

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

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
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

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

Inhalt

Installationshandbuch für NSX	5
1 Übersicht über NSX for vSphere	6
Komponenten für NSX for vSphere	8
Datenebene	8
Steuerungskomponente	9
Managementebene	10
Nutzungsplattform	11
NSX Edge	11
NSX Services	14
2 Vorbereitung für die Installation	16
Systemvoraussetzungen für NSX	16
Für NSX for vSphere erforderliche Ports und Protokolle	18
NSX und vSphere Distributed Switches	21
Beispiel: Arbeiten mit einem vSphere Distributed Switch	23
Grundlegendes zu Replizierungsmodi	31
Installations-Workflow und Beispieltopologie für NSX	33
Cross-vCenter NSX und der erweiterte verknüpfte Modus	35
3 Installieren der virtuellen NSX Manager-Appliance	37
4 Registrieren von vCenter Server mit NSX Manager	43
5 Konfigurieren von Single Sign-On	46
6 Konfigurieren eines Syslog-Servers für NSX Manager	49
7 Installieren und Zuweisen einer Lizenz von NSX for vSphere	51
8 Bereitstellen des NSX Controller-Clusters	53
9 Ausschließen von virtuellen Maschinen vom Schutz durch die Firewall	58
10 Vorbereiten von Host-Clustern für NSX	60
11 Hinzufügen eines Hosts zu einem vorbereiteten Cluster	64

- 12** Entfernen eines Hosts aus einem für NSX vorbereiteten Cluster 65
- 13** Konfigurieren von VXLAN-Transportparametern 67
- 14** Zuweisen des Segment-ID-Pools und des Multicast-Adressbereichs 72
- 15** Hinzufügen einer Transportzone 74
- 16** Hinzufügen eines logischen Switch 79
- 17** Hinzufügen eines Distributed Logical Routers 85
- 18** Hinzufügen eines Edge Services Gateway 99
- 19** Konfigurieren von OSPF auf einem logischen (Distributed) Router 111
- 20** Konfigurieren von OSPF in einem Edge Services Gateway 117
- 21** Installieren von Guest Introspection auf Hostclustern 124
- 22** Deinstallieren von NSX-Komponenten 127
 - Deinstallieren eines Guest Introspection-Moduls 127
 - Deinstallieren eines NSX Edge Services Gateways oder eines Distributed Logical Routers 128
 - Deinstallieren eines logischen Switch 128
 - Deinstallieren von NSX von Hostclustern 129
 - Sicheres Entfernen einer NSX-Installation 130

Installationshandbuch für NSX

Dieses Handbuch, das *Installationshandbuch für NSX*, beschreibt die Installation des VMware NSX[®] for vSphere[®]-Systems mithilfe der NSX Manager-Benutzeroberfläche und von vSphere Web Client. 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 VMware vCenter-Umgebung installieren oder verwenden 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

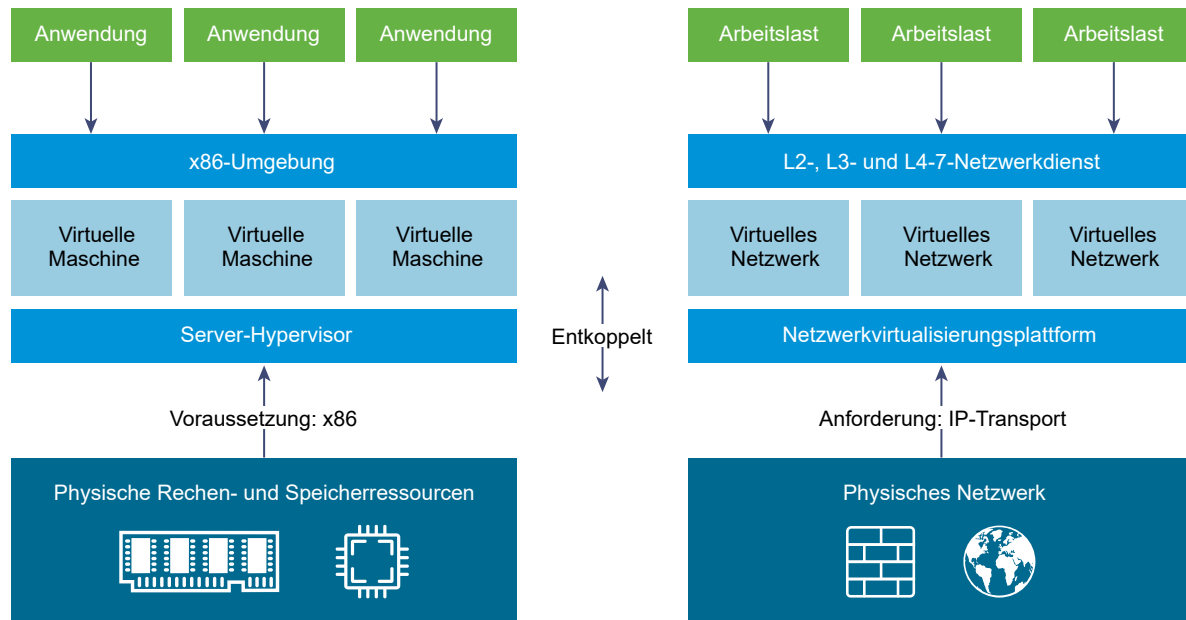
VMware Technical Publications enthält ein Glossar mit Begriffen, die Ihnen möglicherweise unbekannt sind. Definitionen von Begriffen, die in der technischen Dokumentation von VMware verwendet werden, finden Sie unter <http://www.vmware.com/support/pubs>.

Übersicht über NSX for vSphere

1

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.

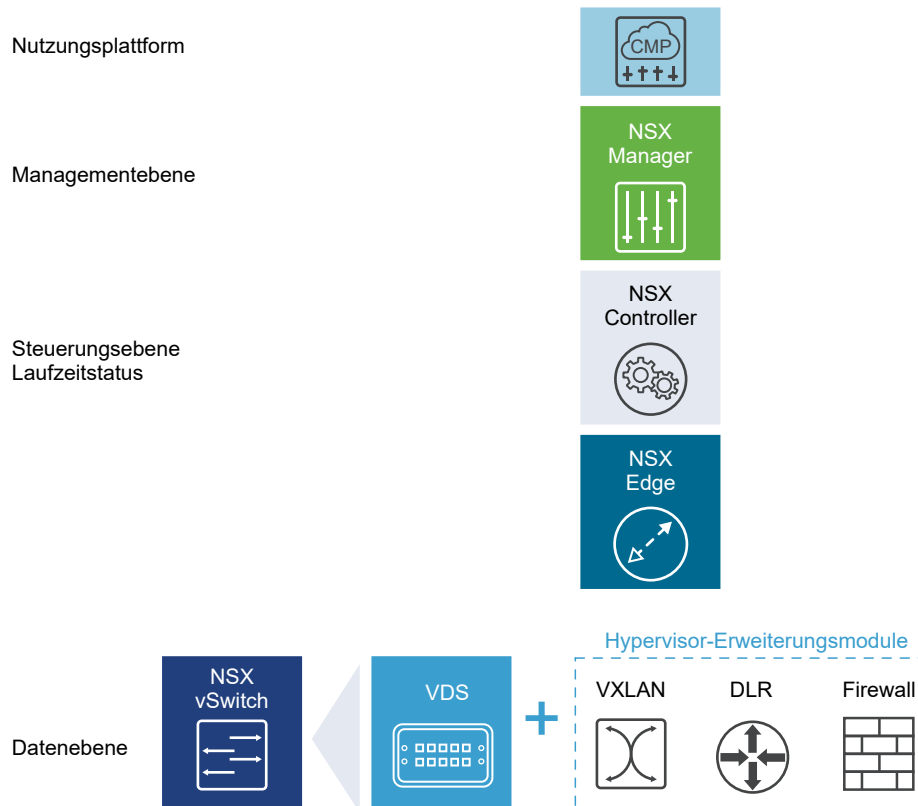
Dieses Kapitel enthält die folgenden Themen:

- **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 Datacenter installieren. Jede virtuelle ESG-Appliance 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

