

# Cross-vCenter- Installationshandbuch für NSX

Update 9

Geändert am 21. FEBRUAR 2020

VMware NSX Data Center for vSphere 6.3



vmware®

Die aktuellste technische Dokumentation finden Sie auf der VMware-Website unter:

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

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie diese an:

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

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

**VMware Global, Inc.**  
Zweigniederlassung Deutschland  
Willy-Brandt-Platz 2  
81829 München  
Germany  
Tel.: +49 (0) 89 3706 17 000  
Fax: +49 (0) 89 3706 17 333  
[www.vmware.com/de](http://www.vmware.com/de)

Copyright © 2010–2020 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

# Inhalt

<b>1</b>	<b>Installationshandbuch zu Cross-vCenter</b>	<b>5</b>
<b>2</b>	<b>Übersicht über NSX for vSphere</b>	<b>6</b>
	Komponenten für NSX for vSphere	8
	Datenebene	8
	Steuerungskomponente	9
	Managementebene	10
	Nutzungsplattform	11
	NSX Edge	11
	NSX Services	14
<b>3</b>	<b>Übersicht über Cross-vCenter Networking and Security</b>	<b>16</b>
	Vorteile von Cross-vCenter NSX	16
	Funktionsweise von Cross-vCenter NSX	17
	Support-Matrix für NSX-Dienste in Cross-vCenter NSX	19
	Globaler Controller-Cluster	20
	Globale Transportzone	20
	Globale logische Switches	20
	Globale logische (Distributed) Router	21
	Universelle Firewallregeln	21
	Globale Netzwerk- und Sicherheitsobjekte	22
	Cross-vCenter NSX-Topologien	23
	Cross-vCenter NSX für mehrere und eine einzelne Site	23
	Lokaler Ausgang	25
	Ändern der NSX Manager-Rollen	26
<b>4</b>	<b>Vorbereitung für die Installation</b>	<b>28</b>
	Systemvoraussetzungen für NSX	28
	Für NSX for vSphere erforderliche Ports und Protokolle	30
	NSX und vSphere Distributed Switches	33
	Beispiel: Arbeiten mit einem vSphere Distributed Switch	35
	Installations-Workflow und Beispieltopologie für NSX	43
	Cross-vCenter NSX und der erweiterte verknüpfte Modus	44
<b>5</b>	<b>Aufgaben für die primären und sekundären NSX Manager</b>	<b>46</b>
	Installieren der virtuellen NSX Manager-Appliance	46
	Konfigurieren von Single Sign-On	51
	Registrieren von vCenter Server mit NSX Manager	53

- Konfigurieren eines Syslog-Servers für NSX Manager 55
- Installieren und Zuweisen einer Lizenz von NSX for vSphere 56
- Ausschließen von virtuellen Maschinen vom Schutz durch die Firewall 58

## **6 Konfigurieren der primären NSX Manager-Instanz 60**

- Bereitstellen des NSX-Controllers auf dem primären NSX Manager 60
- Vorbereiten von Hosts auf dem primären NSX Manager 64
- Konfigurieren des VXLAN vom primären NSX Manager aus 67
- Zuweisen eines Segment-ID-Pools und einer Multicast-Adresse auf dem primären NSX Manager 71
- Zuweisen einer primären Rolle zum NSX Manager 73
- Zuweisen eines globalen Segment-ID-Pools und einer globalen Multicast-Adresse auf dem primären NSX Manager 75
- Hinzufügen einer globalen Transportzone auf dem primären NSX Manager 77
- Hinzufügen eines globalen logischen Switches auf dem primären NSX Manager 78
- Verbinden von virtuellen Maschinen mit einem logischen Switch 80
- Hinzufügen eines globalen logischen (Distributed) Routers auf dem primären NSX Manager 81

## **7 Konfigurieren sekundärer NSX Manager 94**

- Hinzufügen sekundärer NSX Manager 94
- Vorbereiten von Hosts auf einer sekundären NSX Manager-Instanz 96
- Konfigurieren des VXLAN vom sekundären NSX Manager aus 98
- Zuweisen eines Segment-ID-Pools und einer Multicast-Adresse für einen sekundären NSX Manager 100
- Hinzufügen von Clustern zur globalen Transportzone 101

## **8 Vorgehensweise nach der Konfiguration von primären und sekundären NSX Managern 102**

## **9 Deinstallieren von NSX-Komponenten 103**

- Entfernen eines Hosts aus einem für NSX vorbereiteten Cluster 103
- Deinstallieren eines NSX Edge Services Gateways oder eines Distributed Logical Routers 104
- Deinstallieren eines logischen Switch 105
- Deinstallieren von NSX von Hostclustern 105
- Sicheres Entfernen einer NSX-Installation 107

# Installationshandbuch zu Cross-vCenter

1

Dieses Handbuch beschreibt, wie VMware NSX<sup>®</sup> for vSphere<sup>®</sup> in der Cross-vCenter NSX-Umgebung installiert wird. Zu den bereitgestellten Informationen gehören schrittweise Anleitungen für die Konfiguration sowie empfohlene Vorgehensweisen.

## Zielgruppe

Dieses Handbuch ist für alle Benutzer gedacht, die NSX in einer Cross-vCenter NSX-Umgebung installieren möchten. Die Informationen in diesem Handbuch sind für erfahrene Systemadministratoren bestimmt, die mit der Technologie virtueller Maschinen und dem Betrieb virtueller Datencenter vertraut sind. Dieses Handbuch setzt voraus, mit VMware vSphere, einschließlich VMware ESXi, vCenter Server und dem vSphere Web Client vertraut zu sein.

## VMware Technical Publications – Glossar

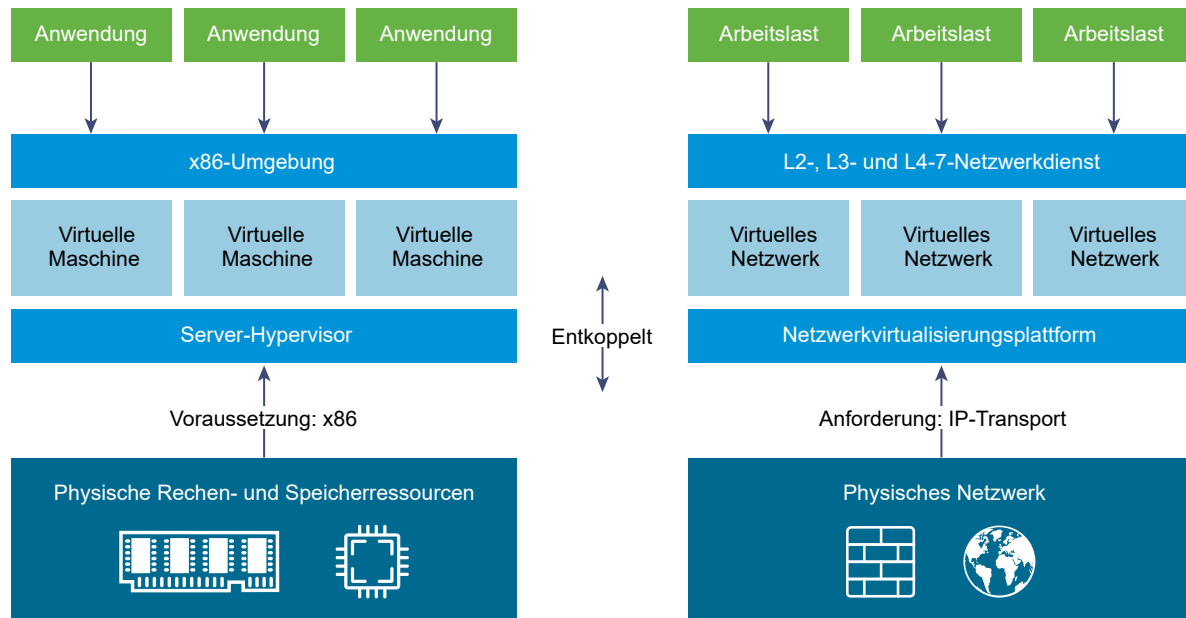
VMware Technical Publications enthält ein Glossar mit Begriffen, die Ihnen möglicherweise unbekannt sind. Definitionen von Begriffen, die in der technischen Dokumentation von VMware verwendet werden, finden Sie unter <http://www.vmware.com/support/pubs>.

# Übersicht über NSX for vSphere

## 2

Viele IT-Unternehmen profitieren erheblich von der Servervirtualisierung. Die Serverkonsolidierung reduziert die physische Komplexität und steigert die betriebliche Effizienz sowie die Fähigkeit zur dynamischen Umgestaltung von grundlegenden Ressourcen für eine schnellere und optimale Anpassung an die Anforderungen dynamischer Geschäftsanwendungen.

Die SDDC- (Software-Defined Datacenter) Architektur von VMware erweitert ihre Virtualisierungstechnologien auf die gesamte physische Datacenter-Infrastruktur. NSX for vSphere ist ein zentrales Produkt in der SDDC-Architektur. Mit NSX for vSphere liefert die Virtualisierung für die Netzwerke das, was sie bereits für Computing und Speicher geleistet hat. Mithilfe der Servervirtualisierung werden softwarebasierte virtuelle Maschinen (VMs) programmgesteuert erstellt, per Snapshot aufgenommen, gelöscht und wiederhergestellt. Mit der NSX for vSphere-Netzwerkvirtualisierung lassen sich ganze softwarebasierte virtuelle Netzwerke programmgesteuert erstellen, per Snapshot aufnehmen, löschen und wiederherstellen. Das Ergebnis ist eine innovative Herangehensweise an das Networking, die es Datacenter-Managern ermöglicht, überragende Flexibilität und Wirtschaftlichkeit zu erreichen, und darüber hinaus ein deutlich vereinfachtes Betriebsmodell für das zugrunde liegende physische Netzwerk anbietet. Dank seiner Kompatibilität mit jedem beliebigen IP-Netzwerk, einschließlich bestehender traditioneller Networking-Modelle und Fabric-Architekturen der nächsten Generation, stellt NSX for vSphere eine unterbrechungsfreie Lösung dar. Somit ist mit NSX for vSphere Ihre bestehende physische Netzwerkinfrastruktur alles, was Sie für die Bereitstellung eines Software-Defined Datacenters benötigen.



In der obigen Abbildung wird eine Analogie zwischen Computing und Netzwerkvirtualisierung hergestellt. Bei der Servervirtualisierung reproduziert eine Software-Abstraktionsschicht (Server-Hypervisor) die bekannten Attribute eines physischen x86-Servers (z. B. CPU, RAM, Festplatte, NIC) in Software und ermöglicht so deren programmgesteuerte Zusammensetzung in jeder beliebigen Kombination, mit der eine spezifische VM in Sekundenschnelle erstellt werden kann.

Bei der Netzwerkvirtualisierung reproduziert das funktionale Äquivalent eines Netzwerk-Hypervisors den kompletten Netzwerkdienstsatz von Schicht 2 bis 7 (z. B. Switching, Routing, Zugriffssteuerung, Firewalls, QoS und Load Balancing) in Software. Als Ergebnis können diese Dienste programmgesteuert in jeder beliebigen Kombination zusammengesetzt werden, um in Sekunden spezifische, isolierte virtuelle Netzwerke zu erstellen.

Damit lassen sich mit der Netzwerkvirtualisierung ähnliche Vorteile erzielen wie mit der Servervirtualisierung. So wie z. B. die VMs unabhängig von der zugrunde liegenden x86-Plattform sind und es IT-Mitarbeitern ermöglichen, die physischen Hosts als Pool für Computing-Ressourcen zu nutzen, sind die virtuellen Netzwerke unabhängig von der zugrunde liegenden IP-Netzwerk-Hardware und ermöglichen es IT-Mitarbeitern, das physische Netzwerk als Pool für Transportkapazitäten zu nutzen, die auf Anforderung verbraucht und umfunktioniert werden können. Anders als herkömmliche Architekturen können virtuelle Netzwerke bereitgestellt, geändert, gespeichert, gelöscht und programmgesteuert wiederhergestellt werden, ohne dass die grundlegende physische Hardware oder Topologie neu konfiguriert werden muss. Diese innovative Herangehensweise ans Networking sorgt für die vollständige Entfaltung des Potenzials eines Software-Defined Datacenters, indem sie alle Funktionalitäten, Leistung und Vorteile bekannter Server- und Speichervirtualisierungslösungen bietet.

NSX for vSphere kann über den vSphere Web Client, eine Befehlszeilenschnittstelle (CLI) und eine REST-API konfiguriert werden.

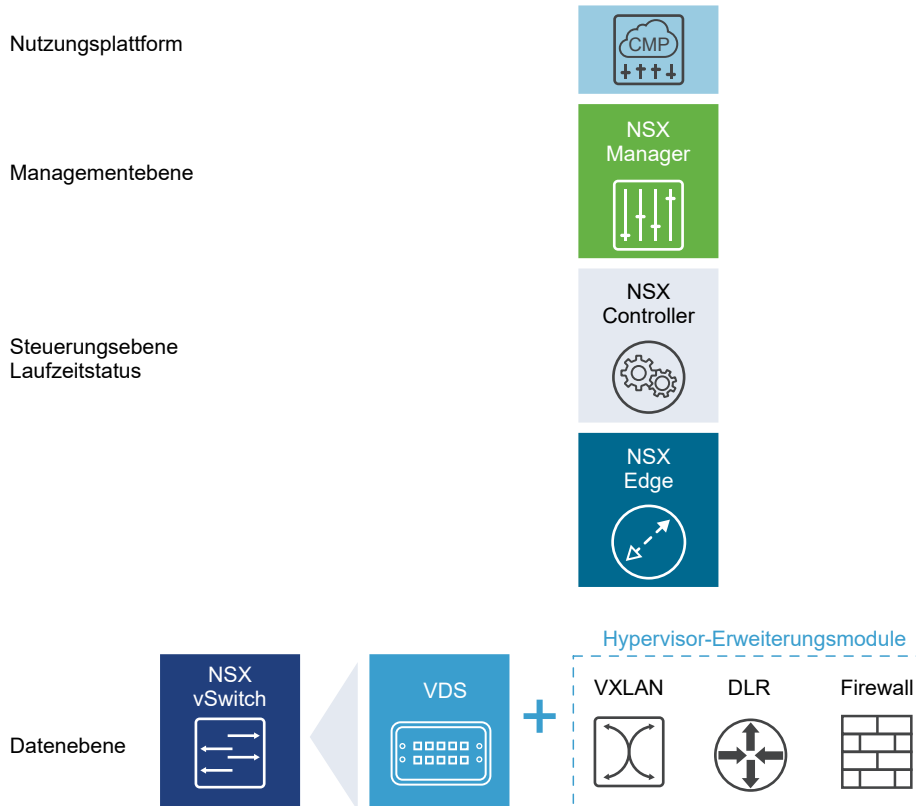
Dieses Kapitel enthält die folgenden Themen:

- **Komponenten für NSX for vSphere**

- [NSX Edge](#)
- [NSX Services](#)

## Komponenten für NSX for vSphere

In diesem Abschnitt werden die Komponenten der NSX for vSphere-Lösung beschrieben.



Beachten Sie, dass eine Cloud-Management-Plattform (CMP) keine Komponente von NSX for vSphere ist. Allerdings kann NSX for vSphere dank REST API und vorgefertigter Integration in VMware CMPs in nahezu jede CMP integriert werden.

## Datenebene

Die NSX-Datenebene besteht aus einem NSX vSwitch, der auf dem vSphere Distributed Switch (VDS) basiert, sowie aus weiteren Komponenten zur Aktivierung von Diensten. NSX-Kernelmodule, Userspace-Agents, Konfigurationsdateien und Installationsskripts werden in VIBs verpackt und innerhalb des Hypervisorkernels gestartet, um Dienste wie verteiltes Routing und logische Firewall bereitzustellen sowie um VXLAN-Bridging-Funktionalitäten zu aktivieren.



Der (vDS-basierte) NSX vSwitch abstrahiert das physische Netzwerk und bietet Switching auf Zugangsebene im Hypervisor. Diese Funktion ist entscheidend für die Netzwerkvirtualisierung, da sie von physischen Konstruktionen unabhängige logische Netzwerke wie etwa VLAN ermöglicht. Einige der Vorteile von vSwitch:

- Support für Overlay-Netzwerke mit Protokollen (wie VXLAN) und zentralisierte Netzwerk-Konfiguration Overlay-Netzwerke ermöglichen folgende Funktionalitäten:
  - Geringere Nutzung von VLAN-IDs im physischen Netzwerk
  - Erstellung eines flexiblen logischen Schicht 2(L2)-Overlays über vorhandene IP-Netzwerke auf vorhandener physischer Infrastruktur, ohne die Datacenter-Netzwerke umstrukturieren zu müssen
  - Bereitstellung von Kommunikation (ost-west und nord-süd) bei gleichzeitiger Bewahrung der Isolation zwischen Mandanten
  - Vom Overlay-Netzwerk unabhängige Arbeitslasten für Anwendungen und virtuelle Maschinen, die betrieben werden können, als wären sie mit einem physischen L2-Netzwerk verbunden
- Unterstützt eine riesige Anzahl an Hypervisoren
- Mehrere Funktionen wie etwa Port-Spiegelung, NetFlow/IPFIX, Konfigurationssicherung und -wiederherstellung, Netzwerk-Systemstatusprüfung, QoS und LACP stellen ein umfassendes Toolkit für Datenverkehr, Überwachung und Problembehebung innerhalb des virtuellen Netzwerks bereit

Die logischen Router stellen L2-Bridging vom logischen Netzwerkraum (VXLAN) zum physischen Netzwerk (VLAN) her.

Als Gatewaygerät dient üblicherweise eine virtuelle NSX Edge-Appliance. NSX Edge bietet L2, L3, Firewall für den Umgrenzungsbereich, Load Balancing sowie weitere Dienste wie SSL VPN und DHCP.

## Steuerungskomponente

Die NSX-Steuerungskomponente wird im NSX Controller-Cluster ausgeführt. NSX Controller ist ein erweitertes, verteiltes Zustandsverwaltungssystem, das Steuerungskomponentenfunktionen für logische Switching- und Routing-Funktionen für NSX bereitstellt. Er ist der zentrale Kontrollpunkt für alle logischen Switches innerhalb eines Netzwerks und enthält Informationen zu allen Hosts, logischen Switches (VXLANs) und verteilten logischen Router.

Der Controller-Cluster ist für die Verwaltung der verteilten Switching- und Routing-Module in den Hypervisoren verantwortlich. Über den Controller wird kein Datenverkehr auf Datenebene übertragen. Controller-Knoten werden in einem Cluster mit drei Mitgliedern bereitgestellt, um High Availability und Skalierung zu aktivieren. Ein Ausfall der Controller-Knoten wirkt sich nicht auf den Datenverkehr auf Datenebene aus.

NSX Controller verteilen die Netzwerkinformationen an Hosts. Um ein hohes Maß an Flexibilität zu erzielen, ist der NSX Controller für Skalierungen und HA geclustert. NSX Controller müssen in einem Cluster mit drei Knoten bereitgestellt werden. Die drei virtuellen Appliances liefern, verwalten und aktualisieren den Zustand aller Netzwerkfunktionen innerhalb der NSX-Domäne. NSX Manager wird zum Bereitstellen der NSX Controller-Knoten verwendet.

Die drei NSX Controller-Knoten bilden einen Controller-Cluster. Der Controller-Cluster benötigt ein Quorum (auch Mehrheit genannt), um ein „Split-Brain-Szenario“ zu vermeiden. In einem Split-Brain-Szenario rühren Dateninkonsistenzen von der Wartung zweier separater Datensätze her, die sich überlappen. Die Inkonsistenzen können durch Ausfälle und Probleme bei der Datensynchronisierung verursacht werden. Da drei Controller-Knoten vorhanden sind, ist bei einem Ausfall einer der NSX Controller-Knoten Datenredundanz sichergestellt.

Ein Controller-Cluster hat mehrere Rollen, darunter:

- API-Anbieter
- Persistenzserver
- Switch-Manager
- Logischer Manager
- Verzeichnisserver

Jede Rolle hat einen Controller-Masterknoten. Wenn ein Controller-Masterknoten für eine Rolle ausfällt, wählt der Cluster aus den verfügbaren NSX Controller-Knoten einen neuen Master für diese Rolle aus. Der neue NSX Controller-Masterknoten für diese Rolle teilt die verlorenen Teile der Arbeit unter den verbliebenen NSX Controller-Knoten neu auf.

NSX unterstützt drei Steuerungskomponenten-Modi von logischen Switches: Multicast, Unicast und Hybrid. Durch die Verwendung eines Controller-Clusters zum Verwalten von VXLAN-basierten logischen Switches wird der Bedarf an Multicast-Support in der physischen Netzwerkinfrastruktur verhindert. Sie müssen keine Multicast-Gruppen-IP-Adressen bereitstellen und auch nicht PIM-Routing oder IGMP-Snooping-Funktionen in physischen Switches oder Routern aktivieren. Somit entkoppeln die Unicast- und Hybrid-Modi NSX aus dem physischen Netzwerk. VXLANs im Unicast-Steuerungskomponentenmodus benötigen das physische Netzwerk nicht, um Multicast für die Verarbeitung von BUM-Datenverkehr (Broadcast, unbekanntes Unicast und Multicast) innerhalb eines logischen Switches zu unterstützen. Der Unicast-Modus repliziert den gesamten BUM-Datenverkehr lokal auf dem Host und benötigt keine physische Netzwerkkonfiguration. Im Hybrid-Modus wird ein Teil der BUM-Datenverkehrsreplizierung zum ersten physischen Hop-Switch ausgelagert, um eine bessere Leistung zu erreichen. Der Hybrid-Modus erfordert IGMP-Snooping auf dem ersten Hop-Switch und Zugriff auf einen IGMP-Abfrager in jedem VTEP-Subnetz.

## Managementebene

Die NSX-Managementebene wird vom NSX Manager, der zentralisierten Netzwerk-Managementkomponente von NSX, erstellt. Sie stellt einen zentralen Konfigurationspunkt und REST API-Einstiegspunkte bereit.

Der NSX Manager wird als virtuelle Appliance auf einem beliebigen ESX™-Host in Ihrer vCenter Server-Umgebung eingesetzt. NSX Manager und vCenter haben eine Eins-zu-eins-Beziehung. Für jede NSX Manager-Instanz gibt es einen vCenter Server. Dies gilt selbst für eine Cross-vCenter NSX-Umgebung.

In einer Cross-vCenter NSX-Umgebung finden sich ein primärer NSX Manager und einer oder mehrere sekundäre NSX Manager. Der primäre NSX Manager ermöglicht es Ihnen, globale logische Switches, globale logische (verteilte) Router sowie globale Firewallregeln zu erstellen. Sekundäre NSX Manager werden zur Verwaltung von den für den jeweiligen NSX Manager lokalen Netzwerkdiensten eingesetzt. In einer Cross-vCenter NSX-Umgebung können bis zu sieben sekundäre NSX Manager mit einem primären NSX Manager verknüpft sein.

## Nutzungsplattform

Die Nutzung von NSX kann direkt durch die Benutzerschnittstelle von NSX Manager gesteuert werden, die im vSphere Web Client verfügbar ist. Üblicherweise koppeln Endbenutzer die Netzwerkvirtualisierung an ihre Cloud Management Plattform für die Bereitstellung von Anwendungen. NSX stellt eine umfassende Integration in nahezu alle CMPs durch REST-APIs bereit. Eine sofort zu verwendende Integration ist auch durch VMware vCloud Automation Center, vCloud Director und OpenStack mit dem Neutron-Plug-In für NSX verfügbar.

## NSX Edge

Sie können NSX Edge als Edge Services Gateway (ESG) oder als verteilten logischen Router (Distributed Logical Router, DLR) installieren.

### Edge Services Gateway

Über das ESG können Sie auf alle NSX Edge-Dienste wie Firewall, NAT, DHCP, VPN, Load Balancing und High Availability zugreifen. Sie können mehrere virtuelle ESG-Appliances in einem Datencenter installieren. Jede virtuelle ESG-Apliance kann über insgesamt zehn Uplink- und interne Netzwerkschnittstellen verfügen. Mit einem Trunk kann ein ESG über bis zu 200 Teilschnittstellen verfügen. Die internen Schnittstellen werden mit gesicherten Portgruppen verbunden und dienen als das Gateway für alle geschützten virtuellen Maschinen in der Portgruppe. Das Subnetz, das der internen Schnittstelle zugewiesen ist, kann ein öffentlich gerouteter IP-Bereich, ein gerouteter privater RFC 1918-Adressbereich oder privater RFC 1918-Adressbereich sein, der NAT verwendet. Firewallregeln und andere NSX Edge-Dienste werden beim Datenverkehr zwischen Schnittstellen erzwungen.

Uplink-Schnittstellen von ESG stellen Verbindungen zu Uplink-Portgruppen her, die Zugriff auf ein gemeinsam genutztes Unternehmensnetzwerk oder einen Dienst haben, das bzw. der Zugriffsschichten im Netzwerk bereitstellt. Mehrere externe IP-Adressen können für Load Balancer-, Site-to-Site-VPN- und NAT-Dienste konfiguriert werden.

### Verteilter logischer Router

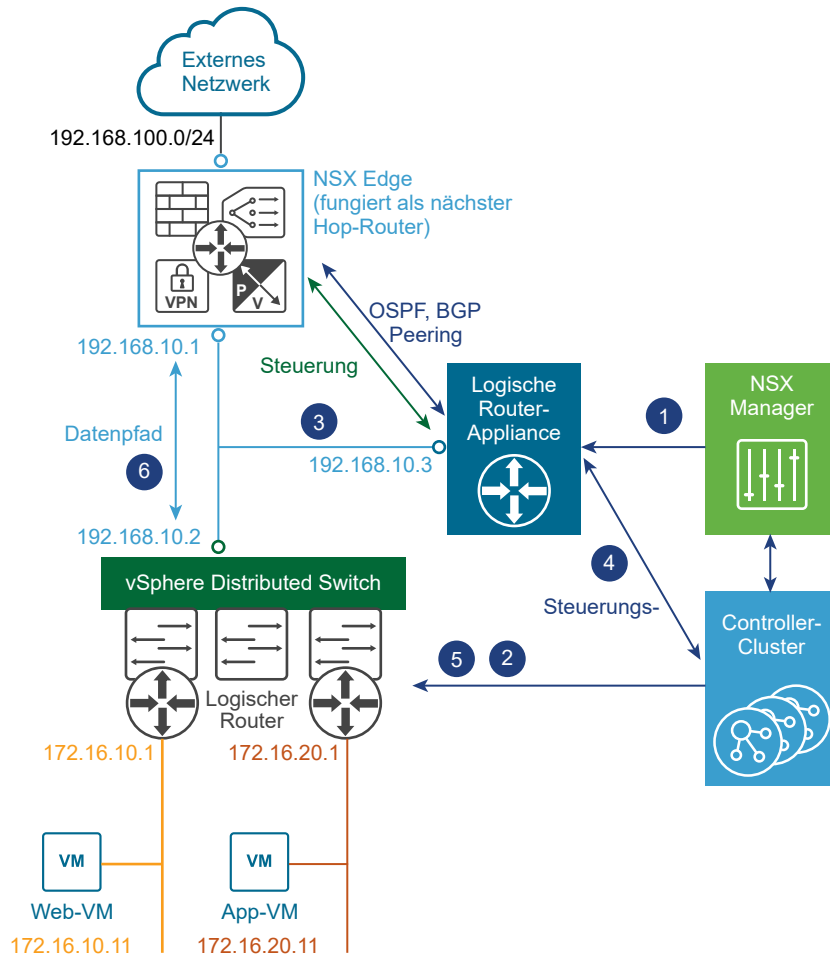
Der DLR stellt horizontal verteiltes Routing mit Mandanten-IP-Adressbereich und Datenpfadisolation bereit. Virtuelle Maschinen oder Arbeitslasten, die auf demselben Host auf verschiedenen Subnetzen vorhanden sind, können miteinander kommunizieren, ohne dass traditionelle Routing-Schnittstellen durchlaufen werden müssen.

Ein logischer Router kann bis zu acht Uplink-Schnittstellen haben und bis zu tausend interne Schnittstellen. Eine Uplink-Schnittstelle auf einem DLR ist in der Regel als Peer eines ESG konfiguriert und nutzt einen intervenierenden logischen Schicht 2-Transit-Switch zwischen dem DLR und dem ESG. Eine interne Schnittstelle auf einem DLR fungiert als Peer einer virtuellen Maschine, die auf einem ESXi-Hypervisor gehostet wird, über einen intervenierenden logischen Switch zwischen der virtuellen Maschine und dem DLR.

Der DLR verfügt über zwei Hauptkomponenten:

- Die DLR-Steuerungskomponente wird von der virtuellen DLR-Appliance bereitgestellt (auch als Kontroll-VM bezeichnet). Diese VM unterstützt dynamische Routing-Protokolle (BGP und OSPF), tauscht Routing-Updates mit dem nächsten Schicht 3-Hop-Gerät aus (normalerweise dem Edge Services Gateway) und kommuniziert mit dem NSX Manager und dem NSX Controller-Cluster. High Availability für die virtuelle DLR-Appliance wird durch Aktiv-Standby-Konfiguration unterstützt: ein Paar virtueller Maschinen in Aktiv-Standby-Modi werden bereitgestellt, wenn Sie den DLR bei aktivierter HA erstellen.
- Auf der Datenebene sind DLR-Kernel-Module (VIBs) vorhanden, die auf den ESXi-Hosts installiert werden, die Teil der NSX-Domäne sind. Die Kernel-Module gleichen den Linecards in einem modularen Gehäuse, das Schicht 3-Routing unterstützt. Die Kernel-Module verfügen über eine Routing-Informationsbasis (Routing Information Base, RIB) – auch als Routing-Tabelle bezeichnet – die per Push vom Controller-Cluster gesendet wird. Die Datenebenenfunktionen von Routensuche und ARP-Eintragssuche werden durch die Kernel-Module ausgeführt. Die Kernel-Module sind mit logischen Schnittstellen (so genannten LIFs) ausgestattet, über die die Verbindung mit den verschiedenen logischen Switches und möglichen VLAN-basierten Portgruppen erfolgt. Jeder LIF ist eine IP-Adresse, die das Standard-IP-Gateway für das logische L2-Segment darstellt, mit dem es verbunden ist, sowie eine vMAC-Adresse zugewiesen. Die IP-Adresse ist für jede LIF eindeutig, allen definierten LIFs hingegen wird dieselbe vMAC zugewiesen.

Abbildung 2-1. Logische Routing-Komponenten



- 1 Eine DLR-Instanz wird über die NSX Manager-Benutzeroberfläche (oder mit API-Aufrufen) erstellt und das Routing wird entweder mittels OSPF oder BGP aktiviert.
- 2 Der NSX Controller nutzt die Steuerungskomponente mit den ESXi-Hosts, um die neue DLR-Konfiguration, einschließlich der LIFs und ihrer zugewiesenen IP- und vMAC-Adressen, per Push zu senden.
- 3 Wenn man davon ausgeht, dass auch ein Routing-Protokoll auf dem nächsten Hop-Gerät (in diesem Beispiel einem NSX Edge [ESG]) aktiviert ist, wird zwischen dem ESG und der DLR-Kontroll-VM OSPF- oder BGP-Peering eingerichtet. Das ESG und der DLR können anschließend Routing-Informationen austauschen:
  - Die DLR-Kontroll-VM kann so konfiguriert werden, dass sie die IP-Präfixe für alle verbundenen logischen Netzwerke (im vorliegenden Beispiel 172.16.10.0/24 und 172.16.20.0/24) in OSPF erneut verteilt. Als Folge davon werden diese Routen-Ankündigungen per Push an das NSX Edge gesendet. Beachten Sie, dass der nächste Hop für diese Präfixe nicht die der Kontroll-VM zugewiesene IP-Adresse (192.168.10.3) ist, sondern die IP-Adresse, die die Datenebenenkomponente des DLR identifiziert (192.168.10.2). Die erste Adresse wird als DLR-„Protokolladresse“ bezeichnet, die zweite ist die „Weiterleitungsadresse“.

- Das NSX Edge sendet die Präfixe per Push an die Kontroll-VM, um IP-Netzwerke im externen Netzwerk zu erreichen. In den meisten Szenarien wird im Normalfall eine einzige Standardroute vom NSX Edge gesendet, weil diese den einzigen Ausgangspunkt zur physischen Netzwerkinfrastruktur darstellt.
- 4 Die DLR-Kontroll-VM sendet die vom NSX Edge erhaltenen IP-Routen per Push an den Controller-Cluster.
  - 5 Der Controller-Cluster ist für die Verteilung der Routen, die ihm von der DLR-Kontroll-VM mitgeteilt wurden, an die Hypervisoren verantwortlich. Jeder Controller-Knoten im Cluster übernimmt die Verantwortung für die Verteilung der Informationen für eine bestimmte logische Router-Instanz. In einer Bereitstellung mit mehreren bereitgestellten logischen Router-Instanzen wird die Last auf die Controller-Knoten verteilt. Normalerweise ist jedem bereitgestellten Mandanten eine separate logische Router-Instanz zugewiesen.
  - 6 Die DLR-Routing-Kernel-Module auf den Hosts verarbeiten den Datenpfad-Datenverkehr für die Kommunikation mit dem externen Netzwerk über das NSX Edge.

## NSX Services

Die NSX-Komponenten arbeiten zusammen, um folgende Funktionsdienste zur Verfügung zu stellen.

### Logische Switches

Eine Cloud-Bereitstellung oder ein virtuelles Datencenter enthalten diverse Anwendungen für zahlreiche Mandanten. Diese Anwendungen und Mandanten müssen aus Sicherheitsgründen, für Fehlerisolierungszwecke und zur Vermeidung der Überschneidung von IP-Adressen voneinander isoliert werden. NSX ermöglicht die Erstellung von mehreren logischen Switches, die jeweils eine eigene logische Broadcast-Domäne darstellen. Eine Anwendung oder eine Mandanten-VM können logisch an einen logischen Switch gebunden werden. Dies ermöglicht eine schnelle, flexible Bereitstellung bei gleichzeitiger Wahrung aller Vorteile von Broadcast-Domänen eines physischen Netzwerks (VLANs) ohne die Probleme von physischen Schicht-2-Sprawls und ohne Spanning-Tree-Probleme.

Ein logischer Switch wird verteilt und kann alle Hosts in vCenter (oder alle Hosts in einer Cross-vCenter NSX-Umgebung) umspannen. Dies ermöglicht die Mobilität virtueller Maschinen (vMotion) innerhalb des Datencenters ohne Beschränkungen durch die Grenzen der physischen Schicht 2 (VLAN). Die physische Infrastruktur ist nicht durch MAC/FIB-Tabellengrenzen beschränkt, weil die Broadcast-Domäne beim logischen Switch in der Software enthalten ist.

### Logische Router

Routing bietet die notwendigen Weiterleitungsinformationen zwischen Schicht 2-Broadcast-Domänen, wodurch Sie die Größe von Schicht 2-Broadcast-Domänen verringern und die Netzwerk-Effizienz und -Größe verbessern können. NSX dehnt diese Informationen auf Orte aus, an denen sich die Arbeitslasten für horizontales Routing befinden. Dies ermöglicht eine direktere Kommunikation zwischen virtuellen Maschinen ohne die kosten- und zeitaufwendige Erweiterung von Hops. Gleichzeitig bieten die logischen NSX-Router auch vertikale Verbindungen, wodurch Mandanten für den Zugriff auf öffentliche Netzwerke aktiviert werden.

## Logische Firewall

Die logische Firewall bietet Sicherheitsmechanismen für dynamische virtuelle Datacenter. Mit der Komponente „verteilte Firewall“ der logischen Firewall können Sie virtuelle Datacenterentitäten, z. B. virtuelle Maschinen, anhand der VM-Namen und -Attribute, Benutzeridentitäten und vCenter-Objekte, z. B. Datacenter und Hosts, segmentieren sowie Segmentierungen anhand herkömmlicher Netzwerkattribute wie IP-Adressen, VLANs usw. durchführen. Die Edge-Firewall-Komponente hilft Ihnen dabei, essenzielle Sicherheitsanforderungen für den Umgrenzungsbereich etwa durch den Aufbau von auf IP/VLAN-Konstrukten basierten DMZs und Mandantenisolierung in virtuellen mehrinstanzfähigen Datacentern zu erfüllen.

