede desinstalar NSX-T Data Center de un host independiente. Los hosts independientes pueden ser ESXi o KVM.

Precaución Desinstalar NSX-T Data Center de un host ESXi resulta disruptivo si las interfaces físicas o las interfaces de VMkernel están conectadas a N-VDS. Si el host o el clúster participan en otras aplicaciones, como vSAN, es posible que estas aplicaciones se vean afectadas por la desinstalación.

Requisitos previos

Si va a desinstalar NSX-T Data Center de un host ESXi independiente, compruebe las siguientes opciones:

- Compruebe que los hosts que desea desinstalar tengan configuradas asignaciones de desinstalación de red. Consulte [Comprobar las asignaciones de red de host para la desinstalación](#).
- Compruebe que los hosts que desea desinstalar estén en modo de mantenimiento en vSphere.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión con privilegios de administrador en NSX Manager.
- 2 Seleccione **Sistema > Tejido > Nodos > Nodos de transporte de host**.
- 3 En el menú desplegable **Administrado por**, seleccione **Ninguno: hosts independientes**.
- 4 Seleccione el host y haga clic en **Eliminar**. En el cuadro de diálogo de confirmación que aparece, asegúrese de que la opción **Desinstalar componentes de NSX** esté seleccionada y de que la opción **Forzar eliminación** esté desmarcada. Haga clic en **Eliminar**.

El software NSX-T Data Center se elimina del host. La desinstalación del software NSX-T Data Center puede tardar hasta 5 minutos en completarse.

- 5 Si se produce un error durante la desinstalación, seleccione el host y haga clic de nuevo en **Eliminar**. En el cuadro de diálogo de confirmación, desmarque **Desinstalar componentes de NSX** y seleccione **Forzar eliminación**.

El nodo de transporte del host se eliminará del plano de administración, pero es posible que el host aún tenga el software NSX-T Data Center instalado.

- 6 Compruebe que el software NSX-T Data Center se haya desinstalado del host.
 - a Inicie sesión en la interfaz de línea de comandos del host como usuario raíz.
 - b Ejecute el comando adecuado para comprobar si hay paquetes del software NSX-T Data Center.

Tabla 10-1. Comandos de lista de paquetes

Sistema operativo del host	Comando
ESXi	<code>esxcli software vib list grep -E 'nsx vsipfwlib'</code>
Red Hat Enterprise Linux y CentOS Linux	<code>rpm -qa grep -E 'nsx vsipfwlib'</code>
Ubuntu	<code>dpkg -l grep -E 'nsx vsipfwlib'</code>
SUSE Linux Enterprise Server	<code>zypper packages --installed-only grep -E 'nsx vsipfwlib'</code>

Si el software NSX-T Data Center se desinstaló correctamente, no aparecerá ningún paquete. Si queda algún paquete de software de NSX en el host, póngase en contacto con el servicio de soporte de VMware.

Instalar componentes de NSX Cloud

11

NSX Cloud proporciona un panel centralizado para administrar las redes de nube pública.

NSX Cloud es independiente de las redes específicas del proveedor que no requieren el acceso de hipervisor en una nube pública.

Ofrece varias ventajas:

- Puede desarrollar y probar las aplicaciones utilizando la misma red y los perfiles de seguridad que se utilizan en el entorno de producción.
- Los desarrolladores pueden administrar sus aplicaciones hasta que estén listos para la implementación.
- Con la recuperación ante desastres, se puede recuperar de una interrupción no planificada o una amenaza de seguridad para su nube pública.
- Si se migran las cargas de trabajo entre nubes públicas, NSX Cloud garantiza que se apliquen directivas de seguridad similares a las máquinas virtuales de carga de trabajo, independientemente de su nueva ubicación.

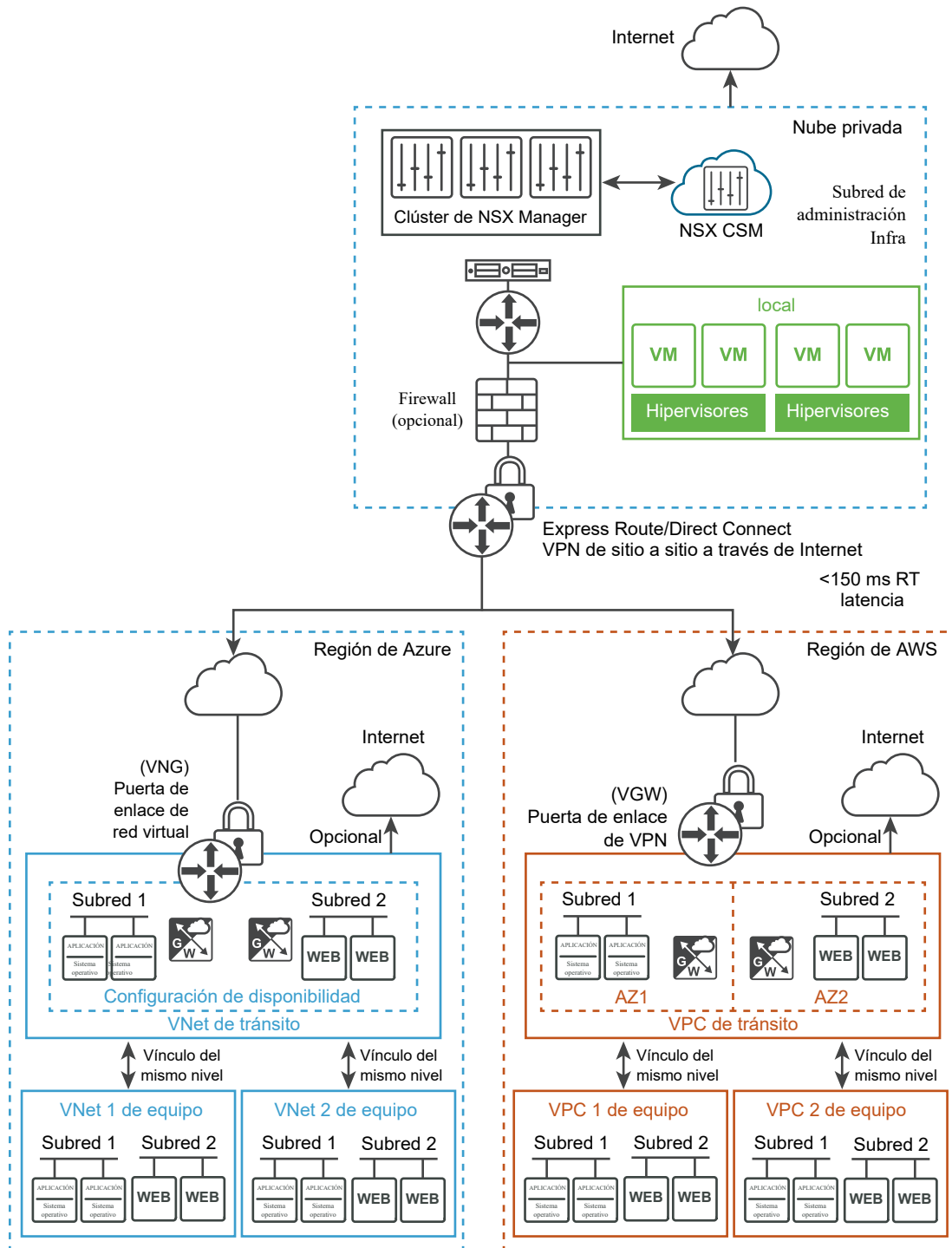
Este capítulo incluye los siguientes temas:

- [Arquitectura y componentes de NSX Cloud](#)
- [Descripción general de la instalación y la configuración de componentes de NSX Cloud para la nube pública](#)
- [Instalar CSM y conectar con NSX Manager](#)
- [Conectar la nube pública con una implementación local](#)
- [Agregar la cuenta de nube pública](#)
- [Implementar o vincular NSX Public Cloud Gateway](#)
- [Anular la implementación de PCG](#)

Arquitectura y componentes de NSX Cloud

NSX Cloud integra los componentes principales de NSX-T Data Center con la nube pública para proporcionar redes y seguridad en todas sus implementaciones.

Figura 11-1. Arquitectura de NSX Cloud



Componentes principales

Los componentes de NSX Cloud principales son:

- *NSX Manager* para el plano de administración en el que se definió el enrutamiento basado en directivas, el control de acceso basado en funciones (Role-Based Access Control, RBAC), el plano de control y los estados de tiempo de ejecución.
- *Cloud Service Manager (CSM)* para la integración con NSX Manager para proporcionar información específica de la nube pública al plano de administración.
- *NSX Public Cloud Gateway (PCG)* para la conectividad con los planos de administración y control de NSX, los servicios de puerta de enlace NSX Edge y las comunicaciones basadas en API con las entidades de nube pública. Consulte [Implementar o vincular NSX Public Cloud Gateway](#) para obtener detalles.
- Funcionalidad de *Agente NSX* que proporciona la ruta de datos administrados por NSX para las máquinas virtuales de la carga de trabajo.

Modos de implementación

NSX Public Cloud Gateway puede ser un dispositivo de puerta de enlace independiente o uno compartido entre las VPC o las VNet de nube pública para lograr una topología de concentrador y radio.

La VPC o la VNet autoadministradas actúan como una VPC de tránsito: cuando se implementa PCG en una VPC o una VNet, la VPC o la VNet se califican como autoadministradas, lo que quiere decir que puede poner las máquinas virtuales hospedadas en esta VPC o esta VNet bajo la administración de NSX. La VPC o la VNet también se califican como VPC o VNet de tránsito, debido a que puede utilizar la PCG implementada en ellas para incorporar máquinas virtuales hospedadas en otras VPC o VNet.

La VPC o la VNet de equipo se vinculan a la VPC o la VNet de tránsito: las VPC o las VNet en las que no se implementó PCG, pero que se vinculan a una VPC o una VNet de tránsito, se denominan VPC o VNet de *equipo*.

Descripción general de la instalación y la configuración de componentes de NSX Cloud para la nube pública

Consulte la lista de comprobación para obtener una descripción general de los pasos que debe realizar para habilitar NSX-T Data Center a fin de administrar las máquinas virtuales de carga de trabajo en la nube pública.

Flujo de trabajo de día 0 para conectar NSX Cloud con la nube pública

Este flujo de trabajo proporciona una descripción general de los pasos necesarios para empezar a utilizar NSX Cloud con la nube pública.

Nota Mientras planifica la implementación, asegúrese de que los dispositivos de NSX-T Data Center locales tengan una buena conectividad con la PCG implementada en la nube pública. Además, las VPC/VNet de tránsito deben estar en la misma región que las VPC o VNet de equipo.

Tabla 11-1. Flujo de trabajo de día 0 para conectar NSX Cloud con la nube pública

Tarea	Instrucciones
<input type="checkbox"/> Instalar CSM y conectar con NSX Manager.	Consulte Instalar CSM y conectar con NSX Manager .
<input type="checkbox"/> Agregue una o varias de sus cuentas de nube pública en CSM.	Consulte Agregar la cuenta de nube pública .
<input type="checkbox"/> Implemente PCG en las VPC o las VNet de tránsito y establezca un vínculo con la VPC o la VNet de equipo.	Consulte Implementar o vincular NSX Public Cloud Gateway .
<input type="checkbox"/> Incorpore las máquinas virtuales de carga de trabajo etiquetándolas en la nube pública e instalando el agente NSX en ellas.	Siga las instrucciones en Incorporar máquinas virtuales de carga de trabajo en la <i>Guía de administración de NSX-T Data Center</i> .