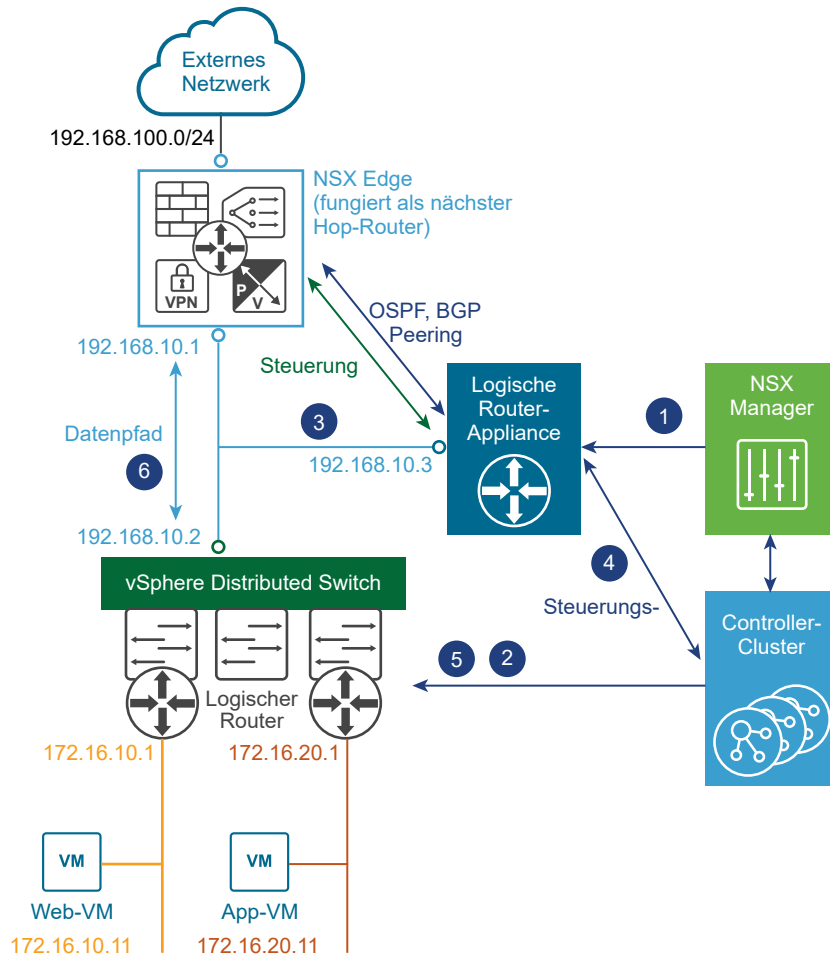
Der DLR stellt horizontal verteiltes Routing mit Mandanten-IP-Adressbereich und Datenpfadisolation bereit. Virtuelle Maschinen oder Arbeitslasten, die auf demselben Host auf verschiedenen Subnetzen vorhanden sind, können miteinander kommunizieren, ohne dass traditionelle Routing-Schnittstellen durchlaufen 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 1-1. 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-Spraws 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.

Vorbereitung für die Installation

2

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](#)
- [Grundlegendes zu Replizierungsmodi](#)
- [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 2-1. 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 2-1. 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 2-2. 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.

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"> ■ ESXi 6.0 oder höher ■ Mit NSX 6.2 oder späteren VIBs vorbereitete Hostcluster

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 2-3. 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 2-3. 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 2-3. 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

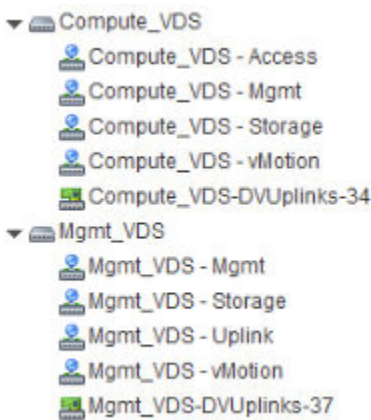
Auf der folgenden Abbildung sieht man, wie diese Cluster in vCenter angezeigt werden.



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.

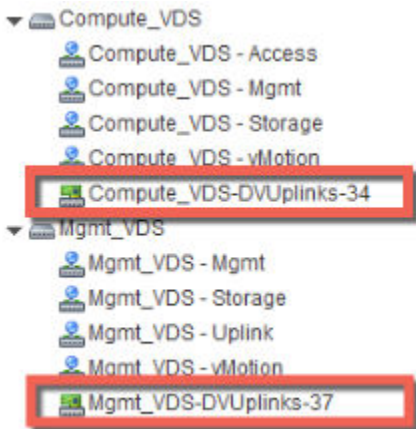


Jede Portgruppe kann wahlweise mit einer VLAN-ID konfiguriert werden. Die folgende Liste zeigt ein Beispiel dafür, wie VLANs den verteilten Portgruppen zugeordnet werden können, um eine logische Trennung zwischen verschiedenen Datenverkehrsarten sicherzustellen:

- 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>.

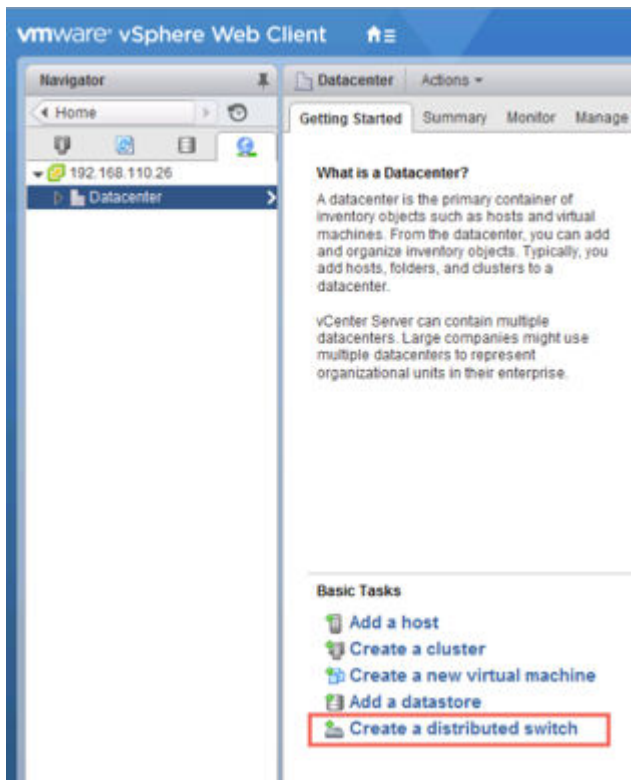
Voraussetzungen

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 Datacenter.

- 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 Beispielseinstellungen 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.

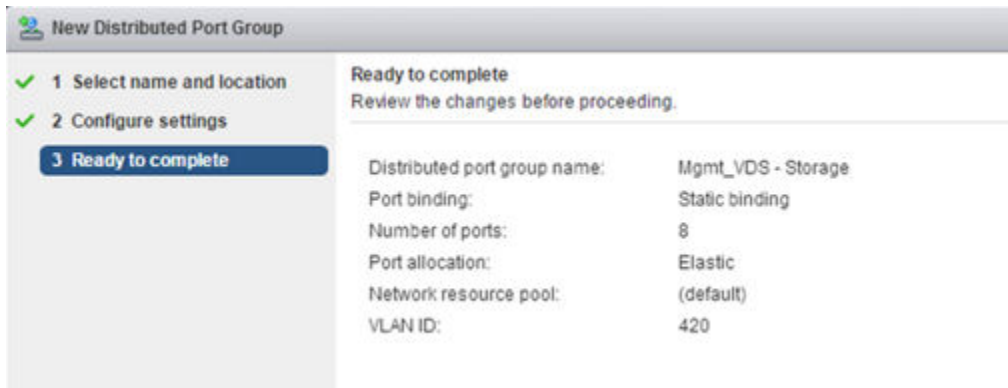
- 5 (Optional) Bearbeiten Sie nach Abschluss des Assistenten „Neuer Distributed Switch“ die Einstellungen der Standard-Portgruppe, um diese in das richtige VLAN für den Verwaltungsdatenverkehr zu platzieren.

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.