Die Flow Monitoring-Funktion zeigt Netzwerkaktivitäten zwischen virtuellen Maschinen auf der Anwendungsprotokollebene an. Sie können diese Informationen zum Überprüfen des Netzwerkverkehrs, zum Definieren und zum Verfeinern von Firewallrichtlinien und zum Identifizieren von Netzwerkbedrohungen verwenden.

## Logische virtuelle private Netzwerke (VPNs)

Mit SSL VPN-Plus können Remotebenutzer auf private Firmenanwendungen zugreifen. IPSec VPN bietet Interkonnektivität verschiedener Sites zwischen einer NSX Edge-Instanz und Remote-Sites mit NSX oder Hardware-Routern/VPN-Gateways von Drittanbietern. Mit L2 VPN können Sie Ihr Datacenter erweitern, indem Sie zulassen, dass virtuelle Maschinen die Netzwerkkonnektivität über geografische Grenzen hinaus wahren und dabei dieselben IP-Adressen beibehalten.

## Logischer Load Balancer

Der Load Balancer von NSX Edge verteilt die Client-Verbindungen, die auf eine einzelne virtuelle IP-Adresse (VIP) ausgerichtet sind, über mehrere Ziele, die als Mitglieder eines Load-Balancing-Pools konfiguriert wurden. Er verteilt eingehende Dienstanforderungen über mehrere Server gleichmäßig auf eine Weise, dass die Lastverteilung für die Benutzer transparent ist. Das Load Balancing hilft deshalb dabei, optimale Ressourcennutzung, maximalen Durchsatz und minimale Reaktionszeit zu erreichen sowie Überlastung zu vermeiden.

## Service Composer

Mit Service Composer können Sie Netzwerk- und Sicherheitsdienste für Anwendungen in einer virtuellen Infrastruktur bereitstellen und zuweisen. Sie können diese Dienste einer Sicherheitsgruppe zuweisen. Diese Dienste werden mithilfe einer Sicherheitsrichtlinie auf die virtuellen Maschinen in der Sicherheitsgruppe angewendet.

## Erweiterbarkeit von NSX

Drittanbieter von Lösungen können ihre Lösungen mit der NSX-Plattform integrieren. Dadurch können ihre Kunden die VMware-Produkte und die Lösungen unserer Partner in integrierter Weise nutzen. Rechenzentrumsbetreiber können komplexe virtuelle Multi-Tier-Netzwerke in Sekundenschnelle bereitstellen, unabhängig von der zugrunde liegenden Netzwerktopologie oder den zugrunde liegenden Komponenten.

# Übersicht über Cross-vCenter Networking and Security

# 3

NSX 6.2 oder höher ermöglicht Ihnen die Verwaltung mehrerer vCenter NSX-Umgebungen von einem einzelnen primären NSX Manager aus.

Dieses Kapitel enthält die folgenden Themen:

- Vorteile von Cross-vCenter NSX
- Funktionsweise von Cross-vCenter NSX
- Support-Matrix für NSX-Dienste in Cross-vCenter NSX
- Globaler Controller-Cluster
- Globale Transportzone
- Globale logische Switches
- Globale logische (Distributed) Router
- Universelle Firewallregeln
- Globale Netzwerk- und Sicherheitsobjekte
- Cross-vCenter NSX-Topologien
- Ändern der NSX Manager-Rollen

## Vorteile von Cross-vCenter NSX

NSX-Umgebungen, die mehr als ein vCenter Server-System enthalten, können zentral verwaltet werden.

Es gibt viele Gründe, warum mehrere vCenter Server-Systeme erforderlich sein können, z. B.:

- Zum Überwinden der Skalierungsgrenzen von vCenter Server
- Zur Aufnahme von Produkten, z. B. Horizon View oder Site Recovery Manager, die dedizierte oder mehrere vCenter Server-Systeme benötigen
- Zum Trennen von Umgebungen, z. B. nach Geschäftseinheit, Mandant, Organisation oder Umgebungstyp



Wenn in NSX 6.1 und früheren Versionen mehrere vCenter NSX-Umgebungen bereitgestellt werden, müssen sie separat verwaltet werden. In NSX 6.2 und höher können Sie auf dem primären NSX Manager universelle Objekte erstellen, die über alle vCenter Server-Systeme in der Umgebung hin synchronisiert werden.

Cross-vCenter NSX enthält diese Funktionen:

- Erhöhte Spanne logischer NSX-Netzwerke. Dieselben logischen Netzwerke stehen in der gesamten vCenter NSX-Umgebung zur Verfügung. Deshalb ist es für virtuelle Maschinen in jedem Cluster auf jedem vCenter Server-System möglich, sich mit demselben logischen Netzwerk zu verbinden.
- Zentrale Verwaltung der Sicherheitsrichtlinien. Firewallregeln werden von einer zentralen Stelle aus verwaltet und gelten für die virtuelle Maschine unabhängig vom Speicherort oder dem vCenter Server-System.
- Unterstützung neuer Mobilitätsgrenzen in vSphere 6, einschließlich Cross-vCenter und vMotion über große Entfernungen zwischen logischen Switches.
- Erweiterte Unterstützung für Multi-Site-Umgebungen, von Metro-Entfernungen bis zu 150 ms RTT. Dies umfasst sowohl Aktiv/Aktiv- als auch Aktiv/Passiv-Datencenter.

Cross-vCenter NSX-Umgebungen haben mehrere Vorteile:

- Zentralisiertes Management von globalen Objekten und eine Reduzierung des Administrationsaufwands.
- Höhere Mobilität der Arbeitslasten – VMs können zwischen vCenter Servern verschoben werden, ohne dass sie neu konfiguriert oder Firewallregeln geändert werden müssen.
- Erweiterte NSX-Multisite- und Notfallplanfunktionen

---

**Hinweis** Die Cross-vCenter NSX-Funktionalität wird mit vSphere 6.0 und höher unterstützt.

---

## Funktionsweise von Cross-vCenter NSX

In einer Cross-vCenter NSX-Umgebung haben Sie mehrere vCenter Server, denen jeweils ein eigener NSX Manager zugeordnet werden muss. Einem NSX Manager wird die Rolle des primären NSX Manager zugeteilt, die übrigen erhalten die Rolle eines sekundären NSX Manager.

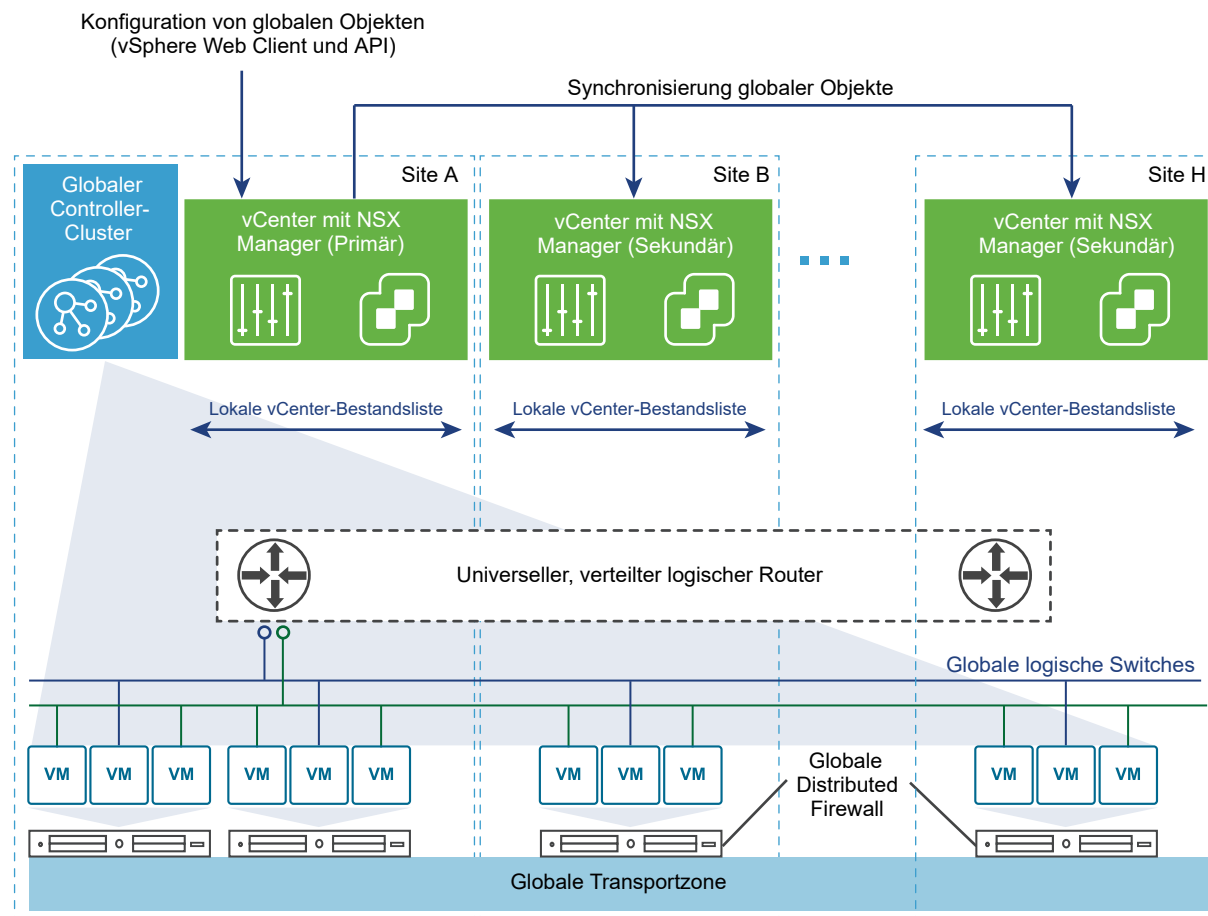
Der primäre NSX Manager wird zur Bereitstellung eines globalen Controller-Clusters genutzt, der die Steuerungsebene für die Cross-vCenter NSX-Umgebung bereitstellt. Die sekundären NSX Manager haben keine eigenen Controller-Cluster.

Der primäre NSX Manager kann globale Objekte wie etwa globale logische Switches erstellen. Diese Objekte werden durch den NSX-Synchronisierungsdienst für alle sekundären NSX Manager synchronisiert. Sie können diese Objekte von einem sekundären NSX Manager anzeigen lassen, können diese dort jedoch nicht bearbeiten. Zur Verwaltung globaler Objekte müssen Sie den primären NSX Manager benutzen. Der primäre NSX Manager kann für die Konfiguration von jedem beliebigen sekundären NSX Manager in der Umgebung verwendet werden.

Sowohl auf dem primären als auch auf jedem sekundären NSX Manager können Objekte wie z. B. logische Switches und logische (verteilte) Router erstellt werden, die für diese spezifische vCenter NSX-Umgebung gelten. Diese existieren nur innerhalb der vCenter NSX-Umgebung, in der sie erstellt wurden. Auf den anderen NSX Managern in der Cross-vCenter NSX-Umgebung werden sie nicht angezeigt.

Einem NSX Manager kann auch eine eigenständige Rolle zugewiesen werden. Diese Zuweisung entspricht Umgebungen vor NSX 6.2 mit einem einzigen NSX Manager und einem vCenter. Ein eigenständiger NSX Manager kann keine globalen Objekte erstellen.

**Hinweis** Wenn Sie die Rolle einer primären NSX Manager-Instanz in „Eigenständig“ ändern und globale Objekte in der NSX-Umgebung vorhanden sind, wird NSX Manager die Transitrolle zugewiesen. Die globalen Objekte sind weiterhin vorhanden, können aber nicht geändert werden. Zudem können keine neuen globalen Objekte erstellt werden. Sie können globale Objekte aus der Transitrolle löschen. Die Transitrolle darf nur vorübergehend verwendet werden, z. B. wenn der primäre NSX Manager geändert wird.



## Support-Matrix für NSX-Dienste in Cross-vCenter NSX

Ein Teil der NSX-Dienste ist für die globale Synchronisierung in Cross-vCenter NSX verfügbar. Dienste, die für die globale Synchronisierung nicht verfügbar sind, können für eine lokale Verwendung mit NSX Manager konfiguriert werden.

**Tabelle 3-1. Support-Matrix für NSX-Dienste in Cross-vCenter NSX**

NSX-Dienst	Details	Unterstützt Cross-vCenter NSX die Synchronisierung?
Logischer Switch	Transportzone	Ja
	Logischer Switch	Ja
L2-Bridges		Nein
Routing	Logischer (verteilter) Router	Ja
	Logische (verteilte) Router-Appliance	Nein, bedingt durch den Systemaufbau. Wenn mehrere Appliances pro globalem logischen Router erforderlich sind, müssen sie auf jedem NSX Manager erstellt werden. Dies ermöglicht unterschiedliche Konfigurationen pro Appliance, was in einer Umgebung mit konfiguriertem lokalem Ausgang möglicherweise erforderlich ist.
	NSX Edge Services Gateway	Nein
Logische Firewall	verteilte Firewall	Ja
	Ausschlussliste	Nein
	SpoofGuard	Nein
	Flow Monitoring für verbundene Flows	Nein
	Netzwerk Service Insertion	Nein
	Edge-Firewall	Nein
VPN		Nein
Logischer Load Balancer		Nein
Andere Edge-Dienste		Nein
Service Composer		Nein
Netzwerk-Erweiterbarkeit		Nein
Netzwerk- und Sicherheitsobjekte	IP-Adressengruppen (IP Set)	Ja
	MAC-Adressengruppen (MAC Set)	Ja
	IP-Pools	Nein

**Tabelle 3-1. Support-Matrix für NSX-Dienste in Cross-vCenter NSX (Fortsetzung)**

NSX-Dienst	Details	Unterstützt Cross-vCenter NSX die Synchronisierung?
	Sicherheitsgruppen	Ja, aber die Konfiguration der Mitgliedschaft unterscheidet sich von der Mitgliedschaft nicht globaler Sicherheitsgruppen. Ausführliche Informationen erhalten Sie unter „Erstellen einer Sicherheitsgruppe“ im Dokument <i>Administratorhandbuch für NSX</i> .
	Dienste	Ja
	Dienstgruppen	Ja
Sicherheits-Tags		Ja
Hardware-Gateway (auch bezeichnet als Hardware-VTEP)		Nein. Ausführliche Informationen erhalten Sie unter „Beispielkonfiguration für ein Hardware-Gateway“ im Dokument <i>Administratorhandbuch für NSX</i> .

## Globaler Controller-Cluster

Jede Cross-vCenter NSX-Umgebung verfügt über einen globalen Controller-Cluster, der dem primären NSX Manager zugeordnet ist. Sekundäre NSX Manager haben keinen Controller-Cluster.

Da der globale Controller-Cluster der einzige Controller-Cluster für die Cross-vCenter NSX-Umgebung ist, verwaltet er Informationen über globale logische Switches und globale logische Router sowie logische Switches und logische Router, die für ein vCenter NSX-Paar lokal sind.

Um Überlappungen von Objekt-IDs zu vermeiden, werden für globale und lokale Objekte separate ID-Pools verwaltet.

## Globale Transportzone

In einer Cross-vCenter NSX-Umgebung darf es nur eine globale Transportzone geben.

Die globale Transportzone wird auf dem primären NSX Manager erstellt und auf die sekundären NSX Manager synchronisiert. Cluster, die an globalen logischen Netzwerken teilnehmen müssen, müssen von ihren NSX Managern zur globalen Transportzone hinzugefügt werden.

## Globale logische Switches

Globale logische Switches ermöglichen Schicht 2-Netzwerke, um mehrere Sites einzuschließen.

Wenn Sie in einer globalen Transportzone einen logischen Switch erstellen, erstellen Sie einen globalen logischen Switch. Dieser Switch ist in allen Clustern in der universellen Transportzone verfügbar. Die universelle Transportzone kann Cluster in einem beliebigen vCenter in der Cross-vCenter NSX-Umgebung umfassen.

Der Segment-ID-Pool dient dem Zuweisen von VNIs zu logischen Switches und der globale Segment-ID-Pool dient dem Zuweisen von VNIs zu globalen logischen Switches. Diese Pools dürfen sich nicht überlappen.

Sie müssen einen globalen logischen Router für das Routing zwischen den globalen logischen Switches verwenden. Für ein Routing zwischen einem globalen logischen Switch und einem logischen Switch müssen Sie ein Edge Services Gateway verwenden.

## Globale logische (Distributed) Router

Globale logische (Distributed) Router ermöglichen eine zentralisierte Verwaltung und eine Routing-Konfiguration, die im globalen logischen Router, Cluster oder auf Host-Ebene angepasst werden können.

Wenn Sie einen globalen logischen Router erstellen, müssen Sie auswählen, ob Sie den lokalen Ausgang aktivieren, da dies nach der Erstellung nicht mehr geändert werden kann. Mit dem lokalen Ausgang können Sie steuern, welche Routen für ESXi-Hosts basierend auf einem Bezeichner, der Gebietsschema-ID, bereitgestellt werden.

Jedem NSX Manager wird eine Gebietsschema-ID zugewiesen, die standardmäßig auf die NSX Manager-UUID festgelegt ist. Sie können die Gebietsschema-ID auf den folgenden Ebenen umgehen:

- Globaler logischer Router
- Cluster
- ESXi-Host

Wenn Sie den lokalen Ausgang nicht aktivieren, wird die Gebietsschema-ID ignoriert und alle mit dem globalen logischen Router verbundenen ESXi-Hosts erhalten dieselben Routen. Ob Sie den lokalen Ausgang in einer Cross-vCenter NSX-Umgebung aktivieren möchten oder nicht, ist eine Designabwägung, die aber nicht für alle Cross-vCenter NSX-Konfigurationen erforderlich ist.

## Universelle Firewallregeln

Mit der verteilten Firewall in einer Cross-vCenter NSX-Umgebung ist eine zentralisierte Verwaltung von Regeln möglich, die auf alle vCenter Server in Ihrer Umgebung angewendet werden. Es unterstützt Cross-vCenter vMotion, wodurch Sie Arbeitslasten oder virtuelle Maschinen aus einem vCenter Server in einen anderen verschieben können, und erweitert die Software-definierte Datensicherheit nahtlos.

Da Ihr Datacenter horizontale Skalierung benötigt, wird der vorhandene vCenter Server möglicherweise nicht auf die gleiche Ebene skaliert. Dadurch müssen Sie möglicherweise einen Satz an Anwendungen auf neuere Hosts verschieben, die von einem anderen vCenter Server verwaltet werden. Alternativ müssen Sie ggf. Anwendungen von Staging bis zur Produktion in eine Umgebung verschieben, in der Staging-Server von einem vCenter-Server und Produktionsserver von einem anderen vCenter-Server verwaltet werden. Die verteilte Firewall unterstützt diese vCenter-übergreifenden vMotion-Szenarien durch sich replizierende Firewall-Richtlinien, die Sie auf bis zu sieben sekundären NSX Manager für den primären NSX Manager definieren können.

Vom primären NSX Manager aus können Sie Regelabschnitte der verteilten Firewall erstellen, die für die globale Synchronisierung markiert sind. Sie können mehrere universelle L2-Regelabschnitte und mehrere universelle L3-Regelabschnitte erstellen. Universelle Abschnitte werden immer am oberen Rand von primären und sekundären NSX Managern aufgeführt. Diese Abschnitte und ihre Regeln werden mit allen sekundären NSX Manager-Instanzen in Ihrer Umgebung synchronisiert. Regeln in anderen Abschnitten bleiben für den entsprechenden NSX Manager lokal.

Die folgenden Funktionen der verteilten Firewall werden in einer Cross-vCenter NSX-Umgebung nicht unterstützt:

- Ausschlussliste
- SpoofGuard
- Flow Monitoring für verbundene Flows
- Netzwerk Service Insertion
- Edge-Firewall

Service Composer unterstützt keine universelle Synchronisierung, daher können Sie damit keine Regeln für die verteilte Firewall im universellen Abschnitt erstellen.

## Globale Netzwerk- und Sicherheitsobjekte

Sie können benutzerdefinierte Netzwerk- und Sicherheitsobjekte zur Verwendung in den Regeln für die verteilte Firewall im universellen Abschnitt erstellen.

Universelle Sicherheitsgruppen (USGs) können Folgendes aufweisen:

- Universelle IP Set
- Universelle MAC Set
- Universelle Sicherheitsgruppen
- Universelle Sicherheits-Tags
- Dynamische Kriterien

Universelle Netzwerk- und Sicherheitsobjekte werden ausschließlich auf dem primären NSX Manager erstellt, gelöscht und aktualisiert. Sie können jedoch auf dem sekundären NSX Manager gelesen werden. Der globale Synchronisierungsdienst synchronisiert globale Objekte sofort in vCenter sowie bei Bedarf mit der erzwungenen Synchronisierung.

Universelle Sicherheitsgruppen werden in zwei Bereitstellungstypen verwendet: mehrere live Cross-vCenter-NSX-Umgebungen und aktive Cross-vCenter NSX-Standby-Bereitstellungen, in denen eine Site zu einem bestimmten Zeitpunkt aktiv ist, während sich die anderen Sites in Standby befinden. Es können nur aktive Standby-Bereitstellungen über universelle Sicherheitsgruppen mit dynamischer Mitgliedschaft basierend auf dem VM-Namen oder mit statischer Mitgliedschaft basierend auf einem globalen

Sicherheits-Tag verfügen. Nachdem eine universelle Sicherheitsgruppe erstellt worden ist, kann sie nicht mehr bearbeitet und somit nicht mehr für die aktive Standby-Szenariofunktionalität aktiviert oder deaktiviert werden. Die Mitgliedschaft wird nur durch eingeschlossene Objekte definiert, Sie können keine ausgeschlossenen Objekte verwenden.

Universelle Sicherheitsgruppen können nicht mit dem Service Composer erstellt werden. Mit dem Service Composer erstellte Sicherheitsgruppen sind lokal für den jeweiligen NSX Manager.

## Cross-vCenter NSX-Topologien

Sie können Cross-vCenter NSX auf einer einzelnen physischen Site oder auf mehreren Sites bereitstellen.

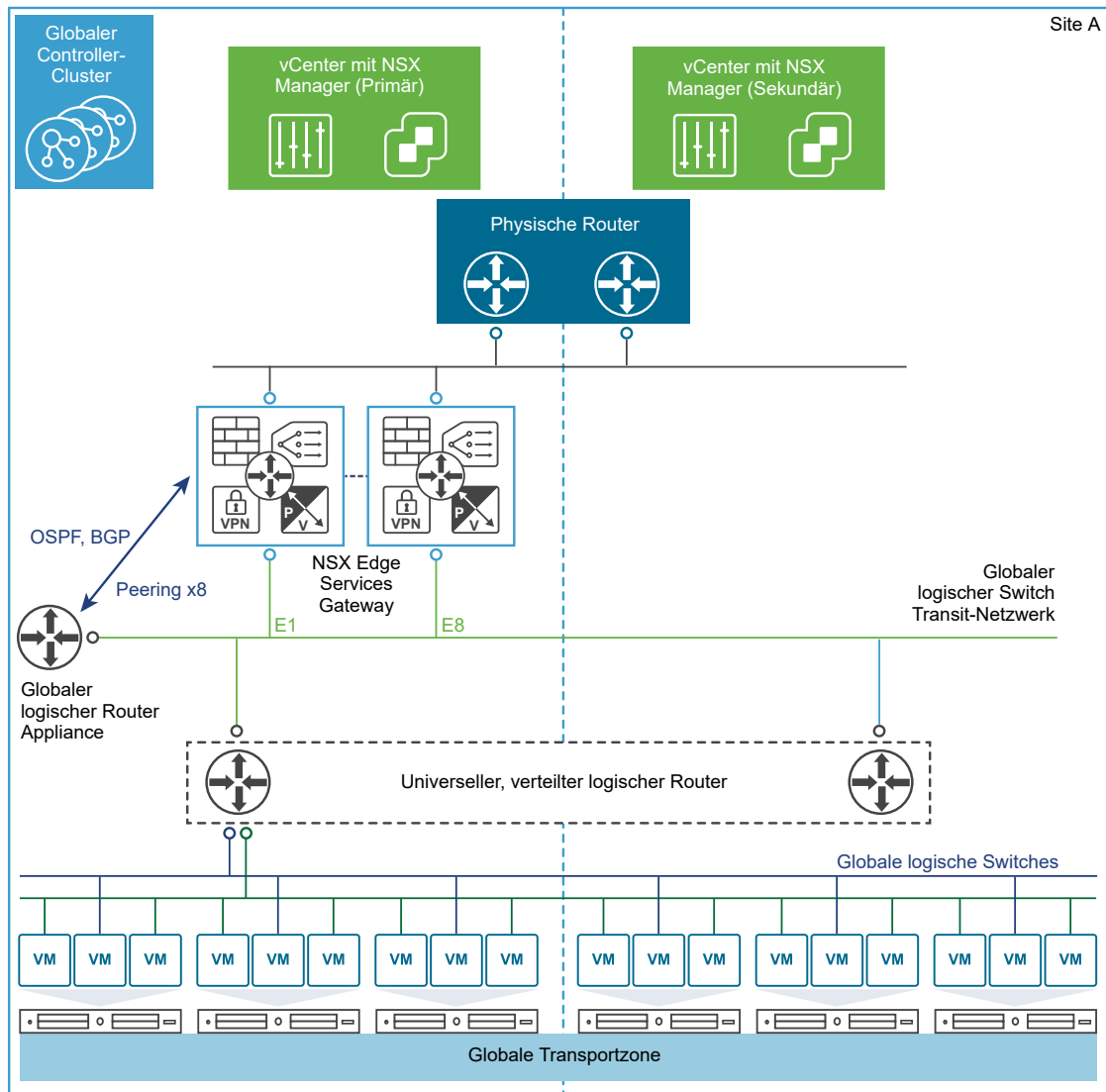
### Cross-vCenter NSX für mehrere und eine einzelne Site

Eine Cross-vCenter NSX-Umgebung ermöglicht Ihnen die Verwendung derselben logischen Switches und weiterer Netzwerkobjekte über mehrere vCenter NSX-Setups hinweg. Die vCenter können sich auf derselben Site oder auf unterschiedlichen Sites befinden.

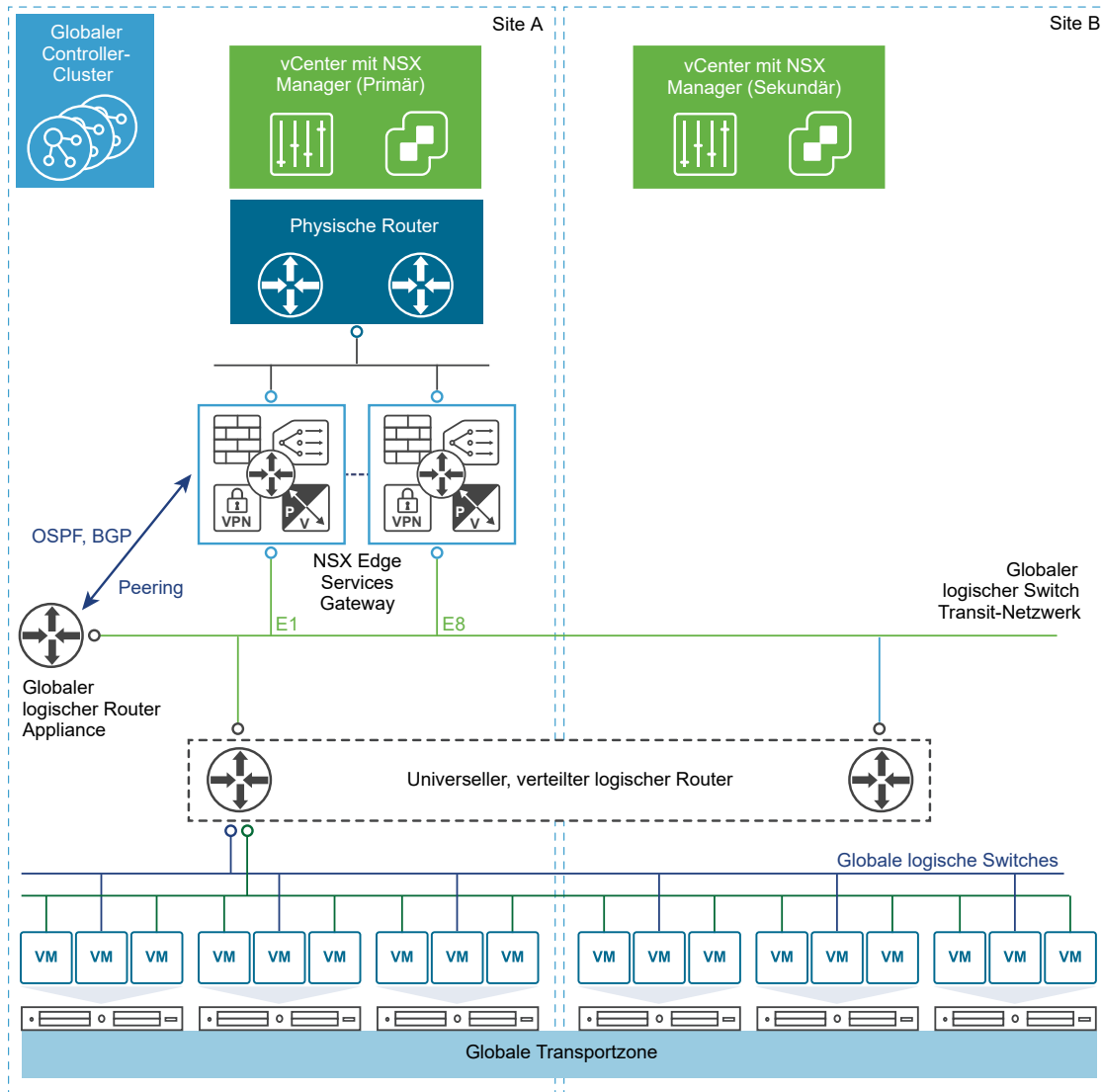
Unabhängig davon, ob die Cross-vCenter NSX-Umgebung innerhalb einer einzelnen Site enthalten ist oder mehrere Sites umspannt, kann eine ähnliche Konfiguration verwendet werden. Diese beiden Beispieltopologien bestehen aus:

- Einer globalen Transportzone, die alle Cluster in der Site oder den Sites enthält.
- Globalen logischen Switches, die der globalen Transportzone zugewiesen sind. Zwei globalen logischen Switches zum Verbinden der virtuellen Maschinen und einem Switch als Transit-Netzwerk für den Router-Uplink.
- Virtuellen Maschinen, die zu den globalen logischen Switches hinzugefügt werden
- Einem globalen logischen Router mit einer NSX Edge-Appliance zum Aktivieren des dynamischen Routings. Die globale logische Router-Appliance verfügt über interne Schnittstellen auf den globalen logischen VM-Switches und über eine Uplink-Schnittstelle auf dem globalen logischen Switch des Transit-Netzwerks.
- Edge Services Gateways (ESGs), die mit dem Transit-Netzwerk und dem physischen Ausgangs-Router-Netzwerk verbunden sind.

Abbildung 3-1. Cross-vCenter NSX in einer einzelnen Site





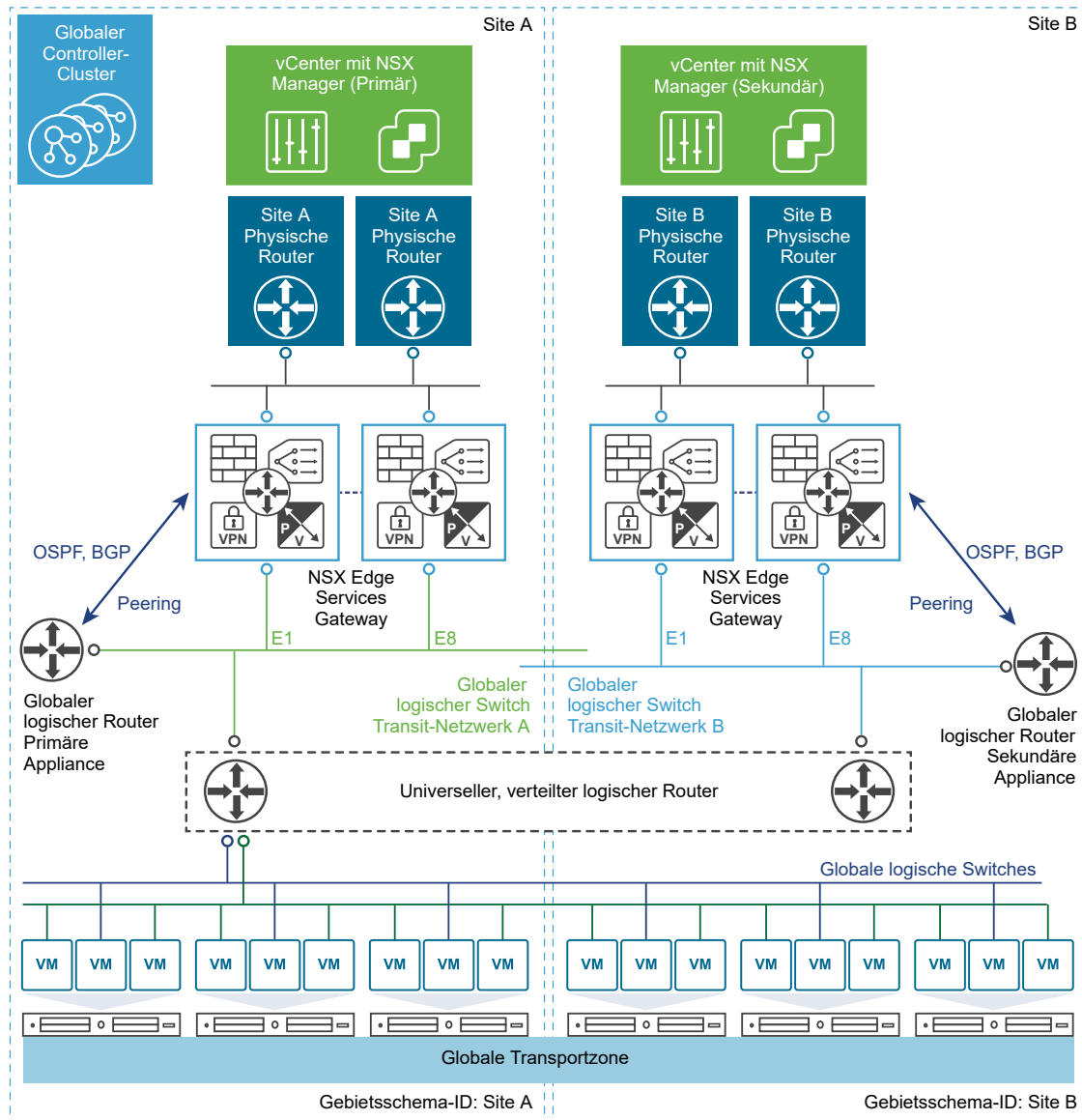
**Abbildung 3-2. Cross-vCenter NSX, die zwei Sites umspannt**

## Lokaler Ausgang

Alle Sites einer Multi-Site-Umgebung von Cross-vCenter NSX können für den ausgehenden Datenverkehr dieselben physischen Router verwenden. Wenn die Routen für den ausgehenden Datenverkehr allerdings angepasst werden müssen, muss beim Erstellen des globalen logischen Routers die Funktion „Lokaler Ausgang“ aktiviert werden.

Über einen lokalen Ausgang können Sie Routen am globalen logischen Router, im Cluster oder auf Hostebene anpassen. In diesem Beispiel einer Cross-vCenter NSX-Umgebung mit mehreren Sites ist der lokale Ausgang aktiviert. Die Edge Services Gateways (ESGs) an jeder Site haben eine Standardroute, auf die der Datenverkehr über die physischen Router dieser Site gesendet wird. Der globale logische Router ist mit zwei Appliances konfiguriert, eine für jede Site. Die Appliances erlernen die Routen von den ESGs ihrer Site. Die erlernten Routen werden an den globalen Controller-Cluster gesendet. Da der lokale

Ausgang aktiviert ist, wird diesen Routen die Gebietsschema-ID für diese Site zugewiesen. Der globale Controller-Cluster sendet die Routen mit den passenden Gebietsschema-IDs an die Hosts. Routen, die an der Site A-Appliance erlernt wurden, werden an die Hosts auf Site A gesendet, und die Routen, die an der Site B-Appliance erlernt wurden, werden an die Hosts auf Site B gesendet.