Instalar CSM y conectar con NSX Manager

Utilice al Asistente de instalación para conectar CSM con NSX Manager y configurar los servidores proxy (si los hay).

Instalar CSM

Cloud Service Manager (CSM) es un componente esencial de NSX Cloud.

Instale CSM después de instalar los componentes principales de NSX-T Data Center.

Consulte [Instalar NSX Manager y los dispositivos disponibles](#) para obtener instrucciones detalladas.

Nota Para instalar NSX Cloud, es necesario habilitar el uso de FQDN (DNS) en las instancias de NSX Manager. Consulte [Publicar los FQDN de las instancias de NSX Manager](#).

Unirse a CSM con NSX Manager

Debe conectar el dispositivo CSM con NSX Manager para permitir que estos componentes se comuniquen entre sí.

Requisitos previos

- NSX Manager debe estar instalado y debe tener el nombre de usuario y la contraseña de la cuenta de administrador para iniciar sesión en NSX Manager.
- CSM debe estar instalado y debe tener la función Administrador empresarial asignada en CSM.

Procedimiento

- 1 En un explorador, inicie sesión en CSM.

- 2 Cuando se le solicite en el Asistente de instalación, haga clic en **Iniciar instalación**.
- 3 Introduzca los siguientes detalles en la pantalla de credenciales de NSX Manager:

Opción	Descripción
Nombre de host de NSX Manager	Introduzca el nombre de dominio totalmente cualificado (FQDN) de NSX Manager, si está disponible. También puede introducir la dirección IP de NSX Manager.
Credenciales administrativas	Introduzca el nombre de usuario administrador empresarial y la contraseña de NSX Manager.
Huella digital del administrador	Si lo desea, introduzca el valor de huella digital de NSX Manager. Si deja este campo en blanco, el sistema identificará la huella digital y la mostrará en la pantalla siguiente.

- 4 (opcional) Si no se ha proporcionado un valor de huella digital para NSX Manager, o si el valor no es correcto, aparecerá la pantalla **Verificar huella digital**. Marque la casilla de verificación para aceptar la huella digital detectada por el sistema.
- 5 Haga clic en **Conectar (Connect)**.

Nota Si esta opción no aparece en el Asistente de configuración, o si desea cambiar la instancia de NSX Manager asociada, inicie sesión en CSM, haga clic en **Sistema > Configuración**, y luego haga clic en **Configurar** en el panel titulado **Nodo de NSX asociado**.

CSM verifica la huella digital de NSX Manager y establece la conexión.

- 6 (opcional) Configure el servidor proxy. Consulte las instrucciones en [\(Opcional\) Configurar servidores proxy](#).

(Opcional) Configurar servidores proxy

Si quiere enrutar y supervisar todo el tráfico de HTTP/HTTPS asociado a Internet a través de un servidor proxy HTTP confiable, puede configurar hasta cinco servidores proxy en CSM.

Todas las comunicaciones de nube pública desde PCG y CSM se enrutan a través del servidor proxy seleccionado.

La configuración de proxy de PCG es independientes de la configuración de proxy de CSM. Puede optar por no tener ningún servidor proxy o por tener otro distinto en PCG.

Se pueden elegir los siguientes niveles de autenticación:

- Autenticación basada en credenciales
- Autenticación basada en certificados para la interceptación de HTTPS
- Ninguna autenticación

Procedimiento

- 1 Haga clic en **Sistema > Configuración**. A continuación, haga clic en **Configurar** en el panel **Servidores proxy**.

Nota También puede proporcionar estos detalles cuando use el Asistente de instalación de CSM, que aparece cuando se instala por CSM primera vez.

- 2 Introduzca los siguientes detalles en la pantalla Configurar servidores proxy:

Opción	Descripción
Predeterminado	Utilice este botón de radio para indicar el servidor proxy predeterminado.
Nombre del perfil	Indique un nombre de perfil de servidor proxy. Esta opción es obligatoria.
Servidor proxy	Introduzca la dirección IP del servidor proxy. Esta opción es obligatoria.
Puerto	Introduzca el puerto del servidor proxy. Esta opción es obligatoria.
Autenticación	Opcional. Si desea configurar más autenticación, active esta casilla de verificación e indique un nombre de usuario y una contraseña válidos.
Nombre de usuario	Esta opción es obligatoria si se ha activado la casilla de verificación Autenticación.
Contraseña	Esta opción es obligatoria si se ha activado la casilla de verificación Autenticación.
Certificado	Opcional. Si quiere proporcionar un certificado de autenticación para la interceptación de HTTPS, active esta casilla de verificación y copie y pegue el certificado en el cuadro de texto que aparece.
Sin proxy	Seleccione esta opción si no quiere usar ninguno de los servidores proxy configurados.

(Opcional) Configurar vIDM para Cloud Service Manager

Si utiliza VMware Identity Manager, puede configurarlo para acceder a CSM desde NSX Manager.

Procedimiento

- 1 Configure vIDM para NSX Manager y CSM. Consulte las instrucciones en la sección sobre cómo [configurar la integración de VMware Identity Manager](#) de la *Guía de administración de NSX-T Data Center*.
- 2 Asigne la misma función al usuario de vIDM para NSX Manager y CSM (por ejemplo, asigne la función **Enterprise Admin** al usuario **vIDM_admin**). Debe iniciar sesión en NSX Manager y CSM y asignar la misma función al mismo nombre de usuario. Consulte instrucciones detalladas en la sección sobre cómo [agregar una asignación de función o identidad principal](#) de la *Guía de administración de NSX-T Data Center*.
- 3 Inicie sesión en NSX Manager. Se le redirigirá al inicio de sesión de vIDM.

- 4 Introduzca las credenciales de usuario de vIDM. Una vez que inicie sesión, puede cambiar entre NSX Manager y CSM haciendo clic en el icono Aplicaciones (Applications).



Conectar la nube pública con una implementación local

Debe usar las opciones de conectividad adecuadas para conectar la implementación local con las suscripciones o las cuentas de nube pública.

Habilitar el acceso a puertos y protocolos en CSM para conectividad híbrida

Abra los puertos de red necesarios y permita los protocolos requeridos en NSX Manager para habilitar la conectividad de nube pública.

Permitir acceso a NSX Manager desde la nube pública

Abra los siguientes puertos de red y protocolos para permitir la conectividad con la implementación de NSX Manager local:

Tabla 11-2.

Desde	Para	Protocolo/puerto	Descripción
PCG	NSX Manager	TCP/5671	Tráfico entrante de la nube pública a la instancia local de NSX-T Data Center para la comunicación del plano de administración.
PCG	NSX Manager	TCP/8080	Tráfico entrante desde la nube pública a la instancia local de NSX-T Data Center para acceder a un repositorio HTTP para actualizar componentes de NSX Cloud.
PCG	NSX Controller	TCP/1234, 1235/TCP	Tráfico entrante de la nube pública a la instancia local de NSX-T Data Center para la comunicación del plano de control.
PCG	DNS	UDP/53	Tráfico entrante de la nube pública al DNS de NSX-T Data Center local (si se utiliza el servidor DNS local).
CSM	PCG	TCP/7442	Inserción de configuración de CSM

Tabla 11-2. (continuación)

Desde	Para	Protocolo/puerto	Descripción
Cualquiera (Any)	NSX Manager	TCP/443	Interfaz de usuario de NSX Manager
Cualquiera (Any)	CSM	TCP/443	Interfaz de usuario de CSM

Importante Todas las comunicaciones de la infraestructura de NSX-T Data Center aprovechan el cifrado basado en SSL. Asegúrese de que el firewall permite el tráfico SSL a través de puertos no estándar.

Conectar la red de Microsoft Azure con la implementación de NSX-T Data Center local

Se debe establecer una conexión entre la red de Microsoft Azure y los dispositivos de NSX-T Data Center locales.

Nota Debe tener NSX Manager ya instalado y conectado con CSM en su implementación local.

Descripción general

- Conecte la suscripción de Microsoft Azure con NSX-T Data Center local.
- Configure su VNet con los bloques CIDR necesarios y las subredes requeridas por NSX Cloud.
- Sincronice la hora en el dispositivo de CSM con el servidor de Microsoft Azure Storage o NTP.

Conectar la suscripción de Microsoft Azure con NSX-T Data Center local

Cada nube pública ofrece opciones para conectarse con una implementación local. Puede elegir cualquiera de las opciones de conectividad disponibles que se adapten a sus requisitos. Para obtener más detalles, consulte la [documentación de referencia de Azure](#).

Nota Debe revisar e implementar las consideraciones de seguridad y las prácticas recomendadas correspondientes de Microsoft Azure; por ejemplo, todas las cuentas de usuario con privilegios que acceden al portal de Microsoft Azure o a la API deben tener habilitada la autenticación multifactor (MFA). La MFA garantiza que solo los usuarios legítimos puedan acceder al portal, y reduce la probabilidad de acceso incluso en caso de robo o pérdida de las credenciales. Para obtener más información y recomendaciones, consulte la [Documentación del centro de seguridad de Azure](#).

Configurar la VNet

En Microsoft Azure, cree bloques CIDR enrutables y configure las subredes requeridas.

- Una subred de administración con un rango recomendado de al menos /28, para controlar:
 - controlar el tráfico a los dispositivos locales
 - tráfico de la API para los endpoints de API del proveedor de nube

- Subred de un vínculo de descarga con un rango recomendado de /24, para las máquinas virtuales de la carga de trabajo.
- Una subred de vínculo superior (o dos para alta disponibilidad) con un rango recomendado de /24, para el enrutamiento de tráfico de norte a sur que sale de la VNet o ingresa en ella.

Consulte [Implementar o vincular NSX Public Cloud Gateway](#) para obtener más información sobre cómo se utilizan estas subredes.

Conectar la red de Amazon Web Services (AWS) con la implementación de NSX-T Data Center local

Se debe establecer una conexión entre la red de Amazon Web Services (AWS) y los dispositivos de NSX-T Data Center locales.

Nota Debe tener NSX Manager ya instalado y conectado con CSM en su implementación local.

Descripción general

- Conecte su cuenta de AWS con dispositivos de NSX Manager locales utilizando cualquiera de las opciones disponibles que mejor se adapte a sus requisitos.
- Configure su VPC con subredes y otros requisitos para NSX Cloud.

Conecte su cuenta de AWS con la implementación de NSX-T Data Center local.

Cada nube pública ofrece opciones para conectarse con una implementación local. Puede elegir cualquiera de las opciones de conectividad disponibles que se adapten a sus requisitos. Para obtener más información, consulte la [documentación de referencia de AWS](#).

Nota Debe revisar e implementar las prácticas recomendadas y las consideraciones de seguridad correspondientes de AWS; consulte [Prácticas recomendadas de seguridad de AWS](#).

Configurar la VPC

Necesita las siguientes configuraciones:

- seis subredes para admitir PCG con alta disponibilidad
- una puerta de enlace de Internet (IGW)
- una tabla de enrutamiento privada y una pública
- asociación de la subred con tablas de enrutamiento
- resolución de DNS y nombres de host de DNS habilitados

Siga estas directrices para configurar su VPC:

- 1 Suponiendo que su nube privada virtual utiliza una red /16, configure tres subredes por cada puerta de enlace que vaya a implementar.