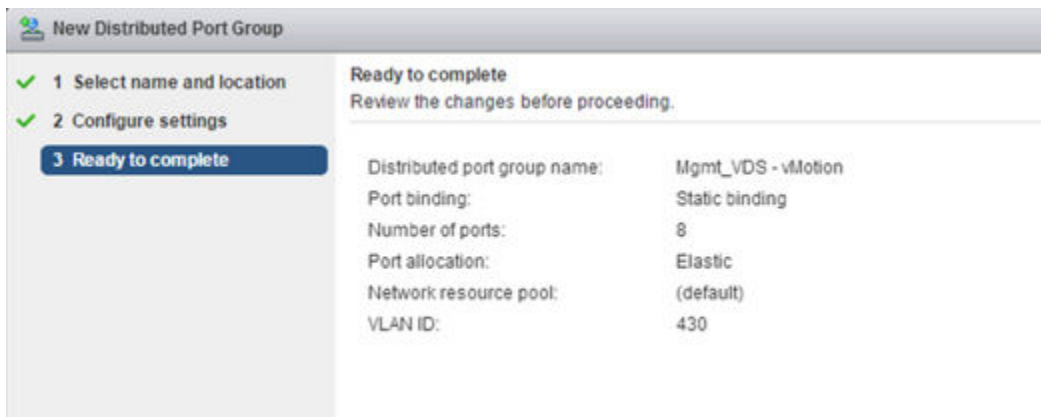
- 6 Klicken Sie nach Abschluss des Assistenten „Neuer Distributed Switch“ mit der rechten Maustaste auf den Distributed Switch und wählen Sie die Option **Neue verteilte Portgruppe (New Distributed Port Group)** aus.

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.

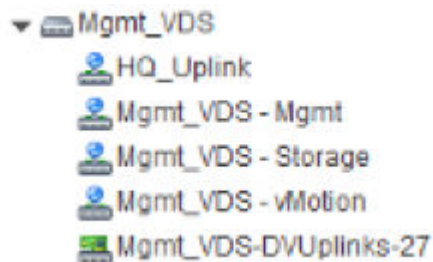
Beispiel für Gruppeneinstellungen für den Speicher.



Beispiel für Gruppeneinstellungen für den vMotion-Datenverkehr.

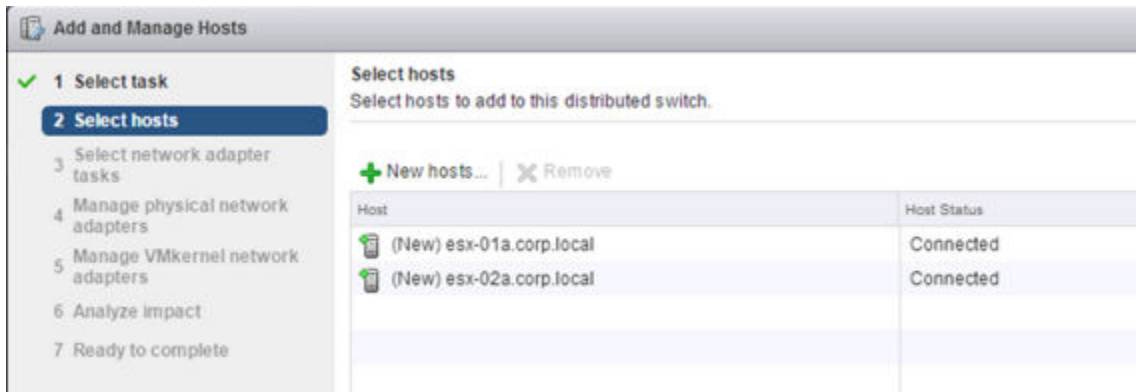


Nach erfolgreicher Erstellung sehen der Distributed Switch und die Portgruppen folgendermaßen aus.

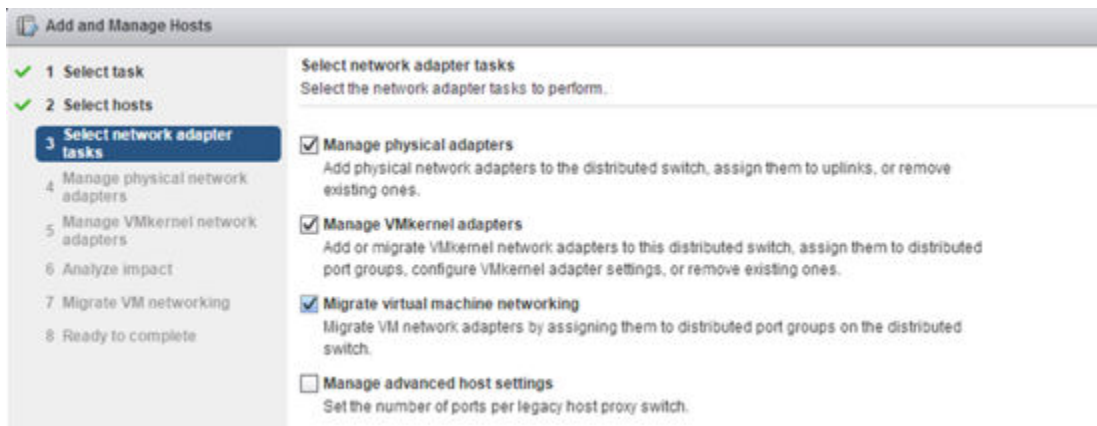


- 7 Klicken Sie mit der rechten Maustaste auf den Distributed Switch, wählen Sie **Hosts hinzufügen und verwalten (Add and Manage Hosts)** und dann **Hosts hinzufügen (Add Hosts)** aus.

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

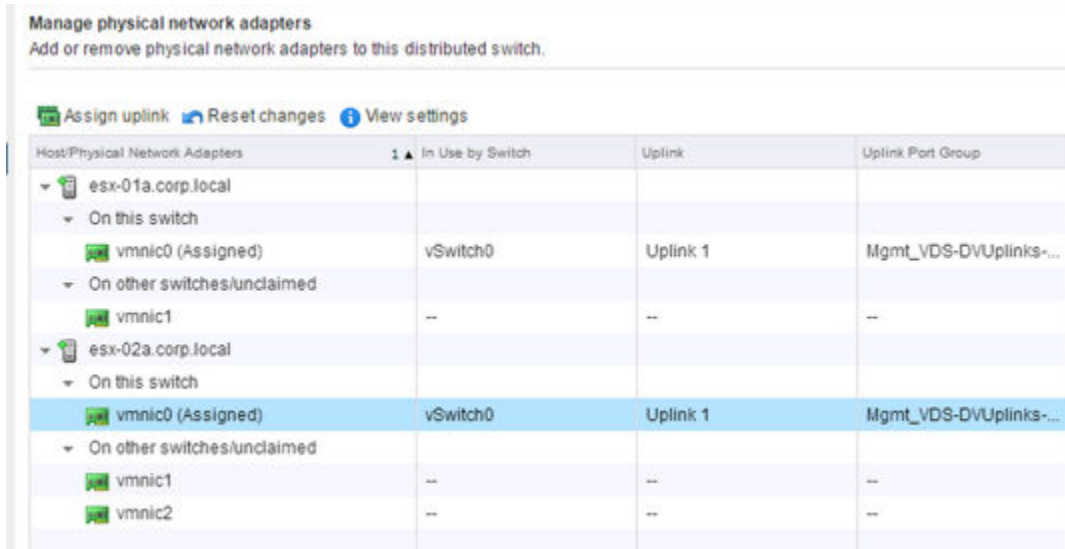


- 8 Wählen Sie die entsprechenden Optionen aus, um physische Adapter, VMkernel-Adapter und das Netzwerk virtueller Maschinen zu migrieren.



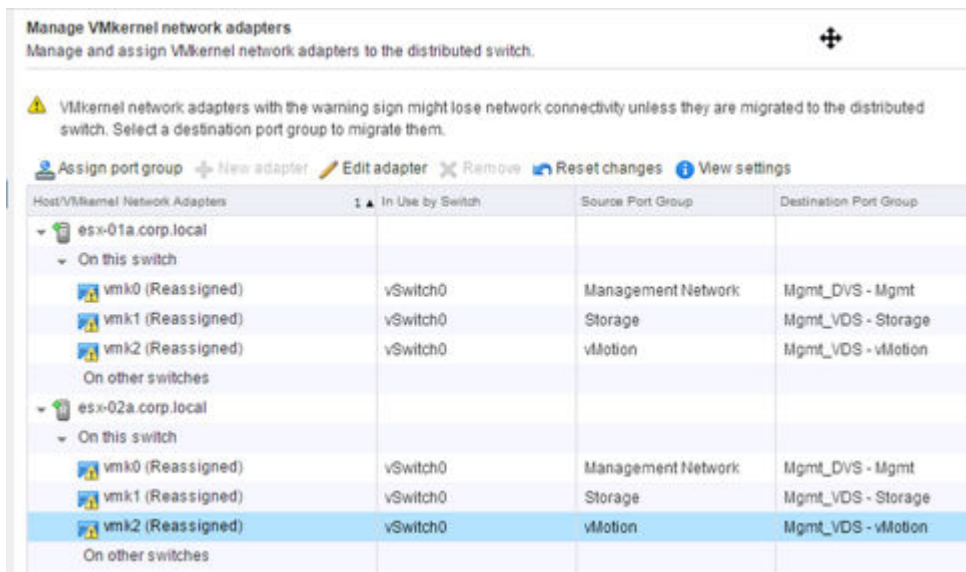
- 9 Wählen Sie eine vmnic aus und klicken Sie auf **Uplink zuweisen (Assign uplink)**, um die vmnic aus dem Standard-vSwitch auf das Distributed Switch zu migrieren. Wiederholen Sie diesen Schritt für jeden Host, den Sie mit dem verteilten vSwitch verbinden.