## Ändern der NSX Manager-Rollen

Einem NSX Manager kann die primäre, sekundäre oder eigenständige Rolle zugewiesen sein. Auf dem primären NSX Manager läuft spezielle Synchronisierungssoftware, die alle globalen Objekte auf sekundäre NSX Manager synchronisiert.

Es ist wichtig zu verstehen, was passiert, wenn Sie die Rolle eines NSX Manager ändern.

**Als primär festlegen**

Mit diesem Vorgang wird die Rolle eines NSX Manager als primär festgelegt und die Synchronisierungssoftware gestartet. Dieser Vorgang schlägt fehl, wenn NSX Manager bereits die primäre oder eine sekundäre Rolle einnimmt.

**Als eigenständig festlegen (von sekundär)**

Dieser Vorgang legt die Rolle von NSX Manager auf den eigenständigen oder Transitmodus fest. Dieser Vorgang schlägt möglicherweise fehl, wenn NSX Manager bereits die eigenständige Rolle einnimmt.

**Als eigenständig festlegen (von primär)**

Dieser Vorgang setzt den primären NSX Manager auf den eigenständigen oder Transitmodus zurück, beendet die Synchronisierungssoftware und entfernt alle sekundären NSX Manager aus der Registrierung. Dieser Vorgang schlägt möglicherweise fehl, wenn NSX Manager bereits die eigenständige Rolle einnimmt oder einer der sekundären NSX Manager nicht erreichbar ist.

**Verbindung zum primären Manager trennen**

Wenn Sie diesen Vorgang auf einem sekundären NSX Manager ausführen, wird der sekundäre NSX Manager einseitig vom primären NSX Manager getrennt. Dieser Vorgang sollte verwendet werden, wenn auf dem primären NSX Manager ein nicht behebbarer Fehler aufgetreten ist und Sie den sekundären NSX Manager bei einem neuen primären Manager registrieren möchten. Wenn der ursprüngliche primäre NSX Manager wieder funktionsfähig ist, führt dessen Datenbank den sekundären NSX Manager weiterhin als registriert auf. Um dieses Problem zu beheben, verwenden Sie die Option **force**, wenn Sie den sekundären Manager vom ursprünglichen primären Manager trennen oder die Registrierung aufheben möchten. Mit der Option **force** wird der sekundäre NSX Manager aus der Datenbank des ursprünglichen primären NSX Manager entfernt.

# Vorbereitung für die Installation

# 4

In diesem Abschnitt werden die Systemanforderungen für NSX for vSphere und die Ports beschrieben, die offen sein müssen.

Dieses Kapitel enthält die folgenden Themen:

- [Systemvoraussetzungen für NSX](#)
- [Für NSX for vSphere erforderliche Ports und Protokolle](#)
- [NSX und vSphere Distributed Switches](#)
- [Beispiel: Arbeiten mit einem vSphere Distributed Switch](#)
- [Installations-Workflow und Beispieltopologie für NSX](#)
- [Cross-vCenter NSX und der erweiterte verknüpfte Modus](#)

## Systemvoraussetzungen für NSX

Bevor Sie NSX installieren oder aktualisieren, prüfen Sie Ihre Netzwerkkonfiguration und -ressourcen. Sie können einen NSX Manager pro vCenter Server, eine Guest Introspection-Instanz pro ESXi™-Host und mehrere NSX Edge-Instanzen pro Datacenter installieren.

## Hardware

Diese Tabelle enthält die Hardwareanforderungen für NSX-Appliances.

**Tabelle 4-1. Hardwareanforderungen für Appliances**

Appliance	Arbeitsspeicher	vCPU	Festplattenspeicher
NSX Manager	16 GB (24 GB für größere NSX-Bereitstellungen)	4 (8 für größere NSX-Bereitstellungen)	60 GB
NSX Controller	4 GB	4	28 GB

**Tabelle 4-1. Hardwareanforderungen für Appliances (Fortsetzung)**

Appliance	Arbeitsspeicher	vCPU	Festplattenspeicher
NSX Edge	Kompakt: 512 MB	Kompakt: 1	Kompakt, Groß: 1 Festplatte mit 584 MB + 1 Festplatte mit 512 MB Quad Large: 1 Festplatte mit 584 MB + 2 Festplatten mit 512 MB Sehr groß: 1 Datenträger 584 MB + 1 Datenträger 2 GB + 1 Datenträger 512 MB
	Groß: 1 GB	Groß: 2	
	Quad Large: 2 GB	Quad Large: 4	
	Sehr groß: 8 GB	Sehr groß: 6	
Guest Introspection	2 GB	2	5 GB (bereitgestellter Speicherplatz: 6,26 GB)

Als allgemeine Richtlinie gilt: Erhöhen Sie die NSX Manager-Ressourcen auf 8 vCPU und 24 GB RAM, wenn Ihre von NSX verwaltete Umgebung mehr als 256 Hypervisoren oder mehr als 2.000 VMs umfasst.

Um spezifische Details zur Größe zu erhalten, wenden Sie sich an den Support von VMware.

Informationen zur Erhöhung der Arbeitsspeicher- und vCPU-Zuteilung für Ihre virtuellen Appliances finden Sie unter „Zuteilen von Arbeitsspeicherressourcen“ und „Ändern der Anzahl virtueller CPUs“ in der Dokumentation *Verwaltung virtueller vSphere-Maschinen*.

Der bereitgestellte Speicherplatz für eine Guest Introspection-Appliance zeigt 6,26 GB für Guest Introspection an. Dies liegt daran, dass vSphere ESX Agent Manager einen Snapshot von der Dienst-VM erstellt, um schnelle Klone zu erstellen, wenn mehrere Hosts in einem Cluster Speicher gemeinsam nutzen. Weitere Informationen zum Deaktivieren dieser Option über ESX Agent Manager finden Sie in der *ESX Agent Manager*-Dokumentation.

## Netzwerklatenz

Stellen Sie sicher, dass die Netzwerklatenz zwischen Komponenten der angegebenen maximalen Latenz entspricht oder niedriger als diese ist.

**Tabelle 4-2. Maximale Netzwerklatenz zwischen Komponenten**

Komponenten	Maximale Latenz
NSX Manager und NSX Controller	150 ms RTT
NSX Manager und ESXi-Hosts	150 ms RTT
NSX Manager und vCenter Server-System	150 ms RTT
NSX Manager und NSX Manager in einer Cross-vCenter NSX-Umgebung	150 ms RTT
NSX Controller und ESXi-Hosts	150 ms RTT

## Software

Die neuesten Interoperabilitätsinformationen finden Sie in den Produkt-Interoperabilitätsmatrizen unter [http://partnerweb.vmware.com/comp\\_guide/sim/interop\\_matrix.php](http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php).

Die empfohlenen Versionen von NSX, vCenter Server und ESXi finden Sie in den Versionshinweisen für die Version von NSX, auf die Sie ein Upgrade vornehmen. Die Versionshinweise finden Sie auf der „NSX for vSphere“-Dokumentationsseite: <https://docs.vmware.com/de/VMware-NSX-for-vSphere/index.html>.

Die folgenden Bedingungen müssen erfüllt sein, damit ein NSX Manager in einer Cross-vCenter NSX-Bereitstellung teilnehmen kann:

Komponente	Version
NSX Manager	6.2 oder höher
NSX Controller	6.2 oder höher
vCenter Server	6.0 oder höher
ESXi	<ul style="list-style-type: none"> <li>■ ESXi 6.0 oder höher</li> <li>■ Mit NSX 6.2 oder späteren VIBs vorbereitete Hostcluster</li> </ul>

Um alle NSX Manager in einer Cross-vCenter NSX-Bereitstellung von einem einzigen vSphere Web Client aus verwalten zu können, müssen Sie Ihre vCenter Server-Instanzen im erweiterten verknüpften Modus verbinden. Erläuterungen dazu finden Sie unter „Verwenden des erweiterten verknüpften Modus“ in der Dokumentation *vCenter Server und Hostverwaltung*.

Informationen zur Überprüfung der Kompatibilität von Partnerlösungen mit NSX finden Sie im „VMware Kompatibilitätshandbuch für Netzwerk und Sicherheit“ unter <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security>.

## Client- und Benutzerzugriff

Die folgenden Elemente sind zur Verwaltung Ihrer NSX-Umgebung erforderlich:

- Vorwärts- und rückwärtsgerichtete Namensauflösung. Dies ist erforderlich, wenn Sie ESXi-Hosts nach Namen zur vSphere-Bestandsliste hinzugefügt haben. Anderenfalls kann NSX Manager die IP-Adressen nicht auflösen.
- Berechtigungen zum Hinzufügen und Einschalten von virtuellen Maschinen
- Zugriff auf den Datenspeicher, in dem Dateien für virtuelle Maschinen gespeichert werden, sowie Kontoberechtigungen zum Kopieren von Dateien in diesen Datenspeicher
- Cookies müssen in Ihrem Webbrowser aktiviert sein, damit Sie auf die NSX Manager-Benutzeroberfläche zugreifen können.
- Port 443 muss zwischen dem NSX Manager und dem ESXi-Host, dem vCenter Server und den bereitzustellenden NSX-Appliances geöffnet sein. Dieser Port wird zum Herunterladen der OVF-Datei auf dem ESXi-Host für die Bereitstellung benötigt.
- Ein für die von Ihnen verwendete Version von vSphere Web Client unterstützter Webbrowser. Ausführliche Informationen erhalten Sie unter „Verwenden des vSphere Web Client“ in der Dokumentation *vCenter Server und Hostverwaltung*.

## Für NSX for vSphere erforderliche Ports und Protokolle

Für einen ordnungsgemäßen Betrieb von NSX for vSphere müssen die folgenden Ports geöffnet sein.

**Hinweis** Wenn Sie eine Cross-vCenter NSX-Umgebung haben und sich Ihre vCenter Server-Systeme im erweiterten verknüpften Modus befinden, müssen alle NSX Manager-Appliances die erforderliche Konnektivität mit allen vCenter Server-Systemen in der Umgebung aufweisen, um einen beliebigen NSX Manager über ein beliebiges vCenter Server-System zu verwalten.

**Tabelle 4-3. Für NSX for vSphere erforderliche Ports und Protokolle**

Quelle	Ziel	Port	Protokoll	Zweck	Sensibel	TLS	Authentifizierung
Client-PC	NSX Manager	443	TCP	Verwaltungsschnittstelle von NSX Manager	Nein	Ja	PAM-Authentifizierung
Client-PC	NSX Manager	443	TCP	VIB-Zugang für NSX Manager	Nein	Nein	PAM-Authentifizierung
ESXi-Host	vCenter Server	443	TCP	Vorbereitung des ESXi-Hosts	Nein	Nein	
vCenter Server	ESXi-Host	443	TCP	Vorbereitung des ESXi-Hosts	Nein	Nein	
ESXi-Host	NSX Manager	5671	TCP	RabbitMQ	Nein	Ja	RabbitMQ-Benutzer/Kennwort
ESXi-Host	NSX Controller	1234	TCP	UWAC (User World Agent Connection)	Nein	Ja	
NSX Controller	NSX Controller	2878, 2888, 3888	TCP	Controller-Cluster – Statussynchronisierung	Nein	Ja	IPsec
NSX Controller	NSX Controller	7777	TCP	RPC-Port für die Kommunikation zwischen Controllern	Nein	Ja	IPsec
NSX Controller	NSX Controller	30865	TCP	Controller-Cluster – Statussynchronisierung	Nein	Ja	IPsec
NSX Manager	NSX Controller	443	TCP	Kommunikation zwischen Controller und Manager	Nein	Ja	Benutzer/Kennwort
NSX Manager	vCenter Server	443	TCP	vSphere Web Access	Nein	Ja	
NSX Manager	vCenter Server	902	TCP	vSphere Web Access	Nein	Ja	
NSX Manager	ESXi-Host	443	TCP	Verwaltungs- und Bereitstellungsverbinding	Nein	Ja	
NSX Manager	ESXi-Host	902	TCP	Verwaltungs- und Bereitstellungsverbinding	Nein	Ja	

**Tabelle 4-3. Für NSX for vSphere erforderliche Ports und Protokolle (Fortsetzung)**

Quelle	Ziel	Port	Protokoll	Zweck	Sensibel	TLS	Authentifizierung
NSX Manager	DNS-Server	53	TCP	DNS-Client-Verbindung	Nein	Nein	
NSX Manager	DNS-Server	53	UDP	DNS-Client-Verbindung	Nein	Nein	
NSX Manager	Syslog-Server	514	TCP	Syslog-Verbindung	Nein	Nein	
NSX Manager	Syslog-Server	514	UDP	Syslog-Verbindung	Nein	Nein	
NSX Manager	NTP-Zeitserver	123	TCP	NTP-Client-Verbindung	Nein	Ja	
NSX Manager	NTP-Zeitserver	123	UDP	NTP-Client-Verbindung	Nein	Ja	
vCenter Server	NSX Manager	80	TCP	Hostvorbereitung	Nein	Ja	
REST-Client	NSX Manager	443	TCP	NSX Manager-REST-API	Nein	Ja	Benutzer/Kennwort
VXLAN Tunnel End Point (VTEP)	VXLAN Tunnel End Point (VTEP)	8472 (Standard vor NSX 6.2.3) oder 4789 (Standard in neuen Installationen von NSX 6.2.3 und höher)	UDP	Transportnetzwerk-Kapselung zwischen VTEPs	Nein	Ja	
ESXi-Host	ESXi-Host	6999	UDP	ARP auf VLAN-LIFs	Nein	Ja	
ESXi-Host	NSX Manager	8301, 8302	UDP	DVS-Synchronisierung	Nein	Ja	
NSX Manager	ESXi-Host	8301, 8302	UDP	DVS-Synchronisierung	Nein	Ja	
Guest Introspection-VM	NSX Manager	5671	TCP	RabbitMQ	Nein	Ja	RabbitMQ-Benutzer/Kennwort
Primärer NSX Manager	Sekundärer NSX Manager	443	TCP	Globaler Synchronisierungsdienst für Cross-vCenter NSX	Nein	Ja	
Primärer NSX Manager	vCenter Server	443	TCP	vSphere-API	Nein	Ja	



**Tabelle 4-3. Für NSX for vSphere erforderliche Ports und Protokolle (Fortsetzung)**

Quelle	Ziel	Port	Protokoll	Zweck	Sensibel	TLS	Authentifizierung
Sekundärer NSX Manager	vCenter Server	443	TCP	vSphere-API	Nein	Ja	
Primärer NSX Manager	Globaler NSX Controller-Cluster	443	TCP	NSX Controller-REST-API	Nein	Ja	Benutzer/Kennwort
Sekundärer NSX Manager	Globaler NSX Controller-Cluster	443	TCP	NSX Controller-REST-API	Nein	Ja	Benutzer/Kennwort
ESXi-Host	Globaler NSX Controller-Cluster	1234	TCP	Protokoll der NSX-Steuerungskomponente	Nein	Ja	
ESXi-Host	Primärer NSX Manager	5671	TCP	RabbitMQ	Nein	Ja	RabbitMQ-Benutzer/Kennwort
ESXi-Host	Sekundärer NSX Manager	5671	TCP	RabbitMQ	Nein	Ja	RabbitMQ-Benutzer/Kennwort

## NSX und vSphere Distributed Switches

In einer NSX-Domäne ist NSX vSwitch die Software, die in Server-Hypervisoren ausgeführt wird, um eine Abstraktionsschicht zwischen Servern und dem physischen Netzwerk zu bilden.

NSX vSwitch basiert auf vSphere Distributed Switches (VDS), die Uplinks für die Hostkonnektivität zu physischen Top-of-Rack- (ToR-)Switches bereitstellen. Als bewährte Methode empfiehlt VMware, dass Sie vor der Installation von NSX for vSphere Ihre vSphere Distributed Switches planen und vorbereiten.

NSX-Dienste werden vom vSphere Standard Switch nicht unterstützt. VM-Arbeitslasten müssen mit vSphere Distributed Switches verbunden werden, damit Sie die NSX-Dienste und -Funktionen nutzen können.

Ein einzelner Host kann an mehrere vSphere Distributed Switches angehängt werden. Ein einzelner VDS kann sich über mehrere Hosts auf mehreren Clustern erstrecken. Für jeden Host-Cluster, der an NSX teilnimmt, müssen alle Hosts im Cluster einem gemeinsamen VDS angehängt werden.

Angenommen, Sie haben einen Cluster mit Host1 und Host2. Host1 wird mit VDS1 und VDS2 verbunden. Host2 wird mit VDS1 und VDS3 verbunden. Wenn Sie einen Cluster für NSX vorbereiten, können Sie auf dem Cluster NSX nur mit VDS1 verknüpfen. Wenn Sie dem Cluster einen weiteren Host (Host3) hinzufügen und Host3 nicht mit VDS1 verbunden wird, ist die Konfiguration ungültig und Host3 steht für NSX-Funktionen nicht bereit.

Um eine Implementierung zu vereinfachen, wird häufig jeder Host-Cluster nur einem VDS zugewiesen, wenngleich einige der VDS sich über mehrere Cluster erstrecken. Beispiel: Ihr vCenter enthält die folgenden Host-Cluster:

- Computing-Cluster A für App-Tier-Hosts
- Computing-Cluster B für Web-Tier-Hosts

- Verwaltungs- und Edge-Cluster für Verwaltungs- und Edge-Hosts

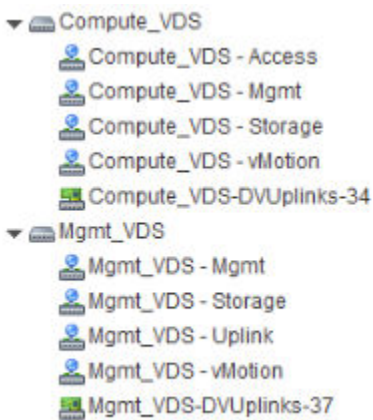
Auf der folgenden Abbildung sieht man, wie diese Cluster in vCenter angezeigt werden.



Für ein solches Cluster-Design könnten Sie beispielsweise zwei VDS mit den Namen Compute\_VDS und Mgmt\_VDS verwenden. Compute\_VDS erstreckt sich über beide Computing-Cluster, während Mgmt\_VDS nur mit dem Verwaltungs- und dem Edge-Cluster verknüpft ist.

Jeder VDS enthält verteilte Portgruppen für die verschiedenen zu übertragenden Datenverkehrstypen. Zu den typischen Datenverkehrstypen gehören Verwaltung, Speicherung und vMotion. In der Regel sind auch Uplink- und Zugriffs-Ports erforderlich. Normalerweise wird auf jedem VDS eine Portgruppe pro Datenverkehrstyp erstellt.

In der folgenden Abbildung wird beispielshalber dargestellt, wie diese verteilten Switches und Ports in vCenter angezeigt werden.

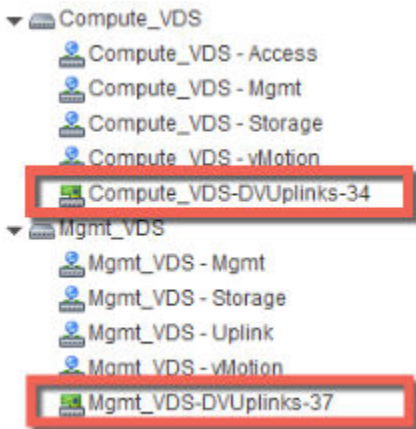


Jede Portgruppe kann wahlweise mit einer VLAN-ID konfiguriert werden. Die folgende Liste zeigt ein Beispiel dafür, wie VLANs den verteilten Portgruppen zugeordnet werden können, um eine logische Trennung zwischen verschiedenen Datenverkehrsarten sicherzustellen:

- Compute\_VDS - Access---VLAN 130
- Compute\_VDS - Mgmt---VLAN 210
- Compute\_VDS - Storage---VLAN 520
- Compute\_VDS - vMotion---VLAN 530
- Mgmt\_VDS - Uplink---VLAN 100

- Mgmt\_VDS - Mgmt---VLAN 110
- Mgmt\_VDS - Storage---VLAN 420
- Mgmt\_VDS - vMotion---VLAN 430

Die Portgruppe für die DVUplinks ist ein VLAN-Trunk, der beim Erstellen eines VDS automatisch erstellt wird. Als Trunk-Port sendet und empfängt sie getaggte Frames. Ihr können standardmäßig alle VLAN-IDs (0-4094) hinterlegt werden. Dies bedeutet, dass der Datenverkehr mit einer beliebigen VLAN-ID über die dem DVUplink-Steckplatz zugewiesenen vmnic-Netzwerkadapter übertragen und von den Hypervisor-Hosts gefiltert werden kann, da der Distributed Switch festlegt, an welche Portgruppe der Datenverkehr weitergegeben werden soll.



Wenn in Ihrer vCenter-Umgebung Standard-vSwitches anstelle von Distributed Switches vorhanden sind, können Sie Ihre Hosts auf Distributed Switches migrieren.

## Beispiel: Arbeiten mit einem vSphere Distributed Switch

In diesem Beispiel wird gezeigt, wie Sie einen neuen vSphere Distributed Switch (VDS) erstellen, wie Sie Portgruppen für den Verwaltungs-, den Storage- und den vMotion-Datenverkehr hinzufügen und wie Sie Hosts auf einem Standard-vSwitch zum neuen Distributed Switch migrieren.

Bitte beachten Sie, dass es sich hierbei nur um ein Beispiel zur Veranschaulichung der Vorgehensweise handelt. Nähere Informationen zu physischen und logischen VDS-Uplinks finden Sie im *Handbuch zum Netzwerkvirtualisierungsdesign in VMware NSX für vSphere (VMware NSX for vSphere Network Virtualization Design Guide)* unter <https://communities.vmware.com/docs/DOC-27683>.

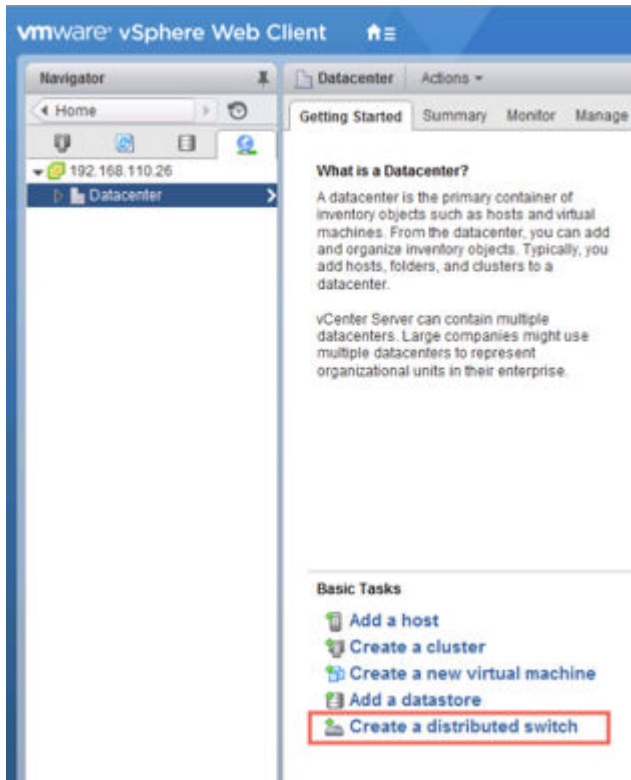
### Voraussetzungen

In diesem Beispiel wird davon ausgegangen, dass jeder mit dem vSphere Distributed Switch zu verbindende ESX-Host über mindestens eine Verbindung mit einem physischen Switch (ein vmnic-Uplink) verfügt. Dieser Uplink kann für den Distributed Switch-Datenverkehr und für den NSX-VXLAN-Datenverkehr verwendet werden.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zu einem Datencenter.

- 2 Klicken Sie auf **Distributed Switch erstellen (Create a Distributed Switch)**.



- 3 Geben Sie dem Switch einen aussagekräftigen Namen, der auf dem Host-Cluster basiert, der diesem Switch zugeordnet wird.

Wird ein Distributed Switch beispielsweise einem Cluster aus Datencenterverwaltungs-Hosts zugeordnet, können Sie dem Switch den Namen VDS\_Mgmt geben.

- 4 Geben Sie mindestens einen Uplink für den Distributed Switch an, lassen Sie IO Control aktiviert und geben Sie einen aussagekräftigen Namen für die Standard-Portgruppe an. Beachten Sie, dass das Erstellen der Standard-Portgruppe nicht obligatorisch ist. Die Portgruppe kann später manuell erstellt werden.

Standardmäßig werden vier Uplinks erstellt. Passen Sie die Anzahl der Uplinks Ihrem VDS-Design entsprechend an. Die erforderliche Anzahl an Uplinks entspricht in der Regel der Anzahl der physischen Netzwerkkarten, die dem VDS zugewiesen werden sollen.

Im nachfolgenden Menüfenster werden Beispiелеinstellungen für den Verwaltungsdatenverkehr auf dem Verwaltungs-Host-Cluster angezeigt.

Die Standard-Portgruppe ist nur eine der Portgruppen, die dieser Switch enthalten wird. Sie haben nach der Erstellung des Switch die Möglichkeit, Portgruppen für verschiedene Datenverkehrstypen hinzuzufügen. Wahlweise können Sie beim Erstellen eines neuen VDS die Option **Standard-Portgruppe erstellen (Create a default port group)** deaktivieren. Dies dürfte die beste Vorgehensweise sein, da bei der Erstellung von Portgruppen möglichst eindeutige Angaben erforderlich sind.

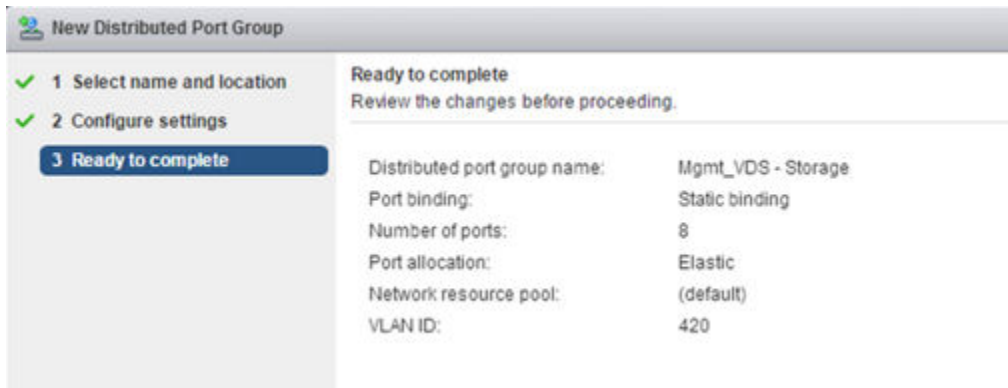
- 5 (Optional) Bearbeiten Sie nach Abschluss des Assistenten „Neuer Distributed Switch“ die Einstellungen der Standard-Portgruppe, um diese in das richtige VLAN für den Verwaltungsdatenverkehr zu platzieren.

Befinden sich Ihre Host-Verwaltungsschnittstellen beispielsweise in VLAN 110, legen Sie die Standard-Portgruppe in VLAN 110 ab. Wenn sich Ihre Host-Verwaltungsschnittstellen in keinem VLAN befinden, überspringen Sie diesen Schritt.

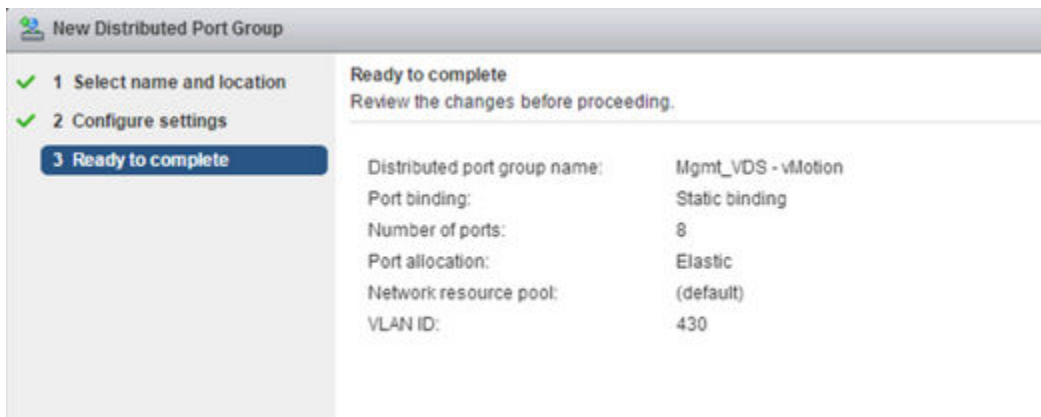
- 6 Klicken Sie nach Abschluss des Assistenten „Neuer Distributed Switch“ mit der rechten Maustaste auf den Distributed Switch und wählen Sie die Option **Neue verteilte Portgruppe (New Distributed Port Group)** aus.

Wiederholen Sie diesen Schritt für jeden Datenverkehrstyp. Achten Sie dabei darauf, jeder Portgruppe einen aussagekräftigen Namen zu geben und entsprechend den die Datenverkehrstrennung betreffenden Anforderungen Ihrer Bereitstellung die richtige VLAN-ID zu konfigurieren.

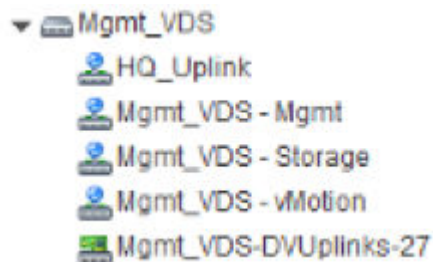
Beispiel für Gruppeneinstellungen für den Speicher.



Beispiel für Gruppeneinstellungen für den vMotion-Datenverkehr.

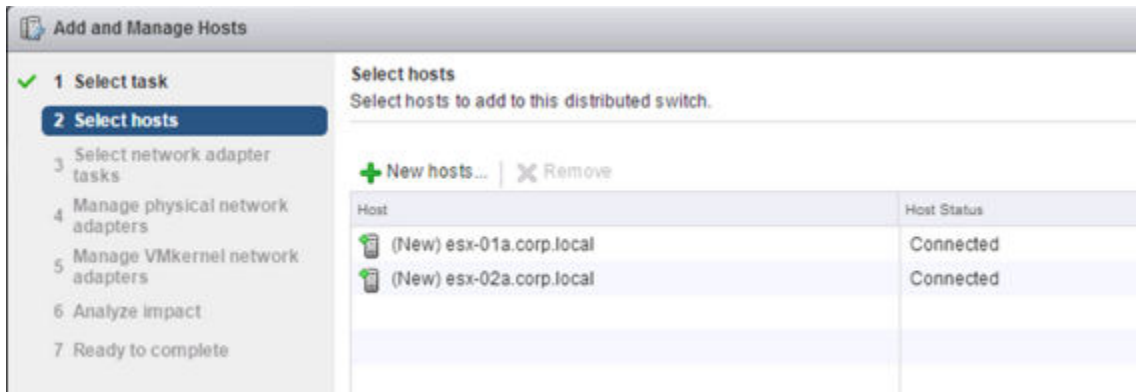


Nach erfolgreicher Erstellung sehen der Distributed Switch und die Portgruppen folgendermaßen aus.

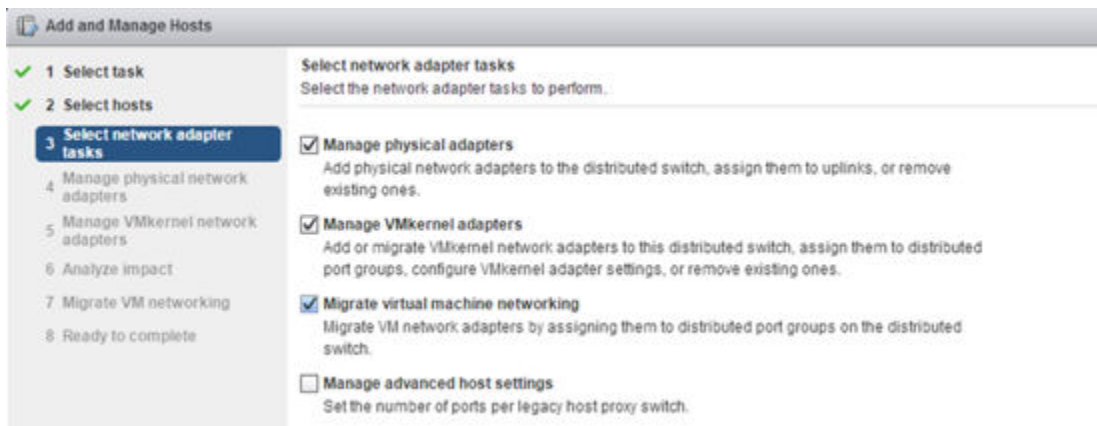


- 7 Klicken Sie mit der rechten Maustaste auf den Distributed Switch, wählen Sie **Hosts hinzufügen und verwalten (Add and Manage Hosts)** und dann **Hosts hinzufügen (Add Hosts)** aus.

Hängen Sie alle Hosts aus dem zugewiesenen Cluster an. Ist der Switch beispielsweise für Verwaltungshosts, wählen Sie alle Hosts, die sich im Verwaltungscluster befinden.



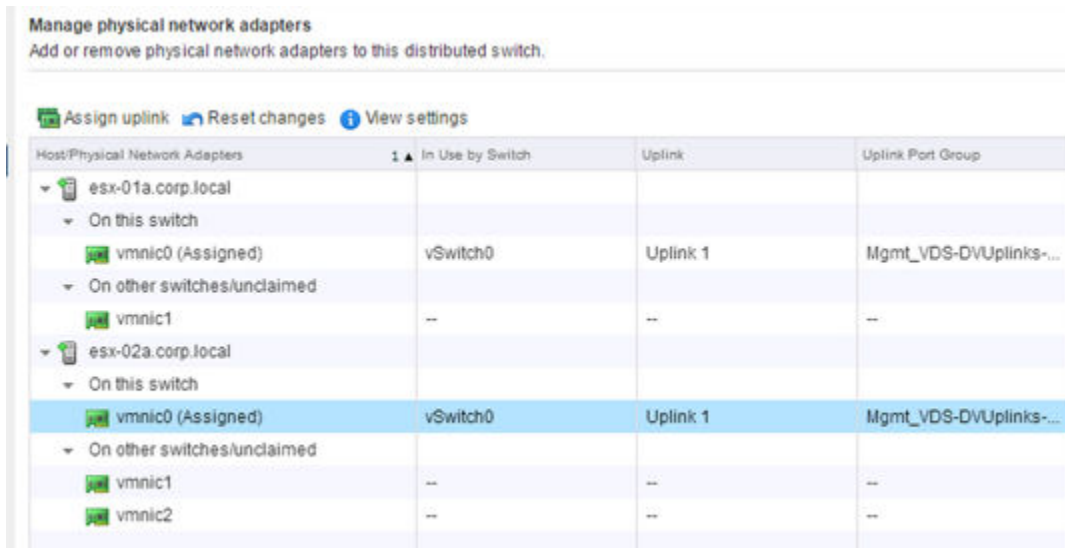
- 8 Wählen Sie die entsprechenden Optionen aus, um physische Adapter, VMkernel-Adapter und das Netzwerk virtueller Maschinen zu migrieren.



- 9 Wählen Sie eine vmnic aus und klicken Sie auf **Uplink zuweisen (Assign uplink)**, um die vmnic aus dem Standard-vSwitch auf das Distributed Switch zu migrieren. Wiederholen Sie diesen Schritt für jeden Host, den Sie mit dem verteilten vSwitch verbinden.