Importante Si utiliza alta disponibilidad, configure tres subredes adicionales en una zona de disponibilidad diferente.

- **Subred de administración:** esta subred se utiliza para tráfico de administración entre la instancia de NSX-T Data Center local y PCG. El rango recomendado es /28.
- **Subred de vínculo superior:** esta subred se utiliza para tráfico de Internet de norte a sur. El rango recomendado es /24.
- **Subred de vínculo inferior:** esta subred abarca el rango de direcciones IP de la máquina virtual de carga de trabajo y su tamaño debe definirse de manera acorde. Tenga en cuenta que posiblemente deba incorporar interfaces adicionales en las máquinas virtuales de carga de trabajo con fines de depuración.

Nota Etiquete las subredes correctamente (por ejemplo, **management-subnet**, **uplink-subnet**, **downlink-subnet**), ya que deberá seleccionarlas al implementar PCG en esta VPC.

Consulte [Implementar o vincular NSX Public Cloud Gateway](#) para obtener detalles.

- 2 Asegúrese de que tiene una puerta de enlace de Internet (IGW) que está asociada a esta nube privada virtual.
- 3 Asegúrese de que la tabla de enrutamiento de la VPC tenga el **Destino** configurado con el valor **0.0.0.0/0** y el **Objetivo** sea la IGW adjunta a la VPC.
- 4 Asegúrese de que dispone de resolución de DNS y nombres de host DNS habilitados para esta nube privada virtual.

Agregar la cuenta de nube pública

Si quiere agregar el inventario de nube pública, debe crear funciones en la nube pública para permitir el acceso a NSX Cloud y, a continuación, agregar la información necesaria en CSM.

Configurar el acceso seguro a su inventario de Microsoft Azure

Para que NSX Cloud funcione en su suscripción, cree una entidad de servicio que conceda los permisos necesarios y las funciones de CSM y PCG según la función de Microsoft Azure para la administración de identidades de los recursos de Azure.

Nota Si ya agregó una cuenta AWS para CSM, actualice el valor de MTU en **NSX Manager > Tejido > Perfiles > Perfiles de vínculo superior > PCG-Uplink-HostSwitch-Profile** con el valor 1.500 antes de agregar la cuenta de Microsoft Azure. Esto también puede hacerse mediante las API de REST de NSX Manager.

Información general:

- La suscripción de Microsoft Azure contiene una o varias VNet que desea poner bajo la administración de NSX-T Data Center. La VNet podría estar en el modo de tránsito o de equipo. La VNet de tránsito es aquella en la que implementa PCG. Puede vincular otras VNet a la VNet de tránsito e incorporar máquinas virtuales de carga de trabajo que estén hospedadas en ellas. Las VNet vinculadas a la VNet de tránsito se denominan VNet de equipos.
- NSX Cloud proporciona un script de PowerShell para generar la entidad de servicio y las funciones que usan la función de identidad administrada de Microsoft Azure para administrar la autenticación a la vez que se siguen protegiendo las credenciales de Microsoft Azure. También puede incluir varias suscripciones en una entidad de servicio que use este script.
- Tiene la opción de volver a utilizar la entidad de servicio en todas sus suscripciones o de crear entidades de servicio nuevas, según crea conveniente. No hay un script adicional si va a crear entidades de servicio independientes para otras suscripciones.
- En el caso de tener varias suscripciones, tanto si utiliza una sola entidad de servicio para todas como si usa varias entidades de servicio, debe actualizar los archivos JSON para las funciones CSM y PCG con el fin de agregar cada nombre de suscripción adicional a la sección *AssignableScopes*.
- Si ya tiene una entidad de servicio de NSX Cloud en su VNet, puede actualizarla. Para ello, tiene que volver a ejecutar los scripts y eliminar el nombre de la entidad de servicio de los parámetros.
- El nombre de la entidad de servicio debe ser único para Microsoft Azure Active Directory. Puede utilizar a la misma entidad de servicio en varias suscripciones del mismo dominio de Active Directory, o usar diferentes entidades de servicio por suscripción. No obstante, no podrá crear dos entidades de servicio con el mismo nombre.
- Debe ser el propietario o tener permisos para crear y asignar funciones en todas las suscripciones de Microsoft Azure.
- Se admiten los siguientes escenarios:
 - **Escenario 1:** tiene una sola suscripción de Microsoft Azure que desea habilitar con NSX Cloud.
 - **Escenario 2:** tiene varias suscripciones de Microsoft Azure en el mismo directorio de Microsoft Azure que desea habilitar con NSX Cloud, pero quiere utilizar una entidad de servicio de NSX Cloud en todas las suscripciones.
 - **Escenario 3:** tiene varias suscripciones de Microsoft Azure en el mismo directorio de Microsoft Azure que desea habilitar con NSX Cloud, pero quiere utilizar distintos nombres de entidad de servicio de NSX Cloud en distintas suscripciones.

A continuación se muestra un resumen del proceso:

- 1 Utilizar el script de PowerShell de NSX Cloud:
 - Crear una cuenta de la entidad de servicio para NSX Cloud.
 - Crear una función para CSM.
 - Crear una función para PCG.

- 2 (Opcional) Crear entidades de servicio para las otras suscripciones que quiera vincular.
- 3 Agregar la suscripción de Microsoft Azure en CSM.

Nota Si utiliza varias suscripciones, e independientemente de si usa la misma entidad de servicio o utiliza varias, debe agregar cada suscripción a CSM por separado.

Generar la entidad de servicio y las funciones

NSX Cloud proporciona scripts de PowerShell que ayudan a generar la entidad de servicio y las funciones que se necesitan para una o varias suscripciones.

Requisitos previos

- Debe tener PowerShell 5.0 o una versión posterior con el módulo AzureRM instalado.
- Debe ser el propietario o tener permisos para crear y asignar funciones en todas las suscripciones de Microsoft Azure.

Nota El tiempo de respuesta de Microsoft Azure puede provocar que el script genere un error cuando se ejecuta por primera vez. Si se produce un error en el script, intente ejecutarlo de nuevo.

Procedimiento

- 1 En un servidor o escritorio Windows o compatible, descargue el archivo ZIP llamado `CreateNSXCloudCredentials.zip` en NSX-T Data Center **Página de descargas > Controladores y herramientas > Scripts de NSX Cloud > Microsoft Azure**.
- 2 Extraiga el siguiente contenido del archivo ZIP en su sistema Windows:

Script/archivo	Descripción
CreateNSXRoles.ps1	<p>El script de PowerShell para generar la entidad de servicio y las funciones de identidad administrada de NSX Cloud para CSM y PCG. El script utiliza los siguientes parámetros:</p> <ul style="list-style-type: none"> ■ <code>-subscriptionId <the Transit_VNet's_Azure_subscription_ID></code> ■ (opcional) <code>-servicePrincipalName <Service_Principal_Name></code> ■ (opcional) <code>-useOneServicePrincipal</code>
AddServicePrincipal.ps1	<p>Un script opcional necesario si desea agregar varias suscripciones y asignar entidades de servicio diferentes a cada suscripción. Consulte el escenario 3 en los siguientes pasos. El script utiliza los siguientes parámetros:</p> <ul style="list-style-type: none"> ■ <code>-computeSubscriptionId <the_Compute_VNet's_Azure_subscription_ID></code> ■ <code>-transitSubscriptionId <the Transit_VNet's_Azure_Subscription_ID></code> ■ <code>-csmRoleName <CSM_Role_Name></code> ■ <code>-servicePrincipalName <Service_Principal_Name></code>

Script/archivo	Descripción
nsx_csm_role.json.	Una plantilla JSON para los permisos y el nombre de la función de CSM. Este archivo se requiere como una entrada para el script de PowerShell y debe estar en la misma carpeta que el script.
nsx_pcg_role.json	Una plantilla JSON para los permisos y el nombre de la función de PCG. Este archivo se requiere como una entrada para el script de PowerShell y debe estar en la misma carpeta que el script. Nota El nombre de la función predeterminado (Puerta de enlace) de PCG es <code>nsx-pcg-role</code> . Debe proporcionar este valor al agregar la suscripción en CSM.

3 **Escenario 1:** tiene una sola suscripción de Microsoft Azure que desea habilitar con NSX Cloud.

- a En una instancia de PowerShell, vaya al directorio donde descargó los archivos JSON y los scripts de Microsoft Azure.
- b Ejecute el script llamado `CreateNSXRoles.ps1` con el parámetro `-SubscriptionId`, como se indica a continuación:

```
.\CreateNSXRoles.ps1 -subscriptionId <the_single_Azure_subscription_ID>
```

Nota Si desea reemplazar el nombre predeterminado de la entidad de servicio de `nsx-service-admin`, también puede usar el parámetro `-servicePrincipalName`. El nombre de la entidad de servicio debe ser único en Microsoft Azure Active Directory.

- 4 Escenario 2:** tiene varias suscripciones de Microsoft Azure en el mismo directorio de Microsoft Azure que desea habilitar con NSX Cloud, pero quiere utilizar una entidad de servicio de NSX Cloud en todas las suscripciones.

- a En una instancia de PowerShell, vaya al directorio donde descargó los archivos JSON y los scripts de Microsoft Azure.
- b Edite cada uno de los archivos JSON para agregar una lista de otros identificadores de suscripción en la sección titulada *"AssignableScopes"*, por ejemplo:

```
"AssignableScopes": [
  "/subscriptions/aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee",
  "/subscriptions/aaaaaaaa-bbbb-cccc-dddd-ffffffffffff",
  "/subscriptions/aaaaaaaa-bbbb-cccc-dddd-000000000000"
```

Nota Debe utilizar el formato que se muestra en el ejemplo para agregar los identificadores de suscripción: `"/subscriptions/<Subscription_ID>"`

- c Ejecute el script llamado `CreateNSXRoles.ps1` con los parámetros `-subscriptionID` y `-useOneServicePrincipal`:

```
.\CreateNSXRoles.ps1 -subscriptionId <the_Transit_VNet's_Azure_subscription_ID> -
useOneServicePrincipal
```

Nota Omita el nombre de la entidad de servicio aquí si desea usar el nombre predeterminado: `nsx-service-admin`. Si ya existe ese nombre de entidad de servicio en Microsoft Azure Active Directory, al ejecutar este script sin un nombre de entidad de servicio, se actualiza dicha entidad de servicio.

- 5 Escenario 3:** tiene varias suscripciones de Microsoft Azure en el mismo directorio de Microsoft Azure que desea habilitar con NSX Cloud, pero quiere utilizar distintos nombres de entidad de servicio de NSX Cloud en distintas suscripciones.

- a En una instancia de PowerShell, vaya al directorio donde descargó los archivos JSON y los scripts de Microsoft Azure.
- b Siga los pasos **b** y **c** del segundo escenario para agregar varias suscripciones a la sección *AssignableScopes* en cada uno de los archivos JSON.