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.



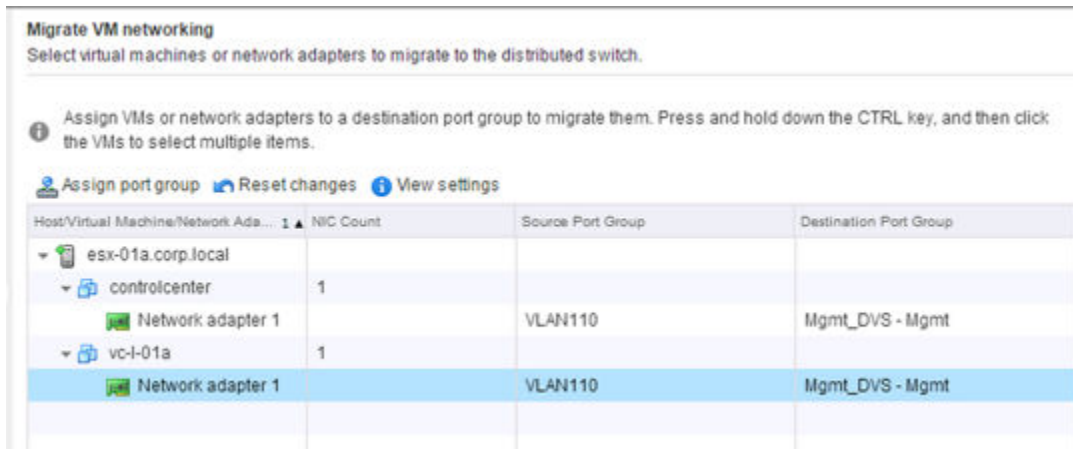
- 10 Wählen Sie einen VMkernel-Netzwerkadapter aus und klicken Sie auf **Portgruppe zuweisen (Assign port group)**. Wiederholen Sie diesen Schritt für alle Netzwerkadapter auf allen Hosts, die Sie mit dem verteilten vSwitch verbinden.

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.

Grundlegendes zu Replizierungsmodi

Wenn Sie eine Transportzone oder einen logischen Switch erstellen, müssen Sie einen Replizierungsmodus auswählen. Ein Verständnis der verschiedenen Modi hilft Ihnen bei der Entscheidung, welcher Modus für Ihre Umgebung am besten geeignet ist.

Jeder für NSX vorbereitete ESXi-Host ist mit einem VXLAN-Tunnel-Endpoint (VTEP) konfiguriert. Jeder VXLAN-Tunnel-Endpoint verfügt über eine IP-Adresse. Diese IP-Adressen können sich im selben Subnetz oder in unterschiedlichen Subnetzen befinden.

Wenn zwei VMs auf verschiedenen ESXi-Hosts direkt kommunizieren, wird der per Unicast-gekapselte Datenverkehr zwischen den beiden VTEP-IP-Adressen ausgetauscht, ohne dass dazu eine Flutung nötig ist. Allerdings muss der Datenverkehr von einer virtuellen Maschine wie bei jedem Schicht-2-Netzwerk überflutet oder an alle anderen VMs gesendet werden, die zu demselben logischen Switch gehören. Schicht-2-Broadcast-, unbekannter Unicast- und Multicast-Datenverkehr werden als BUM-Datenverkehr bezeichnet. Der BUM-Datenverkehr von einer virtuellen Maschine auf einem bestimmten Host muss auf alle anderen Hosts repliziert werden, für die virtuelle Maschinen mit demselben logischen Switch verbunden sind. NSX for vSphere unterstützt drei verschiedene Replizierungsmodi:

- Unicast-Replizierungsmodus
- Multicast-Replizierungsmodus
- Hybrid-Replizierungsmodus

Zusammenfassung der Replizierungsmodi

Tabelle 2-4. Zusammenfassung der Replizierungsmodi

Replizierungsmodus	Methode der BUM-Replizierung auf VTEPs im selben Subnetz	Methode der BUM-Replizierung auf VTEPs in einem anderen Subnetz	Anforderungen an das physische Netzwerk
Unicast	Unicast	Unicast	<ul style="list-style-type: none"> ■ Routing zwischen VTEP-Subnetzen
Multicast	Schicht 2-Multicast	Schicht 3-Multicast	<ul style="list-style-type: none"> ■ Routing zwischen VTEP-Subnetzen ■ Schicht 2-Multicast, IGMP ■ Schicht 3-Multicast, PIM ■ Zuweisung von Multicast-Gruppen zu logischen Switches
Hybrid	Schicht 2-Multicast	Unicast	<ul style="list-style-type: none"> ■ Routing zwischen VTEP-Subnetzen ■ Schicht 2-Multicast, IGMP

Unicast-Replizierungsmodus

Für den Unicast-Replizierungsmodus muss das physische Netzwerk Layer-2- und Layer-3-Multicast nicht unterstützen, um den BUM-Datenverkehr in einem logischen Switch zu verarbeiten. Durch die Verwendung des Unicast-Modus werden logische Netzwerke vollständig vom physischen Netzwerk entkoppelt. Der Unicast-Modus repliziert den gesamten BUM-Datenverkehr lokal auf dem Quellhost und leitet den BUM-Datenverkehr in einem Unicast-Paket an die Remote-Hosts weiter. Im Unicast-Modus können alle VTEPs in einem Subnetz oder in mehreren Subnetzen vorliegen.

Szenario mit einem Subnetz: Wenn alle Host-VTEP-Schnittstellen einem einzelnen Subnetz angehören, leitet der Quell-VTEP den BUM-Datenverkehr an alle Remote-VTEPs weiter. Dies wird als Head-End-Replizierung bezeichnet. Die Head-End-Replizierung führt möglicherweise zu einem erhöhten Host Overhead und einer erhöhten Bandbreitennutzung. Die Auswirkungen sind vom Umfang des BUM-Datenverkehrs und der Anzahl Hosts und VTEPs innerhalb des Subnetzes abhängig.

Szenario mit einem Subnetzen: Wenn die Host-VTEP-Schnittstellen in mehrere IP-Subnetze gruppiert sind, verarbeitet der Quellhost den BUM-Datenverkehr in zwei Teilen. Der Quell-VTEP leitet den BUM-Datenverkehr an jeden VTEP im selben Subnetz weiter (wie beim Szenario mit einem Subnetz). Für VTEPs in Remotesubnetzen leitet der Quell-VTEP den BUM-Datenverkehr an einen Host in jedem VTEP-Remotesubnetz weiter und legt das Replizierungs-Bit fest, um dieses Pakets für die lokale Replizierung zu markieren. Wenn ein Host im Remotesubnetz dieses Paket empfängt und das festgelegte Replizierungs-Bit findet, sendet er das Paket an alle anderen VTEPs in seinem Subnetz, für die ein logischer Switch vorhanden ist.

Aus diesem Grund kann der Unicast-Replizierungsmodus in Netzwerkarchitekturen mit vielen VTEP-IP-Subnetzen gut skaliert werden, da die Last auf mehrere Hosts verteilt ist.