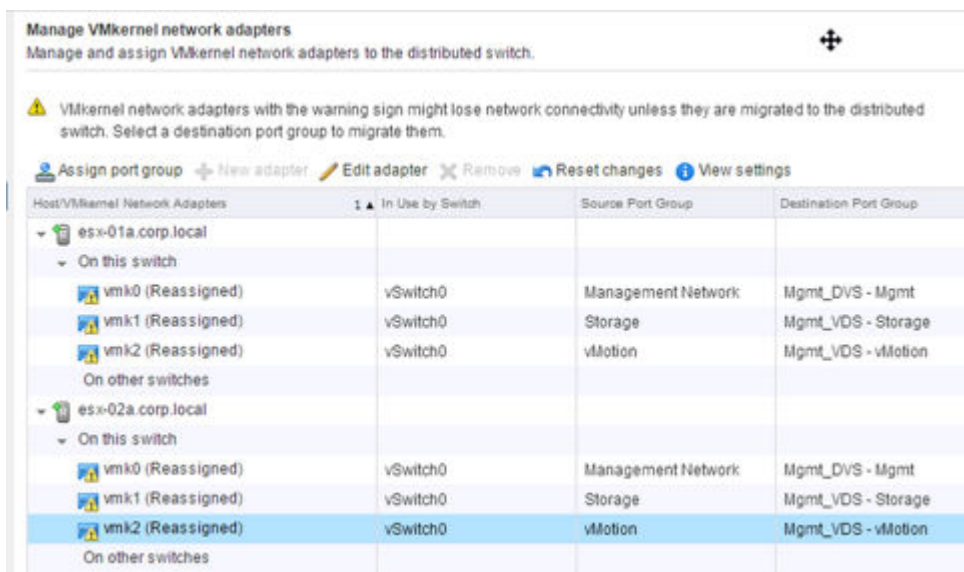
In dieser Abbildung werden beispielsweise zwei Hosts gezeigt, deren vmnic0-Uplinks so konfiguriert sind, dass sie von ihrem jeweiligen Standard-vSwitch auf die verteilte Portgruppe Mgmt\_VDS-DVUplinks migrieren, die ein Trunk-Port ist, dem jede VLAN-ID hinterlegt werden kann.





- 10 Wählen Sie einen VMkernel-Netzwerkadapter aus und klicken Sie auf **Portgruppe zuweisen (Assign port group)**. Wiederholen Sie diesen Schritt für alle Netzwerkadapter auf allen Hosts, die Sie mit dem verteilten vSwitch verbinden.

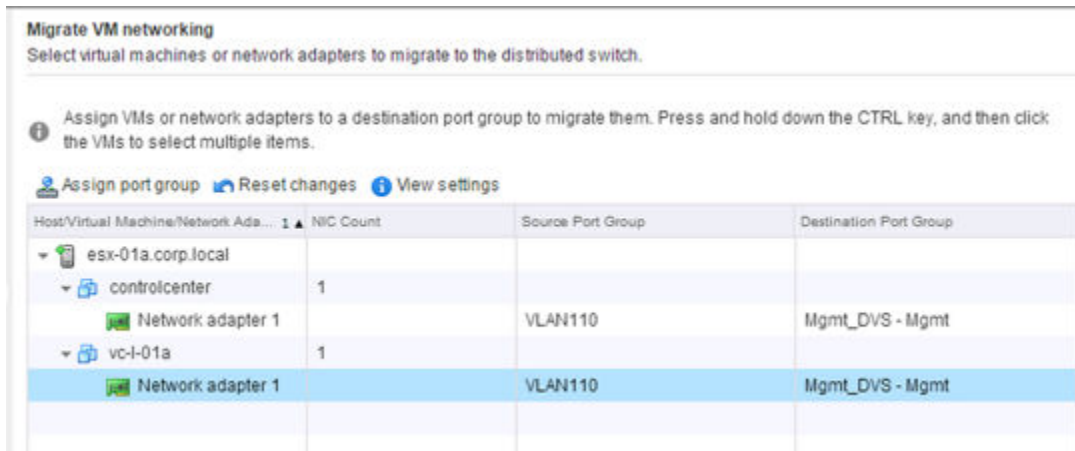
Auf diesem Bildschirm werden beispielsweise drei auf zwei Hosts befindliche vmk-Netzwerkadapter gezeigt, die so konfiguriert sind, dass sie von den Standard-Portgruppen auf die neuen verteilten Portgruppen migriert werden.



- 11 Verschieben Sie alle auf den Hosts befindlichen VMs in eine verteilte Portgruppe.

Auf diesem Bildschirm werden beispielsweise zwei auf einem einzigen Host befindliche VMs gezeigt, die so konfiguriert sind, dass sie von der Standard-Portgruppe auf die neue verteilte Portgruppe migriert werden.





## Ergebnisse

Nach Abschluss des Vorgangs können Sie im CLI des Hosts die Ergebnisse durch Ausführen der folgenden Befehle überprüfen:

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

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

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

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

## ■ ~ # esxcli network ip interface list

## vmk2

```

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

```

## vmk0

```

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

```

## vmk1

```

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

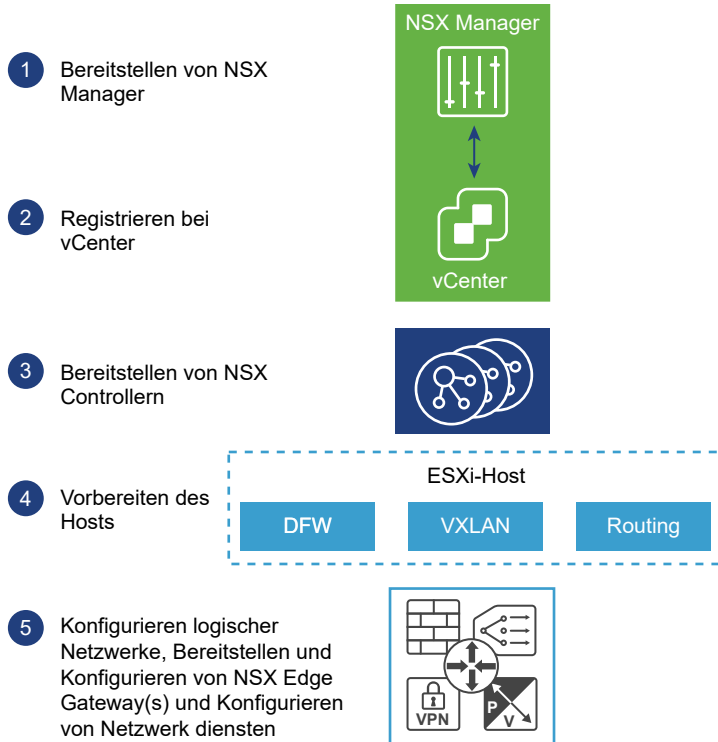
```

**Nächste Schritte**

Wiederholen Sie den Migrationsvorgang für alle vSphere Distributed Switches.

# Installations-Workflow und Beispieltopologie für NSX

Die Installation von NSX beinhaltet die Bereitstellung mehrerer virtueller Appliances, einige vorbereitende Schritte für den ESX-Host sowie etwas Konfiguration, um die Kommunikation zwischen allen physischen und virtuellen Geräten zu ermöglichen.

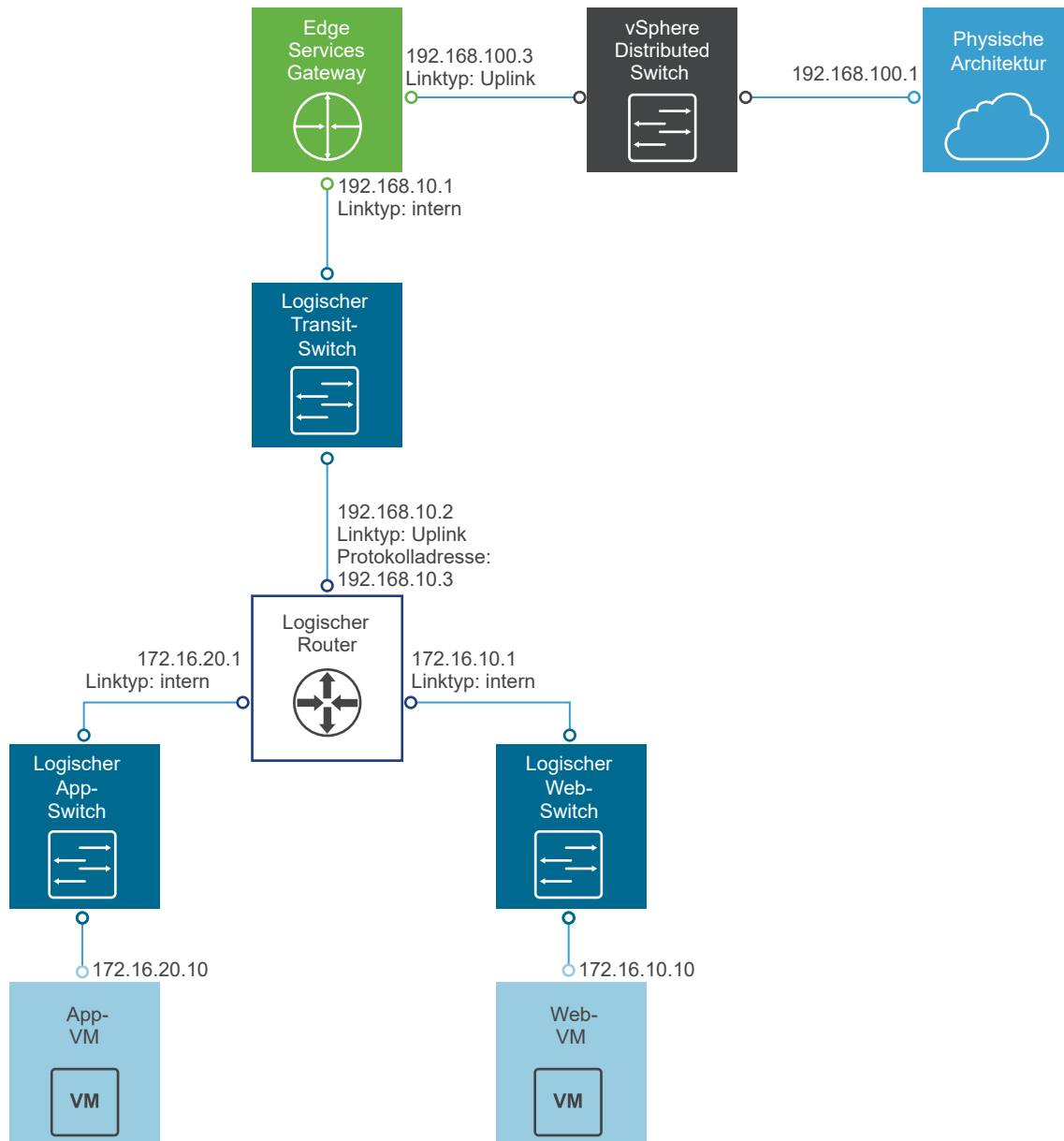


Zu Beginn des Prozesses steht die Bereitstellung einer OVA/OVF-Vorlage für NSX Manager. Zudem muss sichergestellt werden, dass NSX Manager vollständig mit allen Verwaltungsschnittstellen des zu verwaltenden ESX-Hosts verbunden ist. Daraufhin müssen NSX Manager und eine vCenter-Instanz in einem Registrierungsvorgang miteinander verknüpft werden. Dies ermöglicht dann die Bereitstellung eines Clusters aus NSX Controllern. NSX Controller werden ebenso wie NSX Manager als virtuelle Appliances auf ESX-Hosts ausgeführt. Als nächster Schritt erfolgt die Vorbereitung der ESX-Hosts für NSX, indem mehrere VIBs auf den Hosts installiert werden. Diese VIBs ermöglichen die Schicht 2-VXLAN-Funktionalität, verteiltes Routing und die verteilte Firewall. Nach der Konfiguration der VXLANs, Angabe der Bereiche der virtuellen Netzwerkschnittstelle (VNI) und der Erstellung von Transportzonen können Sie den Aufbau Ihrer NSX-Overlay-Topologie vornehmen.

In diesem Installationshandbuch werden die einzelnen Schritte des Verfahrens detailliert beschreiben.

Diese auf jede NSX-Bereitstellung anwendbare Anleitung beschreibt auch durch die Erstellung einer NSX-Overlay-Topologie anhand eines Beispiels, das zu Übungs-, Orientierungs- und Referenzzwecken verwendet werden kann. Das Overlay-Beispiel verfügt über einen einzelnen NSX Distributed Logical Router (manchmal auch als DLR bezeichnet), ein Edge Services Gateway (ESG) und einen logischen

Transit-Switch, der die beiden NSX-Routing-Geräte verbindet. Das Topologie-Beispiel enthält zudem Underlay-Elemente, darunter zwei Beispiel-VMs. Diese virtuellen Maschinen sind jeweils mit einem separaten logischen NSX-Switch verbunden, der die Konnektivität über den logischen NSX-Router (DLR) ermöglicht.



## Cross-vCenter NSX und der erweiterte verknüpfte Modus

vSphere 6.0 führt den erweiterten verknüpften Modus ein, der mehrere vCenter Server-Systeme unter Verwendung eines oder mehrerer Platform Services Controller verknüpft. Auf diese Weise können Sie die Bestandslisten aller verknüpften vCenter Server-Systeme innerhalb des vSphere Web Client anzeigen und durchsuchen. In einer Cross-vCenter NSX-Umgebung ermöglicht der erweiterte verknüpfte Modus Ihnen die Verwaltung aller NSX Manager über einen einzigen vSphere Web Client.

In großen Bereitstellungen mit mehreren vCenter Server-Instanzen kann es sinnvoll sein, Cross-vCenter NSX mit dem erweiterten verknüpften Modus für vCenter zu verwenden. Es handelt sich hierbei zwar um zwei separate Funktionen, die sich jedoch ergänzen.

## **Kombinieren von Cross-vCenter NSX mit dem erweiterten verknüpften Modus**

In Cross-vCenter NSX können ein primärer NSX Manager und mehrere sekundäre NSX Manager vorhanden sein. Jeder dieser NSX Manager ist mit einem separaten vCenter Server verknüpft. Auf dem primären NSX Manager können Sie universelle NSX-Komponenten (z. B. Switches und Router) erstellen, die von den sekundären NSX Manager-Instanzen angezeigt werden können.

Wenn die einzelnen vCenter Server-Instanzen mit dem erweiterten verknüpften Modus bereitgestellt werden, können alle vCenter Server-Instanzen von einem einzigen vCenter Server aus (also in einem einzigen Fenster) angezeigt und verwaltet werden.

Wenn also Cross-vCenter NSX mit dem erweiterten verknüpften Modus für vCenter kombiniert wird, können Sie alle NSX Manager und alle universellen NSX-Komponenten von jedem beliebigen verknüpften vCenter Server anzeigen und verwalten.

## **Verwenden von Cross-vCenter NSX ohne den erweiterten verknüpften Modus**

Der erweiterte verknüpfte Modus ist keine Voraussetzung oder Anforderung für Cross-vCenter NSX. Auch ohne den erweiterten verknüpften Modus können Sie universelle Cross-vCenter-Transportzonen, universelle Switches, universelle Router und universelle Firewallregeln erstellen. Ohne den erweiterten verknüpften Modus müssen Sie sich allerdings bei jedem einzelnen vCenter Server anmelden, um auf die einzelnen NSX Manager-Instanzen zuzugreifen.

## **Weitere Informationen zu vSphere und dem erweiterten verknüpften Modus**

Wenn Sie sich für die Verwendung des erweiterten verknüpften Modus entscheiden, finden Sie die aktuellen Anforderungen für vSphere und den erweiterten verknüpften Modus im Handbuch *Installation und Einrichtung von vSphere* oder im *vSphere-Upgrade-Handbuch*.

# Aufgaben für die primären und sekundären NSX Manager

# 5

In einer Cross-vCenter-Umgebung können ein primärer NSX Manager und bis zu sieben sekundäre NSX Manager vorhanden sein. Einige Setup-Aufgaben werden auf jedem NSX Manager ausgeführt, egal, ob er ein primärer NSX Manager oder ein sekundärer NSX Manager wird.

Dieses Kapitel enthält die folgenden Themen:

- [Installieren der virtuellen NSX Manager-Appliance](#)
- [Konfigurieren von Single Sign-On](#)
- [Registrieren von vCenter Server mit NSX Manager](#)
- [Konfigurieren eines Syslog-Servers für NSX Manager](#)
- [Installieren und Zuweisen einer Lizenz von NSX for vSphere](#)
- [Ausschließen von virtuellen Maschinen vom Schutz durch die Firewall](#)

## Installieren der virtuellen NSX Manager-Appliance

NSX Manager wird als virtuelle Appliance auf einem beliebigen ESX-Host in Ihrer vCenter-Umgebung installiert.

NSX Manager stellt die grafische Benutzeroberfläche (GUI) und die REST-APIs für die Erstellung, Konfiguration und Überwachung von NSX-Komponenten wie Controller, logische Switches und Edge Services Gateways bereit. NSX Manager bietet die Gesamtübersicht über das System und ist die zentrale NSX-Komponente für das Netzwerkmanagement. Die virtuelle NSX Manager-Maschine ist als OVA-Datei gepackt, sodass Sie den vSphere Web Client verwenden können, um den NSX Manager in den Datenspeicher und den virtuellen Maschinenbestand zu importieren.

Zur Sicherstellung von Hochverfügbarkeit empfiehlt VMware die Bereitstellung von NSX Manager in einem mit HA und DRS konfigurierten Cluster. Optional können Sie NSX Manager in einem anderen vCenter als dem, mit dem NSX Manager interagieren wird, installieren. Ein einzelner NSX Manager dient als einzelne vCenter Server-Umgebung.

Stellen Sie bei Cross-vCenter NSX-Installationen sicher, dass jeder NSX Manager eine eindeutige UUID besitzt. Mithilfe von OVA-Dateien bereitgestellte NSX Manager-Instanzen besitzen eindeutige UUIDs. Ein von einer Vorlage bereitgestellter NSX Manager (wie beim Konvertieren einer virtuellen Maschine in eine Vorlage) erhält die gleiche UUID wie der zum Erstellen der Vorlage verwendete ursprüngliche NSX Manager, und diese beiden NSX Manager können nicht in derselben Cross-vCenter NSX-Installation verwendet werden. Anders ausgedrückt müssen Sie, wie in diesem Verfahren beschrieben, für jeden NSX Manager eine neue Appliance von Grund auf neu installieren.

Die Installation der virtuellen NSX Manager-Maschine umfasst VMware Tools. Versuchen Sie nicht, VMware Tools auf dem NSX Manager zu aktualisieren oder zu installieren.

Bei der Installation können Sie auswählen, ob Sie am „Programm zur Verbesserung der Benutzerfreundlichkeit“ (CEIP, Customer Experience Improvement Program) für NSX teilnehmen möchten. Unter „Programm zur Verbesserung der Benutzerfreundlichkeit im *Administratorhandbuch für NSX*“ finden Sie weitere Informationen dazu, inklusive Informationen, wie Sie sich daran beteiligen und wieder abmelden können.

### Voraussetzungen

- Stellen Sie vor der Installation von NSX Manager sicher, dass die erforderlichen Ports geöffnet sind. Weitere Informationen dazu finden Sie unter [Für NSX for vSphere erforderliche Ports und Protokolle](#).
- Stellen Sie sicher, dass auf dem Ziel-ESX-Host ein Datenspeicher konfiguriert und verfügbar ist. Es wird gemeinsam genutzter Speicher empfohlen. Für HA wird gemeinsam genutzter Speicher benötigt, damit die NSX Manager-Appliance auf einem anderen Host neu gestartet werden kann, falls der ursprüngliche Host ausfällt.
- Stellen Sie sicher, dass Sie die IP-Adresse und das Gateway, die IP-Adressen des DNS-Servers, die Domänensuchliste und die IP-Adresse des NTP-Servers, die von NSX Manager verwendet werden, kennen.
- Entscheiden Sie sich, ob NSX Manager nur IPv4-Adressierung, nur IPv6-Adressierung oder eine Dual-Stack-Netzwerkconfiguration nutzen soll. Der Hostname des NSX Managers wird von anderen Elementen verwendet. Aus diesem Grund muss der Hostname des NSX Managers der richtigen IP-Adresse in den DNS-Servern, die in diesem Netzwerk verwendet werden, zugeordnet werden.
- Bereiten Sie eine verteilte Portgruppe für den Verwaltungsdatenverkehr vor, auf der NSX Manager kommunizieren soll. Weitere Informationen dazu finden Sie unter [Beispiel: Arbeiten mit einem vSphere Distributed Switch](#). Die NSX Manager-Verwaltungsschnittstelle sowie die Verwaltungsschnittstellen von vCenter Server und des ESXi-Hosts müssen für NSX Guest Introspection-Instanzen erreichbar sein.
- Das Client-Integrations-Plug-In muss installiert sein. Der Assistent zum Bereitstellen von OVF-Vorlagen funktioniert mit dem Webbrowser Firefox am besten. Bei Verwendung des Webbrowsers Chrome wird manchmal eine die Installation des Client-Integrations-Plug-Ins betreffende Fehlermeldung angezeigt, obwohl das Plug-In bereits erfolgreich installiert ist. So installieren Sie das Client-Integrations-Plug-In:
  - a Öffnen Sie einen Webbrowser und geben Sie die URL für den vSphere Web Client ein.

- b Klicken Sie unten auf der Anmeldeseite von vSphere Web Client auf „Client-Integrations-Plug-In herunterladen“.

Wenn das Client-Integrations-Plug-In bereits auf Ihrem System installiert ist, wird der Link zum Herunterladen des Plug-Ins nicht angezeigt. Nachdem Sie das Client-Integrations-Plug-In deinstalliert haben, wird der Link zum Herunterladen auf der Anmeldeseite des vSphere Web Client angezeigt.

## Verfahren

- 1 Suchen Sie die Open Virtualization Appliance (OVA)-Datei von NSX Manager.  
Kopieren Sie die Download-URL oder laden Sie die OVA-Datei auf Ihren Computer herunter.
- 2 Wechseln Sie zu Firefox und öffnen Sie vCenter.
- 3 Wählen Sie **VMs und Vorlagen (VMs and Templates)** aus, klicken Sie mit der rechten Maustaste auf Ihr Datacenter und wählen Sie die Option **OVF-Vorlage bereitstellen (Deploy OVF Template)** aus.
- 4 Fügen Sie die Download-URL ein oder klicken Sie auf **Durchsuchen (Browse)**, um die Datei auf Ihrem Computer auszuwählen.

---

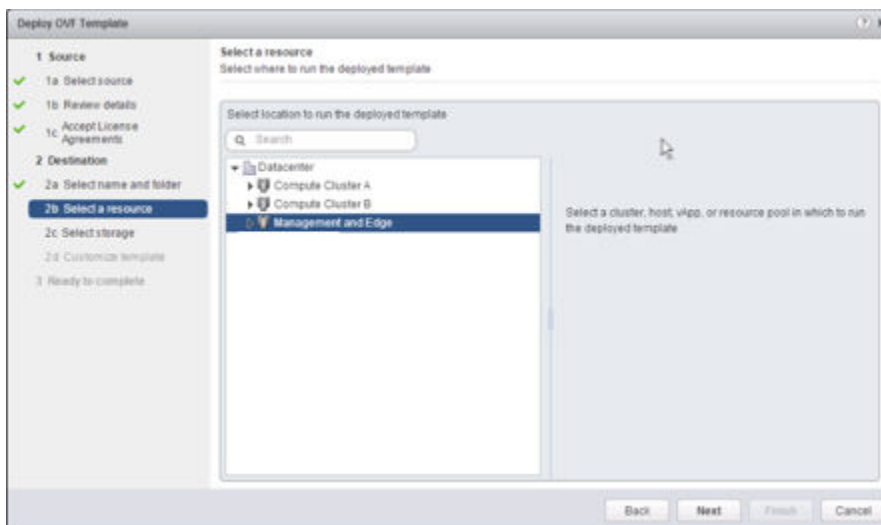
**Hinweis** Wenn die Installation mit der Fehlermeldung Zeitüberschreitung für Vorgang scheitert, müssen Sie prüfen, ob die Speicher- und Netzwerkgeräte Konnektivitätsprobleme aufweisen. Dieses Problem tritt auf, wenn ein Fehler bei der physischen Infrastruktur vorliegt, wie z. B. eine fehlende Konnektivität mit dem Speichergerät oder ein Konnektivitätsproblem mit einer physischen NIC oder einem Switch.

---

- 5 Aktivieren Sie das Kontrollkästchen **Zusätzliche Konfigurationsoptionen akzeptieren (Accept extra configuration options)**.  
Dadurch können Sie IPv4- und IPv6-Adressen, Standard-Gateway-, DNS-, NTP- und SSH-Eigenschaften während der Installation festlegen, anstatt diese Einstellungen nach der Installation manuell konfigurieren zu müssen.
- 6 Akzeptieren Sie die VMware-Lizenzvereinbarungen.
- 7 Bearbeiten Sie den NSX Manager-Namen (falls erforderlich) und wählen Sie den Speicherort für den bereitgestellten NSX Manager aus.  
Der von Ihnen eingegebene Name wird in der vCenter-Bestandsliste angezeigt.  
Der ausgewählte Ordner wird zum Anwenden von Berechtigungen für den NSX Manager verwendet.
- 8 Wählen Sie den Host oder Cluster aus, auf dem die NSX Manager-Appliance bereitgestellt werden soll.

Beispiel:

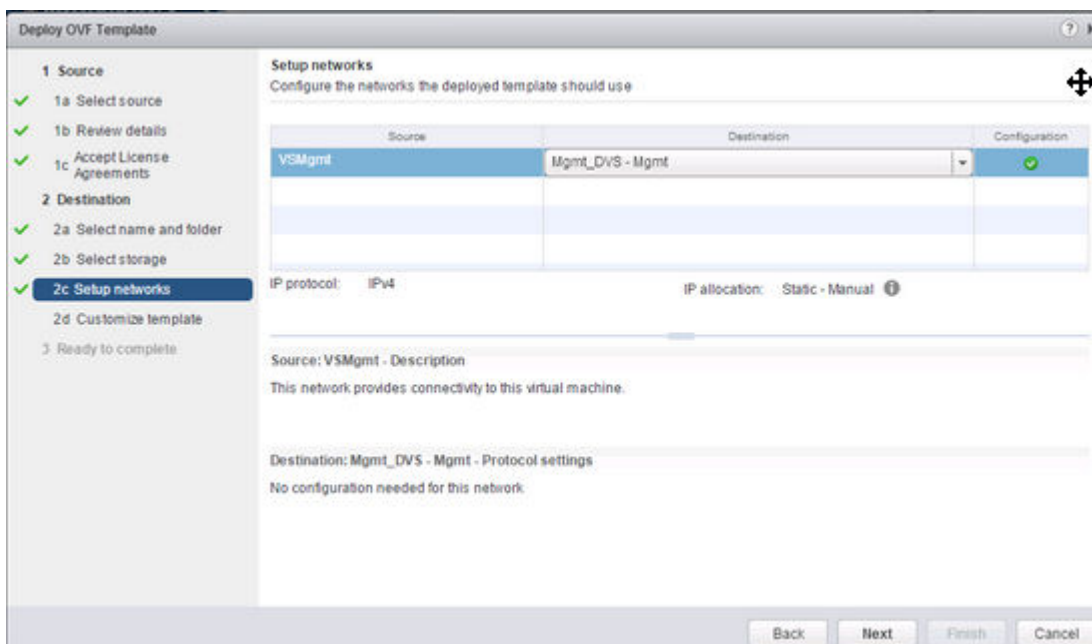




- 9 Ändern Sie das Format für die virtuelle Festplatte in **Thick-Provision (Thick Provision)** und wählen Sie den Zieldatenspeicher für die VM-Konfigurationsdateien und die virtuellen Festplatten aus.

- 10 Wählen Sie die Portgruppe für den NSX Manager aus.

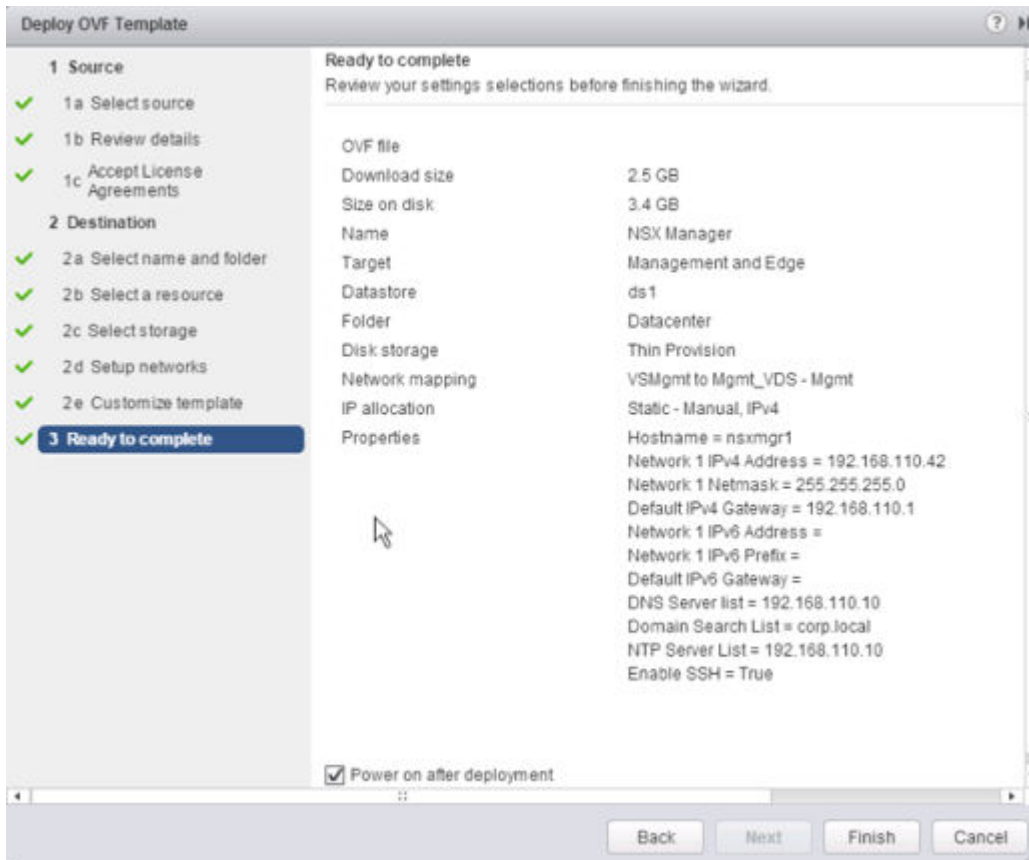
In diesem Screenshot ist beispielsweise die Auswahl für die Portgruppe Mgmt\_DVS - Mgmt dargestellt.



- 11 (Optional) Aktivieren Sie das Kontrollkästchen **Am VMware Customer Experience Improvement Program teilnehmen (Join the Customer Experience Improvement Program)**.

- 12 Legen Sie zusätzlichen Konfigurationsoptionen für NSX Manager fest.

In der folgenden Abbildung wird beispielsweise die Kontrollansicht für die abschließende Überprüfung in einer reinen IPv4-Bereitstellung angezeigt.



## Ergebnisse

Öffnen Sie die Konsole von NSX Manager, um den Startvorgang zu verfolgen.

Melden Sie sich nach dem vollständig abgeschlossenen Start von NSX Manager bei der Befehlszeilenschnittstelle an und führen Sie den Befehl `show interface` aus, um zu überprüfen, ob die IP-Adresse erwartungsgemäß angewendet wurde.

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

Stellen Sie sicher, dass NSX Manager auf allen von ihm verwalteten Hypervisor-Hosts sein Standard-Gateway, seinen NTP-Server, vCenter Server und die IP-Adresse der Verwaltungsschnittstelle anpingen kann.

Stellen Sie eine Verbindung zur Benutzeroberfläche der NSX Manager-Appliance her, indem Sie einen Webbrowser öffnen und zur IP-Adresse oder zum Hostnamen von NSX Manager navigieren.

Nach der Anmeldung als **Administrator (admin)** mit dem bei der Installation eingerichteten Kennwort, klicken Sie auf der Startseite auf **Übersicht anzeigen (View Summary)** und stellen Sie sicher, dass die folgenden Dienste ausgeführt werden:

- vPostgres
- RabbitMQ
- NSX-Verwaltungsdienste

Für eine optimale Leistung empfiehlt VMware, Arbeitsspeicher für die virtuelle NSX Manager-Appliance zu reservieren. Die Arbeitsspeicherreservierung ist eine garantierte Untergrenze für die Menge an physischem Arbeitsspeicher, die der Host für eine virtuelle Maschine reserviert, auch wenn der Arbeitsspeicher mehrfach vergeben wird. Die Reservierung sollte so festgelegt werden, dass NSX Manager über ausreichend Arbeitsspeicher verfügt, um eine effiziente Ausführung sicherzustellen.

### Nächste Schritte

Registrieren Sie vCenter Server bei NSX Manager.

## Konfigurieren von Single Sign-On

SSO macht vSphere und NSX sicherer, da es die Kommunikation der verschiedenen Komponenten untereinander über einen sicheren Token-Austauschmechanismus ermöglicht. Dadurch ist es nicht mehr nötig, dass jede Komponente einen Benutzer separat authentifizieren muss.

Sie können Lookup Service im NSX Manager konfigurieren und die SSO-Administratoranmeldedaten zum Registrieren von NSX Management Service als SSO-Benutzer bereitstellen. Durch das Integrieren des Single Sign On-Diensts (SSO) in NSX wird die Sicherheit der Benutzerauthentifizierung für vCenter-Benutzer erhöht und NSX ermöglicht, Benutzer aus anderen Identitätsdiensten, wie z. B. AD, NIS und LDAP, zu authentifizieren. Mit SSO unterstützt NSX die Authentifizierung mithilfe authentifizierter SAML-Token (Security Assertion Markup Language) einer vertrauenswürdigen Quelle über REST-API-Aufrufe. NSX Manager kann auch Authentifizierungs-SAML-Token für die Verwendung mit anderen VMware-Lösungen erwerben.

NSX speichert Gruppeninformationen für SSO-Benutzer zwischen. Die Weitergabe von Änderungen an Gruppenmitgliedschaften vom Identitätsanbieter (z. B. Active Directory) an NSX kann bis zu 60 Minuten dauern.

### Voraussetzungen

- Sie benötigen zum Verwenden von SSO auf NSX Manager vCenter Server 5.5 oder höher und der Single Sign On-Dienst (SSO-Dienst) muss auf dem vCenter Server installiert sein. Beachten Sie, dass dies für eingebettetes SSO gilt. Ihre Bereitstellung verwendet möglicherweise stattdessen einen externen, zentralisierten SSO-Server.

Informationen zu den von vSphere bereitgestellten SSO-Diensten finden Sie unter <http://kb.vmware.com/kb/2072435> und <http://kb.vmware.com/kb/2113115>.

- Der NTP-Server muss angegeben werden, um sicherzugehen, dass die Zeit des SSO-Servers und von NSX Manager synchron sind.

Beispiel:

Time Settings

Unconfigure NTP Servers

Edit



Specify NTP server below. For SSO configuration to work correctly it is required that the time on this virtual appliance and NTP server should be in sync. It is recommended to use the same NTP server used by the SSO server.

NTP Server	192.168.110.10
Timezone	UTC
Date/Time	12/28/2016 21:31:49

## Verfahren

- 1 Melden Sie sich bei der virtuellen NSX Manager-Appliance an.  
Navigieren Sie in einem Web-Browser zur NSX Manager Appliance-GUI unter <https://<nsx-manager-ip>> oder <https://<nsx-manager-hostname>> und melden Sie sich als Administrator mit dem Kennwort an, das Sie bei der Installation von NSX Manager konfiguriert haben.
- 2 Melden Sie sich bei der virtuellen NSX Manager-Appliance an.
- 3 Klicken Sie auf der Startseite auf **Appliance-Einstellungen verwalten (Manage Appliance Settings) > NSX-Verwaltungsdienst (NSX Management Service)**.
- 4 Klicken Sie im Bereich „Lookup Service-URL“ auf **Bearbeiten (Edit)**.
- 5 Geben Sie die IP-Adresse oder den Namen des Hosts mit dem Lookup Service ein.
- 6 Geben Sie die Portnummer ein.  
Geben Sie Port 443 ein, wenn Sie vSphere 6.0 verwenden. Für vSphere 5.5 verwenden Sie die Portnummer 7444.  
Die URL des Lookup Service wird basierend auf dem angegebenen Host und Port angezeigt.
- 7 Geben Sie den Benutzernamen und das Kennwort des SSO-Administrators ein und klicken Sie auf **OK**.  
Der Fingerabdruck des Zertifikats für den SSO-Server wird angezeigt.
- 8 Überprüfen Sie, ob der Fingerabdruck des Zertifikats mit dem des SSO-Serverzertifikats übereinstimmt.  
Wenn Sie auf dem Server der Zertifizierungsstelle ein von der Zertifizierungsstelle signiertes Zertifikat installiert haben, erhalten Sie den Fingerabdruck des von der Zertifizierungsstelle signierten Zertifikats. Anderenfalls erhalten Sie ein selbstsigniertes Zertifikat.
- 9 Vergewissern Sie sich, dass der Status von Lookup Service **Verbunden (Connected)** lautet.