- c Ejecute el script llamado `CreateNSXRoles.ps1` con los parámetros `-subscriptionID`:

```
.\CreateNSXRoles.ps1 -subscriptionId <One of the subscription_IDs>
```

Nota Omita el nombre de la entidad de servicio aquí si desea usar el nombre predeterminado: `nsx-service-admin`. Si existe ese nombre de entidad de servicio en Microsoft Azure Active Directory, al ejecutar este script sin un nombre de entidad de servicio, se actualiza dicha entidad de servicio.

- d Ejecute el script llamado `AddServicePrincipal.ps1` con los siguientes parámetros:

Parámetro	Valor
<code>-computeSubscriptionId</code>	Identificador de suscripción de Azure de Compute_VNet
<code>-transitSubscriptionId</code>	Identificador de suscripción de Azure de la VNet de tránsito
<code>-csmRoleName</code>	Obtenga este valor del archivo <code>nsx_csm_role.JSON</code>
<code>-servicePrincipalName</code>	Nuevo nombre de entidad de servicio

```
./AddServicePrincipal.ps1 -computeSubscriptionId <the_Compute_VNet's_Azure_subscription_ID>
-transitSubscriptionId <the_Transit_VNet's_Azure_Subscription_ID>
-csmRoleName <CSM_Role_Name>
-servicePrincipalName <new_Service_Principal_Name>
```

- 6 Busque un archivo en el mismo directorio donde se ejecutó el script de PowerShell. Debe tener un nombre similar a este:
`NSXCloud_ServicePrincipal_<your_subscription_ID>_<NSX_Cloud_Service_Principal_name>`. Este archivo contiene la información que se necesita para agregar la suscripción de Microsoft Azure en CSM.

- ID de cliente
- Clave de cliente
- ID de tenant
- Identificador de suscripción

Resultados

Se crearán las siguientes construcciones:

- Una aplicación de Azure AD para NSX Cloud.
- Una entidad de servicio de Azure Resource Manager para la aplicación NSX Cloud.
- Una función para la instancia de CSM asociada a la cuenta de la entidad de servicio.
- Una función de PCG para que pueda funcionar en el inventario de nube pública.

- Un archivo con un nombre similar a `NSXCloud_ServicePrincipal_<su_identificador_de_suscripción>_<nombre_de_entidad_de_servicio_de_NSX_Cloud>` se crea en el mismo directorio en el que se ejecutó el script de PowerShell. Este archivo contiene la información que se necesita para agregar la suscripción de Microsoft Azure en CSM.

Nota Consulte los archivos JSON que se utilizan para crear las funciones CSM y PCG si desea obtener una lista de los permisos disponibles para ellos después de que se crean las funciones.

Pasos siguientes

Agregar la suscripción de Microsoft Azure en CSM

Nota Cuando habilita NSX Cloud para varias suscripciones, debe agregar cada suscripción independiente a CSM de forma individual, por ejemplo, si tiene cinco suscripciones en total, debe agregar cinco cuentas de Microsoft Azure en CSM con todos los demás valores iguales, pero diferentes identificadores de suscripción.

Agregar la suscripción de Microsoft Azure en CSM

Una vez que tenga los detalles de la entidad de servicio de NSX Cloud y las funciones de PCG en CSM, estará listo para agregar la suscripción de Microsoft Azure en CSM.

Requisitos previos

- Debe tener la función Administrador empresarial (Enterprise Administrator) en NSX-T Data Center.
- Debe tener el resultado del script de PowerShell con detalles de la entidad de servicio de NSX Cloud.
- Debe tener el valor de la función de PCG que proporcionó al ejecutar el script de PowerShell para crear las funciones y la entidad de servicio. El valor predeterminado es `nsx-pcg-role`.

Procedimiento

- 1 Inicie sesión en CSM mediante una cuenta con la función Administrador empresarial (Enterprise Administrator).
- 2 Vaya a **CSM > Clouds (Nubes) > Azure**.
- 3 Haga clic en **+Agregar (+Add)** e introduzca los siguientes detalles:

Opción	Descripción
Nombre (Name)	Proporcione un nombre adecuado para identificar esta cuenta en CSM. Es posible que tenga varias suscripciones a Microsoft Azure que estén asociadas con el mismo identificador de tenant de Microsoft Azure. Otorgue el nombre a su cuenta; puede nombrarla según corresponda en CSM, por ejemplo, Azure-DevOps-Cuenta, Azure-Finance-Cuenta, etc.
ID de cliente (Client ID)	Copie y pegue este valor de la salida del script de PowerShell.
Clave (Key)	Copie y pegue este valor de la salida del script de PowerShell.

Opción	Descripción
Identificador de suscripción (Subscription ID)	Copie y pegue este valor de la salida del script de PowerShell.
ID de tenant (Tenant ID)	Copie y pegue este valor de la salida del script de PowerShell.
Nombre de la función de puerta de enlace	El valor predeterminado es <code>nsx-pcg-role</code> . Este valor está disponible en el archivo <code>nsx_pcg_role.json</code> si cambió el valor predeterminado.
etiquetas de nube	De forma predeterminada, esta opción está habilitada y permite que sus etiquetas de Microsoft Azure sean visibles en NSX Manager.

4 Haga clic en **Guardar**.

CSM agrega la cuenta, y podrá verla en la sección **Cuentas** en 3 minutos.

Pasos siguientes

[Implementar PCG en una VNet de tránsito o autoadministrada](#)

Configurar el acceso seguro a su inventario de AWS

Podría tener una o varias cuentas de AWS con VPC y máquinas virtuales de carga de trabajo que desea poner bajo la administración de NSX-T Data Center.

Información general:

- Puede utilizar la topología de VPC de tránsito o de equipo en la que se implementa PCG en una VPC (convirtiéndola en la VPC de tránsito) y vincular otras VPC a ella, las cuales se denominan VPC de equipo.
- NSX Cloud proporciona un script de shell que se puede ejecutar desde la CLI de AWS de su cuenta de AWS para crear la función y el perfil de IAM, y para crear una relación de confianza para las VPC de tránsito y de equipo.
- Se admiten los siguientes escenarios:
 - **Escenario 1:** desea utilizar una sola cuenta de AWS con NSX Cloud.
 - **Escenario 2:** desea utilizar varias subcuentas de AWS que administra una cuenta de AWS principal.
 - **Escenario 3:** desea utilizar varias cuentas de AWS con NSX Cloud.

A continuación se muestra un resumen del proceso:

- 1 Utilice el script de shell NSX Cloud, que requiere la CLI de AWS, para hacer lo siguiente:
 - Crear un perfil de IAM.
 - Crear una función para PCG.
 - (Opcional) Cree una relación de confianza entre la cuenta de AWS que aloja la VPC de tránsito y la cuenta de AWS que aloja la VPC de equipo.
- 2 Agregar la cuenta de AWS en CSM.

Generar el perfil de IAM y la función de PCG

NSX Cloud proporciona un script de shell para ayudar a configurar una o varias de las cuentas de AWS mediante la generación de un perfil de IAM y una función de PCG asociada al perfil que ofrece los permisos necesarios para la cuenta de AWS.

Si planea hospedar una VPC de tránsito vinculada a varias VPC de equipo en dos diferentes cuentas de AWS, puede utilizar el script para crear una relación de confianza entre estas cuentas.

Nota De forma predeterminada, el nombre de la función (Puerta de enlace) de PCG es `nsx_pcg_service`. Si desea un valor diferente para el nombre de la función de puerta de enlace, puede cambiarlo en el script. No obstante, asegúrese de anotar este valor, ya que es necesario para agregar la cuenta de AWS a CSM.

Requisitos previos

Antes de ejecutar el script, debe instalar y configurar lo siguiente en su sistema Linux o uno compatible:

- CLI de AWS
- `jq` (un analizador de JSON)
- `openssl`

Nota Si se utilizan varias cuentas de AWS, estas deben emparejarse con un método adecuado.

Procedimiento

- 1 En un servidor o un escritorio Linux (o compatible), descargue el script de shell denominado `nsx_csm_iam_script.sh` de NSX-T Data Center en **Página de descarga > Controladores y herramientas > Scripts de NSX Cloud > AWS**.

- 2 **Escenario 1:** desea utilizar una sola cuenta de AWS con NSX Cloud.

- a Ejecute el script, por ejemplo:

```
bash nsx_csm_iam_script.sh
```

- b Introduzca `yes` cuando aparezca la pregunta `Do you want to create an IAM user for CSM and an IAM role for PCG?` `[yes/no]`
 - c Introduzca un nombre para el usuario de IAM cuando aparezca la pregunta `What do you want to name the IAM User?`

Nota El nombre de usuario de IAM debe ser único en la cuenta de AWS.

- d Introduzca `no` cuando aparezca la pregunta `Do you want to add trust relationship for any Transit VPC account?` `[yes/no]`

Cuando el script se ejecuta correctamente, se crea el perfil de IAM y una función para PCG en su cuenta de AWS. Los valores se guardan en el archivo de salida denominado `aws_details.txt` ubicado en el mismo directorio en el que se ejecutó el script. A continuación, siga las instrucciones que aparecen en [Agregar la cuenta de AWS en CSM](#) y en [Implementar PCG en una VPC de tránsito o autoadministrada](#) para finalizar el proceso de configuración de una VPC de tránsito o autoadministrada.

3 Escenario 2: desea utilizar varias subcuentas en AWS que una cuenta de AWS principal administra.

- a Ejecute el script desde la cuenta principal de AWS.

```
bash nsx_csm_iam_script.sh
```

- b Introduzca `yes` cuando aparezca la pregunta `Do you want to create an IAM user for CSM and an IAM role for PCG? [yes/no]`
- c Introduzca un nombre para el usuario de IAM cuando aparezca la pregunta `What do you want to name the IAM User?`

Nota El nombre de usuario de IAM debe ser único en la cuenta de AWS.

- d Introduzca `no` cuando aparezca la pregunta `Do you want to add trust relationship for any Transit VPC account? [yes/no]`

Nota Con una cuenta de AWS principal, si su VPC de tránsito tiene permiso para ver VPC de equipo en las subcuentas, no es necesario establecer una relación de confianza con las subcuentas. De lo contrario, siga los pasos del **escenario 3** para configurar varias cuentas.

Cuando el script se ejecuta correctamente, se crea el perfil de IAM y una función para PCG en su cuenta de AWS principal. En el archivo de salida, los valores se guardan en el mismo directorio donde se ejecutó el script. El nombre del archivo es `aws_details.txt`. A continuación, siga las instrucciones que aparecen en [Agregar la cuenta de AWS en CSM](#) y en [Implementar PCG en una VPC de tránsito o autoadministrada](#) para finalizar el proceso de configuración de una VPC de tránsito o autoadministrada.

4 Escenario 3: desea utilizar varias cuentas de AWS con NSX Cloud.

Nota Compruebe que las cuentas de AWS están emparejadas antes de continuar.

- a Anote el número de la cuenta de AWS de 12 dígitos donde desea hospedar la VPC de tránsito.
- b Configure la VPC de tránsito en la cuenta de AWS siguiendo los pasos a d para el **escenario 1** y finalice el proceso de agregar la cuenta en CSM e implementar una PCG en ella.
- c Descargue y ejecute el script NSX Cloud desde un sistema Linux o compatible en la otra cuenta de AWS donde desea hospedar las VPC de equipo.

Nota Si lo prefiere, puede usar perfiles AWS con credenciales de cuenta distintas con el fin de utilizar el mismo sistema para volver a ejecutar el script para la otra cuenta de AWS.