Multicast-Replizierungsmodus

Für den Multicast-Replizierungsmodus müssen Schicht-3- und Schicht-2-Multicasts in der physischen Infrastruktur aktiviert sein. Zum Konfigurieren des Multicast-Modus ordnet der Netzwerkadministrator jedem logischen Switch eine IP-Multicast-Gruppe zu. Bei ESXi-Hosts, die VMs auf einem bestimmten logischen Switch hosten, treten die zugehörigen VTEPs mithilfe von IGMP der Multicast-Gruppe bei. Die Router verfolgen die IGMP-Beitritte und erstellen mithilfe eines Multicast-Routing-Protokolls eine Multicast-Verteilungsstruktur zwischen ihnen.

Wenn Hosts den BUM-Datenverkehr zu VTEPs im selben IP-Subnetz replizieren, wird dabei Schicht-2-Multicast verwendet. Wenn Hosts den BUM-Datenverkehr auf VTEPs in unterschiedlichen IP-Subnetzen replizieren, wird dabei Schicht-3-Multicast verwendet. In beiden Fällen wird die Replizierung des BUM-Datenverkehrs auf Remote-VTEPs von der physischen Infrastruktur verarbeitet.

Obwohl IP-Multicast eine bekannte Technologie ist, gilt die Bereitstellung von IP-Multicast im Datacenter aus diversen technischen, operativen oder administrativen Gründen häufig als Hürde. Der Netzwerkadministrator muss die maximal unterstützten Multicast-Zustände in der physischen Infrastruktur sorgfältig definieren, um die 1:1-Zuordnung zwischen dem logischen Switch und der Multicast-Gruppe zu

ermöglichen. Einer der Vorteile der Virtualisierung besteht darin, dass sie die Skalierung der virtuellen Infrastruktur ermöglicht, ohne dass der physischen Infrastruktur zusätzliche Zustände mitgeteilt werden. Dieses Modell wird durch das Zuordnen von logischen Switches zu „physischen“ Multicast-Gruppen unterbrochen.

Hinweis Im Multicast-Replizierungsmodus wird der NSX Controller-Cluster für logische Switches nicht verwendet.

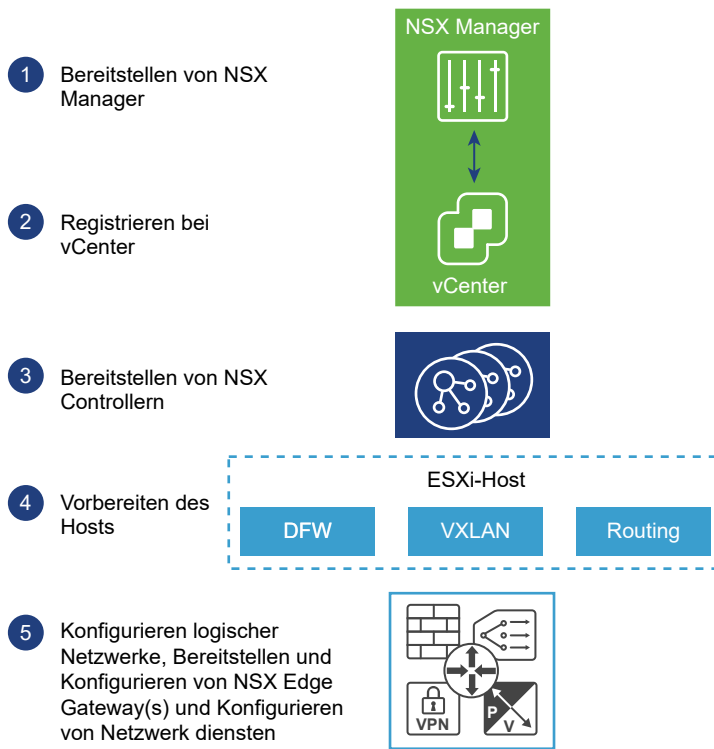
Hybrid-Replizierungsmodus

Beim Hybrid-Modus handelt es sich um eine Mischung aus den Unicast- und Multicast-Replizierungsmodi. Im Hybrid-Replizierungsmodus verwenden Host-VTEPs Schicht-2-Multicast, um BUM-Datenverkehrs an Peer-VTEPs im selben Subnetz zu verteilen. Wenn Host-VTEPs den BUM-Datenverkehr auf VTEPs in verschiedenen Subnetzen replizieren, leiten sie den Datenverkehr als Unicast-Pakete an jeweils einen Host pro VTEP-Subnetz weiter. Dieser empfangende Host verwendet wiederum Schicht 2-Multicast, um die Pakete an andere VTEPs in seinem Subnetz zu senden.

Schicht-2-Multicast wird in Kundennetzwerken häufiger verwendet als Schicht-3-Multicast, da die Bereitstellung in der Regel einfach ist. Die Replizierung auf verschiedene VTEPs im selben Subnetz wird im physischen Netzwerk verarbeitet. Die Hybrid-Replizierung kann eine erhebliche Entlastung für den Quellhost des BUM-Datenverkehrs sein, wenn sich viele Peer-VTEPs im selben Subnetz befinden. Mit der Hybrid-Replizierung können Sie eine dichte Umgebung mit geringer oder keiner Segmentierung vertikal hochskalieren.

Installations-Workflow und Beispieltopologie für NSX

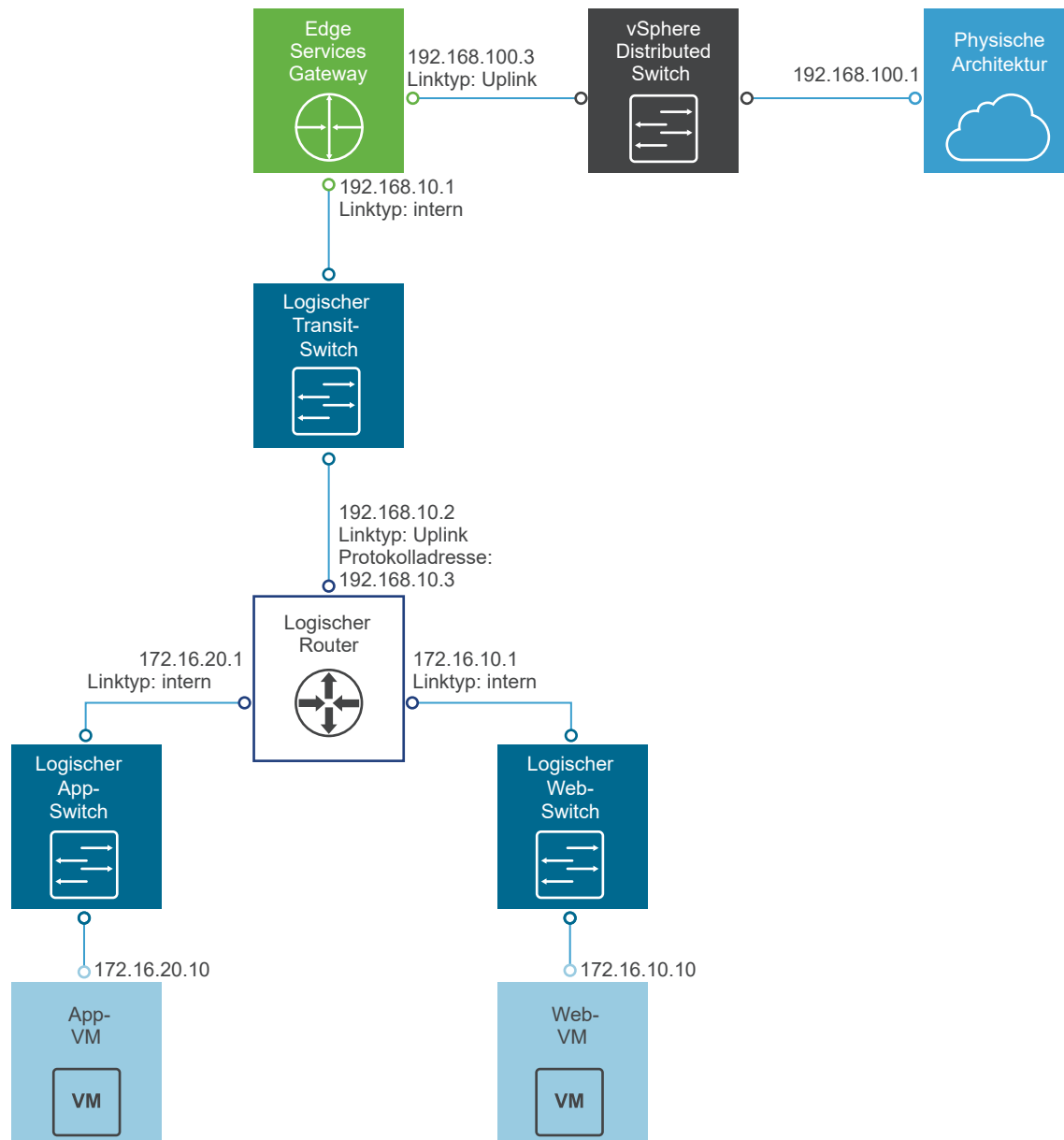
Die Installation von NSX beinhaltet die Bereitstellung mehrerer virtueller Appliances, einige vorbereitende Schritte für den ESX-Host sowie etwas Konfiguration, um die Kommunikation zwischen allen physischen und virtuellen Geräten zu ermöglichen.