Beispiel:

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

### Nächste Schritte

Siehe „Zuweisen einer Rolle zu einem vCenter-Benutzer“ im *Administratorhandbuch für NSX*.

## Registrieren von vCenter Server mit NSX Manager

NSX Manager und vCenter Server haben eine 1:1-Beziehung. Für jede NSX Manager-Instanz gibt es einen vCenter Server, selbst in einer Cross-vCenter NSX-Umgebung.

Es kann jeweils nur ein NSX Manager bei einem vCenter Server-System registriert sein. Das Ändern der vCenter-Registrierung eines konfigurierten NSX Manager wird nicht unterstützt.

Wenn Sie die vCenter-Registrierung eines vorhandenen NSX Manager ändern möchten, müssen Sie zunächst alle NSX-Konfigurationen entfernen. Anschließend entfernen Sie das NSX Manager-Plug-in aus dem vCenter Server-System. Eine Anleitung dafür finden Sie unter [Sicheres Entfernen einer NSX-Installation](#). Alternativ können Sie eine neue NSX Manager-Appliance für die Registrierung beim neuen vCenter Server-System bereitstellen.

### Voraussetzungen

- Der NSX Management Service muss ausgeführt werden. Klicken Sie in der Web-Benutzeroberfläche von NSX Manager unter `https://<nsx-manager-ip>` auf **Home > Übersicht anzeigen (View Summary)**, um den Dienststatus anzuzeigen.
- Sie müssen ein vCenter Server-Benutzerkonto verwenden, das Mitglied der Gruppe der **Administratoren** für vCenter Single Sign-On ist, um NSX Manager mit dem vCenter Server-System zu synchronisieren. Wenn das Kennwort für Ihr Konto Nicht-ASCII-Zeichen enthält, müssen Sie es ändern, bevor Sie NSX Manager mit dem vCenter Server-System synchronisieren. Verwenden Sie nicht das Root-Konto.

Informationen zum Hinzufügen von Benutzern finden Sie unter „Verwalten von vCenter Single Sign On-Benutzern und -Gruppen“ in der Dokumentation zur *Platform Services Controller-Verwaltung*.

- Stellen Sie sicher, dass die vorwärts- und rückwärtsgerichtete Namensauflösung funktioniert und dass die folgenden Systeme ihre DNS-Namen gegenseitig auflösen können:
  - NSX Manager-Appliances
  - vCenter Server-Systeme
  - Platform Services Controller-Systeme
  - ESXi-Hosts

## Verfahren

- 1 Melden Sie sich bei der virtuellen NSX Manager-Appliance an.

Navigieren Sie in einem Web-Browser zur NSX Manager Appliance-GUI unter <https://<nsx-manager-ip>> oder <https://<nsx-manager-hostname>> und melden Sie sich als Administrator mit dem Kennwort an, das Sie bei der Installation von NSX Manager konfiguriert haben.

- 2 Klicken Sie auf der Startseite auf **vCenter-Registrierung verwalten (Manage vCenter Registration)**.
- 3 Bearbeiten Sie das vCenter Server-Element so, dass es auf die IP-Adresse oder den Hostnamen des vCenter Server-Systems verweist, und geben Sie den Benutzernamen und das Kennwort des vCenter Server-Systems ein.
- 4 Überprüfen Sie, ob der Fingerabdruck des Zertifikats mit dem des vCenter Server-Systems übereinstimmt.

Wenn Sie auf dem vCenter Server-System ein von der Zertifizierungsstelle signiertes Zertifikat installiert haben, erhalten Sie den Fingerabdruck des von der Zertifizierungsstelle signierten Zertifikats. Anderenfalls erhalten Sie ein selbstsigniertes Zertifikat.

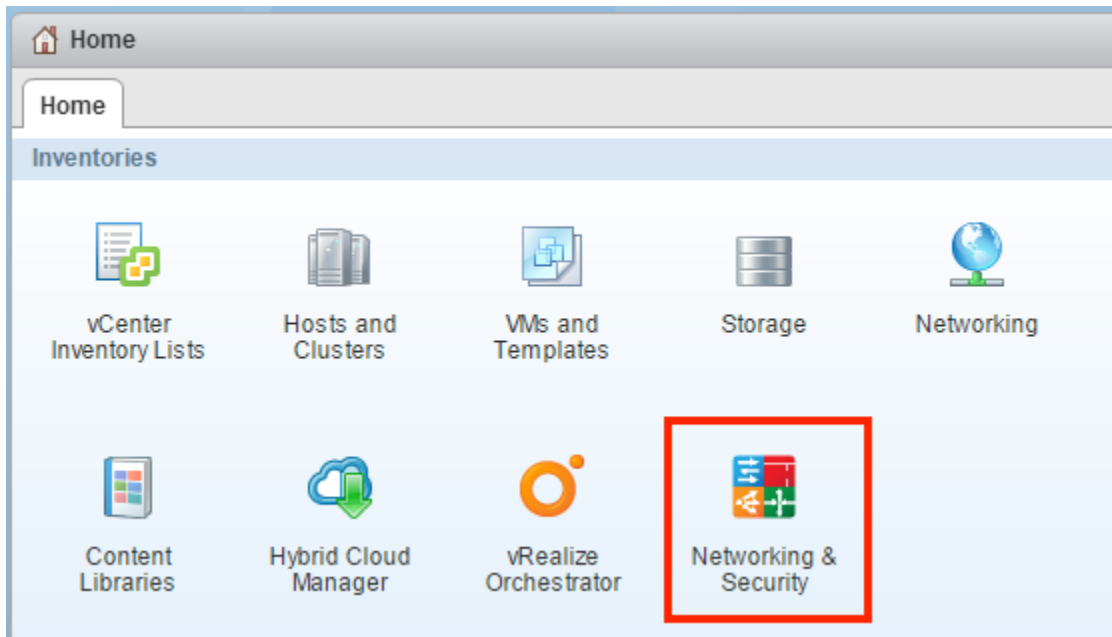
- 5 Aktivieren Sie die Option **Speicherort für Downloads für das Plug-In-Skript ändern (Modify plugin script download location)** nicht, es sei denn, NSX Manager befindet sich hinter einem Maskierungsgerät vom Typ Firewall.

Diese Option ermöglicht Ihnen die Eingabe einer alternativen IP-Adresse für NSX Manager. Das Platzieren von NSX Manager hinter einer Firewall dieses Typs wird nicht empfohlen.

- 6 Bestätigen Sie, dass der vCenter Server-Systemstatus **Verbunden (Connected)** ist.
- 7 Wenn vSphere Web Client bereits geöffnet ist, melden Sie sich ab und dann erneut mit dem Konto an, das zur Registrierung von NSX Manager mit vCenter Server verwendet wird.

Wenn Sie sich nicht ab- und erneut anmelden, wird in vSphere Web Client nicht das Symbol **Netzwerk und Sicherheit (Networking & Security)** auf der Registerkarte **Home** angezeigt.

Klicken Sie auf das Symbol **Netzwerk und Sicherheit (Networking & Security)**, und bestätigen Sie, dass Sie den neu bereitgestellten NSX Manager sehen.



### Nächste Schritte

Planen Sie eine Sicherung der NSX Manager-Daten unmittelbar nach der Installation von NSX Manager. Weitere Informationen finden Sie unter „NSX-Sicherung und -Wiederherstellung“ im *Administratorhandbuch für NSX*.

Wenn Sie über eine NSX for vSphere-Partnerlösung verfügen, finden Sie in der Partnerdokumentation weitere Informationen zum Registrieren der Partnerkonsole bei NSX Manager.

Sie können jetzt NSX for vSphere-Komponenten installieren und konfigurieren.

## Konfigurieren eines Syslog-Servers für NSX Manager

Wenn Sie einen Syslog-Server angeben, sendet NSX Manager alle Überwachungsprotokolle und Systemereignisse an den Syslog-Server.

Syslog-Daten sind hilfreich bei der Problembeseitigung und bei der Überprüfung von Daten, die während der Installation und Konfiguration protokolliert worden sind.

NSX Edge unterstützt zwei Syslog-Server. NSX Manager und NSX Controller unterstützen einen Syslog-Server.

### Verfahren

- 1 Melden Sie sich bei der virtuellen NSX Manager-Appliance an.

Navigieren Sie in einem Web-Browser zur NSX Manager Appliance-GUI unter <https://<nsx-manager-ip>> oder <https://<nsx-manager-hostname>> und melden Sie sich als Administrator mit dem Kennwort an, das Sie bei der Installation von NSX Manager konfiguriert haben.

- 2 Klicken Sie auf der Startseite auf **Appliance-Einstellungen verwalten (Manage Appliance Settings) > Allgemein (General)**.

- 3 Klicken Sie neben **Syslog-Server (Syslog Server)** auf **Bearbeiten (Edit)**.
- 4 Geben Sie die IP-Adresse oder den Hostnamen, Port und Protokoll des Syslog-Servers ein.

Beispiel:

**Syslog Server** [X]

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

Syslog Server:

Port:

Protocol:

[OK] [Cancel]

- 5 Klicken Sie auf **OK**.

### Ergebnisse

Die Remoteprotokollierung von NSX Manager ist aktiviert und die Protokolle werden auf Ihrem eigenständigen Syslog-Server gespeichert.

## Installieren und Zuweisen einer Lizenz von NSX for vSphere

Sie können, nachdem die Installation von NSX Manager abgeschlossen ist, eine Lizenz von NSX for vSphere installieren und zuweisen, indem Sie vSphere Web Client verwenden.

Ab der Version NSX 6.2.3 wird als Standardlizenz diejenige für NSX für vShield Endpoint installiert. Mit dieser Lizenz können Benutzer mit NSX vShield Endpoint nur für die Antivirenfunktion bereitstellen und verwalten. Außerdem wird die Nutzung von VXLAN, Firewall und Edge-Diensten durch Blockierung der Hostvorbereitung und der Erstellung von Edges stark eingeschränkt.

Wenn Sie andere NSX-Funktionen benötigen, z. B. logische Switches, logische Router, die verteilte Firewall oder NSX Edge, müssen Sie entweder eine NSX-Lizenz für die Verwendung dieser Funktionen erwerben oder eine Evaluierungslizenz für einen befristeten Test der Funktionen anfordern.

Informationen zu den NSX-Lizenzierungseditionen und zugehörigen Funktionen finden Sie unter <https://kb.vmware.com/kb/2145269>.



## Verfahren

- ◆ In vSphere 5.5 führen Sie die im Folgenden aufgeführten Schritte zum Hinzufügen einer Lizenz für NSX durch.
  - a Melden Sie sich beim vSphere Web Client an.
  - b Klicken Sie auf **Verwaltung (Administration)** und dann auf **Lizenzen (Licenses)**.
  - c Klicken Sie auf die Registerkarte **Lösungen (Solutions)**.
  - d Wählen Sie in der Liste „Lösungen“ die Option „NSX for vSphere“ aus. Klicken Sie auf **Lizenzschlüssel zuweisen (Assign a license key)**.
  - e Wählen Sie im Dropdown-Menü **Neuen Lizenzschlüssel zuweisen (Assign a new license key)** aus.
  - f Geben Sie den Lizenzschlüssel und eine optionale Bezeichnung für den neuen Schlüssel ein.
  - g Klicken Sie auf **Entschlüsseln (Decode)**.  
Entschlüsseln Sie den Lizenzschlüssel, um sicherzustellen, dass er das richtige Format aufweist und über genügend Kapazität verfügt, um die Assets zu lizenzieren.
  - h Klicken Sie auf **OK**.
- ◆ In vSphere 6.0 führen Sie die im Folgenden aufgeführten Schritte zum Hinzufügen einer Lizenz für NSX durch.
  - a Melden Sie sich beim vSphere Web Client an.
  - b Klicken Sie auf **Verwaltung (Administration)** und dann auf **Lizenzen (Licenses)**.
  - c Klicken Sie auf die Registerkarte **Assets** und dann auf die Registerkarte **Lösungen (Solutions)**.
  - d Wählen Sie in der Liste „Lösungen“ die Option „NSX for vSphere“ aus. Im Dropdown-Menü **Alle Aktionen (All Actions)** wählen Sie **Lizenz zuweisen... (Assign license...)** aus.
  - e Klicken Sie auf das Symbol **Hinzufügen (Add) (+)**. Geben Sie einen Lizenzschlüssel ein und klicken Sie auf **Weiter (Next)**. Fügen Sie einen Namen für die Lizenz hinzu und klicken Sie auf **Weiter (Next)**. Klicken Sie zum Hinzufügen der Lizenz auf **Beenden (Finish)**.
  - f Wählen Sie die neue Lizenz aus.
  - g (Optional) Klicken Sie auf das Symbol **Funktionen anzeigen (View Features)**, um darzustellen, welche Funktionen mit dieser Lizenz aktiviert sind. In der Spalte **Kapazität (Capacity)** wird der Leistungsumfang der Lizenz angegeben.
  - h Klicken Sie auf **OK**, um NSX die neue Lizenz zuzuweisen.

## Nächste Schritte

Weitere Informationen zur NSX-Lizenzierung finden Sie unter <http://www.vmware.com/files/pdf/vmware-product-guide.pdf>.

# Ausschließen von virtuellen Maschinen vom Schutz durch die Firewall

Sie können virtuelle Maschinen vom Schutz durch die verteilte Firewall von NSX ausschließen.

NSX Manager, NSX Controller und NSX Edge-VMs werden automatisch vom Schutz der Verteilten Firewall von NSX ausgeschlossen. Darüber hinaus wird empfohlen, dass Sie folgende Dienst-VMs in die Ausschlussliste aufnehmen, um freien Datenverkehr zu ermöglichen.

- vCenter Server. vCenter Server kann in einen Cluster verschoben werden, der von der Firewall geschützt wird, er muss jedoch bereits in der Ausschlussliste vorhanden sein, um Verbindungsprobleme zu vermeiden.

---

**Hinweis** vCenter Server muss unbedingt der Ausschlussliste hinzugefügt werden, bevor die Standardregel „allow any any“ von „Zulassen“ in „Blockieren“ geändert wird. Wird dies nicht durchgeführt, wird der Zugriff auf vCenter Server blockiert, wenn eine Regel „Alle verweigern“ erstellt (oder die Standardregel zum Blockieren von Aktionen geändert) wird. Ist dies der Fall, setzen Sie die DFW auf die standardmäßige Firewallregel zurück, indem Sie den folgenden API-Befehl ausführen: `https://NSX_Manager_IP/api/4.0/firewall/globalroot-0/config`. Die Anforderung muss den Status 204 zurückgeben. Mit dieser Option wird die Standardrichtlinie (mit der Standardregel „Zulassen“) für die DFW wiederhergestellt und der Zugriff auf vCenter Server und vSphere Web Client wieder ermöglicht.

---

- Partner-Dienst-VMs.
- Virtuelle Maschinen, die den Promiscuous-Modus erfordern. Werden diese virtuellen Maschinen durch die verteilte Firewall von NSX geschützt, so wirkt sich das nachteilig auf ihre Leistung aus.
- SQL-Server, der von Ihrem Windows-basierten vCenter genutzt wird.
- vCenter-Webserver, wenn Sie diesen getrennt betreiben.

## Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Networking & Security**.
- 2 Klicken Sie in **Networking & Security (Networking & Security Inventory)** auf **NSX Manager (NSX Managers)**.
- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und dann auf die Registerkarte **Ausschlussliste (Exclusion List)**.
- 5 Klicken Sie auf das Symbol **Hinzufügen (Add)** (+).
- 6 Wählen Sie die auszuschließenden virtuellen Maschinen aus, und klicken Sie auf **Hinzufügen (Add)**.
- 7 Klicken Sie auf **OK**.

## Ergebnisse

Wenn eine virtuelle Maschine über mehrere vNICs verfügt, werden alle vom Schutz ausgeschlossen. Wenn Sie vNICs zu einer virtuellen Maschine hinzufügen möchten, nachdem diese in die Ausschlussliste aufgenommen worden ist, dann wird die Firewall automatisch auf den neu hinzugefügten vNICs bereitgestellt. Um diese vNICs vom Firewallschutz auszuschließen, müssen Sie die virtuelle Maschine aus der Ausschlussliste entfernen und erneut hinzufügen. Eine weitere Umgehung wäre, die virtuelle Maschine ab- und wieder einzuschalten, die erste Option führt allerdings zu weniger Unterbrechungen.

# Konfigurieren der primären NSX Manager-Instanz

## 6

In einer Cross-vCenter NSX-Umgebung gibt es nur einen primären NSX Manager. Wählen Sie aus, welcher NSX Manager Ihr primärer NSX Manager sein soll und führen Sie die Konfigurationsaufgaben aus, um die NSX-Installation abzuschließen, weisen Sie dem NSX Manager die primäre Rolle zu und erstellen Sie universelle Objekte.

Der primäre NSX Manager wird zur Bereitstellung eines globalen Controller-Clusters genutzt, der die Steuerungsebene für die Cross-vCenter NSX-Umgebung bereitstellt. Die sekundären NSX Manager haben keine eigenen Controller-Cluster.

Dieses Kapitel enthält die folgenden Themen:

- [Bereitstellen des NSX-Controllers auf dem primären NSX Manager](#)
- [Vorbereiten von Hosts auf dem primären NSX Manager](#)
- [Konfigurieren des VXLAN vom primären NSX Manager aus](#)
- [Zuweisen eines Segment-ID-Pools und einer Multicast-Adresse auf dem primären NSX Manager](#)
- [Zuweisen einer primären Rolle zum NSX Manager](#)
- [Zuweisen eines globalen Segment-ID-Pools und einer globalen Multicast-Adresse auf dem primären NSX Manager](#)
- [Hinzufügen einer globalen Transportzone auf dem primären NSX Manager](#)
- [Hinzufügen eines globalen logischen Switches auf dem primären NSX Manager](#)
- [Verbinden von virtuellen Maschinen mit einem logischen Switch](#)
- [Hinzufügen eines globalen logischen \(Distributed\) Routers auf dem primären NSX Manager](#)

## Bereitstellen des NSX-Controllers auf dem primären NSX Manager

NSX Controller ist ein erweitertes verteiltes Zustandsverwaltungssystem, das Steuerungsebenenfunktionen für logische Switching- und Routing-Funktionen von NSX bereitstellt. Das System fungiert als zentraler Kontrollpunkt für alle logischen Switches innerhalb eines Netzwerks und pflegt Informationen zu allen Hosts, logischen Switches (VXLANs) und Distributed Logical Routern. Controller sind erforderlich, wenn Sie Distributed Logical Router oder VXLAN im Unicast- oder Hybrid-Modus bereitstellen möchten. Sobald dem NSX Manager in Cross-vCenter NSX die primäre Rolle

zugewiesen wurde, werden seine Controller-Cluster zum universellen Controller-Cluster für die gesamte Cross-vCenter NSX-Umgebung.

Unabhängig von der Größe der NSX-Bereitstellung ist es für VMware erforderlich, dass jeder NSX Controller-Cluster drei Controller-Knoten enthält. Eine andere Anzahl an Controller-Knoten wird nicht unterstützt.

Für den Cluster ist es erforderlich, dass das Datenspeichersystem jedes Controllers über eine Spitzenschreiblatenz von weniger als 300 ms und eine durchschnittliche Schreiblatenz von weniger als 100 ms verfügt. Erfüllt das Speichersystem diesen Anforderungen nicht, kann der Cluster instabil werden und zu einem Systemausfall führen.

### Voraussetzungen

- Bevor Sie NSX Controller bereitstellen, müssen Sie eine NSX Manager-Appliance bereitstellen und vCenter bei NSX Manager registrieren.
- Legen Sie die IP-Pool-Einstellungen für Ihren Controller-Cluster, einschließlich des Gateways und des IP-Adressbereichs, fest. DNS-Einstellungen sind optional. Das IP-Netzwerk des NSX Controllers muss mit dem NSX Manager und den Verwaltungsschnittstellen auf den ESXi-Hosts verbunden sein.

### Verfahren

- 1 Melden Sie sich mithilfe des vSphere Web Client bei dem vCenter Server-System an, das bei dem NSX Manager registriert ist, der zum primären NSX Manager werden soll.

Wenn sich die vCenter Server-Systeme in Ihrer Cross-vCenter NSX-Umgebung im erweiterten verknüpften Modus befinden, können Sie auf jeden zugeordneten NSX Manager von jedem verknüpften vCenter Server-System aus durch Auswahl im Dropdown-Menü **NSX Manager** zugreifen.

- 2 Navigieren Sie zu **Startseite > Networking & Security > Installation (Home > Networking & Security > Installation)** und wählen Sie die Registerkarte **Management** aus.

Beispiel:



NSX Manager	IP Address
192.168.110.15	192.168.110.15
192.168.210.15	192.168.210.15

Wenn für Ihre vCenter Server-Systeme der erweiterte verknüpfte Modus aktiviert ist, werden hier alle zugeordneten NSX Manager aufgeführt.

- 3 Im Abschnitt der NSX Manager wählen Sie den NSX Manager aus, der zum primären NSX Manager gemacht werden soll.
- 4 Klicken Sie im Bereich der NSX Controller-Knoten auf das Symbol **Knoten hinzufügen (Add Node)** (+).
- 5 Geben Sie die für Ihre Umgebung geeigneten NSX Controller-Einstellungen ein.

NSX Controller müssen für eine vSphere Standard Switch- oder vSphere Distributed Switch-Portgruppe bereitgestellt werden, die nicht auf VXLAN basiert und die über eine Konnektivität zum NSX Manager, zu anderen Controllern und zu Hosts über IPv4 verfügt.

Beispiel:

**Add Controller** ?

Name: \* controller-1

NSX Manager: \* 192.168.110.15 ▼

Datacenter: \* Datacenter Site A ▼

Cluster/Resource Pool: \* Management & Edge Cl... ▼

Datastore: \* ds-site-a-nfs01 ▼

Host: esxmgmt-01a.corp.local ▼

Folder: NSX Controllers ▼

Connected To: \* vds-mgt\_Managem... Change Remove

IP Pool: \* controller-pool Select

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

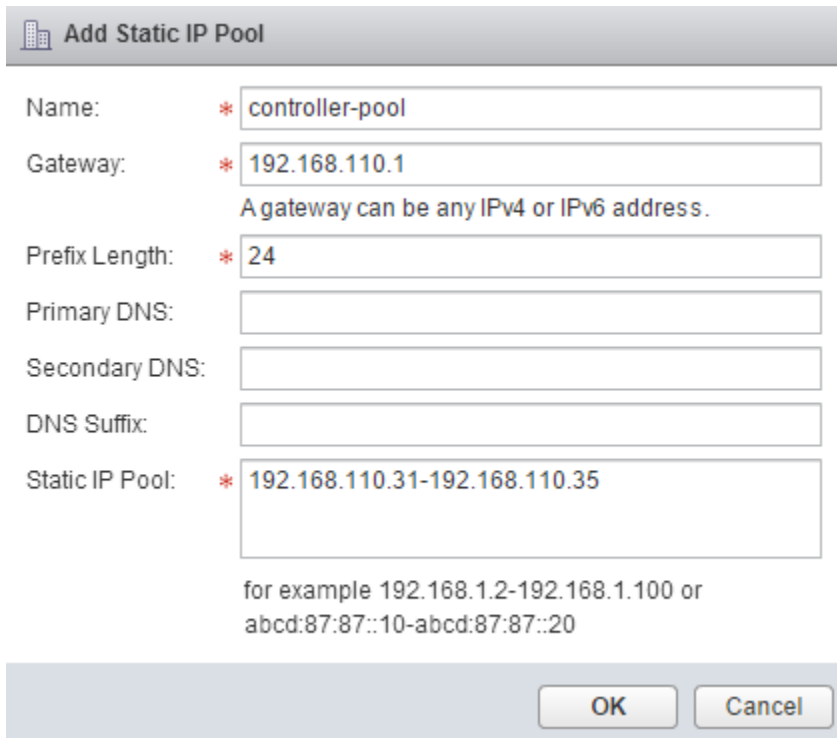
Confirm password: \* \*\*\*\*\*

OK Cancel

- 6 Wenn Sie noch keinen IP-Pool für Ihren Controller-Cluster konfiguriert haben, tun Sie dies jetzt, indem Sie auf **Neuer IP-Pool (New IP Pool)** klicken.

Falls erforderlich, können einzelne Controller sich in separaten IP-Subnetzen befinden.

Beispiel:

 **Add Static IP Pool**

Name: \*

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

Prefix Length: \*

Primary DNS:

Secondary DNS:

DNS Suffix:

Static IP Pool: \*   
for example 192.168.1.2-192.168.1.100 or  
abcd:87:87::10-abcd:87:87::20

- 7 Geben Sie ein Kennwort für den Controller einmal und dann erneut ein.

**Hinweis** Der Benutzername darf nicht als Teilzeichenfolge im Kennwort enthalten sein. Zeichen dürfen maximal zweimal hintereinander wiederholt werden.

Das Kennwort muss mindestens 12 Zeichen lang sein und 3 der 4 folgenden Regeln folgen:

- mindestens ein Großbuchstabe
- mindestens ein Kleinbuchstabe
- mindestens eine Zahl
- mindestens ein Sonderzeichen

- 8 Stellen Sie nach der vollständigen Bereitstellung des ersten Controllers zwei weitere Controller bereit.

Es müssen drei Controller vorhanden sein. Es wird empfohlen, eine DRS-Anti-Affinitätsregel zu konfigurieren, mit der verhindert wird, dass sich die Controller auf demselben Host befinden.

### Ergebnisse

Nach erfolgreicher Bereitstellung werden für die Controller der Status **Verbunden (Connected)** und ein grünes Häkchen angezeigt.

Wenn die Bereitstellung nicht erfolgreich war, schlagen Sie unter dem Abschnitt zum Bereitstellen von NSX Controllern im *Fehlerbehebungshandbuch zu NSX* nach.

## Vorbereiten von Hosts auf dem primären NSX Manager

Bei der Hostvorbereitung handelt es sich um den Vorgang, bei dem NSX Manager zum einen NSX-Kernel-Module auf ESXi-Hosts, die Mitglieder von vCenter-Clustern sind, installiert; und zum anderen das Fabric der Steuerungsebene und der Verwaltungsebene für NSX errichtet. In VIB-Dateien gepackte NSX-Kernel-Module werden im Hypervisor-Kernel ausgeführt und stellen Dienste wie Distributed Routing, verteilte Firewall und VXLAN-Bridging-Funktionen bereit.

Um Ihre Umgebung für die Netzwerkvirtualisierung vorzubereiten, müssen Sie die Netzwerkinfrastruktur gegebenenfalls für jeden vCenter Server pro Cluster installieren. Auf diese Weise wird die erforderliche Software auf allen Hosts im Cluster bereitgestellt. Wird ein neuer Host zu diesem Cluster hinzugefügt, wird die Software darauf automatisch installiert.

Wenn Sie ESXi im statusfreien Modus verwenden (ESXi seinen Status nach Neustarts also nicht aktiv beibehält), müssen Sie die NSX-VIBs manuell herunterladen und sie dem Host-Image hinzufügen. Die Download-Pfade für die NSX-VIBs finden Sie auf der folgenden Seite: [https://<NSX\\_MANAGER\\_IP>/bin/vdn/nwfabric.properties](https://<NSX_MANAGER_IP>/bin/vdn/nwfabric.properties). Beachten Sie, dass die Download-Pfade von Version zu Version von NSX variieren können. Um die jeweils richtigen VIBs zu erhalten, informieren Sie sich stets auf der Seite [https://<NSX\\_MANAGER\\_IP>/bin/vdn/nwfabric.properties](https://<NSX_MANAGER_IP>/bin/vdn/nwfabric.properties). Unter „Bereitstellen von VXLAN durch automatische Bereitstellung“ <https://kb.vmware.com/kb/2041972> finden Sie weitere Informationen.

### Voraussetzungen

- Registrieren Sie vCenter Server bei NSX Manager und stellen Sie NSX Controller bereit.
- Stellen Sie sicher, dass das DNS-Reverse-Lookup einen vollständig qualifizierten Domännennamen zurückgibt, wenn dieser mit der IP-Adresse von NSX Manager abgefragt wird. Beispiel:

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

Name:    nsxmgr-1-01a.corp.local
Address: 192.168.110.42
```

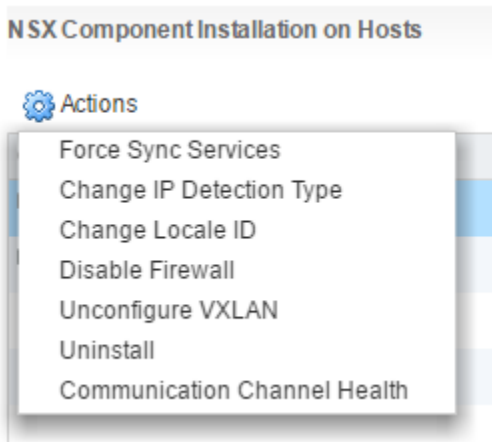
- Überprüfen Sie, ob die Hosts den DNS-Namen von vCenter Server auflösen können.
- Überprüfen Sie, ob die Hosts sich über Port 80 mit vCenter Server verbinden können.
- Stellen Sie sicher, dass die Netzwerkzeit auf vCenter Server und ESXi-Hosts synchronisiert ist.
- Überprüfen Sie für jeden Host-Cluster, der an NSX teilnimmt, ob dessen Hosts einem gemeinsamen vSphere Distributed Switch (VDS) angefügt sind.



Angenommen, Sie haben einen Cluster mit Host1 und Host2. Host1 wird mit VDS1 und VDS2 verbunden. Host2 wird mit VDS1 und VDS3 verbunden. Wenn Sie einen Cluster für NSX vorbereiten, können Sie auf dem Cluster NSX nur mit VDS1 verknüpfen. Wenn Sie dem Cluster einen weiteren Host (Host3) hinzufügen und Host3 nicht mit VDS1 verbunden wird, ist die Konfiguration ungültig und Host3 steht für NSX-Funktionen nicht bereit.

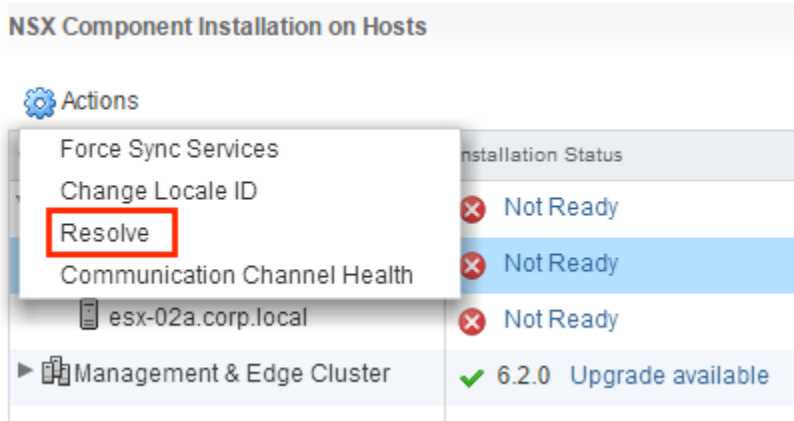
- Wenn in Ihrer Umgebung vSphere Update Manager (VUM) vorhanden ist, müssen Sie diesen vor der Vorbereitung von Clustern für die Netzwerkvirtualisierung deaktivieren. Informationen dazu, wie man überprüft, ob VUM aktiviert ist und wie man VUM bei Bedarf deaktiviert, finden Sie unter <http://kb.vmware.com/kb/2053782>.
- Stellen Sie vor Beginn der NSX-Hostvorbereitung immer sicher, dass der Cluster sich im aufgelösten Zustand befindet und die Option **Auflösen (Resolve)** nicht in der **Aktionsliste (Actions)** des Clusters angezeigt wird.

Beispiel:



Die Option **Auflösen (Resolve)** wird manchmal angezeigt, weil einer oder mehrere Hosts im Cluster neu gestartet werden müssen.

In anderen Fällen wird die Option **Auflösen (Resolve)** angezeigt, weil ein Fehler vorliegt, der behoben werden muss. Klicken Sie auf den Link **Nicht bereit (Not Ready)**, um den Fehler anzuzeigen. Löschen Sie, soweit möglich, den Fehler. Wenn Sie einen Fehler auf einem Cluster nicht löschen können, können Sie das Problem umgehen, indem Sie die Hosts auf einen neuen oder einen anderen Cluster verschieben und den alten Cluster löschen.



Wenn die Option **Auflösen (Resolve)** das Problem nicht behebt, informieren Sie sich im *Fehlerbehebungshandbuch zu NSX*. Eine Liste aller Probleme, die mit der Option **Auflösen (Resolve)** behoben wurden, finden Sie unter *NSX-Protokollierung und -Systemereignisse*.

### Verfahren

- 1 Melden Sie sich mithilfe des vSphere Web Client bei dem vCenter Server-System an, das bei dem NSX Manager registriert ist, der zum primären NSX Manager werden soll.

Wenn sich die vCenter Server-Systeme in Ihrer Cross-vCenter NSX-Umgebung im erweiterten verknüpften Modus befinden, können Sie auf jeden zugeordneten NSX Manager von jedem verknüpften vCenter Server-System aus durch Auswahl im Dropdown-Menü **NSX Manager** zugreifen.

- 2 Wechseln Sie zu **Home > Networking & Security > Installation** und wählen Sie die Registerkarte **Hostvorbereitung (Host Preparation)** aus.
- 3 Klicken Sie bei allen Clustern, die ein logisches NSX-Switching, NSX-Routing und NSX-Firewalls erfordern, auf **Aktionen (Actions)** (⚙️) und dann auf **Installieren (Install)**.

Ein Computing-Cluster ist ein Cluster mit Anwendungs-VMs (Web, Datenbank usw.). Wenn ein Computing-Cluster über NSX-Switching, NSX-Routing oder NSX-Firewalls verfügen soll, klicken Sie für den Computing-Cluster auf **Installieren (Install)**.

In einem (wie im Beispiel dargestellten) gemeinsam genutzten „Management- und Edge-Cluster“ teilen sich NSX Manager- und NSX Controller-VMs einen Cluster mit Edge-Geräten wie zum Beispiel Distributed Logical Routers (DLRs) und Edge Services Gateways (ESGs). In diesem Fall ist es obligatorisch, für den gemeinsam genutzten Cluster auf **Installieren (Install)** zu klicken.

Verfügen Management und Edge hingegen – wie in einer Produktionsumgebung empfohlen – jeweils über einen eigenen, nicht gemeinsam genutzten Cluster, klicken Sie im Falle des Edge-Clusters auf **Installieren (Install)**, im Falle des Management-Clusters jedoch nicht.

---

**Hinweis** Führen Sie während der Installation keine Upgrades aus, stellen Sie keine Dienste oder Komponenten bereit und deinstallieren Sie keine Dienste oder Komponenten.

---

- 4 Überwachen Sie die Installation, bis in der Spalte **Installationsstatus (Installation Status)** ein grünes Häkchen angezeigt wird.

Wenn in der Spalte **Installationsstatus (Installation Status)** ein rotes Warnsymbol und **Nicht bereit (Not Ready)** angezeigt wird, klicken Sie auf **Auflösen (Resolve)**. Durch Klicken auf **Auflösen (Resolve)** könnte ein Neustart des Hosts ausgelöst werden. Wenn die Installation immer noch nicht erfolgreich ist, klicken Sie auf das Warnsymbol. Alle Fehler werden angezeigt. Führen Sie die nötige(n) Aktion(en) aus und klicken Sie wieder auf **Auflösen (Resolve)**.

Wenn die Installation abgeschlossen ist, werden in der Spalte **Installationsstatus (Installation Status)** die Version und das Build des installierten NSX angezeigt. Die Spalte **Firewall** enthält die Anzeige **Aktiviert (Enabled)**. Beide Spalten zeigen ein grünes Häkchen an. Wenn in der Spalte **Installationsstatus (Installation Status)** „Auflösen“ angezeigt wird, klicken Sie auf „Auflösen“ und aktualisieren Sie danach Ihr Browser-Fenster.

## Ergebnisse

Bei allen Hosts innerhalb des vorbereiteten Clusters werden VIBs installiert und registriert: Der installierten VIBs sind unterschiedlich, je nachdem, die welche Versionen von NSX und ESXi installiert sind.

ESXi-Version	NSX-Version	Installierte VIBs
5.5	Alle 6.3.x	<ul style="list-style-type: none"> <li>■ esx-vsip</li> <li>■ esx-vxlan</li> </ul>
6.0 oder höher	6.3.2 oder früher	<ul style="list-style-type: none"> <li>■ esx-vsip</li> <li>■ esx-vxlan</li> </ul>
6.0 oder höher	6.3.3 oder höher	<ul style="list-style-type: none"> <li>■ esx-nsxv</li> </ul>

Um zu überprüfen, SSH auf jeden host und führen Sie den Befehl `esxcli software vib list` und die Kontrollkästchen für die relevanten VIBs. Neben den VIBs wird durch diesen Befehl auch die Version der installierten VIBs angezeigt.

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

Wenn Sie einem vorbereiteten Cluster einen Host hinzufügen, werden die NSX VIBs automatisch auf dem Host installiert.

Wenn Sie einen Host auf einen nicht vorbereiteten Cluster verschieben, werden die NSX VIBs automatisch vom Host deinstalliert.

## Konfigurieren des VXLAN vom primären NSX Manager aus

Das VXLAN-Netzwerk wird für logisches Schicht-2-Switching über Hosts hinweg verwendet, die mehrere zugrunde liegende Schicht-3-Domänen umfassen können. Sie konfigurieren VXLAN pro Cluster, wobei Sie jeden Cluster, der an NSX teilnehmen soll, einem vSphere Distributed Switch (VDS) zuordnen. Wenn Sie einem verteilten Switch einen Cluster zuordnen, wird jeder Host in diesem Cluster für logische

Switches aktiviert. Die hier gewählten Einstellungen werden beim Erstellen der VMkernel-Schnittstelle verwendet.

Wenn Sie logisches Routing und Switching benötigen, müssen für alle Cluster, für die NSX VIBs auf den Hosts installiert sind, auch VXLAN-Transportparameter konfiguriert werden. Wenn Sie vorhaben, nur die verteilte Firewall bereitzustellen, brauchen Sie keine VXLAN-Transportparameter zu konfigurieren.

Wenn Sie ein VXLAN-Netzwerk konfigurieren, müssen Sie einen vSphere Distributed Switch bereitstellen, eine VLAN-ID, eine MTU-Größe, einen IP-Adressmechanismus (DHCP oder IP-Pool) und eine NIC-Gruppierungsrichtlinie.

Die MTU für jeden Switch muss auf 1550 oder höher festgelegt werden. Standardmäßig ist 1600 festgelegt. Wenn die MTU-Größe des vSphere Distributed Switch größer als die VXLAN-MTU ist, wird die vSphere Distributed Switch-MTU nicht nach unten angepasst. Wenn dafür ein geringerer Wert festgelegt ist, wird er angepasst, um der VXLAN-MTU zu entsprechen. Beispiel: Wenn die vSphere Distributed Switch-MTU auf 2000 festgelegt ist und Sie den Standardwert von 1600 für die VXLAN-MTU akzeptieren, werden keine Änderungen an der vSphere Distributed Switch-MTU vorgenommen. Wenn die vSphere Distributed Switch-MTU auf 1500 festgelegt ist und die VXLAN-MTU auf 1600, wird die vSphere Distributed Switch-MTU auf 1600 geändert.

VTEPs ist eine VLAN-ID zugeordnet. Sie können jedoch VLAN-ID = 0 für VTEPs angeben, was bedeutet, dass Frames nicht gekennzeichnet werden.

Sie können für Ihre Verwaltungscluster und Ihre Computing-Cluster unterschiedliche IP-Adresseinstellungen verwenden. Das hängt vom Design des physischen Netzwerks ab und wahrscheinlich ist es in kleinen Bereitstellungen nicht erforderlich.

### Voraussetzungen

- Alle Hosts im Cluster müssen mit einem gemeinsamen vSphere Distributed Switch verbunden sein.
- NSX Manager muss installiert werden.
- NSX-Controller müssen installiert sein, es sei denn, Sie verwenden den Multicast-Replikationsmodus für die Steuerungskomponente.
- Planen Sie die NIC-Gruppierungsrichtlinie. Ihre NIC-Gruppierungsrichtlinie bestimmt die Load-Balancing- und Failover-Einstellungen des vSphere Distributed Switch.

Kombinieren Sie keine unterschiedlichen Gruppierungsrichtlinien für unterschiedliche Portgruppen bei einem vSphere Distributed Switch, wenn einige Portgruppen Etherchannel oder LACPv1 bzw. LACPv2 und andere Portgruppen eine andere Gruppierungsrichtlinie verwenden. Wenn in diesen unterschiedlichen Gruppierungsrichtlinien Uplinks gemeinsam genutzt werden, wird der Datenverkehr unterbrochen. Wenn logische Router vorhanden sind, kommt es zu Routing-Problemen. Solch eine Konfiguration wird nicht unterstützt und sollte nicht verwendet werden.

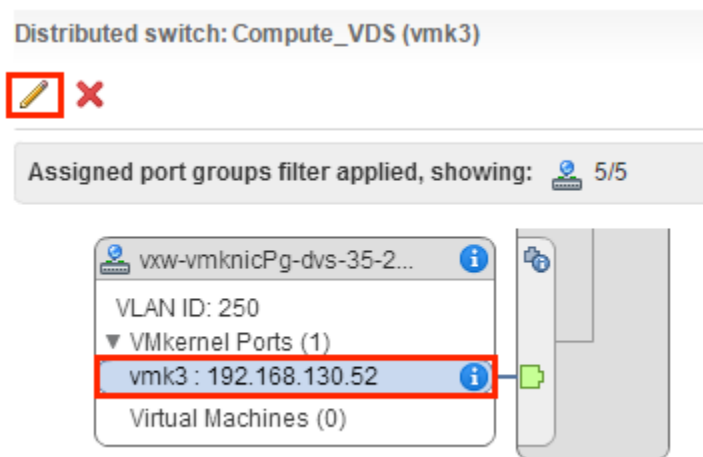
Die empfohlene Vorgehensweise für IP-hashbasiertes Teaming (EtherChannel, LACPv1 oder LACPv2) besteht darin, alle Uplinks auf dem vSphere Distributed Switch im Team, aber keine Portgruppen auf diesem vSphere Distributed Switch mit unterschiedlichen Teaming-Richtlinien zu verwenden. Weitere Informationen finden Sie im *Handbuch zum Netzwerkvirtualisierungsdesign für VMware® NSX for vSphere* unter <https://communities.vmware.com/docs/DOC-27683>.

- Planen Sie das IP-Adressschema für die VXLAN-Tunnelendpunkte (VTEPs). VTEPs sind die Quell- und Ziel-IP-Adressen, die im externen IP-Header verwendet werden, um die ESX-Hosts eindeutig zu identifizieren, bei denen die VXLAN-Kapselung von Frames beginnt und endet. Verwenden Sie entweder DHCP oder manuell konfigurierte IP-Pools für VTEP-IP-Adressen.

Wenn eine bestimmte IP-Adresse einem VTEP zugewiesen werden soll, haben Sie folgende Möglichkeiten: 1) Verwenden Sie eine feste DHCP-Adresse oder Reservierung, die eine MAC-Adresse einer bestimmten IP-Adresse auf dem DHCP-Server zuweist, oder 2) verwenden Sie einen IP-Pool und bearbeiten Sie dann manuell die VTEP-IP-Adresse, die dem vmknic unter **Hosts und Cluster (Hosts and Clusters) > Host > Verwalten (Manage) > Netzwerk (Networking) > Virtuelle Switches (Virtual Switches)** zugewiesen wurde.

**Hinweis** Wenn Sie die IP-Adresse manuell bearbeiten, stellen Sie sicher, dass die IP-Adresse KEINE Ähnlichkeiten zum ursprünglichen IP-Pool-Bereich aufweist.

Beispiel:



- Für Cluster, die Mitglieder des gleichen VDS sind, muss die VLAN-ID für die VTEPs und die NIC-Gruppierung die gleiche sein.
- Best Practice ist, die vSphere Distributed Switch-Konfiguration zu exportieren, bevor Sie den Cluster für VXLAN vorbereiten. Weitere Informationen dazu finden Sie unter <http://kb.vmware.com/kb/2034602>.

## Verfahren

- 1 Melden Sie sich mithilfe des vSphere Web Client bei dem vCenter Server-System an, das bei dem NSX Manager registriert ist, der zum primären NSX Manager werden soll.

Wenn sich die vCenter Server-Systeme in Ihrer Cross-vCenter NSX-Umgebung im erweiterten verknüpften Modus befinden, können Sie auf jeden zugeordneten NSX Manager von jedem verknüpften vCenter Server-System aus durch Auswahl im Dropdown-Menü **NSX Manager** zugreifen.

- 2 Wechseln Sie zu **Home > Networking & Security > Installation** und wählen Sie die Registerkarte **Hostvorbereitung (Host Preparation)** aus.
- 3 Stellen Sie sicher, dass der richtige NSX Manager im Dropdown-Menü **NSX Manager** ausgewählt ist.
- 4 Klicken Sie auf **Nicht konfiguriert (Not Configured)** in der Spalte **VXLAN**.
- 5 Richten Sie logische Netzwerke ein.

Dazu müssen Sie einen vSphere Distributed Switch, eine VLAN-ID, eine MTU-Größe, einen IP-Adressmechanismus und eine NIC-Gruppierungsrichtlinie auswählen.

Diese Beispiele zeigen eine Konfiguration für einen Verwaltungs-Cluster mit einem IP-Pool-Adressbereich von 182.168.150.1-192.168.150.100, gesichert von VLAN 150, und einer Failover-NIC-Gruppierungsrichtlinie.

**Configure VXLAN networking**

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

Switch: \* Mgmt\_VDS

VLAN: \* 150

MTU: \* 1600

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

IP Pool: New IP Pool...

VMKNic Teaming Policy: \* Fail Over

VTEP: \* 1

OK Cancel

Die Anzahl der VTEPs ist in der Benutzeroberfläche nicht bearbeitbar. Die VTEP-Anzahl ist so festgelegt, dass sie der Anzahl der dvUplinks auf dem vSphere Distributed Switch entspricht, die vorbereitet werden.

**Add Static IP Pool**

Name: \* mgmt-edge-ip-pool

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

Prefix Length: \* 24

Primary DNS: 192.168.110.10

Secondary DNS:

DNS Suffix: corp.local

Static IP Pool: \* 182.168.150.1-192.168.150.100  
for example 192.168.1.2-192.168.1.100 or  
abcd:87:87::10-abcd:87:87::20

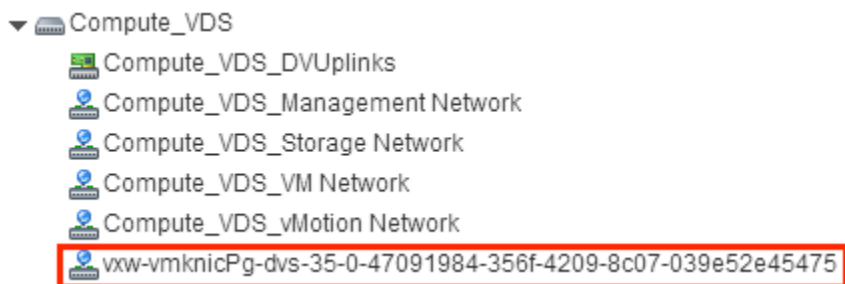
OK Cancel

Für Rechen-Cluster können Sie andere IP-Adresseinstellungen verwenden (z. B. 192.168.250.0/24 mit VLAN 250). Das hängt vom Design des physischen Netzwerks ab und wahrscheinlich ist es in kleinen Bereitstellungen nicht erforderlich.

## Ergebnisse

Die Konfiguration von VXLAN ergibt eine neue verteilte Portgruppe im angegebenen vSphere Distributed Switch.

Beispiel:



Weitere Informationen zur VXLAN-Fehlerbehebung finden Sie im *Fehlerbehebungshandbuch zu NSX*.

## Zuweisen eines Segment-ID-Pools und einer Multicast-Adresse auf dem primären NSX Manager

VXLAN-Segmente werden zwischen den VXLAN-Tunnelendpunkten (VTEPs) erstellt. Jeder VXLAN-Tunnel verfügt über eine Segment-ID. Sie müssen für den primären NSX Manager einen Segment-ID-Pool angeben, um Ihren Netzwerkdatenverkehr zu isolieren. Wenn in Ihrer Umgebung kein NSX-Controller bereitgestellt ist, müssen Sie zudem einen Multicast-Adressbereich für das Verteilen des

Datenverkehrs im Netzwerk hinzufügen, um die Überlastung einer einzelnen Multicast-Adresse zu vermeiden.

Beachten Sie bei der Bestimmung der Größe der einzelnen Segment-ID-Pools, dass der Segment-ID-Bereich die Anzahl der logischen Switches steuert, die erstellt werden können. Wählen Sie eine kleine Teilmenge der 16 Millionen potenziellen VNIs aus. Konfigurieren Sie nicht mehr als 10.000 VNIs in einem einzelnen vCenter, da vCenter die Anzahl der dvPortgroups auf 10.000 beschränkt.

Alle NSX Manager in Ihrer Cross-vCenter NSX-Umgebung müssen nicht überlappende Segment-ID-Pools verwenden. Zudem dürfen die universellen Segment-ID-Pools nicht mit Segment-ID-Pools in der Cross-vCenter NSX-Umgebung überlappen. Nicht überlappende VNIs werden in einer Umgebung mit einem NSX Manager und vCenter automatisch erzwungen. Es ist jedoch wichtig, dass Sie sicherstellen, dass VNIs sich nicht in Ihren getrennten NSX-Bereitstellungen überlappen. Nicht überlappende VNIs sind nützlich für Nachverfolgungszwecke und helfen sicherzustellen, dass Ihre Bereitstellungen für eine Cross-vCenter NSX-Umgebung bereit sind.

Wenn eine Ihrer Transportzonen den Multicast- oder Hybrid-Replikationsmodus verwendet, müssen Sie eine Multicast-Adresse oder einen Bereich von Multicast-Adressen hinzufügen.

Durch einen Bereich von Multicast-Adressen wird der Datenverkehr über das Netzwerk verteilt und die Überlastung einer einzelnen Multicast-Adresse verhindert. Damit wird auch die BUM-Replikation besser eingegrenzt.

Sie müssen sicherstellen, dass die angegebene Multicast-Adresse bzw. der angegebene Adressbereich nicht mit anderen Multicast-Adressen in Konflikt steht, die auf einem NSX Manager in der Cross-vCenter NSX-Umgebung zugewiesen wurden.

Verwenden Sie 239.0.0.0/24 oder 239.128.0.0/24 nicht als Multicast-Adressbereich, da diese Netzwerke für die Steuerung des lokalen Subnetzes verwendet werden, was bedeutet, dass die physischen Switches den gesamten Datenverkehr fluten, der diese Adressen verwendet. Weitere Informationen zu nicht verwendbaren Multicast-Adressen finden Sie unter <https://tools.ietf.org/html/draft-ietf-mboned-ipv4-mcast-unusable-01>.

Wenn VXLAN-Multicast- und Hybrid-Replikationsmodi konfiguriert sind und korrekt funktionieren, wird eine Kopie des Multicast-Datenverkehrs nur an die Hosts geliefert, die IGMP-Beitrittsmeldungen gesandt haben. Andernfalls überflutet das physische Netzwerk den gesamten Multicast-Datenverkehr an alle Hosts in derselben Broadcast-Domäne. Um diese Überflutung zu verhindern, gehen Sie wie folgt vor:

- Vergewissern Sie sich, dass der zugrunde liegende physische Switch mit einer MTU größer oder gleich 1600 konfiguriert ist.
- Vergewissern Sie sich, dass der zugrunde liegende physische Switch korrekt mit IGMP-Snooping und einem IGMP-Abfrager in Netzwerksegmenten, die VTEP-Datenverkehr übertragen, konfiguriert ist.
- Stellen Sie sicher, dass die Transportzone mit dem empfohlenen Multicast-Adressbereich konfiguriert ist. Der empfohlene Multicast-Adressbereich beginnt bei 239.0.1.0/24 und schließt 239.128.0.0/24 aus.



Die vSphere Web Client-Schnittstelle ermöglicht die Konfiguration eines einzelnen Segment-ID-Bereichs und einer einzelnen Multicast-Adresse oder eines Multicast-Adressbereichs. Wenn Sie mehrere Segment-ID-Bereiche oder mehrere Multicast-Adresswerte konfigurieren möchten, steht Ihnen dafür die NSX API zur Verfügung. Weitere Informationen finden Sie unter *Handbuch zu NSX-API*.

### Verfahren

- 1 Melden Sie sich mithilfe des vSphere Web Client bei dem vCenter Server-System an, das bei dem NSX Manager registriert ist, der zum primären NSX Manager werden soll.

Wenn sich die vCenter Server-Systeme in Ihrer Cross-vCenter NSX-Umgebung im erweiterten verknüpften Modus befinden, können Sie auf jeden zugeordneten NSX Manager von jedem verknüpften vCenter Server-System aus durch Auswahl im Dropdown-Menü **NSX Manager** zugreifen.

- 2 Wechseln Sie zu **Home > Networking & Security > Installation** und wählen Sie die Registerkarte **Vorbereitung des logischen Netzwerks (Logical Network Preparation)** aus.
- 3 Stellen Sie sicher, dass der richtige NSX Manager im Dropdown-Menü **NSX Manager** ausgewählt ist.
- 4 Klicken Sie auf **Segment-ID > Bearbeiten (Segment ID > Edit)**.
- 5 Geben Sie einen Bereich für die Segment-IDs ein, z. B. **5000–5999**.
- 6 (Optional) Wenn eine Ihrer Transportzonen den Multicast- oder Hybrid-Replikationsmodus verwendet, müssen Sie eine Multicast-Adresse oder einen Bereich von Multicast-Adressen hinzufügen.
  - a Aktivieren Sie das Kontrollkästchen **Multicast-Adressierung aktivieren (Enable Multicast addressing)**.
  - b Geben Sie eine Multicast-Adresse oder einen Multicast-Adressbereich ein, z. B. **239.0.0.0–239.255.255.255**.

### Ergebnisse

Wenn Sie logische Switches konfigurieren, erhält jeder logische Switch eine Segment-ID aus dem Pool.

## Zuweisen einer primären Rolle zum NSX Manager

Der primäre NSX Manager führt den Controller-Cluster aus. Weitere NSX Manager sind sekundär. Der vom primären NSX Manager bereitgestellte Controller-Cluster ist ein gemeinsam genutztes Objekt, welches als globaler Controller-Cluster bezeichnet wird. Sekundäre NSX Manager importieren den globalen Controller-Cluster automatisch. Es können ein primärer NSX Manager und bis zu sieben sekundäre NSX Manager in einer Cross-vCenter NSX-Umgebung vorhanden sein.

NSX Manager können eine von vier Rollen aufweisen:

- Primär
- Sekundär
- Eigenständig
- Transit

Um die Rolle einer NSX Manager-Instanz anzuzeigen, melden Sie sich bei der mit dem NSX Manager verknüpften vCenter-Instanz an, navigieren Sie zu **Startseite (Home) > Networking & Security > Installation** und wählen Sie dann die Registerkarte **Management** aus. Die Rolle wird in der Spalte „Rolle“ im NSX Manager-Abschnitt angezeigt. Wenn keine Spalte „Rolle“ angezeigt wird, weist der NSX Manager die Rolle „Eigenständig“ auf.

### Voraussetzungen

- Die Versionen der NSX Manager (der primären NSX Manager-Instanz und der NSX Manager, denen die Rolle „Sekundär“ zugewiesen wird) müssen übereinstimmen.
- Die Knoten-IDs der primären NSX Manager-Instanz und der NSX Manager, denen die Rolle „Sekundär“ zugewiesen wird, müssen vorhanden sein und dürfen nicht übereinstimmen. Mithilfe von OVA-Dateien bereitgestellte NSX Manager-Instanzen besitzen eindeutige Knoten-IDs. Ein von einer Vorlage bereitgestellter NSX Manager (wie beim Konvertieren einer virtuellen Maschine in eine Vorlage) erhält die gleiche Knoten-ID wie der zum Erstellen der Vorlage verwendete ursprüngliche NSX Manager, und diese beiden NSX Manager können nicht in derselben Cross-vCenter NSX-Installation verwendet werden.

**Hinweis** Sie können die NSX Manager-Knoten-ID mit dem folgenden REST API-Aufruf anzeigen:

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

- Jeder NSX Manager muss bei einem eigenen, eindeutigen vCenter Server-System registriert sein.
- Die für VXLAN verwendeten UDP-Ports müssen für alle NSX Manager identisch sein.

**Hinweis** Sie können den VXLAN-Port mithilfe des vSphere Web Client unter **Networking & Security > Installation > Vorbereitung des logischen Netzwerks (Logical Network Preparation)** anzeigen und ändern. Weitere Informationen erhalten Sie unter „Ändern des VXLAN-Ports“ im *Administratorhandbuch für NSX*.

- Beim Zuweisen der Rolle „Sekundär“ zu einem NSX Manager darf das mit diesem NSX Manager verknüpfte vCenter Server-System keine bereitgestellten NSX-Controller enthalten.
- Der Segment-ID-Pool der NSX Manager-Instanz, der die Rolle „Sekundär“ zugewiesen wird, darf sich nicht mit den Segment-ID-Pools der primären NSX Manager-Instanz oder dem Segment-ID-Pool einer anderen sekundären NSX Manager-Instanz überlappen.
- Der NSX Manager, dem die Rolle „Sekundär“ zugewiesen wird, muss die Rolle „Eigenständig“ oder „Transit“ aufweisen.

### Verfahren

- 1 Melden Sie sich unter Verwendung von vSphere Web Client bei der mit dem primären NSX Manager verknüpften vCenter-Instanz an.
- 2 Navigieren Sie zu **Startseite > Networking & Security > Installation (Home > Networking & Security > Installation)** und wählen Sie die Registerkarte **Management** aus.

- 3 Wählen Sie den NSX Manager aus, den Sie als primär zuweisen möchten, und klicken Sie auf **Aktionen (Actions)**. Klicken Sie dann auf **Primäre Rolle zuweisen (Assign Primary Role)**.

Dem ausgewählten NSX Manager wird die primäre Rolle zugewiesen. Für die anderen NSX Manager in der Cross-vCenter NSX-Umgebung wird jetzt die Rolle **Eigenständig** angezeigt.

## Zuweisen eines globalen Segment-ID-Pools und einer globalen Multicast-Adresse auf dem primären NSX Manager

Der globale Segment-ID-Pool legt den Bereich fest, der beim Erstellen logischer Netzwerksegmente verwendet wird. Bei Cross-vCenter NSX-Bereitstellungen wird ein eindeutiger globaler Segment-ID-Pool verwendet, um sicherzustellen, dass die VXLAN-Netzwerkbezeichner (VNIs) von globalen logischen Switches über alle sekundären NSX Manager hinweg konsistent sind.

Der globale Segment-ID-Pool wird einmal auf dem primären NSX Manager zugewiesen und dann für alle sekundären NSX Manager synchronisiert. Beachten Sie, dass der Segment-ID-Bereich über alle NSX Manager, die Sie in einer Cross-vCenter NSX-Umgebung nutzen möchten, eindeutig sein muss. In diesem Beispiel wird ein hoher Bereich verwendet, um künftig Skalierbarkeit bereitzustellen.

Beachten Sie bei der Bestimmung der Größe der einzelnen Segment-ID-Pools, dass der Segment-ID-Bereich die Anzahl der logischen Switches steuert, die erstellt werden können. Wählen Sie eine kleine Teilmenge der 16 Millionen potenziellen VNIs aus. Konfigurieren Sie nicht mehr als 10.000 VNIs in einem einzelnen vCenter, da vCenter die Anzahl der dvPortgroups auf 10.000 beschränkt.

Wenn VXLAN in einer anderen NSX-Bereitstellung platziert ist, überlegen Sie, welche VNIs bereits verwendet werden, und vermeiden Sie überlappende VNIs. Nicht überlappende VNIs werden in einer Umgebung mit einem NSX Manager und vCenter automatisch erzwungen. Lokale VNI-Bereiche können nicht überlappend sein. Es ist jedoch wichtig, dass Sie sicherstellen, dass VNIs sich nicht in Ihren getrennten NSX-Bereitstellungen überlappen. Nicht überlappende VNIs sind nützlich für Nachverfolgungszwecke und helfen sicherzustellen, dass Ihre Bereitstellungen für eine Cross-vCenter-Umgebung bereit sind.

Wenn eine Ihrer Transportzonen den Multicast- oder Hybrid-Replikationsmodus verwendet, müssen Sie eine Multicast-Adresse oder einen Bereich von Multicast-Adressen hinzufügen.

Sie müssen sicherstellen, dass die angegebene Multicast-Adresse bzw. der angegebene Adressbereich nicht mit anderen Multicast-Adressen in Konflikt steht, die auf einem NSX Manager in der Cross-vCenter NSX-Umgebung zugewiesen wurden.

Durch einen Bereich von Multicast-Adressen wird der Datenverkehr über das Netzwerk verteilt und die Überlastung einer einzelnen Multicast-Adresse verhindert. Damit wird auch die BUM-Replikation besser eingegrenzt.

Verwenden Sie 239.0.0.0/24 oder 239.128.0.0/24 nicht als Multicast-Adressbereich, da diese Netzwerke für die Steuerung des lokalen Subnetzes verwendet werden, was bedeutet, dass die physischen Switches den gesamten Datenverkehr fluten, der diese Adressen verwendet. Weitere Informationen zu nicht verwendbaren Multicast-Adressen finden Sie unter <https://tools.ietf.org/html/draft-ietf-mboned-ipv4-mcast-unusable-01>.

Wenn VXLAN-Multicast- und Hybrid-Replikationsmodi konfiguriert sind und korrekt funktionieren, wird eine Kopie des Multicast-Datenverkehrs nur an die Hosts geliefert, die IGMP-Beitrittsmeldungen gesandt haben. Andernfalls überflutet das physische Netzwerk den gesamten Multicast-Datenverkehr an alle Hosts in derselben Broadcast-Domäne. Um diese Überflutung zu verhindern, gehen Sie wie folgt vor:

- Vergewissern Sie sich, dass der zugrunde liegende physische Switch mit einer MTU größer oder gleich 1600 konfiguriert ist.
- Vergewissern Sie sich, dass der zugrunde liegende physische Switch korrekt mit IGMP-Snooping und einem IGMP-Abfrager in Netzwerksegmenten, die VTEP-Datenverkehr übertragen, konfiguriert ist.
- Stellen Sie sicher, dass die Transportzone mit dem empfohlenen Multicast-Adressbereich konfiguriert ist. Der empfohlene Multicast-Adressbereich beginnt bei 239.0.1.0/24 und schließt 239.128.0.0/24 aus.

Die vSphere Web Client-Schnittstelle ermöglicht die Konfiguration eines einzelnen Segment-ID-Bereichs und einer einzelnen Multicast-Adresse oder eines Multicast-Adressbereichs. Wenn Sie mehrere Segment-ID-Bereiche oder mehrere Multicast-Adresswerte konfigurieren möchten, steht Ihnen dafür die NSX API zur Verfügung. Weitere Informationen finden Sie unter *Handbuch zu NSX-API*.

## Verfahren

- 1 Melden Sie sich mithilfe des vSphere Web Client bei dem vCenter Server-System an, das bei dem NSX Manager registriert ist, der zum primären NSX Manager werden soll.

Wenn sich die vCenter Server-Systeme in Ihrer Cross-vCenter NSX-Umgebung im erweiterten verknüpften Modus befinden, können Sie auf jeden zugeordneten NSX Manager von jedem verknüpften vCenter Server-System aus durch Auswahl im Dropdown-Menü **NSX Manager** zugreifen.

- 2 Wechseln Sie zu **Home > Networking & Security > Installation** und wählen Sie die Registerkarte **Vorbereitung des logischen Netzwerks (Logical Network Preparation)** aus.
- 3 Stellen Sie sicher, dass der richtige NSX Manager im Dropdown-Menü **NSX Manager** ausgewählt ist.
- 4 Klicken Sie auf **Segment-ID > Bearbeiten (Segment ID > Edit)**.
- 5 Geben Sie einen Bereich für globalen Segment-IDs ein, z. B. 900000-909999.

---

**Vorsicht** Stellen Sie sicher, dass der Bereich sich nicht mit anderen Bereichen überschneidet, die auf NSX Managern in der Cross-vCenter NSX-Umgebung zugewiesen wurden.

---

- 6 (Optional) Wenn eine Ihrer Transportzonen den Multicast- oder Hybrid-Replizierungsmodus verwendet, aktivieren Sie **Globale Multicast-Adressierung aktivieren (Enable Universal multicast addressing)** aus und geben Sie eine universelle Multicast-Adresse oder einen Bereich universeller Multicast-Adressen ein.

---

**Vorsicht** Stellen Sie sicher, dass die angegebene Multicast-Adresse nicht mit anderen Multicast-Adressen in Konflikt gerät, die auf einer beliebigen NSX Manager-Instanz in der Cross-vCenter NSX-Umgebung zugewiesen sind.

---

## Ergebnisse

Später, nachdem Sie globale logische Switches konfiguriert haben, erhält jeder globale logische Switch eine globale Segment-ID aus dem Pool.

## Hinzufügen einer globalen Transportzone auf dem primären NSX Manager

Globale Transportzonen steuern die Hosts, welche ein globaler logischer Switch erreichen kann. Eine globale Transportzone wird vom primären NSX Manager erstellt und für die sekundären NSX Manager repliziert. Globale Transportzonen können sich über ein oder mehrere vSphere-Cluster in der Cross-vCenter NSX-Umgebung erstrecken.

Nach der Erstellung ist eine globale Transportzone auf allen sekundären NSX Managern in der Cross-vCenter NSX-Umgebung verfügbar. Es kann nur eine globale Transportzone geben.


## Voraussetzungen

Konfiguriert nach der Erstellung einer primären NSX Manager-Instanz eine globale Transportzone.

## Verfahren

- 1 Melden Sie sich mithilfe des vSphere Web Client bei dem vCenter Server-System an, das bei dem primären NSX Manager registriert ist.

Wenn sich die vCenter Server-Systeme in Ihrer Cross-vCenter NSX-Umgebung im erweiterten verknüpften Modus befinden, können Sie auf jeden zugeordneten NSX Manager von jedem verknüpften vCenter Server-System aus durch Auswahl im Dropdown-Menü **NSX Manager** zugreifen.

- 2 Wechseln Sie zu **Home > Networking & Security > Installation** und wählen Sie die Registerkarte **Vorbereitung des logischen Netzwerks (Logical Network Preparation)** aus.
- 3 Stellen Sie sicher, dass der richtige NSX Manager im Dropdown-Menü **NSX Manager** ausgewählt ist.
- 4 Klicken Sie auf **Transportzonen (Transport Zones)** und anschließend auf das Symbol **Neue Transportzone (New Transport Zone)** (  ).

**5 Wählen Sie **Dieses Objekt für globale Synchronisierung markieren (Mark this object for universal synchronization)**.**

Diese Transportzone wird mit den sekundären NSX Managern synchronisiert.

**6 Wählen Sie den Steuerungsebenen-Modus aus:**

- **Multicast:** Multicast-IP-Adressen auf dem physischen Netzwerk werden für die Steuerungskomponente verwendet. Dieser Modus wird nur empfohlen, wenn Sie Upgrades von älteren VXLAN-Bereitstellungen aus durchführen wollen. Erfordert PIM/IGMP im physischen Netzwerk.
- **Unicast:** Die Steuerungskomponente wird von einem NSX Controller verwendet. Der komplette Unicast-Datenverkehr verwendet die optimierte Kopfundereplikation. Es sind keine Multicast-IP-Adressen oder bestimmte Netzwerkkonfigurationen erforderlich.
- **Hybrid:** Lagert eine Replizierung des lokalen Datenverkehrs auf das physische Netzwerk aus (L2 Multicast). Erfordert IGMP-Snooping auf dem ersten Hop-Switch und Zugriff auf einen IGMP-Abfrager in jedem VTEP-Subnetz, aber keinen PIM. Der erste Hop-Switch steuert die Datenverkehrsreplizierung für das Subnetz.

**7 Wählen Sie die Cluster aus, die zur Transportzone hinzugefügt werden sollen.**

### Ergebnisse

Die globale Transportzone ist auf allen NSX Managern in der Cross-vCenter NSX-Umgebung verfügbar.

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

### Nächste Schritte

Erstellen Sie als Nächstes einen globalen logischen Switch.

## Hinzufügen eines globalen logischen Switches auf dem primären NSX Manager

In einer Cross-vCenter NSX-Bereitstellung können Sie globale logische Switches erstellen, die alle vCenter überspannen können. Die Transportzone bestimmt, ob der neue Switch ein logischer oder ein globaler logischer Switch ist. Wenn Sie einer globalen Transportzone einen logischen Switch hinzufügen, ist dieser logische Switch global.

Wenn Sie einen logischen Switch erstellen, müssen Sie zusätzlich zur Auswahl einer Transportzone und eines Replizierungsmodus zwei Optionen konfigurieren: die IP-Ermittlung und der MAC-Lernvorgang.

Die IP-Ermittlung minimiert das Fluten durch den ARP-Datenverkehr innerhalb einzelner VXLAN-Segmente – mit anderen Worten zwischen VMs, die mit demselben logischen Switch verbunden sind. Die IP-Ermittlung ist standardmäßig aktiviert.

**Hinweis** Sie können die IP-Ermittlung nicht deaktivieren, wenn Sie einen globalen logischen Switch erstellen. Sie haben aber die Möglichkeit, die IP-Ermittlung nach der Erstellung des globalen logischen Switch über die API zu deaktivieren. Diese Einstellung wird auf jedem NSX Manager gesondert verwaltet. Weitere Informationen finden Sie unter *Handbuch zu NSX-API*.

Der MAC-Lernvorgang erstellt auf jeder vNIC eine VLAN/MAC-Paar-Lerntabelle. Diese Tabelle wird als Teil der dvfilter-Daten gespeichert. Während eines vMotion-Vorgangs speichert dvfilter die Tabelle und stellt sie am neuen Speicherort wieder her. Der Switch gibt anschließend RARPs für alle VLAN/MAC-Einträge in der Tabelle aus. Sie möchten eventuell den MAC-Lernvorgang aktivieren, wenn Ihre virtuellen Maschinen über mehrere MAC-Adressen verfügen oder virtuelle Netzwerkkarten verwenden, die das VLAN-Trunking unterstützen.

## Voraussetzungen

**Tabelle 6-1. Voraussetzungen für die Erstellung von logischen oder globalen logischen Switches.**

Logischer Switch	Globaler logischer Switch
<ul style="list-style-type: none"> <li>■ vSphere Distributed Switches müssen konfiguriert werden.</li> <li>■ NSX Manager muss installiert werden.</li> <li>■ Controller müssen bereitgestellt werden.</li> <li>■ Hostcluster müssen für NSX vorbereitet werden.</li> <li>■ VXLAN muss konfiguriert werden.</li> <li>■ Eine Transportzone muss erstellt werden.</li> <li>■ Ein Segment-ID-Pool muss konfiguriert werden.</li> </ul>	<ul style="list-style-type: none"> <li>■ vSphere Distributed Switches müssen konfiguriert werden.</li> <li>■ NSX Manager muss installiert werden.</li> <li>■ Controller müssen bereitgestellt werden.</li> <li>■ Hostcluster müssen für NSX vorbereitet werden.</li> <li>■ VXLAN muss konfiguriert werden.</li> <li>■ Es muss ein primärer NSX Manager zugewiesen sein.</li> <li>■ Es muss eine globale Transportzone erstellt sein.</li> <li>■ Es muss ein globaler Segment-ID-Pool konfiguriert sein.</li> </ul>

## Verfahren

- 1 Wechseln Sie zu **Home > Networking & Security > Logische Switches (Home > Networking & Security > Logical Switches)**:
- 2 Wählen Sie den primären NSX Manager aus.
- 3 Klicken Sie auf das Symbol **Neuer logischer Switch (New Logical Switch)** (+).
- 4 Geben Sie einen Namen und eine optionale Beschreibung für den logischen Switch ein.

- 5 Klicken Sie im Transportzonen-Bereich auf **Ändern (Change)**, um eine Transportzone auszuwählen. Wählen Sie die globale Transportzone aus, um einen globalen logischen Switch zu erstellen.

**Wichtig** Wenn Sie einen universellen logischen Switch erstellen und als Replizierungsmodus den Hybridmodus auswählen, müssen Sie sicherstellen, dass die verwendete Multicast-Adresse nicht mit anderen Multicast-Adressen in Konflikt steht, die auf einem NSX Manager in der Cross-vCenter NSX-Umgebung zugewiesen wurden.

- 6 (Optional) Überschreiben Sie den Replizierungsmodus, wie von der Transportzone festgelegt.

Sie können auch einen anderen verfügbaren Modus auswählen. Die verfügbaren Modi sind Unicast, Hybrid und Multicast.

Der Fall, in dem Sie möglicherweise den aus der Transportzone übernommenen Steuerungskomponenten-Modus der Replikation für einen einzelnen logischen Switch überschreiben möchten, tritt dann ein, wenn der logische Switch, den Sie erstellen, eindeutig andere Merkmale in Bezug auf den Umfang des übertragenen BUM-Datenverkehrs aufweist. In diesem Fall können Sie eine Transportzone erstellen, die den Unicast-Modus verwendet, und den Hybrid- oder Multicast-Modus für den einzelnen logischen Switch verwenden.

- 7 (Optional) Klicken Sie auf **MAC-Lernvorgang aktivieren (Enable MAC learning)**.

## Beispiel: Logischer Switch und globaler logischer Switch

Die App ist ein logischer Switch, der mit einer Transportzone verbunden ist. Er ist nur auf dem NSX Manager verfügbar, auf dem er erstellt worden ist.

Universal-App ist ein globaler logischer Switch, der mit einer globalen Transportzone verbunden ist. Er ist auf jedem NSX Manager innerhalb der Cross-vCenter NSX-Umgebung verfügbar.

Der logische Switch und der globale logische Switch haben Segment-IDs aus unterschiedlichen Segment-ID-Pools.

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

### Nächste Schritte

Fügen Sie VMs zu einem globalen logischen Switch hinzu.


Erstellen Sie optional einen globalen logischen Router und fügen Sie diesen an die globalen logischen Switches an, um eine Konnektivität zwischen VMs zu ermöglichen, die mit unterschiedlichen globalen logischen Switches verbunden sind.

## Verbinden von virtuellen Maschinen mit einem logischen Switch

Sie können virtuelle Maschinen mit einem logischen oder einem globalen logischen Switch verbinden.



## Verfahren

- 1 Wählen Sie in **Logische Switches (Logical Switches)** den logischen Switch, dem Sie die virtuellen Maschinen hinzufügen möchten.
- 2 Klicken Sie auf das Symbol **Virtuelle Maschine hinzufügen (Add Virtual Machine)** ().
- 3 Wählen Sie die virtuellen Maschinen aus, die Sie zum logischen Switch hinzufügen möchten.
- 4 Wählen Sie die vNICs aus, die Sie verbinden möchten.
- 5 Klicken Sie auf **Weiter (Next)**.
- 6 Überprüfen Sie die von Ihnen ausgewählten vNICs.
- 7 Klicken Sie auf **Beenden (Finish)**.

## Hinzufügen eines globalen logischen (Distributed) Routers auf dem primären NSX Manager

Logische Router-Kernel-Module im Host sind für das Routing zwischen VXLAN-Netzwerken sowie zwischen virtuellen und physischen Netzwerken zuständig. Ein NSX Edge Appliance liefert nach Bedarf eine dynamische Routing-Funktion. Ein globaler logischer Router bietet Ost-West-Routing zwischen globalen logischen Switches.

Beachten Sie beim Bereitstellen eines neuen logischen Routers Folgendes:

- In NSX-Version 6.2 und höher ist es möglich, mit logischen Routern geroutete logische Schnittstellen (LIFs) mit einem VXLAN zu verbinden, das zu einem VLAN überbrückt ist.
- Logische Router- und Bridging-Schnittstellen können nicht mit einer dvPortgroup verbunden werden, wenn die VLAN-ID auf 0 festgelegt ist.
- Eine bestimmte Instanz eines logischen Routers kann nicht mit logischen Switches aus unterschiedlichen Transportzonen verbunden werden. Dadurch soll sichergestellt werden, dass alle logischen Switches und logischen Router-Instanzen aufeinander abgestimmt sind.
- Es kann keine Verbindung zwischen einem logischen Router und VLAN-gestützten Portgruppen hergestellt werden, wenn der logische Router mit logischen Switches verbunden ist, die sich über mehr als einen vSphere Distributed Switch (VDS) erstrecken. Dadurch wird die ordnungsgemäße Ausrichtung logischer Router-Instanzen mit den dvPortgroups logischer Switches über Hosts hinweg sichergestellt.
- Logische Router-Schnittstellen sollten nicht auf zwei unterschiedlichen verteilten Portgruppen (dvPortgroups) mit derselben VLAN-ID erstellt werden, wenn sich die beiden Netzwerke im gleichen vSphere Distributed Switch befinden.

- Logische Router-Schnittstellen sollten nicht auf zwei unterschiedlichen dvPortgroups mit derselben VLAN-ID erstellt werden, wenn sich zwei Netzwerke in unterschiedlichen vSphere Distributed Switches befinden, aber sich die beiden vSphere Distributed Switches dieselben Hosts teilen. In anderen Worten: Logische Router-Schnittstellen können auf zwei unterschiedlichen Netzwerken mit derselben VLAN-ID erstellt werden, wenn sich die beiden dvPortgroups in zwei unterschiedlichen vSphere Distributed Switches befinden, solange sich die vSphere Distributed Switches keinen Host teilen.
- Wenn VXLAN konfiguriert ist, müssen logische Router-Schnittstellen auf dem vSphere Distributed Switch mit verteilten Portgruppen verbunden sein, auf dem VXLAN konfiguriert ist. Verbinden Sie die logischen Router-Schnittstellen nicht mit Portgruppen auf anderen vSphere Distributed Switches.

In der folgenden Liste wird die Unterstützung von Funktionen durch Schnittstellentypen (Uplink und intern) auf dem logischen Router beschrieben:

- Dynamische Routing-Protokolle (BGP und OSPF) werden nur auf Uplink-Schnittstellen unterstützt.
- Firewallregeln gelten nur auf Uplink-Schnittstellen und sind auf Kontrolle und Verwaltung von Datenverkehr beschränkt, der die virtuelle Edge-Appliance zum Ziel hat.
- Weitere Informationen über die DLR-Verwaltungsschnittstelle finden Sie im Knowledgebase-Artikel „Interface Guide: DLR Control VM – NSX“ <http://kb.vmware.com/kb/2122060>.

---

**Wichtig** Wenn Sie die Hochverfügbarkeit (High Availability, HA) auf einem NSX Edge in einer Cross-vCenter NSX-Umgebung aktivieren, müssen sich die aktive und die Standby-NSX Edge-Appliance im selben vCenter Server befinden. Wenn Sie ein Mitglied eines NSX Edge-HA-Paares auf ein anderes vCenter Server-System migrieren, können die beiden HA-Appliances nicht mehr als HA-Paar ausgeführt werden. Dies kann zu einer Unterbrechung des Datenverkehrs führen.

---

### Voraussetzungen

- Ihnen muss die Rolle **Enterprise-Administrator** oder **NSX-Administrator** zugewiesen worden sein.
- Sie müssen selbst dann einen lokalen Segment-ID-Pool erstellen, wenn Sie nicht vorhaben, logische NSX-Switches zu erstellen.
- Stellen Sie vor der Erstellung oder Änderung der Konfiguration eines logischen Routers sicher, dass der Controller-Cluster eingerichtet und verfügbar ist. Ein logischer Router kann ohne die Hilfe von NSX Controllern keine Routing-Informationen an Hosts verteilen. Ein logischer Router verlässt sich auf die Funktion von NSX Controllern, was bei Edge Services Gateways (ESGs) nicht der Fall ist.
- Wenn ein logischer Router mit VLAN-dvPortgroups verbunden werden soll, stellen Sie sicher, dass alle Hypervisor-Hosts mit einer installierten logischen Router-Appliance einander auf UDP-Port 6999 erreichen können. Die Kommunikation über diesen Port ist erforderlich, damit der auf dem VLAN des logischen Routers basierende ARP-Proxy funktioniert.
- Legen Sie fest, wo die logische Router-Appliance bereitgestellt werden soll.
  - Der Zielhost muss Teil derselben Transportzone wie die logischen Switches sein, die mit den Schnittstellen des neuen logischen Routers verbunden sind.

- Vermeiden Sie eine Platzierung auf demselben Host als ein oder mehrere vorgeschaltete ESGs, sofern Sie ESGs in einer ECMP-Einrichtung verwenden. Um dies durchzusetzen, können Sie DRS-Regeln für Anti-Affinität verwenden, wodurch die Auswirkungen eines Hostfehlers auf die Weiterleitung logischer Router reduziert werden. Diese Richtlinie gilt nicht, wenn Sie ein ESG alleine oder im HA-Modus verwenden. Weitere Informationen finden Sie im *Handbuch zum Netzwerkvirtualisierungsdesign für VMware NSX for vSphere* unter <https://communities.vmware.com/docs/DOC-27683>.
- Stellen Sie sicher, dass das Hostcluster, auf dem Sie die logische Router-Appliance installieren möchten, für NSX vorbereitet ist. Informationen dazu erhalten Sie unter „Vorbereiten der Hostcluster für NSX“ in der Dokumentation *Installationshandbuch für NSX*.
- Bestimmen Sie, ob Sie den lokalen Ausgang aktivieren müssen. Mit dem lokalen Ausgang können Sie selektiv Routen an Hosts senden. Wenn Ihre NSX-Bereitstellung mehrere Sites umfasst, ist diese Option hilfreich. Weitere Informationen hierzu finden Sie unter [Cross-vCenter NSX-Topologien](#). Sie können den lokalen Ausgang nach der Erstellung des globalen logischen Routers nicht mehr aktivieren.

## Verfahren

- 1 Navigieren Sie auf vSphere Web Client zu **Start > Netzwerk und Sicherheit > NSX Edges (Home > Networking & Security > NSX Edges)**.
- 2 Wählen Sie den primären NSX Manager aus, um einen globalen logischen Router hinzuzufügen.
- 3 Klicken Sie auf das Symbol **Hinzufügen (Add)** (+).
- 4 Wählen Sie **Globaler logischer (Distributed) Router (Universal Logical (Distributed) Router)** aus.
- 5 (Optional) Aktivieren Sie den lokalen Ausgang.
- 6 Geben Sie einen Namen für das Gerät ein.

Dieser Name wird in Ihrer vCenter-Bestandsliste angezeigt. Der Name muss über alle logischen Router eines einzelnen Mandanten hinweg eindeutig sein.

Sie können optional auch einen Hostnamen eingeben. Dieser Name wird in der Befehlszeilenschnittstelle angezeigt. Wenn Sie keinen Hostnamen angeben, wird die automatisch erstellte Edge-ID in CLI angezeigt.

Sie können optional eine Beschreibung und einen Mandanten eingeben.

- 7 (Optional) Stellen Sie eine Edge-Appliance bereit.

**Edge-Appliance bereitstellen (Deploy Edge Appliance)** ist standardmäßig ausgewählt. Eine Edge-Appliance (auch als logische virtuelle Router-Appliance bezeichnet) ist für das dynamische Routing und die Firewall der logischen Router-Appliance erforderlich, die für logische Router-Pings, SSH-Zugriff und dynamisches Routing gilt.

Sie können die Auswahl der Edge-Appliance-Option aufheben, wenn Sie nur statische Routen benötigen und keine Edge-Appliance bereitstellen möchten. Sie können keine Edge-Appliance zum logischen Router hinzufügen, nachdem der logische Router erstellt wurde.

**8** (Optional) Aktivieren Sie High Availability.

**High Availability aktivieren (Enable High Availability)** ist nicht standardmäßig ausgewählt. Wählen Sie **High Availability aktivieren (Enable High Availability)** aus, um High Availability zu aktivieren und zu konfigurieren. High Availability ist erforderlich, wenn Sie dynamisches Routing anwenden möchten.

**9** Geben Sie ein Kennwort für den logischen Router ein und bestätigen Sie es durch erneute Eingabe.

Das Kennwort muss zwischen 12 und 255 Zeichen umfassen und Folgendes enthalten:

- Mindestens ein Großbuchstabe
- Mindestens ein Kleinbuchstabe
- mindestens eine Zahl
- Mindestens ein Sonderzeichen

**10** (Optional) Aktivieren Sie SSH.

SSH ist standardmäßig deaktiviert. Wenn Sie SSH nicht aktivieren, können Sie auf den logischen Router weiterhin zugreifen, indem Sie die virtuelle Appliance-Konsole öffnen. In diesem Fall führt das Aktivieren von SSH dazu, dass der SSH-Vorgang für die virtuelle Appliance des logischen Routers ausgeführt wird. Sie müssen die Firewallkonfiguration für den logischen Router manuell so anpassen, dass SSH auf die Protokolladresse des logischen Routers zugreifen kann. Die Protokolladresse wird konfiguriert, wenn Sie dynamisches Routing auf dem logischen Router konfigurieren.

**11** (Optional) Aktivieren Sie den FIPS-Modus und legen Sie die Protokollierungsebene fest.

Der FIPS-Modus ist standardmäßig deaktiviert. Aktivieren Sie das Kontrollkästchen **FIPS-Modus aktivieren (Enable FIPS mode)**, um den FIPS-Modus zu aktivieren. Wenn Sie den FIPS-Modus aktivieren, werden für die sichere Kommunikation zum oder vom NSX Edge kryptografische Algorithmen oder Protokolle verwendet, die laut FIPS zulässig sind.

Als Protokollierungsebene ist standardmäßig „Notfall“ eingestellt.

Beispiel:

**Settings**

---

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

User Name: \*

Password: \*

Confirm password: \*

☐ Enable SSH access

☐ Enable FIPS mode

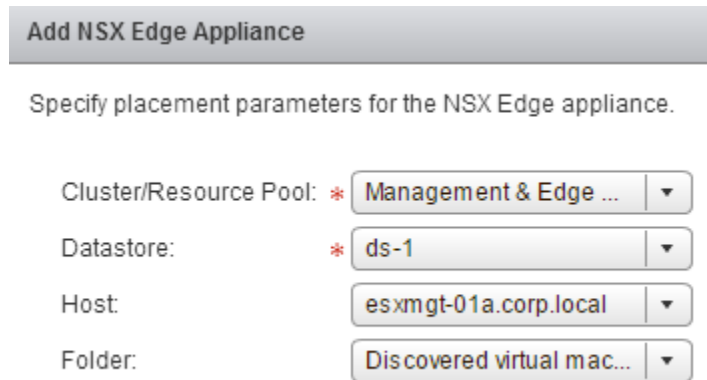
Edge Control Level Logging

*Set the Edge Control Level Logging*

## 12 Konfigurieren Sie die Bereitstellung.

- ◆ Wenn Sie die Option **Edge-Appliance bereitstellen (Deploy Edge Appliance)** nicht ausgewählt haben, wird das Symbol **Hinzufügen (Add)** (  ) ausgeblendet dargestellt. Klicken Sie auf **Weiter (Next)**, um mit der Konfiguration fortzufahren.
- ◆ Wenn Sie **Edge-Appliance bereitstellen (Deploy Edge Appliance)** ausgewählt haben, geben Sie die Einstellungen für die virtuelle Appliance des logischen Routers ein.

Beispiel:



**Add NSX Edge Appliance**

Specify placement parameters for the NSX Edge appliance.

Cluster/Resource Pool: \* Management & Edge ... ▼

Datastore: \* ds-1 ▼

Host: esxmgt-01a.corp.local ▼

Folder: Discovered virtual mac... ▼

### 13 Konfigurieren Sie Schnittstellen. Auf logischen Routern wird nur IPv4-Adressierung unterstützt.

- a Konfigurieren Sie die Verbindung der HA-Schnittstelle und optional eine IP-Adresse.

Wenn Sie die Option **Edge-Appliance bereitstellen (Deploy Edge Appliance)** ausgewählt haben, müssen Sie die HA-Schnittstelle mit einer verteilten Portgruppe oder mit einem logischen Switch verbinden. Wenn Sie diese Schnittstelle nur als HA-Schnittstelle nutzen, verwenden Sie einen logischen Switch. Es wird ein /30-Subnetz aus dem lokalen Bereich 169.254.0.0/16 des Links zugewiesen und für die Bereitstellung einer IP-Adresse für jede der beiden NSX Edge-Appliances verwendet.

Wenn Sie diese Schnittstelle für die Herstellung einer Verbindung mit dem NSX Edge verwenden möchten, können Sie optional eine zusätzliche IP-Adresse und ein zusätzliches Präfix für die HA-Schnittstelle angeben.

---

**Hinweis** Vor NSX 6.2 wurde die HA-Schnittstelle als „Verwaltungsschnittstelle“ bezeichnet. Eine SSH-Verbindung mit der HA-Schnittstelle ist nur möglich, wenn die Verbindung nicht von außerhalb des IP-Subnetzes aufgebaut wird, in dem sich auch die HA-Schnittstelle befindet. Sie können keine statischen Routen konfigurieren, die aus der HA-Schnittstelle herausführen. Dies bedeutet, dass RPF den eingehenden Datenverkehr ablehnt. Sie könnten RPF theoretisch deaktivieren, was jedoch kontraproduktiv für die Hochverfügbarkeit ist. Für den SSH-Zugriff können Sie auch die Protokolladresse des logischen Routers verwenden. Diese wird später beim Konfigurieren des dynamischen Routing konfiguriert.

In NSX 6.2 und höher wird die HA-Schnittstelle eines logischen Routers automatisch von der Route Redistribution ausgeschlossen.

---

- b Konfigurieren Sie Schnittstellen dieses NSX Edge.

In **Schnittstellen dieses NSX Edge konfigurieren (Configure interfaces of this NSX Edge)**: Die internen Schnittstellen dienen Verbindungen zu Switches, die eine Kommunikation zwischen virtuellen Maschinen (manchmal als horizontales Routing bezeichnet) zulässt. Interne Schnittstellen werden auf der logischen virtuellen Router-Appliance als Pseudo-vNICs erstellt. Uplink-Schnittstellen dienen nicht der vertikalen Kommunikation. Die Uplink-Schnittstelle eines logischen Routers kann eine Verbindung zu einem Edge Services Gateway oder einer Drittanbieter-Router-VM herstellen. Sie müssen über mindestens eine Uplink-Schnittstelle verfügen, damit das dynamische Routing funktioniert. Uplink-Schnittstellen werden auf der logischen virtuellen Router-Appliance als vNICs erstellt.

Die Schnittstellen-Konfiguration, die Sie hier eingeben, kann später geändert werden. Sie können nach der Bereitstellung eines logischen Routers Schnittstellen hinzufügen, entfernen und verändern.

Das folgende Beispiel zeigt eine mit der verteilten Verwaltungsportgruppe verbundene HA-Schnittstelle. Das Beispiel zeigt zudem zwei interne Schnittstellen (App und Web) sowie eine Uplink-Schnittstelle (zu ESG).

**New NSX Edge**

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

### Configure interfaces

#### HA interface Configuration

Connected To:  [Change](#) [Remove](#)

+ ✎ ✕

IP Address	Subnet Prefix Length
192.168.110.60*	24

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

#### Configure interfaces of this NSX Edge

+ ✎ ✕

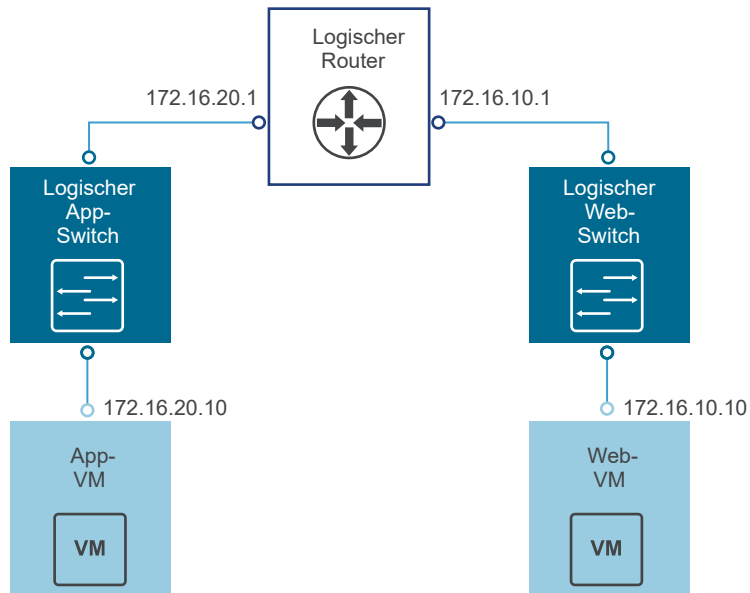
Name	IP Address	Subnet Prefix Length	Connected To
app	172.16.20.1*	24	app
web	172.16.10.1*	24	web
to-ESG	192.168.10.2*	29	transit

Back Next Finish Cancel

- 14 Stellen Sie sicher, dass die Standard-Gateways aller an die logischen Switches angehängten VMs ordnungsgemäß auf die IP-Adressen der logischen Router-Schnittstellen eingestellt sind.

## Ergebnisse

In der folgenden Beispiel-Topologie ist das Standard-Gateway der App-VM 172.16.20.1. Das Standard-Gateway der Web-VM ist 172.16.10.1. Stellen Sie sicher, dass die VMs ihre Standard-Gateways und sich gegenseitig pingen können.



Stellen Sie mit SSH oder über die Konsole eine Verbindung mit dem NSX Manager her und führen Sie die folgenden Befehle aus:

- Führen Sie alle Informationen zur logischen Router-Instanz auf.