- d Introduzca **yes** cuando aparezca la pregunta *Do you want to create an IAM user for CSM and an IAM role for PCG?* [yes/no]

Nota Si ya agregó esta cuenta de AWS en CSM y desea volver a utilizar el script para conectarse a una cuenta de AWS diferente, puede introducir **no** y omitir la creación del usuario de IAM.

- e Introduzca un nombre para el usuario de IAM cuando aparezca la pregunta *What do you want to name the IAM User?*

Nota El nombre de usuario de IAM debe ser único en la cuenta de AWS.

- f Introduzca **yes** cuando aparezca la pregunta *Do you want to add trust relationship for any Transit VPC account?* [yes/no]

- g Escriba o bien copie y pegue el número de cuenta de AWS de 12 dígitos que anotó en el paso 1 cuando apareció la pregunta *What is the Transit VPC account number?*

Se establece una relación de confianza de IAM entre las dos cuentas de AWS y el script genera un identificador externo.

Cuando el script se ejecuta correctamente, se crea el perfil de IAM y una función para PCG en su cuenta de AWS principal. En el archivo de salida, los valores se guardan en el mismo directorio donde se ejecutó el script. El nombre del archivo es `aws_details.txt`. A continuación, siga las instrucciones en [Agregar la cuenta de AWS en CSM](#) y, luego, en [Vincular a una VPC o VNet de tránsito](#) para finalizar el proceso de vinculación a una VPC de tránsito.

Agregar la cuenta de AWS en CSM

Agregue la cuenta de AWS con valores generados por el script.

Procedimiento

- 1 Inicie sesión en CSM con la función Administrador empresarial.
- 2 Vaya a **CSM > Nubes > AWS**.
- 3 Haga clic en **+Agregar** e introduzca los siguientes detalles con el archivo de salida `aws_details.txt` generado a partir del script de NSX Cloud:

Opción	Descripción
Nombre	Introducir un nombre descriptivo para esta cuenta de AWS.
clave de acceso	Introducir la clave de acceso a la cuenta.
Clave secreta	Introducir la clave secreta de su cuenta.
etiquetas de nube	De forma predeterminada, esta opción está habilitada y permite que las etiquetas AWS sean visibles en NSX Manager.
Nombre de la función de puerta de enlace	El valor predeterminado es <code>nsx_pcg_service</code> . Puede encontrar este valor en la salida del script en el archivo <code>aws_details.txt</code> .

Resultados

Se agrega la cuenta de AWS en CSM.

En la pestaña VPC de CSM, puede ver todas las VPC de la cuenta de AWS.

En la pestaña Instancias de CSM, puede ver las instancias de EC2 en esta VPC.

Pasos siguientes

[Implementar PCG en una VPC de tránsito o autoadministrada](#)

Implementar o vincular NSX Public Cloud Gateway

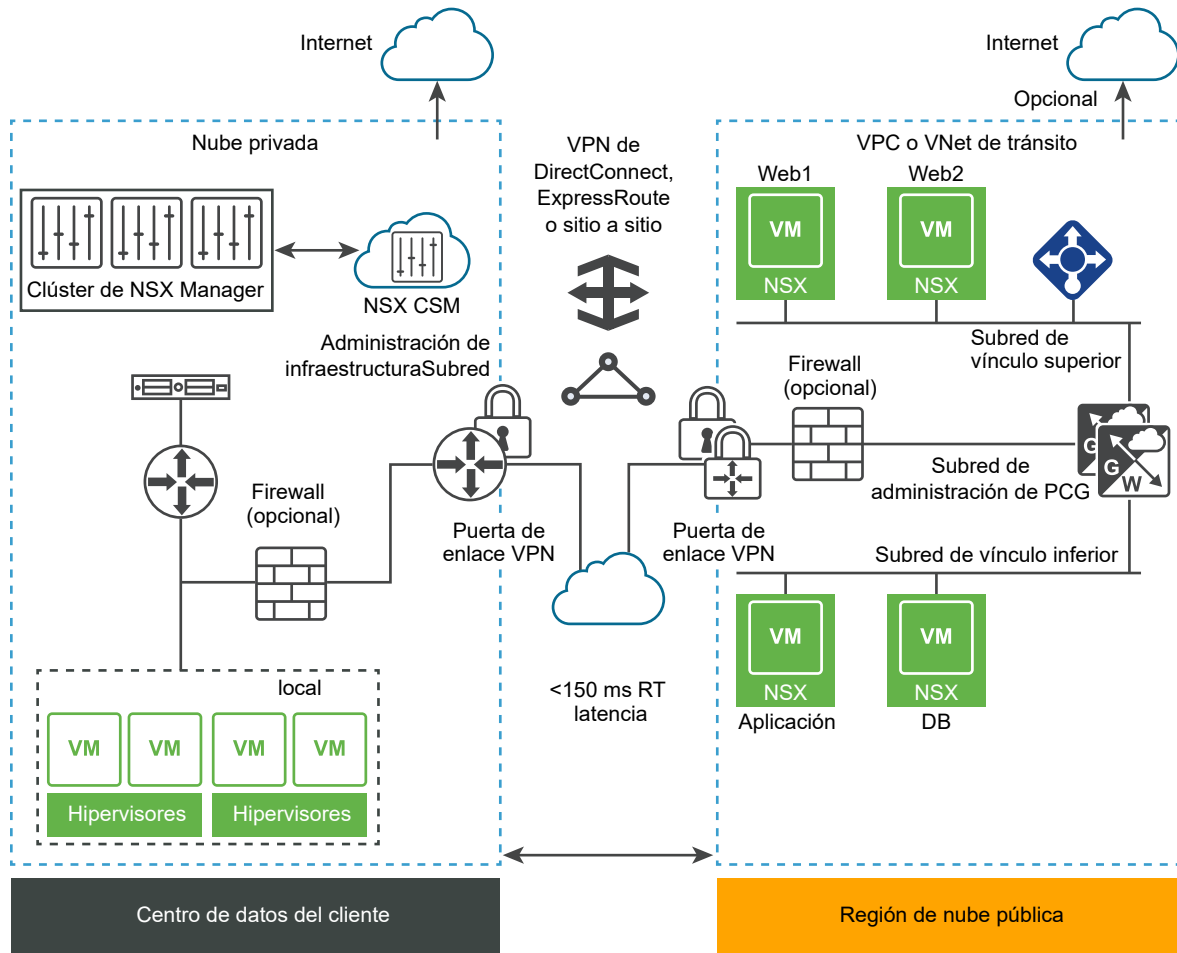
NSX Public Cloud Gateway (PCG) proporciona conectividad norte-sur entre la nube pública y los componentes de administración locales de NSX-T Data Center.

PCG puede ser un dispositivo de puerta de enlace independiente o uno compartido entre las VPC o las VNet de nube pública para lograr una topología de concentrador y radio.

Nota PCG se implementa en un único tamaño predeterminado para cada nube pública compatible:

Nube pública	Tipo de instancia PCG
AWS	c4.xlarge
	Nota Es posible que algunas regiones no admitan el tipo de instancia C4.xlarge. Para obtener información, consulte la documentación de AWS.
Microsoft Azure	DS3 v2 estándar

Figura 11-2. Arquitectura de NSX Public Cloud Gateway



VPC o VNet de tránsito o autoadministradas: cuando se implementa PCG en una VPC o una VNet, la VPC o la VNet se califican como *autoadministradas*, lo que quiere decir que puede poner las máquinas virtuales hospedadas en esta VPC o esta VNet bajo la administración de NSX. La VPC o la VNet también se califican como VPC o VNet de *tránsito* debido a que puede utilizar la PCG implementada en ellas para incorporar máquinas virtuales hospedadas en otras VPC o VNet. PCG utiliza las siguientes subredes que configuró en la VPC o la VNet. Consulte [Conectar la red de Microsoft Azure con la implementación de NSX-T Data Center local](#) o [Conectar la red de Amazon Web Services \(AWS\) con la implementación de NSX-T Data Center local](#).

- **Subred de administración:** esta subred se utiliza para tráfico de administración entre la instancia de NSX-T Data Center local y PCG. El rango recomendado es /28.
- **Subred de vínculo superior:** esta subred se utiliza para tráfico de Internet de norte a sur. El rango recomendado es /24.
- **Subred de vínculo inferior:** esta subred abarca el rango de direcciones IP de la máquina virtual de carga de trabajo y su tamaño debe definirse de manera acorde. Tenga en cuenta que posiblemente deba incorporar interfaces adicionales en las máquinas virtuales de carga de trabajo con fines de depuración.

VPC o VNet de equipo: las VPC o las VNet en las que no se implementó PCG, pero que se vinculan a una VPC o una VNet de tránsito, se denominan VPC o VNet *de equipo*.

La implementación de PCG se alinea con el plan de direcciones de red con nombres de dominio completos para los componentes de NSX-T Data Center y un servidor DNS que pueda resolver estos nombres de dominio completos.

Nota No se recomienda utilizar direcciones IP para la conexión de la nube pública con NSX-T Data Center mediante PCG, pero, si elige esta opción, no cambie las direcciones IP.

Implementar PCG en una VNet de tránsito o autoadministrada

Siga estas instrucciones para implementar PCG en su VNet de Microsoft Azure.

La VNet donde se va a implementar PCG puede actuar como una VNet de tránsito a la que pueden conectarse otras instancias de VNet (conocidas como VNet de equipos). Esta VNet también puede administrar máquinas virtuales y actuar como una VNet autoadministrada.

Siga estas instrucciones para implementar una instancia de PCG. Si desea vincular a una VNet de tránsito existente, consulte [Vincular a una VPC o VNet de tránsito](#).

Requisitos previos

- Las cuentas de nube pública ya deben estar agregadas en CSM.
- La VNet donde va a implementar PCG debe tener las subredes necesarias ajustadas de forma adecuada a la alta disponibilidad: *vínculo superior*, *vínculo inferior* y *administración*.

Procedimiento

- 1 Inicie sesión en CSM mediante una cuenta con la función Administrador empresarial (Enterprise Administrator).
- 2 Haga clic en **Nubes > Azure** y vaya a la pestaña **VNet**.
- 3 Haga clic en una VNet donde desee implementar PCG.
- 4 Haga clic en **Implementar puertas de enlace**. Se abre el asistente **Implementar puerta de enlace principal**.
- 5 Para las propiedades generales, siga estas directrices:

Opción	Descripción
Clave pública de SSH (SSH Public Key)	Proporcione una clave pública de SSH que se pueda validar mientras se implementa PCG. Esto es necesario para cada implementación de PCG.
Directiva de cuarentena en la VNet asociada	Deje esta opción en el modo predeterminado deshabilitado (disabled) la primera vez que implemente PCG. Puede cambiar este valor después de la incorporación de máquinas virtuales. Consulte Administrar directiva de cuarentena en <i>Guía de administración de NSX-T Data Center</i> para obtener más información.