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*.

Installieren der virtuellen NSX Manager-Appliance

3

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.

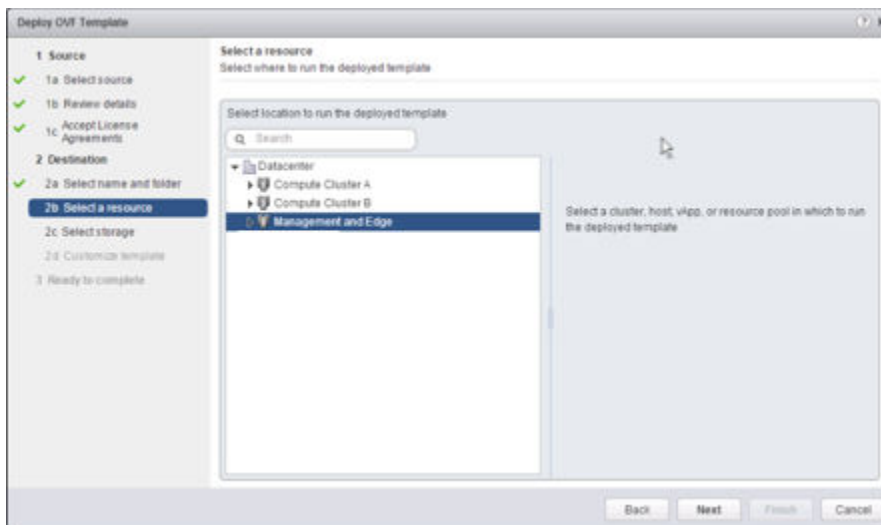
- 7 Bearbeiten Sie den NSX Manager-Namen (falls erforderlich) und wählen Sie den Speicherort für den bereitgestellten NSX Manager aus.

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.

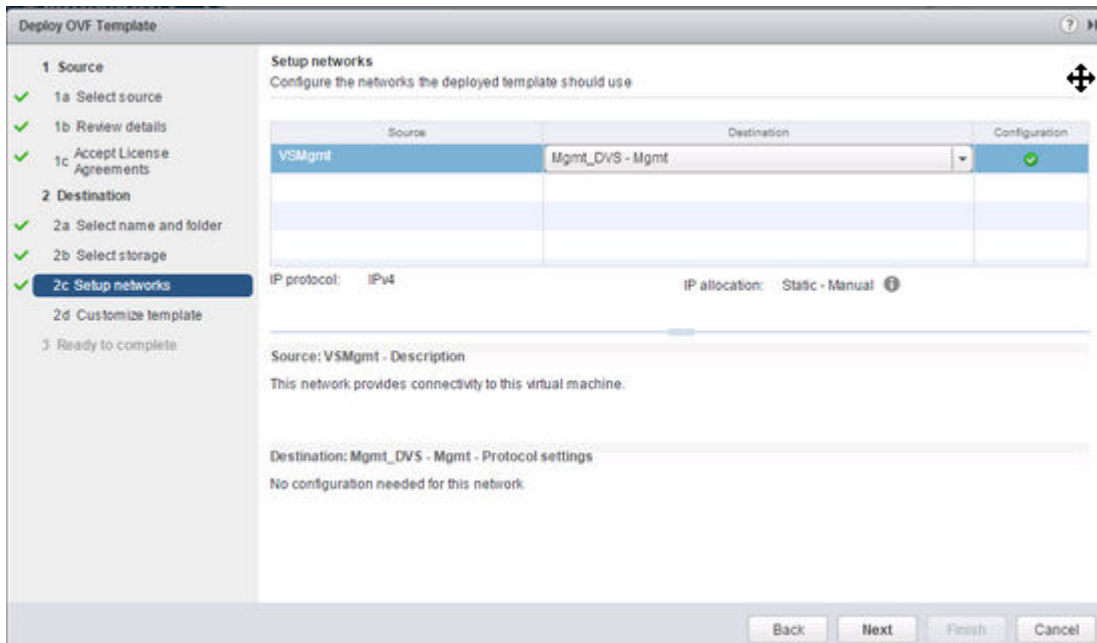
Beispiel:



- 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.

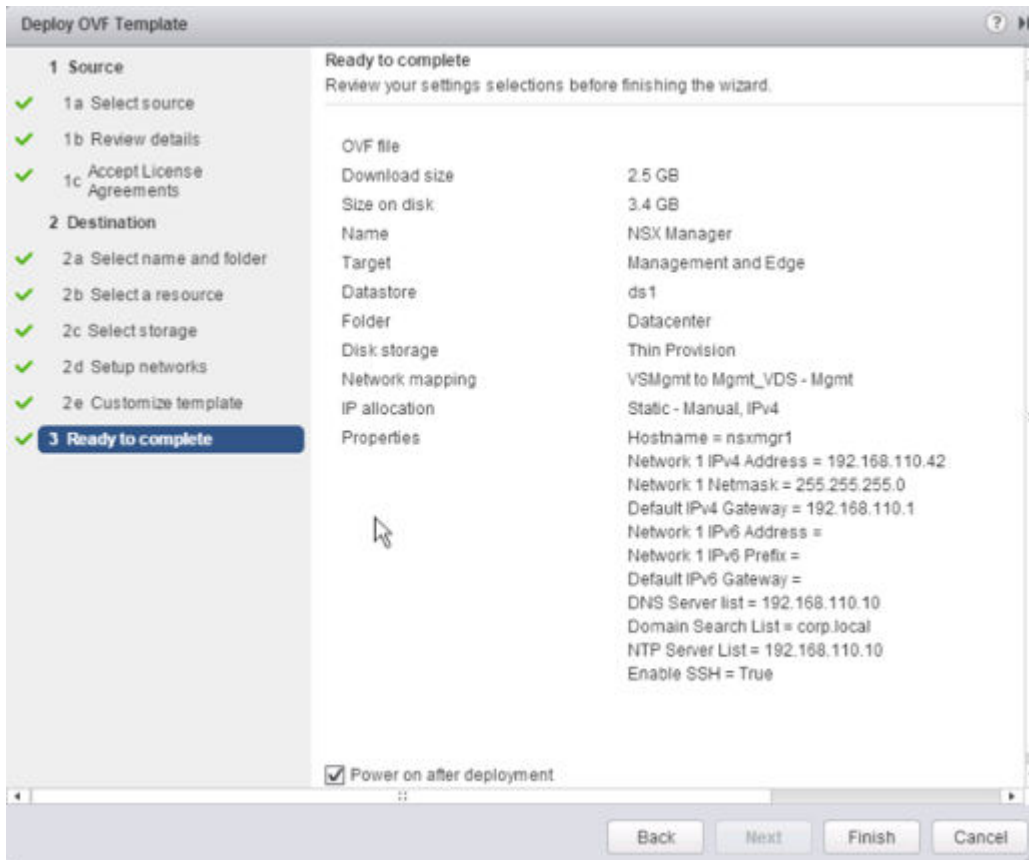
In diesem Screenshot ist beispielsweise die Auswahl für die Portgruppe Mgmt_DVS - Mgmt dargestellt.



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.

Registrieren von vCenter Server mit NSX Manager

4

NSX Manager und vCenter Server haben eine 1:1-Beziehung. Für jede NSX Manager-Instanz gibt es einen vCenter Server. Dies gilt auch für Cross-vCenter NSX-Umgebungen.

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 die gesamte NSX for vSphere-Konfiguration 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.

Bei Bedarf können Sie das vCenter Server-Benutzerkonto ändern, das für die Registrierung mit NSX Manager verwendet wird. Das vCenter Server-Benutzerkonto, das für die Registrierung verwendet wird, muss Mitglied der Gruppe der vCenter Single Sign-On-**Administratoren** sein.