```
nsxmgr-l-01a> show logical-router list all
```

Edge-id	Vdr Name	Vdr id	#Lifs
edge-1	default+edge-1	0x00001388	3

- Führen Sie die Hosts auf, die vom Controller-Cluster Routing-Informationen für den logischen Router empfangen haben.

```
nsxmgr-l-01a> show logical-router list dlr edge-1 host
```

ID	HostName
host-25	192.168.210.52
host-26	192.168.210.53
host-24	192.168.110.53

Die Ausgabe umfasst alle Hosts von allen Hostclustern, die als Mitglieder der Transportzone konfiguriert wurden, welche den mit dem angegebenen logischen Router verbundenen logischen Switch besitzt (in diesem Beispiel edge-1).

- Führen Sie die Routing-Tabelleninformationen auf, die vom logischen Router zu den Hosts übertragen werden. Einträge der Routing-Tabelle sollten über sämtliche Hosts hinweg einheitlich sein.

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

VDR default+edge-1 Route Table

Legend: [U: Up], [G: Gateway], [C: Connected], [I: Interface]

Legend: [H: Host], [F: Soft Flush] [!: Reject] [E: ECMP]

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



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

- Führen Sie zusätzliche Informationen über den Router aus der Sicht eines Hosts auf. Diese Ausgabe ist hilfreich, um festzustellen, welcher Controller mit dem Host kommuniziert.

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