Opción	Descripción
Cuenta de almacenamiento local (Local Storage Account)	<p>Cuando se agrega una suscripción de Microsoft Azure a CSM, aparece una lista de sus cuentas de almacenamiento de Microsoft Azure disponible para CSM. Seleccione la cuenta de almacenamiento del menú desplegable. Al continuar con la implementación de PCG, CSM copia el disco duro virtual (VHD) disponible al público de PCG en esta cuenta de almacenamiento de la región seleccionada.</p> <p>Nota Si la imagen de VHD ya se copió en esta cuenta de almacenamiento en la región para una implementación de PCG anterior, la imagen se utiliza desde esta ubicación para las implementaciones posteriores a fin de reducir el tiempo de implementación total.</p>
URL DE VHD (VHD URL)	<p>Si desea utilizar una imagen de PCG diferente que no está disponible en el repositorio de VMware público, puede introducir la dirección URL del disco duro virtual de PCG aquí. El disco duro virtual debe estar presente en la misma cuenta y región donde se creó esta VNet.</p> <p>Nota El disco duro virtual debe tener el formato de URL correcto. Le recomendamos que use la opción Haga clic para copiar de Microsoft Azure.</p>
Servidor proxy	<p>Seleccione el servidor proxy que desea utilizar para el tráfico hacia Internet desde esta PCG. Los servidores proxy se configuran en CSM. Puede seleccionar el mismo servidor proxy como CSM, seleccionar un servidor proxy diferente de CSM o seleccionar No hay servidor proxy.</p> <p>Consulte (Opcional) Configurar servidores proxy para obtener más información sobre cómo configurar los servidores proxy en CSM.</p>
Avanzado (Advanced)	<p>La configuración de DNS avanzada ofrece flexibilidad en la selección de servidores DNS para resolver los componentes de administración de NSX-T Data Center.</p>
Obtener a través del DHCP del proveedor de nube pública	<p>Seleccione esta opción si desea utilizar la configuración de DNS de Microsoft Azure. Se trata de la configuración de DNS predeterminada si no selecciona alguna de las opciones para reemplazarla.</p>
Reemplazar servidor DNS del proveedor de nube pública (Override Public Cloud Provider's DNS Server)	<p>Seleccione esta opción si desea proporcionar manualmente la dirección IP de uno o varios servidores DNS para resolver los dispositivos de NSX-T Data Center, así como las máquinas virtuales de la carga de trabajo en esta VNet.</p>
Usar el servidor DNS del proveedor de nube pública solo para dispositivos de NSX-T Data Center (Use Public Cloud Provider's DNS server only for NSX-T Appliances)	<p>Seleccione esta opción si desea utilizar el servidor DNS de Microsoft Azure para resolver los componentes de administración de NSX-T Data Center. Con esta opción, puede utilizar dos servidores DNS: uno para PCG que resuelve los dispositivos de NSX-T Data Center; el otro para la VNet que resuelve las máquinas virtuales de la carga de trabajo en esta VNet.</p>

6 Haga clic en **Siguiente** (Next).

7 Para las **Subredes** (Subnets), utilice las siguientes directrices:

Opción	Descripción
Habilitar HA para la puerta de enlace de nube NSX (Enable HA for NSX Cloud Gateway)	<p>Seleccione esta opción para habilitar la alta disponibilidad.</p>
Subredes (Subnets)	<p>Seleccione esta opción para habilitar la alta disponibilidad.</p>

Opción	Descripción
IP pública en la NIC de admin. (Public IP on Mgmt NIC)	Seleccione Asignar nueva dirección IP (Allocate New IP address) para proporcionar una dirección IP pública para la NIC de administración. Puede proporcionar la dirección IP pública manualmente si desea volver a utilizar una dirección IP pública libre.
IP pública en la NIC de vínculo superior	Seleccione Asignar nueva dirección IP para proporcionar una dirección IP pública para la NIC de vínculo superior. Puede proporcionar la dirección IP pública manualmente si desea volver a utilizar una dirección IP pública libre.

Pasos siguientes

Incorpore las máquinas virtuales de carga de trabajo. Consulte **Incorporación y administración de máquinas virtuales de cargas de trabajo** en *Guía de administración de NSX-T Data Center* para el flujo de trabajo del día N.

Implementar PCG en una VPC de tránsito o autoadministrada

Siga estas instrucciones para implementar PCG en su VPC de AWS.

La VPC en la que se implementa PCG puede actuar como una VPC de tránsito a la que pueden conectarse otras VPC (conocidas como VPC de equipo). Esta VPC también puede administrar máquinas virtuales y actuar como una VPC autoadministrada.

Siga estas instrucciones para implementar una instancia de PCG. Si desea vincular a una VPC de tránsito existente, consulte [Vincular a una VPC o VNet de tránsito](#).

Requisitos previos

- Las cuentas de nube pública ya deben estar agregadas en CSM.
- La VPC en la que va a implementar PCG debe tener las subredes necesarias correctamente ajustadas a la alta disponibilidad: *vínculo superior*, *vínculo inferior* y *administración*.
- La configuración de ACL de la red de VPC debe incluir una regla ALLOW entrante.

Procedimiento

- 1 Inicie sesión en CSM mediante una cuenta con la función Administrador empresarial (Enterprise Administrator).
- 2 Haga clic en **Nubes > AWS > <AWS_account_name>** y vaya a la pestaña **VPC**.
- 3 En la pestaña **VPC**, seleccione un nombre de región de AWS, por ejemplo, us-west. La región de AWS debe ser la misma donde se creó la VPC del equipo.
- 4 Seleccione una VPC de equipo configurada para NSX Cloud.
- 5 Haga clic en Implementar puertas de enlace.

6 Complete los detalles generales de la puerta de enlace:

Opción	Descripción
Archivo PEM	<p>Seleccione uno de los archivos PEM en el menú desplegable. Este archivo debe estar en la misma región donde se implementó NSX Cloud y donde se creó la VPC del equipo.</p> <p>Es un identificador único de la cuenta de AWS.</p>
Directiva de cuarentena en la VPC asociada	<p>Deje esta opción en el modo predeterminado deshabilitado (disabled) la primera vez que implemente PCG. Puede cambiar este valor después de la incorporación de máquinas virtuales. Consulte Administrar directiva de cuarentena en <i>Guía de administración de NSX-T Data Center</i> para obtener más información.</p>
Servidor proxy	<p>Seleccione el servidor proxy que desea utilizar para el tráfico hacia Internet desde esta PCG. Los servidores proxy se configuran en CSM. Puede seleccionar el mismo servidor proxy como CSM, seleccionar un servidor proxy diferente de CSM o seleccionar No hay servidor proxy.</p> <p>Consulte (Opcional) Configurar servidores proxy para obtener más información sobre cómo configurar los servidores proxy en CSM.</p>
Avanzado	<p>La configuración avanzada ofrece opciones adicionales si es necesario.</p>
Anular el identificador de AMI	<p>Utilice esta función avanzada para proporcionar un identificador de AMI distinto al que está disponible en la cuenta de AWS para PCG.</p>
Obtener a través del DHCP del proveedor de nube pública	<p>Seleccione esta opción si desea utilizar la configuración de AWS. Se trata de la configuración de DNS predeterminada si no selecciona alguna de las opciones para reemplazarla.</p>
Reemplazar servidor DNS del proveedor de nube pública (Override Public Cloud Provider's DNS Server)	<p>Seleccione esta opción si desea proporcionar manualmente la dirección IP de uno o varios servidores DNS para resolver los dispositivos de NSX-T Data Center, así como las máquinas virtuales de carga de trabajo en esta VPC.</p>
Usar el servidor DNS del proveedor de nube pública solo para dispositivos de NSX-T Data Center (Use Public Cloud Provider's DNS server only for NSX-T Appliances)	<p>Seleccione esta opción si desea utilizar el servidor DNS de AWS para resolver los componentes de administración de NSX-T Data Center. Con esta opción, puede utilizar dos servidores DNS: uno para PCG que resuelve los dispositivos de NSX-T Data Center; el otro para la VPC que resuelve las máquinas virtuales de carga de trabajo en esta VPC.</p>

7 Haga clic en Siguiente.

8 Complete los detalles de la subred.

Opción	Descripción
Habilitar alta disponibilidad para la puerta de enlace de nube pública	<p>La configuración recomendada es Habilitar, que configura un par de alta disponibilidad de activo/en espera para evitar un tiempo de inactividad no programado.</p>
Configuración de la puerta de enlace principal	<p>Seleccione una zona de disponibilidad, por ejemplo us-west-1a, en el menú desplegable como la puerta de enlace principal para alta disponibilidad.</p> <p>Asigne las subredes de vínculo superior, vínculo inferior y administración en el menú desplegable.</p>

Opción	Descripción
Configuración de la puerta de enlace secundaria	<p>Seleccione otra zona de disponibilidad, por ejemplo us-west-1b, en el menú desplegable como la puerta de enlace secundaria para alta disponibilidad.</p> <p>La puerta de enlace secundaria se utiliza cuando se produce un error en la puerta de enlace principal.</p> <p>Asigne las subredes de vínculo superior, vínculo inferior y administración en el menú desplegable.</p>
IP pública en la NIC de admin. (Public IP on Mgmt NIC)	<p>Seleccione Asignar nueva dirección IP (Allocate New IP address) para proporcionar una dirección IP pública para la NIC de administración. Puede proporcionar la dirección IP pública manualmente si desea volver a utilizar una dirección IP pública libre.</p>
IP pública en la NIC de vínculo superior	<p>Seleccione Asignar nueva dirección IP para proporcionar una dirección IP pública para la NIC de vínculo superior. Puede proporcionar la dirección IP pública manualmente si desea volver a utilizar una dirección IP pública libre.</p>

Haga clic en Implementar.

- 9 Supervisar el estado de la implementación de PCG principal (y la secundaria, si la seleccionó). Este proceso puede tardar entre 10 y 12 minutos.
- 10 Cuando PCG se implemente correctamente, haga clic en Finalizar.

Pasos siguientes

Incorpore las máquinas virtuales de carga de trabajo. Consulte **Incorporación y administración de máquinas virtuales de cargas de trabajo** en *Guía de administración de NSX-T Data Center* para el flujo de trabajo del día N.

Vincular a una VPC o VNet de tránsito

Puede vincular una o más VPC o VNet de equipo a una VPC o una VNet de tránsito.

Requisitos previos

- Compruebe que tiene una VPC o VNet de tránsito con una PCG en el estado **Activo**.
- Compruebe que la VPC/VNet que desea vincular esté conectada a la VPC o VNet de tránsito a través de VPN o emparejamiento.

- Compruebe que las VPC/VNet de tránsito estén en la misma región que las VPC/VNet de equipo.

Nota En la configuración de VPN de IPSec basada en rutas, debe especificar la dirección IP del puerto de la interfaz de túnel virtual (VTI). Esta IP debe estar en una subred diferente que las máquinas virtuales de carga de trabajo. Así se evitará que el tráfico entrante de las máquinas virtuales de carga de trabajo se dirija al puerto VTI, desde el que se descartará.

Nota En la nube pública, existe un límite predeterminado para la cantidad de reglas entrantes y salientes por grupo de seguridad, y NSX Cloud crea grupos de seguridad predeterminados. Eso afecta a la cantidad de VPC/VNet de equipo que se pueden vincular a una VPC/VNet de tránsito. Suponiendo 1 bloque CIDR por VPC/VNet, NSX Cloud admite 10 VPC o VNet de equipo por VPC/VNet de tránsito. Si tiene más de 1 CIDR en cualquier VPC/VNet de equipo, se reducirá el número de VPC de equipo compatibles por VPC/VNet de tránsito. Para ajustar los límites predeterminados, puede acceder a su proveedor de nube pública.