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 Webbrowser zur NSX Manager-Appliance-GUI unter <https://<nsx-manager-ip>> oder <https://<nsx-manager-hostname>> und melden Sie sich als **Admin** oder mit einem Benutzerkonto mit der Rolle **Enterprise-Administrator** an.

- 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.

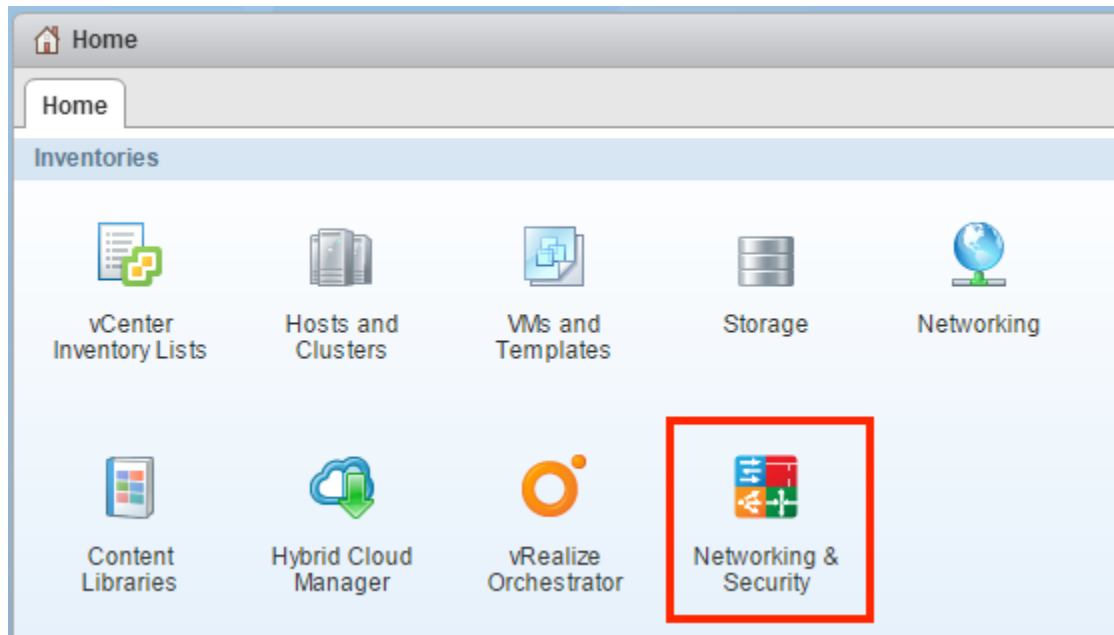
- 5 Aktivieren Sie die Option **Speicherort für Downloads für das Plug-In-Skript ändern (Modify plugin script download location)** nicht, es sei denn, NSX Manager befindet sich hinter einem Maskierungsgerät vom Typ Firewall.

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 von Single Sign-On

5

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	
<div style="text-align: right;"> Unconfigure NTP Servers Edit </div>	
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 Webbrowser zur NSX Manager-Appliance-GUI unter <https://<nsx-manager-ip>> oder <https://<nsx-manager-hostname>> und melden Sie sich als **Admin** oder mit einem Benutzerkonto mit der Rolle **Enterprise-Administrator** an.

- 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*.

Konfigurieren eines Syslog-Servers für NSX Manager

6

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 Webbrowser zur NSX Manager-Appliance-GUI unter <https://<nsx-manager-ip>> oder <https://<nsx-manager-hostname>> und melden Sie sich als **Admin** oder mit einem Benutzerkonto mit der Rolle **Enterprise-Administrator** an.
- 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:

The screenshot shows a dialog box titled "Syslog Server" with a close button (X) in the top right corner. Below the title bar, there is a text instruction: "You can specify the IP address or name of the syslog server that can be resolved using the above mentioned DNS Server(s)." Below this instruction, there are three input fields: "Syslog Server:" with the value "syslog-01a.corp.local", "Port:" with the value "514", and "Protocol:" with a dropdown menu showing "UDP". At the bottom right of the dialog box, there are two buttons: "OK" and "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

7

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>.

Bereitstellen des NSX Controller-Clusters

8

NSX Controller ist ein erweitertes, verteiltes Zustandsverwaltungssystem, das Steuerungskomponentenfunktionen für logische Switching- und Routing-Funktionen für 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.

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.

Vorsicht Während ein Controller-Status **Wird bereitgestellt (Deploying)** angezeigt, dürfen Sie in Ihrer Umgebung keine logischen Switches oder verteiltes Routing hinzufügen oder ändern. Fahren Sie auch nicht mit dem Verfahren zur Hostvorbereitung fort. Nachdem der neue Controller zum Controller-Cluster hinzugefügt wurde, sind alle Controller eine kurze Zeit lang inaktiv (maximal 5 Minuten). Während dieser Downtime können alle Vorgänge im Zusammenhang mit Controllern (z. B. die Hostvorbereitung) zu unerwarteten Ergebnissen führen. Obwohl die Hostvorbereitung vollständig erfolgreich zu sein gewesen scheint, kann das SSL-Zertifikat möglicherweise nicht korrekt eingerichtet werden, was zu Problemen im VXLAN-Netzwerk führt.

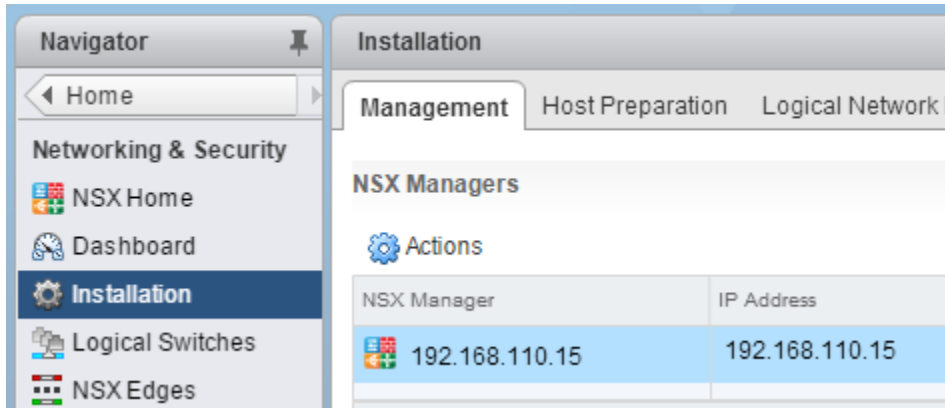
Voraussetzungen

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

Beispiel:



- 3 Klicken Sie im Bereich der NSX Controller-Knoten auf das Symbol **Knoten hinzufügen (Add Node)** (+).
- 4 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: esxmgt-01a.corp.local ▼

Folder: NSX Controllers ▼

Connected To: * vds-mgt_Managem [Change](#) [Remove](#)

IP Pool: * controller-pool [Select](#)

Password: * *****

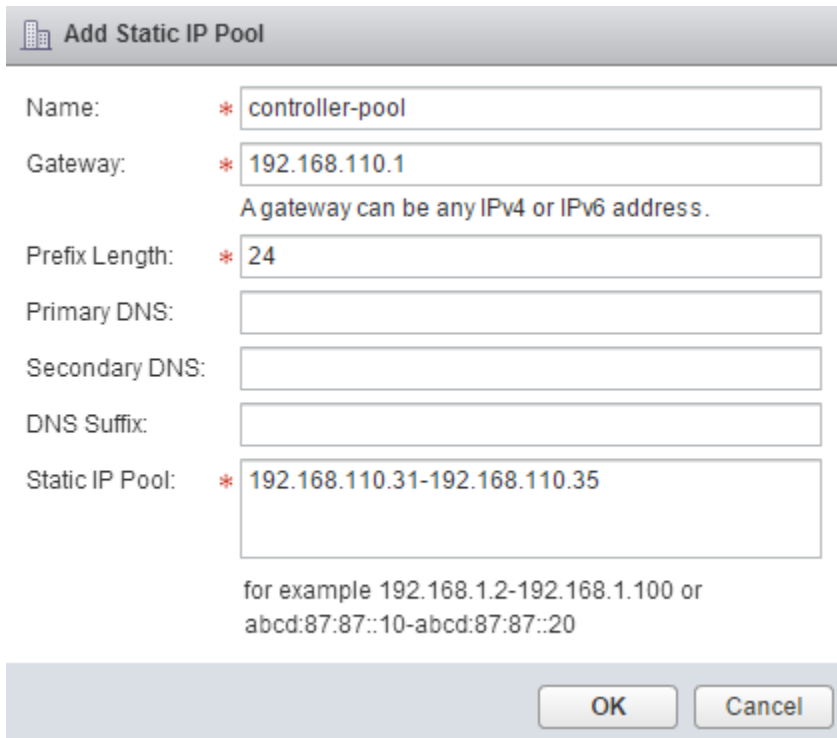
Confirm password: * *****

OK Cancel

- 5 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: * controller-pool

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

Prefix Length: * 24

Primary DNS:

Secondary DNS:

DNS Suffix:

Static IP Pool: * 192.168.110.31-192.168.110.35

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

OK Cancel

- 6 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

- 7 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.