```
VDR Instance Information :
```

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

Überprüfen Sie das Controller-IP-Feld in der Ausgabe des `show logical-router host host-25 dlr edge-1 verbose`-Befehls.

Verschlüsseln Sie SSH zu einem Controller und führen Sie die folgenden Befehle aus, um die erlernten Informationen des Controllers zum VNI-, VTEP-, MAC- und ARP-Tabellenstatus anzuzeigen.

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

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

Die Ausgabe für VNI 5000 zeigt null Verbindungen an und führt Controller 192.168.110.201 als Besitzer für VNI 5000 auf. Melden Sie sich bei diesem Controller an, um weitere Informationen über VNI 5000 zu sammeln.

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

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

Die Ausgabe auf 192.168.110.201 zeigt drei Verbindungen an. Überprüfen Sie zusätzliche VNIs.

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

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

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

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

Da 192.168.110.201 alle drei VNI-Verbindungen besitzt, sollten auf dem anderen Controller, 192.168.110.203, erwartungsgemäß null Verbindungen angezeigt werden.

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

- Pingen Sie vor der Überprüfung der MAC- und ARP-Tabellen eine VM durch die andere VM.

Von App-VM zu Web-VM:

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

Überprüfen Sie die MAC-Tabellen.

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

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

Überprüfen Sie die ARP-Tabellen.

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

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

Überprüfen Sie die Informationen zum logischen Router. Jede logische Router-Instanz wird durch einen der Controller-Knoten bedient.

Der instance-Unterbefehl des `show control-cluster logical-routers`-Befehls zeigt eine Liste mit logischen Routern an, die mit diesem Controller verbunden sind.

Der interface-summary-Unterbefehl zeigt die LIFs an, die der Controller vom NSX Manager abgerufen hat. Diese Informationen werden an die Hosts gesendet, die sich in den unter der Transportzone verwalteten Hostclustern befinden.

Der `routes`-Unterbefehl zeigt die Routing-Tabelle an, die von der virtuellen Appliance des logischen Routers (auch als Kontroll-VM bezeichnet) an diesen Controller gesendet wird. Anders als bei ESXi-Hosts enthält diese Routing-Tabelle keine direkt verbundenen Subnetze, da diese Informationen von der LIF-Konfiguration bereitgestellt werden. Route-Informationen auf den ESXi-Hosts umfassen direkt verbundene Subnetze, da es sich in diesem Fall um eine vom Datenpfad des ESXi-Host verwendete Weiterleitungstabelle handelt.

- Listen Sie alle logischen Router auf, die mit diesem Controller verbunden sind.

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

Notieren Sie die LR-ID und verwenden Sie sie im folgenden Befehl.

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

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

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

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

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

VMkernel Routes:

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

- Zeigen Sie die Verbindungen des Controllers mit dem speziellen VNI an.

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

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

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

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

Bei diesen Host-IP-Adressen handelt es sich nicht um VTEPs, sondern um vmk0-Schnittstellen. Verbindungen zwischen ESXi-Hosts und Controllern werden im Verwaltungsnetzwerk erstellt. Bei den Portnummern hier handelt es sich um flüchtige TCP-Ports, die vom ESXi-Host-IP-Stack zugewiesen werden, wenn der Host eine Verbindung zum Controller herstellt.

- Auf dem Host können Sie die mit der Portnummer übereinstimmende Controller-Netzwerkverbindung anzeigen.

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

- Zeigen Sie aktive VNIs auf dem Host an. Beobachten Sie, wie die Ausgabe über die Hosts hinweg unterschiedlich ist. Nicht alle VNIs sind auf allen Hosts aktiv. Ein VNI ist auf einem Host aktiv, wenn der Host eine mit dem logischen Switch verbundene VM aufweist.

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

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

**Hinweis** Führen Sie zur Aktivierung des VXLAN-Namespace in vSphere 6,0 und höher den `/etc/init.d/hostd restart`-Befehl aus.

Für logische Switches im Hybrid- oder Unicast-Modus enthält der `esxcli network vswitch dvs vmware vxlan network list --vds-name <vds-name>`-Befehl folgende Ausgabe:

- Die Steuerungskomponente ist aktiviert.
- Multicast-Proxy und ARP-Proxy sind aufgeführt. Der AARP-Proxy wird aufgelistet, auch wenn Sie die IP-Ermittlung deaktiviert haben.
- Eine gültige Controller-IP-Adresse ist aufgeführt und die Verbindung ist aktiv.
- Wenn ein logischer Router mit dem ESXi-Host verbunden ist, beträgt die Portanzahl mindestens 1, auch wenn auf dem mit dem logischen Switch verbundenen Host keine VMs vorhanden sind. Dieser eine Port ist der vdrPort, bei welchem es sich um einen speziellen dvPort handelt, der mit dem Kernelmodul des logischen Routers auf dem ESXi-Host verbunden ist.

- Pingen Sie zuerst mit einer VM die andere VM auf einem anderen Subnetz an und zeigen Sie anschließend die MAC-Tabelle an. Beachten Sie, dass „Inner MAC“ der Eintrag der VM ist, während sich „Outer MAC“ und „Outer IP“ auf den VTEP beziehen.

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

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

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

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

### Nächste Schritte

Wenn Sie eine NSX Edge-Appliance installieren, aktiviert NSX das automatische Starten/Herunterfahren von virtuellen Maschinen auf dem Host, wenn die vSphere HA auf dem Cluster deaktiviert ist. Wenn die Appliance-VMs später auf andere Hosts im Cluster migriert werden, ist auf den neuen Hosts das automatische Starten/Herunterfahren von virtuellen Maschinen möglicherweise nicht aktiviert. Aus diesem Grund wird von VMware empfohlen, bei der Installation von NSX Edge-Appliances auf Clustern, auf denen die vSphere HA deaktiviert ist, alle Hosts im Cluster zu überprüfen, um sicherzustellen, dass das automatische Starten/Herunterfahren aktiviert ist. Weitere Informationen erhalten Sie unter „Bearbeiten der Einstellungen zum Starten/Herunterfahren virtueller Maschinen“ im Dokument *Verwaltung virtueller vSphere-Maschinen*.

Doppelklicken Sie nach der Bereitstellung des Routers auf die ID des logischen Routers, um weitere Einstellungen zu konfigurieren, wie z. B. Schnittstellen, Routing, Firewall, Bridging und DHCP-Relay.

# Konfigurieren sekundärer NSX Manager

# 7

Nachdem ein primärer Cross-vCenter NSX-Manager konfiguriert wurde, können Sie die sekundären NSX Manager konfigurieren. Sekundäre NSX Manager verwenden denselben universellen Controller-Cluster, der vom primären NSX Manager bereitgestellt wurde. In einer Cross-vCenter NSX-Umgebung können bis zu sieben sekundäre NSX Manager vorhanden sein. Sobald einem NSX Manager die Rolle „Sekundär“ zugewiesen wurde, kann er globale Objekte wie etwa universelle logische Switches verwenden.

Schließen Sie die Konfigurationsaufgaben für jeden sekundären NSX Manager in der Cross-vCenter NSX-Umgebung ab.

## Hinzufügen sekundärer NSX Manager

In einer Cross-vCenter NSX-Umgebung können Sie bis zu sieben sekundäre NSX Manager hinzufügen. Auf dem primären NSX Manager erstellte globale Objekte werden mit den sekundären NSX Manager-Instanzen synchronisiert.

NSX Manager können eine von vier Rollen aufweisen:

- Primär
- Sekundär
- Eigenständig
- Transit

Um die Rolle einer NSX Manager-Instanz anzuzeigen, melden Sie sich bei der mit dem NSX Manager verknüpften vCenter-Instanz an, navigieren Sie zu **Startseite (Home) > Networking & Security > Installation** und wählen Sie dann die Registerkarte **Management** aus. Die Rolle wird in der Spalte „Rolle“ im NSX Manager-Abschnitt angezeigt. Wenn keine Spalte „Rolle“ angezeigt wird, weist der NSX Manager die Rolle „Eigenständig“ auf.

### Voraussetzungen

- Es sollten mindestens zwei NSX Manager vorhanden sein, einer mit der Rolle „Primär“ und einer mit der Rolle „Eigenständig“ oder „Transit“.
- Die Versionen der NSX Manager (der primären NSX Manager-Instanz und der NSX Manager, denen die Rolle „Sekundär“ zugewiesen wird) müssen übereinstimmen.

- Die Knoten-IDs der primären NSX Manager-Instanz und der NSX Manager, denen die Rolle „Sekundär“ zugewiesen wird, müssen vorhanden sein und dürfen nicht übereinstimmen. Mithilfe von OVA-Dateien bereitgestellte NSX Manager-Instanzen besitzen eindeutige Knoten-IDs. Ein von einer Vorlage bereitgestellter NSX Manager (wie beim Konvertieren einer virtuellen Maschine in eine Vorlage) erhält die gleiche Knoten-ID wie der zum Erstellen der Vorlage verwendete ursprüngliche NSX Manager, und diese beiden NSX Manager können nicht in derselben Cross-vCenter NSX-Installation verwendet werden.

**Hinweis** Sie können die NSX Manager-Knoten-ID mit dem folgenden REST API-Aufruf anzeigen:

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

- Jeder NSX Manager muss bei einem eigenen, eindeutigen vCenter Server-System registriert sein.
- Die für VXLAN verwendeten UDP-Ports müssen für alle NSX Manager identisch sein.

**Hinweis** Sie können den VXLAN-Port mithilfe des vSphere Web Client unter **Networking & Security > Installation > Vorbereitung des logischen Netzwerks (Logical Network Preparation)** anzeigen und ändern. Weitere Informationen erhalten Sie unter „Ändern des VXLAN-Ports“ im *Administratorhandbuch für NSX*.

- Beim Zuweisen der Rolle „Sekundär“ zu einem NSX Manager darf das mit diesem NSX Manager verknüpfte vCenter Server-System keine bereitgestellten NSX-Controller enthalten.
- Der Segment-ID-Pool der NSX Manager-Instanz, der die Rolle „Sekundär“ zugewiesen wird, darf sich nicht mit den Segment-ID-Pools der primären NSX Manager-Instanz oder dem Segment-ID-Pool einer anderen sekundären NSX Manager-Instanz überlappen.
- Der NSX Manager, dem die Rolle „Sekundär“ zugewiesen wird, muss die Rolle „Eigenständig“ oder „Transit“ aufweisen.
- Damit die globale Synchronisierung ordnungsgemäß funktioniert, müssen sowohl primäre wie sekundäre NSX Manager über die gleiche TLS-Version verfügen.

Stellen Sie sicher, dass der sekundäre NSX Manager für die Verwendung von mindestens einer der TLS-Versionen konfiguriert ist, die auf dem primären NSX Manager konfiguriert sind. Siehe „Ändern des FIPS-Modus und der TLS-Einstellungen für NSX Manager“ im Dokument *Administratorhandbuch für NSX*.

## Verfahren

- 1 Melden Sie sich bei der mit dem primären NSX Manager verknüpften vCenter-Instanz an.
- 2 Navigieren Sie zu **Startseite (Home) > Networking & Security > Installation** und wählen Sie die Registerkarte **Management** aus.
- 3 Wählen Sie den primären NSX Manager aus. Wählen Sie dann **Aktionen (Actions) > Sekundären NSX Manager hinzufügen (Add Secondary NSX Manager)** aus.

- 4 Geben Sie die IP-Adresse, den Benutzernamen und das Kennwort der sekundären NSX Manager-Instanz ein.





---

**Hinweis** Sie sollten den Hostnamen zum Konfigurieren des sekundären NSX Managers verwenden, wenn der primäre NSX Manager eine IPv6-Adresse verwendet.

---

- 5 Klicken Sie auf **OK**.
- 6 Überprüfen Sie, ob der Fingerabdruck des Zertifikats mit dem des sekundären NSX Managers übereinstimmt.
- 7 Nach der erfolgreichen Registrierung ändert sich die Rolle von Eigenständig (Standalone) zu Sekundär.

Wenn sich Ihre vCenter Server-Systeme im erweiterten verknüpften Modus befinden, können Sie die Rollen aller diesen vCenter Server-Systemen zugeordneten NSX Manager über die Registerkarte **Startseite (Home) > Networking & Security > Installation** anzeigen.

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

Wenn Ihre Umgebung den erweiterten verknüpften Modus nicht einsetzt, melden Sie sich bei der vCenter-Instanz an, die mit dem sekundären NSX Manager verknüpft ist, um die Rolle der NSX Manager-Instanz anzuzeigen.

Wenn die Änderung der NSX Manager-Rolle nicht angezeigt wird, melden Sie sich beim vSphere Web Client ab und dann wieder an.

---

**Hinweis** Anfangs wird der Controller-Status eventuell als „Getrennt“ angezeigt. Warten Sie einige Sekunden und aktualisieren Sie den vSphere Web Client dann. Der Status sollte sich zu „Normal“ ändern.

---

## Vorbereiten von Hosts auf einer sekundären NSX Manager-Instanz

Während der Hostvorbereitung installiert der sekundäre NSX Manager NSX-Kernel-Module auf ESXi-Hosts, die Mitglieder von vCenter-Clustern sind und generiert das Fabric der Steuerungskomponente und der Verwaltungsebene für NSX. In VIB-Dateien gepackte NSX-Kernel-Module werden im Hypervisor-Kernel ausgeführt und stellen Dienste wie Distributed Routing, verteilte Firewall und VXLAN-Bridging-Funktionen bereit.

### Voraussetzungen


Details zu den Voraussetzungen für die Hostvorbereitung finden Sie unter [Vorbereiten von Hosts auf dem primären NSX Manager](#)



## Verfahren

- 1 Sie können sich mithilfe des vSphere Web Client bei dem vCenter Server-System anmelden, das bei dem NSX Manager registriert ist, der geändert werden soll.

Wenn sich die vCenter Server-Systeme in Ihrer Cross-vCenter NSX-Umgebung im erweiterten verknüpften Modus befinden, können Sie auf jeden zugeordneten NSX Manager von jedem verknüpften vCenter Server-System aus durch Auswahl im Dropdown-Menü **NSX Manager** zugreifen.

- 2 Wechseln Sie zu **Home > Networking & Security > Installation** und wählen Sie die Registerkarte **Hostvorbereitung (Host Preparation)** aus.
- 3 Stellen Sie sicher, dass der richtige NSX Manager im Dropdown-Menü **NSX Manager** ausgewählt ist.
- 4 Klicken Sie bei allen Clustern, die ein logisches NSX-Switching, NSX-Routing und NSX-Firewalls erfordern, auf **Aktionen (Actions)** (  ) und dann auf **Installieren (Install)**.

Ein Computing-Cluster ist ein Cluster mit Anwendungs-VMs (Web, Datenbank usw.). Wenn ein Computing-Cluster über NSX-Switching, NSX-Routing oder NSX-Firewalls verfügen soll, klicken Sie für den Computing-Cluster auf **Installieren (Install)**.

In einem (wie im Beispiel dargestellten) gemeinsam genutzten „Management- und Edge-Cluster“ teilen sich NSX Manager- und NSX Controller-VMs einen Cluster mit Edge-Geräten wie zum Beispiel Distributed Logical Routers (DLRs) und Edge Services Gateways (ESGs). In diesem Fall ist es obligatorisch, für den gemeinsam genutzten Cluster auf **Installieren (Install)** zu klicken.

Verfügen Management und Edge hingegen – wie in einer Produktionsumgebung empfohlen – jeweils über einen eigenen, nicht gemeinsam genutzten Cluster, klicken Sie im Falle des Edge-Clusters auf **Installieren (Install)**, im Falle des Management-Clusters jedoch nicht.

---

**Hinweis** Führen Sie während der Installation keine Upgrades aus, stellen Sie keine Dienste oder Komponenten bereit und deinstallieren Sie keine Dienste oder Komponenten.

---

- 5 Überwachen Sie die Installation, bis in der Spalte **Installationsstatus (Installation Status)** ein grünes Häkchen angezeigt wird.

Wenn in der Spalte **Installationsstatus (Installation Status)** eine rotes Warnsymbol und **Nicht bereit (Not Ready)** angezeigt wird, klicken Sie auf **Auflösen (Resolve)**. Durch Klicken auf **Auflösen (Resolve)** könnte ein Neustart des Hosts ausgelöst werden. Wenn die Installation immer noch nicht erfolgreich ist, klicken Sie auf das Warnsymbol. Alle Fehler werden angezeigt. Führen Sie die nötige(n) Aktion(en) aus und klicken Sie wieder auf **Auflösen (Resolve)**.

Wenn die Installation abgeschlossen ist, werden in der Spalte **Installationsstatus (Installation Status)** die Version und das Build des installierten NSX angezeigt. Die Spalte **Firewall** enthält die Anzeige **Aktiviert (Enabled)**. Beide Spalten zeigen ein grünes Häkchen an. Wenn in der Spalte **Installationsstatus (Installation Status)** „Auflösen“ angezeigt wird, klicken Sie auf „Auflösen“ und aktualisieren Sie danach Ihr Browser-Fenster.

## Ergebnisse

Bei allen Hosts innerhalb des vorbereiteten Clusters werden VIBs installiert und registriert: Der installierten VIBs sind unterschiedlich, je nachdem, die welche Versionen von NSX und ESXi installiert sind.

| ESXi-Version   | NSX-Version       | Installierte VIBs                                                                 |
|----------------|-------------------|-----------------------------------------------------------------------------------|
| 5.5            | Alle 6.3.x        | <ul style="list-style-type: none"> <li>■ esx-vsip</li> <li>■ esx-vxlan</li> </ul> |
| 6.0 oder höher | 6.3.2 oder früher | <ul style="list-style-type: none"> <li>■ esx-vsip</li> <li>■ esx-vxlan</li> </ul> |
| 6.0 oder höher | 6.3.3 oder höher  | <ul style="list-style-type: none"> <li>■ esx-nsxv</li> </ul>                      |

Um zu überprüfen, SSH auf jeden host und führen Sie den Befehl `esxcli software vib list` und die Kontrollkästchen für die relevanten VIBs. Neben den VIBs wird durch diesen Befehl auch die Version der installierten VIBs angezeigt.

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

Wenn Sie einem vorbereiteten Cluster einen Host hinzufügen, werden die NSX VIBs automatisch auf dem Host installiert.

Wenn Sie einen Host auf einen nicht vorbereiteten Cluster verschieben, werden die NSX VIBs automatisch vom Host deinstalliert.

## Konfigurieren des VXLAN vom sekundären NSX Manager aus

Das VXLAN-Netzwerk wird für logisches Schicht-2-Switching über Hosts hinweg verwendet, die mehrere zugrunde liegende Schicht-3-Domänen umfassen können. Sie konfigurieren VXLAN pro Cluster, wobei Sie jeden Cluster, der an NSX teilnehmen soll, einem vSphere Distributed Switch (VDS) zuordnen. Wenn Sie einem verteilten Switch einen Cluster zuordnen, wird jeder Host in diesem Cluster für logische Switches aktiviert. Die hier gewählten Einstellungen werden beim Erstellen der VMkernel-Schnittstelle verwendet.

### Voraussetzungen

Weitere Informationen zu den Voraussetzungen finden Sie unter [Konfigurieren des VXLAN vom primären NSX Manager aus](#).

## Verfahren

- 1 Sie können sich mithilfe des vSphere Web Client bei dem vCenter Server-System anmelden, das bei dem NSX Manager registriert ist, der geändert werden soll.

Wenn sich die vCenter Server-Systeme in Ihrer Cross-vCenter NSX-Umgebung im erweiterten verknüpften Modus befinden, können Sie auf jeden zugeordneten NSX Manager von jedem verknüpften vCenter Server-System aus durch Auswahl im Dropdown-Menü **NSX Manager** zugreifen.

- 2 Wechseln Sie zu **Home > Networking & Security > Installation** und wählen Sie die Registerkarte **Hostvorbereitung (Host Preparation)** aus.
- 3 Stellen Sie sicher, dass der richtige NSX Manager im Dropdown-Menü **NSX Manager** ausgewählt ist.
- 4 Klicken Sie auf **Nicht konfiguriert (Not Configured)** in der Spalte **VXLAN**.
- 5 Richten Sie logische Netzwerke ein.

Dazu müssen Sie einen vSphere Distributed Switch, eine VLAN-ID, eine MTU-Größe, einen IP-Adressmechanismus und eine NIC-Gruppierungsrichtlinie auswählen.

Diese Beispiele zeigen eine Konfiguration für einen Verwaltungs-Cluster mit einem IP-Pool-Adressbereich von 182.168.150.1-192.168.150.100, gesichert von VLAN 150, und einer Failover-NIC-Gruppierungsrichtlinie.

**Configure VXLAN networking**

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

Switch: \* Mgmt\_VDS

VLAN: \* 150

MTU: \* 1600

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

IP Pool: New IP Pool...

VMKNic Teaming Policy: \* Fail Over

VTEP: \* 1

OK Cancel

Die Anzahl der VTEPs ist in der Benutzeroberfläche nicht bearbeitbar. Die VTEP-Anzahl ist so festgelegt, dass sie der Anzahl der dvUplinks auf dem vSphere Distributed Switch entspricht, die vorbereitet werden.

**Add Static IP Pool**

Name: \* mgmt-edge-ip-pool

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

Prefix Length: \* 24

Primary DNS: 192.168.110.10

Secondary DNS:

DNS Suffix: corp.local

Static IP Pool: \* 192.168.150.1-192.168.150.100

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

OK Cancel

Für Rechen-Cluster können Sie andere IP-Adresseinstellungen verwenden (z. B. 192.168.250.0/24 mit VLAN 250). Das hängt vom Design des physischen Netzwerks ab und wahrscheinlich ist es in kleinen Bereitstellungen nicht erforderlich.

## Zuweisen eines Segment-ID-Pools und einer Multicast-Adresse für einen sekundären NSX Manager

Der sekundäre NSX Manager zeigt den globalen Segment-ID-Pool an, der mit dem primären NSX Manager synchronisiert wird. Außerdem können Sie einen Segment-ID-Pool erstellen, der für den sekundären NSX Manager lokal ist und der zum Erstellen logischer Switches verwendet wird, die für diesen NSX Manager lokal sind. Wenn Sie nur globale logische Switches erstellen, müssen Sie keinen lokalen Segment-ID-Pool für den sekundären NSX Manager hinzufügen.

### Voraussetzungen

Details zu den Voraussetzungen sowie Anleitungen für die Planung von Segment-ID-Pools und Multicast-Adressen finden Sie unter [Zuweisen eines Segment-ID-Pools und einer Multicast-Adresse auf dem primären NSX Manager](#)

### Verfahren

- 1 Sie können sich mithilfe des vSphere Web Client bei dem vCenter Server-System anmelden, das bei dem NSX Manager registriert ist, der geändert werden soll.

Wenn sich die vCenter Server-Systeme in Ihrer Cross-vCenter NSX-Umgebung im erweiterten verknüpften Modus befinden, können Sie auf jeden zugeordneten NSX Manager von jedem verknüpften vCenter Server-System aus durch Auswahl im Dropdown-Menü **NSX Manager** zugreifen.

- 2 Wechseln Sie zu **Home > Networking & Security > Installation > Vorbereitung des logischen Netzwerks (Logical Network Preparation)** und wählen Sie die Registerkarte **Segment-ID (Segment ID)** aus.
- 3 Stellen Sie sicher, dass der richtige NSX Manager im Dropdown-Menü **NSX Manager** ausgewählt ist.
- 4 Geben Sie einen Bereich für lokale Segment-IDs ein, z. B. **20000–29999**.

---

**Vorsicht** Die angegebenen Bereiche für lokale und globale Segment-IDs dürfen sich nicht überschneiden.

---

- 5 (Optional) Wenn eine Ihrer Transportzonen den Multicast- oder Hybrid-Replizierungsmodus verwendet, wählen Sie **Multicast-Adressierung aktivieren (Enable multicast addressing)** aus und geben Sie eine Multicast-Adresse oder einen Bereich von Multicast-Adressen ein.

---

**Vorsicht** Stellen Sie sicher, dass die angegebene Multicast-Adresse nicht mit anderen Multicast-Adressen in Konflikt gerät, die auf einer beliebigen NSX Manager-Instanz in der Cross-vCenter NSX-Umgebung zugewiesen sind.

---

## Ergebnisse

Der sekundäre NSX Manager verfügt jetzt sowohl über importierte globale Segment-IDs, die vom primären NSX Manager bereitgestellt wurden, als auch über lokale Segment-IDs.

## Hinzufügen von Clustern zur globalen Transportzone

Sie müssen die Cluster, die den sekundären NSX Managern zugeordnet sind, der globalen Transportzone hinzufügen. Dann können Sie die VMs auf diesen Clustern mit den globalen logischen Switches verbinden.

### Verfahren

- 1 Sie können sich mithilfe des vSphere Web Client bei dem vCenter Server-System anmelden, das bei dem NSX Manager registriert ist, der geändert werden soll.

Wenn sich die vCenter Server-Systeme in Ihrer Cross-vCenter NSX-Umgebung im erweiterten verknüpften Modus befinden, können Sie auf jeden zugeordneten NSX Manager von jedem verknüpften vCenter Server-System aus durch Auswahl im Dropdown-Menü **NSX Manager** zugreifen.

- 2 Wechseln Sie zu **Home > Networking & Security > Installation > Vorbereitung des logischen Netzwerks (Logical Network Preparation)** und wählen Sie die Registerkarte **Transportzonen (Transport Zones)** aus.
- 3 Stellen Sie sicher, dass der richtige NSX Manager im Dropdown-Menü **NSX Manager** ausgewählt ist.
- 4 Wählen Sie die globale Transportzone aus und klicken Sie auf **Aktionen (Actions)** (⚙️) > **Cluster verbinden (Connect Clusters)**. Wählen Sie die Cluster aus, die zur globalen Transportzone hinzugefügt werden sollen, und klicken Sie auf „OK“.

# Vorgehensweise nach der Konfiguration von primären und sekundären NSX Managern

## 8

Sie haben jetzt einen primären NSX Manager und mindestens einen sekundären NSX Manager konfiguriert. Zusätzlich zu globalen Objekten vom primären NSX Manager können Objekte erstellt werden, die nur für diese spezifische vCenter NSX-Umgebung gelten, z. B. logische Switches, logische (verteilte) Router und Edge Services Gateways. Diese können auf den primären oder auf den sekundären NSX Manager-Instanzen erstellt werden. Diese existieren nur innerhalb der vCenter NSX-Umgebung, in der sie erstellt wurden. Auf den anderen NSX Managern in der Cross-vCenter-NSX-Umgebung sind sie nicht sichtbar. Außerdem können Sie Hosts zu Clustern hinzufügen oder daraus entfernen.

Details zu weiteren Verwaltungsaufgaben, die Sie möglicherweise durchführen möchten, finden Sie im *Administratorhandbuch für NSX*.

# Deinstallieren von NSX-Komponenten

# 9

In diesem Kapitel werden die erforderlichen Schritte zur Deinstallation von NSX-Komponenten aus Ihrer vCenter-Bestandsliste beschrieben.

---

**Hinweis** Entfernen Sie keine Appliances (wie etwa Controller oder Edges), die von NSX direkt von vCenter bereitgestellt wurden. Verwenden Sie zum Verwalten und Entfernen von NSX-Appliances immer die Registerkarte **Networking & Security** von vSphere Web Client.

---

Dieses Kapitel enthält die folgenden Themen:

- [Entfernen eines Hosts aus einem für NSX vorbereiteten Cluster](#)
- [Deinstallieren eines NSX Edge Services Gateways oder eines Distributed Logical Routers](#)
- [Deinstallieren eines logischen Switch](#)
- [Deinstallieren von NSX von Hostclustern](#)
- [Sicheres Entfernen einer NSX-Installation](#)

## Entfernen eines Hosts aus einem für NSX vorbereiteten Cluster

In diesem Abschnitt wird das Entfernen eines Hosts aus einem für die Netzwerkvirtualisierung vorbereiteten Cluster beschrieben. Dieses bietet sich beispielsweise dann an, wenn der betreffende Host nicht Teil von NSX sein soll.

---

**Wichtig** Auf einem Host mit NSX 6.3.0 oder höher und ESXi 6.0 oder höher müssen Sie zum Deinstallieren von VIBs den Host nicht neu starten. In früheren Versionen von NSX und ESXi ist für den Abschluss der VIB-Deinstallation ein Neustart erforderlich.

---

### Verfahren

- 1 Versetzen Sie den Host in den Wartungsmodus und warten Sie, bis DRS diesen entfernt, oder verschieben Sie die laufenden VMs per vMotion manuell vom Host.
- 2 Entfernen Sie den Host aus dem vorbereiteten Cluster, indem Sie ihn entweder in einen nicht vorbereiteten Cluster verschieben oder ihn zu einem eigenständigen, keinem Cluster angehörenden Host umwandeln.

NSX deinstalliert die Netzwerkvirtualisierungskomponenten und die Dienst-VMs auf dem Host.

- 3 Wenn auf dem Host NSX 6.2.x oder früher oder ESXi 5.5 installiert ist, starten Sie den Host neu.
- 4 Stellen Sie sicher, dass die VIB-Deinstallation abgeschlossen ist.
  - a Überprüfen Sie den Bereich „Aktuelle Aufgaben“ im vSphere Web Client.
  - b Überprüfen Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)**, ob für den Installationsstatus des Clusters, von dem der Host entfernt wurde, ein grünes Häkchen angezeigt wird.

Wenn der Installationsstatus `Wird installiert` lautet, läuft die Deinstallation noch.

- 5 Sobald die Deinstallation abgeschlossen ist, beenden Sie den Wartungsmodus für den Host.

### Ergebnisse

Die NSX-VIBs werden vom Host entfernt. Verbinden Sie sich zur Überprüfung per SSH mit dem Host und führen Sie den Befehl `esxcli software vib list | grep esx` aus. Stellen Sie sicher, dass die folgenden VIBs auf dem Host nicht vorhanden sind:

- `esx-vsip`
- `esx-vxlan`

Wenn sich die VIBs weiterhin auf dem Host befinden, können Sie die Protokolle anzeigen, um herauszufinden, warum die automatische Entfernung der VIBs fehlgeschlagen ist.

Sie können die VIBs manuell entfernen, indem Sie die folgenden Befehle ausführen:

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

## Deinstallieren eines NSX Edge Services Gateways oder eines Distributed Logical Routers

Sie können NSX Edge mithilfe von vSphere Web Client deinstallieren.

### Voraussetzungen

Ihnen muss die Rolle „Enterprise-Administrator“ oder „NSX-Administrator“ zugewiesen worden sein.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **NSX Edges**.
- 3 Wählen Sie ein NSX Edge aus und klicken Sie auf das Symbol **Löschen (Delete)** (✖).




## Deinstallieren eines logischen Switch

Sie müssen vor der Deinstallation eines logischen Switch alle virtuellen Maschinen daraus entfernen. In einer Cross-vCenter NSX-Umgebung müssen Sie alle virtuellen Maschinen aus dem globalen logischen Switch auf allen NSX Managern entfernen.

### Voraussetzungen

Ihnen muss die Rolle „Enterprise-Administrator“ oder „NSX-Administrator“ zugewiesen worden sein.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Home > Netzwerk und Sicherheit > Logische Switches (Home > Networking & Security > Logical Switches)**.
- 2 Entfernen Sie alle virtuellen Maschinen aus einem logischen Switch.
  - a Wählen Sie einen logischen Switch aus und klicken Sie auf das Symbol „Virtuelle Maschine entfernen“ ().
  - b Verschieben Sie alle virtuellen Maschinen von „Verfügbare Objekte“ nach „Ausgewählte Objekte“ und klicken Sie auf **OK**.

Wenn Sie einen globalen logischen Switch deinstallieren, sind an diesen eventuell virtuelle Maschinen auf den primären und sekundären NSX Managern angefügt. Wiederholen Sie diese Schritte für alle NSX Manager in Ihrer Cross-vCenter NSX-Umgebung, um alle virtuellen Maschinen aus dem globalen logischen Switch zu entfernen.

- 3 Klicken Sie bei ausgewähltem logischem Switch auf das Symbol **Löschen (Delete)** (.

Wenn Sie einen globalen logischen Switch deinstallieren, müssen Sie diesen vom primären NSX Manager löschen.

## Deinstallieren von NSX von Hostclustern

Sie können NSX von allen Hosts in einem Cluster deinstallieren.

Weitere Informationen zum Entfernen von NSX von einzelnen Hosts (statt aus dem gesamten Cluster) finden Sie hier: [Entfernen eines Hosts aus einem für NSX vorbereiteten Cluster](#)

### Voraussetzungen

- Trennen Sie VMs auf dem Cluster von den logischen Switches.

### Verfahren

- 1 Entfernen Sie den Cluster aus seiner Transportzone.

Gehen Sie zu **Vorbereitung des logischen Netzwerks > Transportzonen (Logical Network Preparation > Transport Zones)** und trennen Sie den Cluster von der Transportzone.

Wenn der Cluster abgeblendet ist und Sie ihn nicht von der Transportzone trennen können, besteht die Ursache möglicherweise darin, dass ein Host im Cluster getrennt oder nicht eingeschaltet ist oder dass der Cluster eine oder mehrere virtuelle Maschinen oder Appliances enthalten kann, die mit der Transportzone verbunden sind. Beispiel: Wenn sich der Host in einem Management-Cluster befindet und auf ihm NSX-Controller installiert sind, entfernen oder verschieben Sie diese Controller zunächst.

- 2 Deinstallieren Sie die NSX-VIBs. Navigieren Sie im vCenter Web Client zu **Networking & Security > Installation > Hostvorbereitung (Networking & Security > Installation > Host Preparation)**.

Wählen Sie ein Cluster aus, klicken Sie auf **Aktionen (Actions)** (  ), und wählen Sie **Deinstallieren (Uninstall)** aus.

Für den Installationsstatus wird **Nicht bereit (Not Ready)** angezeigt. Wenn Sie auf **Nicht bereit (Not Ready)** klicken, wird in dem Dialogfeld die folgende Meldung angezeigt: Host muss in den Wartungsmodus versetzt werden, um die Agent-VIB-Installation abzuschließen.

- 3 Wählen Sie das Cluster aus, und klicken Sie auf die Aktion **Auflösen (Resolve)**, um die Deinstallation abzuschließen.
  - Bei einem Host mit NSX 6.2.x oder früher oder mit ESXi Version 5.5 ist für den Abschluss der Deinstallation ein Neustart erforderlich. Wenn der Cluster DRS-fähig ist, versucht die DRS, die Hosts auf kontrollierte Weise neu zu speichern, sodass die VMs weiterhin ausgeführt werden können. Wenn der DRS aus irgendeinem Grund fehlschlägt, wird die Aktion **Auflösen (Resolve)** gestoppt. In diesem Fall müssen Sie die VMs ggf. manuell verschieben und dann die Maßnahme **Auflösen (Resolve)** ausprobieren. Alternativ können Sie die Hosts manuell neu starten.
  - Hosts mit NSX 6.3.0 oder höher und ESXi 6.0 oder höher müssen für den Abschluss der Deinstallation in den Wartungsmodus versetzt werden. Wenn der Cluster DRS-fähig ist, versucht der DRS, die Hosts auf kontrollierte Weise in den Wartungsmodus zu versetzen, sodass die VMs weiterhin ausgeführt werden können. Wenn der DRS aus irgendeinem Grund fehlschlägt, wird die Aktion **Auflösen (Resolve)** gestoppt. In diesem Fall müssen Sie die virtuellen Maschinen ggf. manuell verschieben und dann die Aktion **Auflösen (Resolve)** erneut probieren. Alternativ können Sie die Hosts manuell in den Wartungsmodus setzen.

---

**Wichtig** Wenn Sie Hosts manuell in den Wartungsmodus versetzen, müssen Sie sicherstellen, dass die Host-VIB-Deinstallation abgeschlossen wurde, bevor Sie den Wartungsmodus für den Host beenden.

- a Überprüfen Sie den Bereich „Aktuelle Aufgaben“ im vSphere Web Client.
- b Überprüfen Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)**, ob für den Installationsstatus des Clusters, von dem der Host entfernt wurde, ein grünes Häkchen angezeigt wird.

Wenn der Installationsstatus **Wird installiert** lautet, läuft die Deinstallation noch.

---

## Sicheres Entfernen einer NSX-Installation

Eine vollständige Deinstallation von NSX entfernt die Host-VIBs, den NSX Manager, die Controller, die gesamte VXLAN-Konfiguration, die logischen Switches, logische Router, die NSX-Firewall und das vCenter NSX-Plug-In. Führen Sie die Schritte für alle Hosts im Cluster aus. VMware empfiehlt die Deinstallation der Netzwerkvirtualisierungskomponenten von einem Cluster, bevor das NSX-Plug-In von vCenter Server entfernt wird.

---

**Hinweis** Entfernen Sie keine Appliances, die von NSX direkt in vCenter erstellt wurden, z. B. NSX Edge-Appliances. Verwenden Sie zum Verwalten und Entfernen dieser Appliances immer die Registerkarte „Networking & Security“ von vSphere Web Client.

---

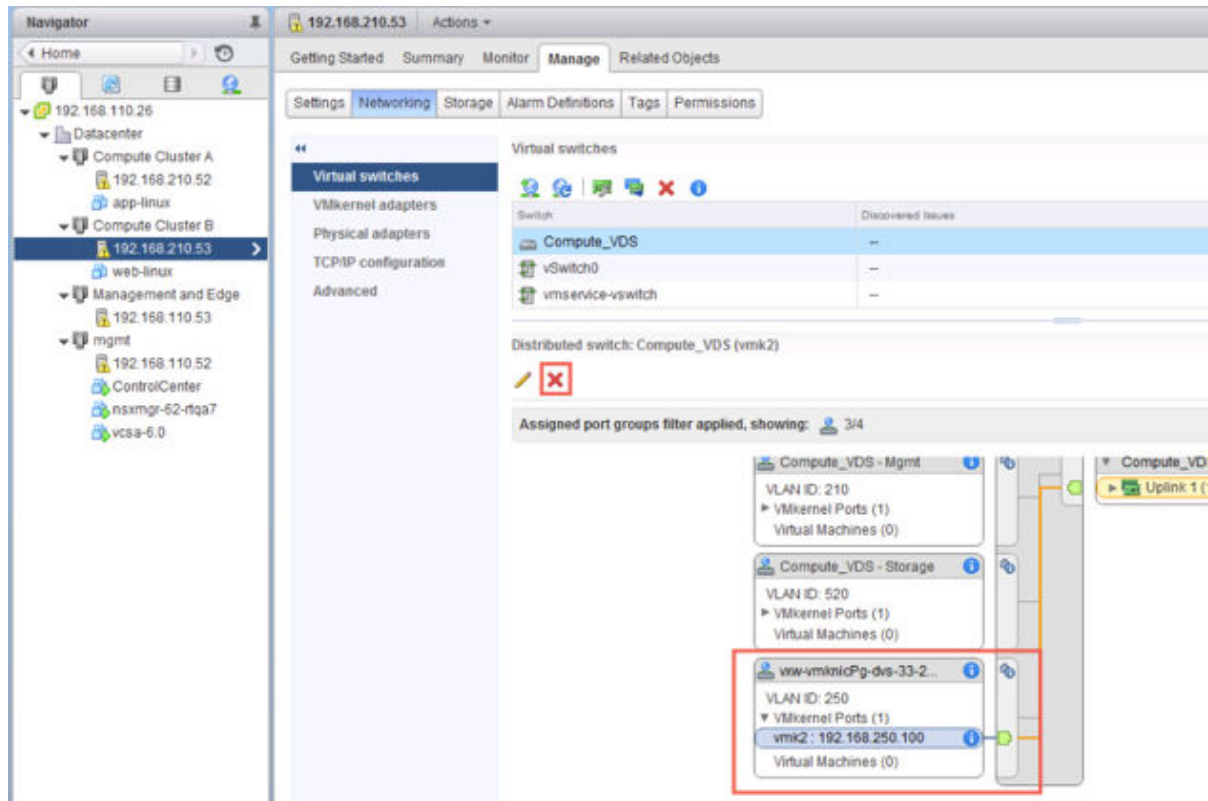
### Voraussetzungen

- Ihnen muss die Rolle „Enterprise-Administrator“ oder „NSX-Administrator“ zugewiesen worden sein.
- Entfernen Sie jegliche registrierten Partnerlösungen sowie Endpoint-Dienste, bevor Sie die Hostvorbereitung umkehren, sodass die Dienst-VMs im Cluster ordnungsgemäß entfernt werden.
- Löschen Sie alle NSX Edges. Weitere Informationen dazu finden Sie unter [Deinstallieren eines NSX Edge Services Gateways oder eines Distributed Logical Routers](#).
- Lösen Sie die Verbindung der virtuellen Maschinen zu den logischen Switches in der Transportzone und löschen Sie die logischen Switches. Weitere Informationen dazu finden Sie unter [Deinstallieren eines logischen Switch](#).
- Deinstallieren von NSX von Host-Clustern. Weitere Informationen dazu finden Sie unter [Deinstallieren von NSX von Hostclustern](#).

### Verfahren

- 1 Löschen Sie die Transportzone.
- 2 Löschen Sie die NSX Manager-Appliance und alle NSX Controller-Appliance-VMs von der Festplatte.
- 3 Entfernen Sie jeglichen VTEP vmkernel-Benutzeroberflächen.

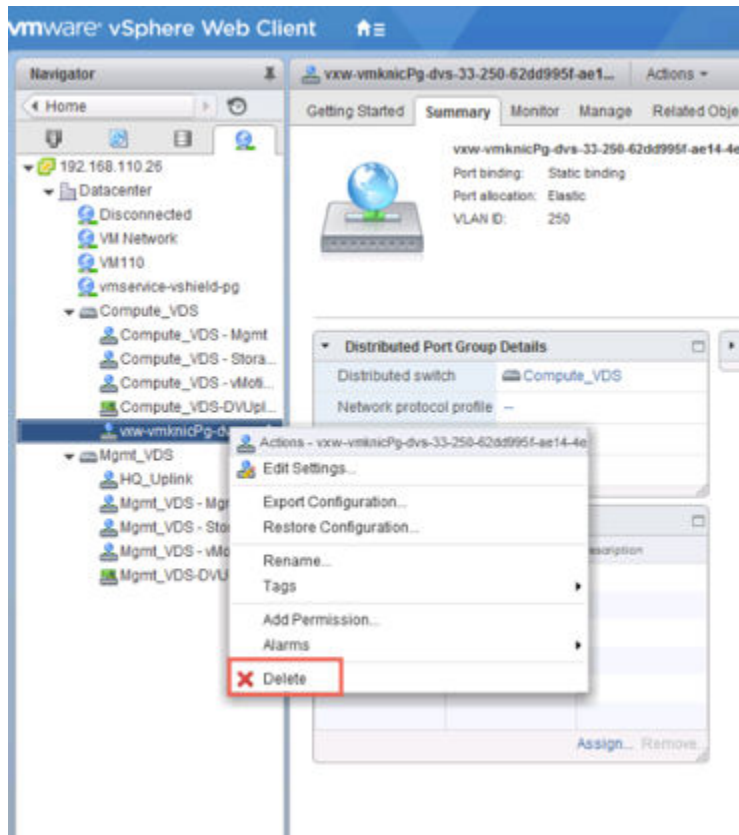
Beispiel:



Generell sind die VTEP vmkernel-Schnittstellen bereits aufgrund von früheren Deinstallationen gelöscht.

- 4 Entfernen Sie alle restlichen, für VTEPs verwendeten dvPortgroups.

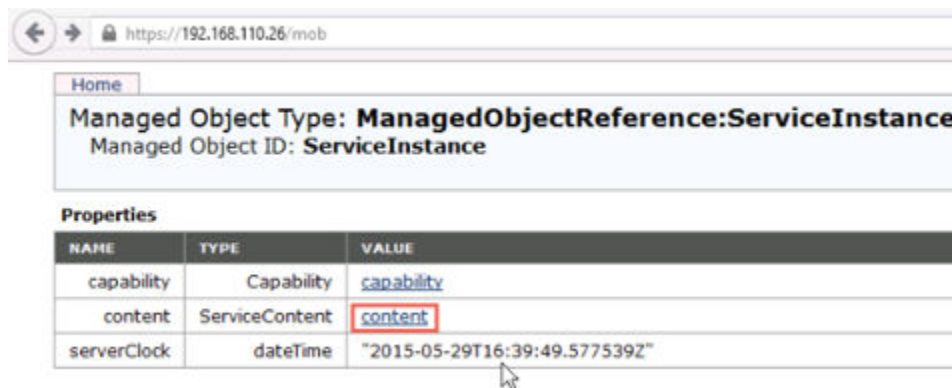
Beispiel:



Generell sind die für VTEPs verwendeten dvPortgroups bereits aufgrund von früheren Deinstallationen gelöscht.

- 5 Wenn Sie VTEP vmkernel-Schnittstellen oder dvPortgroups entfernt haben, starten Sie die Hosts neu.
- 6 Melden Sie sich bei dem vCenter, von dem Sie das NSX Manager Plug-In entfernen wollen, beim Managed Object Browser unter [https://your\\_vc\\_server/mob](https://your_vc_server/mob) an.
- 7 Klicken Sie auf **Inhalt (Content)**.

Beispiel:



8 Klicken Sie auf **ExtensionManager**.

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

Home

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

**Properties**

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

9 Klicken Sie auf **UnregisterExtension**.

**Methods**

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

- 10 Geben Sie die Zeichenfolge **com.vmware.vShieldManager** ein und klicken Sie auf **Methode aufrufen (Invoke Method)**.

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

**void UnregisterExtension**

---

**Parameters**

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

Invoke Method

- 11 Wenn Sie die vSphere 6 vCenter-Appliance ausführen, starten Sie die Konsole und aktivieren Sie unter **Optionen für den Fehlerbehebungsmodus (Troubleshooting Mode Options)** die bash-Shell.

**Troubleshooting Mode Options**

**Disable BASH Shell**

Disable SSH

<Up/Down> Select

**Disable BASH Shell**

BASH Shell is Enabled

Change current state of the BASH Shell

<Enter> Change      <Esc>Exit

Eine weitere Methode zum Aktivieren der bash-Shell besteht darin, sich als Root anzumelden und den Befehl `shell.set --enabled true` auszuführen.

## 12 Löschen Sie die vSphere Web Client-Verzeichnisse für NSX und starten Sie den Web-Client-Dienst dann neu.

Die vSphere Web Client-Verzeichnisse für NSX werden als `com.vmware.vShieldManager.**` bezeichnet und befinden sich hier:

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

Führen Sie für die vCenter Server Appliance den Befehl `service vsphere-client restart` in der Shell der Appliance aus.

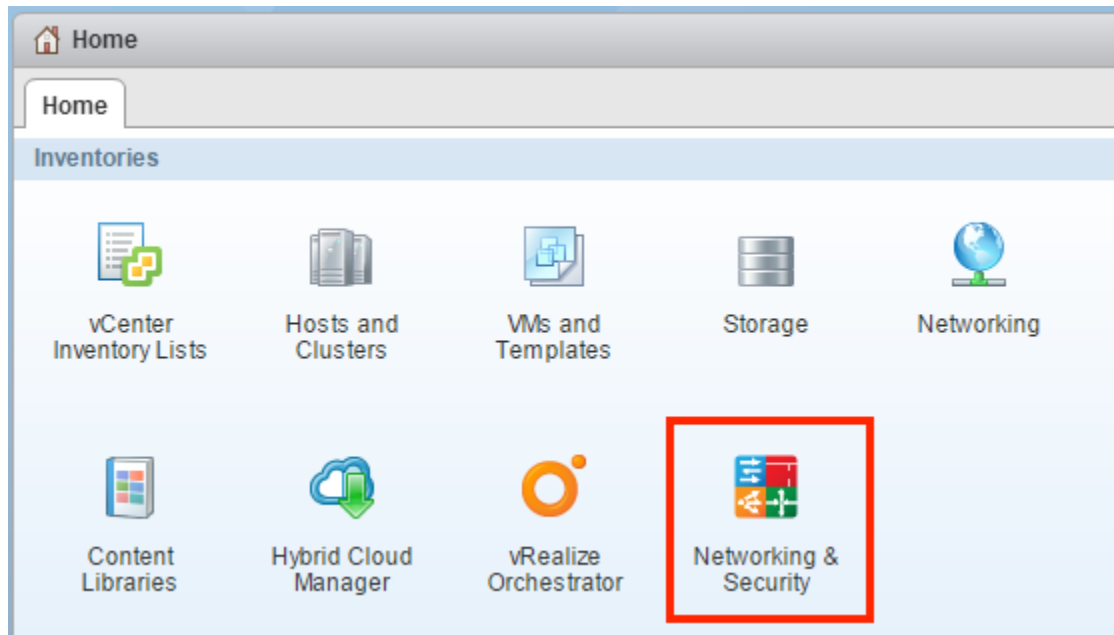
Führen Sie für ein Windows-basiertes vCenter `services.msc` aus. Klicken Sie mit der rechten Maustaste auf **vSphere Web Client** und klicken Sie dann auf **Start**.

### Ergebnisse

Das NSX Manager-Plug-In wird aus vCenter entfernt. Zur Bestätigung melden Sie sich bei vCenter ab und wieder an.

Das NSX Manager-Plug-In-Symbol **Networking & Security** wird nicht mehr auf dem Startbildschirm des vCenter Web Client angezeigt.





Wechseln Sie zu **Administration > Client-Plug-Ins (Administration > Client Plug-Ins)** und stellen Sie sicher, dass die Liste der Plug-Ins kein **NSX-Benutzeroberflächen-Plug-In (NSX User Interface plugin)** umfasst.