Procedimiento

- 1 Inicie sesión en CSM mediante una cuenta con la función Administrador empresarial (Enterprise Administrator).
- 2 Haga clic en **Nubes > AWS/Azure > <public cloud_account_name>** y vaya a la pestaña **VPC/VNet**.
- 3 En la pestaña **VPC** o **VNet**, seleccione el nombre de una región donde se alojan una o más VPC o VNet de equipo.
- 4 Seleccione una VPC o una VNet de equipo configurada para NSX Cloud.
- 5 Haga clic en **VINCULAR A VPC DE TRÁNSITO** o **VINCULAR A VNET DE TRÁNSITO**
- 6 Complete las opciones en la ventana **Vincular a VPC o VNet de tránsito**:

Opción	Descripción
VPC o VNet de tránsito	<p>En el menú desplegable, seleccione una VPC o VNet de tránsito. La VPC o VNet de tránsito que seleccione ya debe estar vinculada a esta VPC por medio de VPN o emparejamiento.</p> <p>Nota Si se conecta a VNet de tránsito, debe haber un reenviador de DNS configurado en esa VNet. Consulte la documentación de Microsoft Azure para obtener más información.</p>
Directiva predeterminada de cuarentena	<p>Deje esta opción en el modo predeterminado deshabilitado (disabled) la primera vez que implemente PCG. Puede cambiar este valor después de la incorporación de máquinas virtuales. Consulte Administrar directiva de cuarentena en <i>Guía de administración de NSX-T Data Center</i> para obtener más información.</p>

Pasos siguientes

Incorpore las máquinas virtuales de carga de trabajo. Consulte **Incorporación y administración de máquinas virtuales de cargas de trabajo** en *Guía de administración de NSX-T Data Center* para el flujo de trabajo del día N.

Entidades lógicas creadas automáticamente y grupos de seguridad nativos de la nube

La implementación de PCG en una VPC o una VNet de tránsito y su vinculación a una VPC o una VNet de equipo activa las configuraciones necesarias en NSX-T Data Center y la nube pública.

Entidades lógicas de NSX-T creadas automáticamente

En NSX-T Data Center se crea un conjunto de entidades lógicas.

Importante No elimine ninguna de estas entidades que se crean automáticamente.

Entidades del sistema

Las siguientes entidades se pueden ver en el **sistema**:

Tabla 11-3. Entidades del sistema creadas automáticamente

Entidad lógica del sistema	¿Cuántas se crean?	Nomenclatura	Ámbito
Zonas de transporte	Se crean dos zonas de transporte para cada VPC o VNet de tránsito	<ul style="list-style-type: none"> ■ TZ- <identificador_de_VPC /VNet>-OVERLAY ■ TZ- <identificador_de_VPC /VNet>-VLAN 	Ámbito: global
Nodos de transporte de Edge	Se crea un nodo de transporte de Edge para cada PCG que se implementa, dos en el caso de que se haga en el modo de alta disponibilidad.	<ul style="list-style-type: none"> ■ PublicCloudGatewayT N- <identificador_de_VPC /VNet> ■ PublicCloudGatewayT N- <identificador_de_VPC /VNet>-preferred 	Ámbito: global
Clúster de Edge	Se crea un clúster de Edge por cada PCG que se implementa, ya sea uno o en un par de alta disponibilidad.	PCG-cluster- <identificador_de_VPC/ VNet>	Ámbito: global

Entidades de inventario

Las siguientes entidades se crean en **Inventario**:

Tabla 11-4. Entidades de inventario creadas automáticamente

Entidad lógica de inventario	¿Cuántas se crean?	Nomenclatura	Ámbito
<p>Dominio</p> <p>Nota El objeto Dominio es una función experimental de NSX-T Data Center 2.4 y los dominios creados automáticamente están visibles en la interfaz de usuario. Sin embargo, los dominios ya no están visibles en la interfaz de usuario de NSX-T Data Center 2.4.1.</p>	Uno por VPC o VNet de tránsito	cloud-<identificador_de_VPC/VNet_de_tránsito>	Ámbito: se comparte entre todas las instancias de PCG.
<p>Grupos</p> <p>Nota En NSX-T Data Center, puede ver el dominio predeterminado. Sin embargo, en NSX-T Data Center 2.4.1, el objeto de dominio no está visible.</p>	<p>Dos grupos en el dominio default</p>	<ul style="list-style-type: none"> ■ cloud-default-route ■ cloud-metadata services 	Ámbito: se comparte entre todas las instancias de PCG
Grupos	<p>Un grupo</p> <p>Creado en el nivel de VPC o VNet de tránsito como un grupo principal de segmentos individuales que se crean en el nivel de VPC o VNet de equipo.</p>	cloud-<identificador_de_VPC/VNet_de_tránsito>-all-segments	Ámbito: compartido en todas las VPC o VNet de equipo
Grupos	<p>Dos grupos:</p> <ul style="list-style-type: none"> ■ Grupo de CIDR de red para todos los CIDR de la VPC o la VNet de equipo ■ Grupo de segmentos local para todos los segmentos administrados dentro de la VPC o la VNet de equipo 	<ul style="list-style-type: none"> ■ cloud-<identificador_de_VPC/VNet_de_equipo>-cidr ■ cloud-<identificador_de_VPC/VNet_de_equipo>-local-segments 	Ámbito: compartido en todas las VPC o VNet de equipo

Entidades de seguridad

Tabla 11-5. Entidades de seguridad creadas automáticamente

Entidad lógica de seguridad	¿Cuántas se crean?	Nomenclatura	Ámbito
Firewall distribuido (este-oeste)	Dos por VPC o VNet de tránsito: <ul style="list-style-type: none"> ■ Sin estado ■ Con estado 	<ul style="list-style-type: none"> ■ cloud-stateless-<ID VPC/VNet> ■ cloud-stateful-<ID VPC/VNet> 	<ul style="list-style-type: none"> ■ Regla con estado para permitir el tráfico dentro de segmentos administrados locales ■ Regla con estado para rechazar el tráfico procedente de máquinas virtuales no administradas
Firewall de puerta de enlace (norte-sur)	Uno por VPC o VNet de tránsito	cloud-<ID VPC/VNet tránsito>	

Entidades de redes

Las siguientes entidades se crean en diferentes etapas de la incorporación:

Figura 11-3. Entidades de redes de NSX-T Data Center creadas automáticamente una vez que se implementa PCG

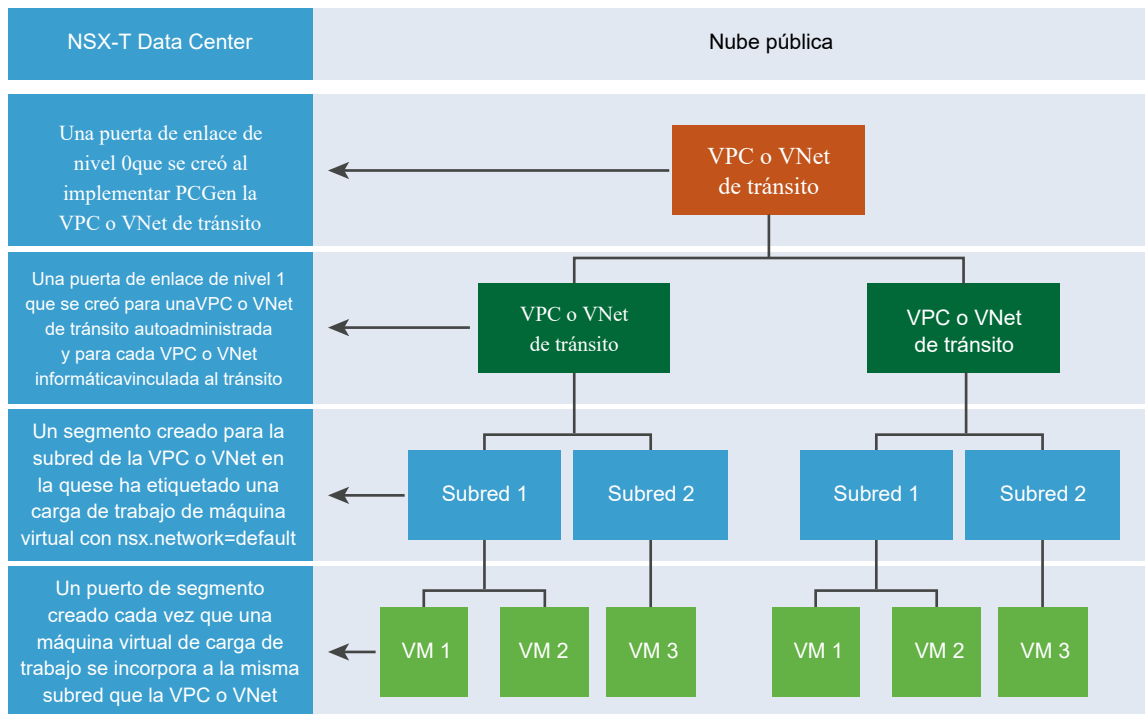


Tabla 11-6. Entidades de redes creadas automáticamente

Tarea de incorporación	Entidades lógicas creadas en NSX-T Data Center
PCG implementada en la VPC o la VNet de tránsito.	<ul style="list-style-type: none"> ■ Puerta de enlace de nivel 0 ■ Infrasegmento (conmutador de VLAN predeterminado) ■ Enrutador de nivel 1
VPC o VNet de equipo vinculadas a la VPC o la VNet de tránsito.	<ul style="list-style-type: none"> ■ Enrutador de nivel 1
Una máquina virtual de carga de trabajo en el que se instaló el agente NSX se etiqueta con el par clave:valor "nsx.network:default" en una subred de una VPC o una VNet autoadministradas o de equipo.	<ul style="list-style-type: none"> ■ Se crea un segmento para esta subred específica de la VPC o la VNet autoadministradas o de equipo. ■ Se crean puertos híbridos para cada máquina virtual de carga de trabajo etiquetada que tenga instalado el agente NSX en ella.
Se etiquetan más máquinas virtuales de carga de trabajo en la misma subred de la VPC o la VNet autoadministradas o de equipo.	<ul style="list-style-type: none"> ■ Se crean puertos híbridos para cada máquina virtual de carga de trabajo etiquetada que tenga instalado el agente NSX en ella.

Directivas de reenvío

Se configuran las siguientes tres reglas de reenvío para una VPC o una VNet de equipo, incluidas la VPC o la VNet de tránsito autoadministradas:

- Acceder a cualquier CIDR de la misma VPC de equipo a través de la red de la nube pública (subordinación)
- Enrutar el tráfico perteneciente a los servicios de metadatos de la nube pública a través de la red de la nube pública (subordinación)
- Enrutar todo lo que no esté en el bloque CIDR de la VPC o la VNet de equipo, o un servicio conocido, a través de la red de NSX-T Data Center (superposición)

Grupos de seguridad nativos de la nube creados automáticamente

En las nubes públicas se crean grupos de seguridad nativos de la nube.

Configuraciones de nube pública

En AWS:

- En la VPC de AWS, se agrega un nuevo conjunto de registros tipo A con el nombre `nsx-gw.vmware.local` en una zona hospedada privada de Amazon Route 53. La dirección IP asignada a este registro coincide con la dirección IP de administración de PCG que asigna AWS a través de DHCP y es diferente para cada VPC. Esta entrada DNS en la zona hospedada privada de Amazon Route 53 la utiliza NSX Cloud para resolver la dirección IP de PCG.

Nota Cuando se utilizan nombres de dominio DNS personalizados que están definidos en una zona hospedada privada de Amazon Route 53, los atributos **Resolución de DNS** y **Nombres de host de DNS** se deben establecer en **Sí** en la configuración de VPC de AWS.

- Se crea una dirección IP secundaria para la interfaz de vínculo superior de PCG. Una dirección IP elástica de AWS se asocia con esta dirección IP secundaria. Esta configuración es para SNAT.

En AWS y Microsoft Azure:

Los grupos de seguridad **gw** se aplican a las respectivas interfaces de PCG.

Tabla 11-7. Grupos de seguridad de nube pública creados por NSX Cloud para interfaces de PCG

Nombre del grupo de seguridad	¿Disponible en Microsoft Azure?	¿Disponible en AWS?	Nombre completo
gw-mgmt-sg	Sí	Sí	Grupo de seguridad de administración de puerta de enlace
gw-uplink-sg	Sí	Sí	Grupo de seguridad de vínculo superior de puerta de enlace
gw-vtep-sg	Sí	Sí	Grupo de seguridad de vínculo inferior de puerta de enlace

Tabla 11-8. Grupos de seguridad de nube pública creados por NSX Cloud para máquinas virtuales de carga de trabajo

Nombre del grupo de seguridad	¿Disponible en Microsoft Azure?	¿Disponible en AWS?	Descripción
cuarentena	Sí	No	Grupo de seguridad de cuarentena para Microsoft Azure
default	No	Sí	Grupo de seguridad de cuarentena para AWS
vm-underlay-sg	Sí	Sí	Grupo de seguridad que no es de máquina virtual de superposición
vm-override-sg	Sí	Sí	Grupo de seguridad de anulación de máquina virtual
vm-overlay-sg	Sí	Sí	Grupo de seguridad de máquina virtual de superposición (no se utiliza en la versión actual)

Tabla 11-8. Grupos de seguridad de nube pública creados por NSX Cloud para máquinas virtuales de carga de trabajo (continuación)

Nombre del grupo de seguridad	¿Disponible en Microsoft Azure?	¿Disponible en AWS?	Descripción
vm-outbound-bypass-sg	Sí	Sí	Grupo de seguridad de omisión saliente de máquina virtual (no se utiliza en la versión actual)
vm-inbound-bypass-sg	Sí	Sí	Grupo de seguridad de omisión entrante de máquina virtual (no se utiliza en la versión actual)

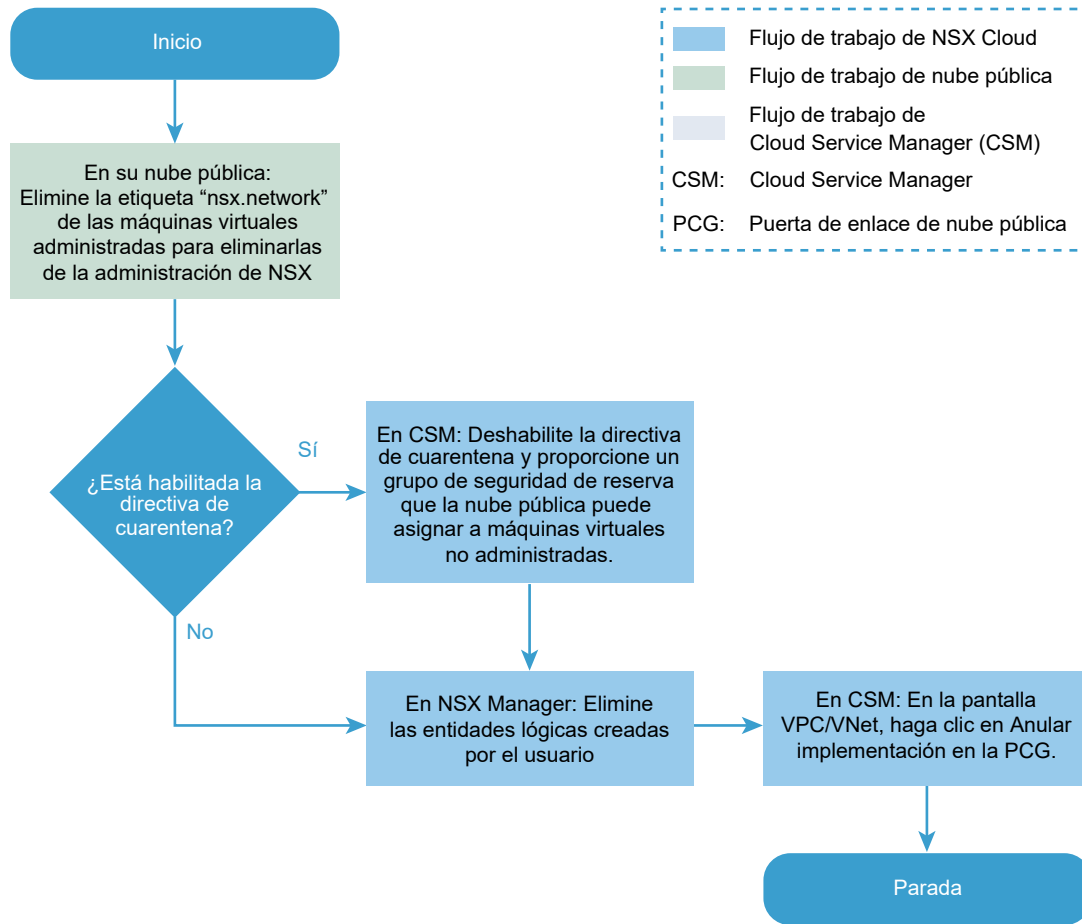
Anular la implementación de PCG

Consulte en este diagrama de flujo los pasos necesarios para anular la implementación de PCG.

Antes de anular la implementación de PCG, debe hacer lo siguiente:

- Asegúrese de que ninguna máquina virtual de carga de trabajo en la VPC o VNet esté administrada por NSX.
- Deshabilite la directiva de cuarentena.
- Elimine todas las entidades lógicas creadas por el usuario asociadas con la PCG.

Figura 11-4. Anular la implementación de PCG



Procedimiento

1 Desetiquetar máquinas virtuales en la nube pública

Antes de poder anular la implementación de PCG, todas las máquinas virtuales deben dejar de administrarse.

2 Deshabilitar la directiva de cuarentena, si está habilitada

Si se habilitó anteriormente, la directiva de cuarentena debe deshabilitarse para anular la implementación de PCG.

3 Eliminar entidades lógicas creadas por el usuario

Se deben eliminar todas las entidades lógicas asociadas con PCG creadas por el usuario.

4 Anular implementación de CSM

Para anular la implementación de PCG después de completar los requisitos previos, haga clic en Anular la implementación de la puerta de enlace en **Nubes > <Nube pública> > <VNet/VPC>** en CSM.

Desetiquetar máquinas virtuales en la nube pública

Antes de poder anular la implementación de PCG, todas las máquinas virtuales deben dejar de administrarse.

Vaya a la VPC o VNet en su nube pública y elimine la etiqueta `nsx.network` de las máquinas virtuales administradas.

Deshabilitar la directiva de cuarentena, si está habilitada

Si se habilitó anteriormente, la directiva de cuarentena debe deshabilitarse para anular la implementación de PCG.

Con la directiva de cuarentena habilitada, las máquinas virtuales se asignan a grupos de seguridad definidos por NSX Cloud. Al anular la implementación de PCG, deberá deshabilitar la directiva de cuarentena y especificar un grupo de seguridad de reserva que se pueda asignar a las máquinas virtuales cuando se eliminan de los grupos de seguridad de NSX Cloud.

Nota El grupo de seguridad de reserva debe ser un grupo de seguridad existente definido por el usuario en la nube pública. No puede usar cualquier grupo de seguridad de NSX Cloud como grupo de seguridad de reserva. Consulte [Entidades lógicas creadas automáticamente y grupos de seguridad nativos de la nube](#) para acceder a una lista de los grupos de seguridad de NSX Cloud.

Deshabilite la directiva de cuarentena para la VPC o VNet en la cual está anulando la implementación de PCG:

- Vaya a la VPC o VNet en CSM.
- En **Acciones > Editar configuraciones** >, desactive la opción **Cuarentena predeterminada**.
- Introduzca un valor para un grupo de seguridad de reserva que se asignará a las máquinas virtuales.

The screenshot shows the 'Edit VPC' configuration interface. At the top, there's a title 'Edit VPC:' followed by a dropdown menu. Below this, the 'Default Quarantine' toggle is shown in the 'Off' position. A yellow highlight is placed over the 'Fallback Security Group ID' field, which is marked with an asterisk and a help icon. A tooltip box is open over this field, containing the text: 'Provide the ID of an existing Security Group in your VPC that NSX Cloud can assign unmanaged VMs to. This is required when the Quarantine Policy is disabled.' To the right of the tooltip, there's a dropdown menu showing 'profile-1a' and a 'SAVE' button.

- Se le asignará un grupo de seguridad de reserva a todas las máquinas virtuales que están sin administrar o en cuarentena en esta VPC o VNet.
- Si todas las máquinas virtuales están sin administrar, se les asignará un grupo de seguridad de reserva.
- Si hay máquinas virtuales administradas mientras se deshabilita esta directiva de cuarentena, conservarán los grupos de seguridad de reserva asignados por NSX Cloud. La primera vez que se quita la etiqueta `nsx.network` de estas máquinas virtuales para que dejen de estar administradas por NSX, se les asigna el grupo de seguridad de reserva.

Nota Consulte **Administración de directivas de cuarentena** en la *Guía de administración de NSX-T Data Center* para obtener instrucciones y más información sobre los efectos de habilitar y deshabilitar la directiva de cuarentena.

Eliminar entidades lógicas creadas por el usuario

Se deben eliminar todas las entidades lógicas asociadas con PCG creadas por el usuario.

Identifique las entidades asociados a PCG y elimínelas.

Nota No elimine las entidades lógicas creadas automáticamente. Estas se eliminan automáticamente después de hacer clic en **Anular implementación de puerta de enlace** en CSM. Consulte [Entidades lógicas creadas automáticamente y grupos de seguridad nativos de la nube](#) para obtener la lista de las entidades lógicas creadas automáticamente.

Anular implementación de CSM

Para anular la implementación de PCG después de completar los requisitos previos, haga clic en Anular la implementación de la puerta de enlace en **Nubes > <Nube pública> > <VNet/VPC>** en CSM.

1 Inicie sesión en CSM y vaya a la nube pública:

- Si utiliza AWS, vaya a **Nubes > AWS > VPC**. Haga clic en la instancia de VPC en la que una o un par de instancias de PCG están implementadas y en ejecución.
- Si utiliza Microsoft Azure, vaya a **Nubes > Azure > VNet**s. Haga clic en la VNet en la que una o un par de instancias de PCG están implementadas y en ejecución.

2 Haga clic en Anular la implementación de la puerta de enlace.

Las entidades predeterminadas creadas por NSX Cloud se eliminan automáticamente cuando se anula la implementación de una PCG.