Auf den Hosts, auf denen die NSX Controller-Knoten zuerst bereitgestellt werden, aktiviert NSX automatisch das Starten/Herunterfahren von virtuellen Maschinen. Wenn die Controller-Knoten-VMs später zu anderen Hosts migriert werden, ist auf dem neuen Hosts das automatische Starten/Herunterfahren von virtuellen Maschinen möglicherweise nicht aktiviert. Aus diesem Grund empfiehlt VMware, dass Sie alle Hosts im Cluster überprüfen, um sicherzustellen, dass das automatische Starten/Herunterfahren von virtuellen Maschinen aktiviert ist. Weitere Informationen dazu finden Sie unter http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-5FE08AC7-4486-438E-AF88-80D6C7928810.html.

Beispiel

Ausschließen von virtuellen Maschinen vom Schutz durch die Firewall

9

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.

Vorbereiten von Host-Clustern für NSX

10

Bei der Hostvorbereitung handelt es sich um den Vorgang, bei dem NSX Manager zum einen Kernelmodule auf ESXi-Hosts, die Mitglieder von vCenter-Clustern sind, installiert; und zum anderen das Fabric der Steuerungsebene und der Verwaltungsebene für errichtet. In VIB-Dateien gepackte NSX for vSphere-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. 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. 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-l-01a.corp.local
Address: 192.168.110.42
```

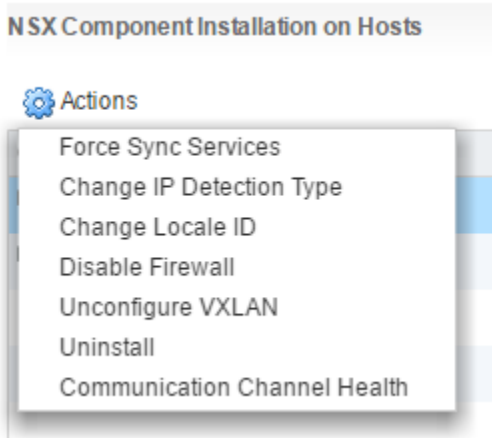
- Überprüfen Sie, ob die Hosts den DNS-Namen von vCenter Server auflösen können.

- 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.

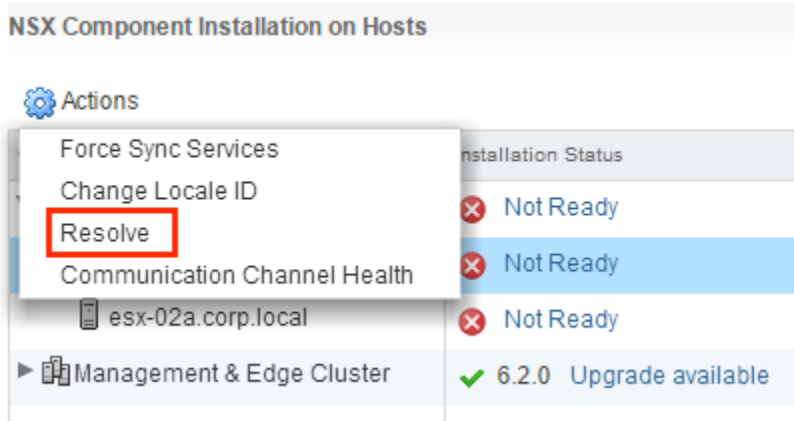
- Wenn in Ihrer Umgebung vSphere Update Manager (VUM) vorhanden ist, müssen Sie diesen vor der Vorbereitung von Clustern für die Netzwerkvirtualisierung deaktivieren. Informationen dazu, wie man überprüft, ob VUM aktiviert ist und wie man VUM bei Bedarf deaktiviert, finden Sie unter <http://kb.vmware.com/kb/2053782>.
- 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 beim vSphere Web Client an.
- 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"> ■ esx-vsip ■ esx-vxlan
6.0 oder höher	6.3.2 oder früher	<ul style="list-style-type: none"> ■ esx-vsip ■ esx-vxlan
6.0 oder höher	6.3.3 oder höher	<ul style="list-style-type: none"> ■ esx-nsxv

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.

Hinzufügen eines Hosts zu einem vorbereiteten Cluster

11

In diesem Abschnitt wird beschrieben, wie Sie einen Host zu einem Cluster hinzufügen, der für die Netzwerkvirtualisierung vorbereitet ist.

Verfahren

- 1 Fügen Sie den Host zu vCenter Server als eigenständigen Host hinzu.

Information dazu finden Sie in der *ESXi- und vCenter Server-Dokumentation*.

- 2 Fügen Sie den Host zu dem vSphere Distributed Switch hinzu, der dem Cluster zugeordnet ist, zu welchem Sie den Host hinzufügen möchten.

Alle Hosts im Cluster müssen sich in dem vSphere Distributed Switch befinden, der von NSX genutzt wird.

- 3 Klicken Sie mit der rechten Maustaste auf den Ziel-Host und wählen Sie **Wartungsmodus (Maintenance Mode) > In Wartungsmodus wechseln (Enter Maintenance Mode)** aus.

- 4 Ziehen Sie den Ziel-Host in den vorhandenen Cluster, der für NSX aktiviert ist.

Da es sich um einen vorbereiteten Cluster handelt, wird die erforderliche Software automatisch auf dem neu hinzugefügten Host installiert.

- 5 Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **Wartungsmodus (Maintenance Mode) > Wartungsmodus beenden (Exit Maintenance Mode)** aus.

DRS gleicht virtuelle Maschinen auf dem Host aus.

Entfernen eines Hosts aus einem für NSX vorbereiteten Cluster

12

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`

Konfigurieren von VXLAN-Transportparametern

13

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.

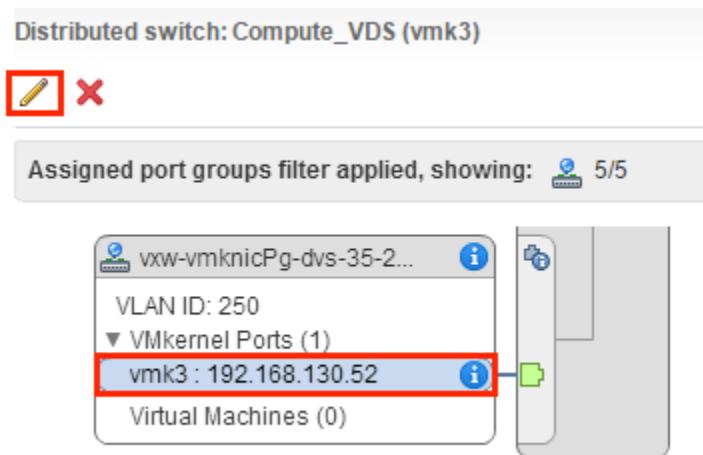
Die empfohlene Vorgehensweise für IP-hashbasiertes Teaming (EtherChannel, LACPv1 oder LACPv2) besteht darin, alle Uplinks auf dem vSphere Distributed Switch im Team, aber keine Portgruppen auf diesem vSphere Distributed Switch mit unterschiedlichen Teaming-Richtlinien zu verwenden. Weitere Informationen 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 beim vSphere Web Client an.
- 2 Wechseln Sie zu **Home > Networking & Security > Installation** und wählen Sie die Registerkarte **Hostvorbereitung (Host Preparation)** aus.
- 3 Klicken Sie auf **Nicht konfiguriert (Not Configured)** in der Spalte **VXLAN**.
- 4 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

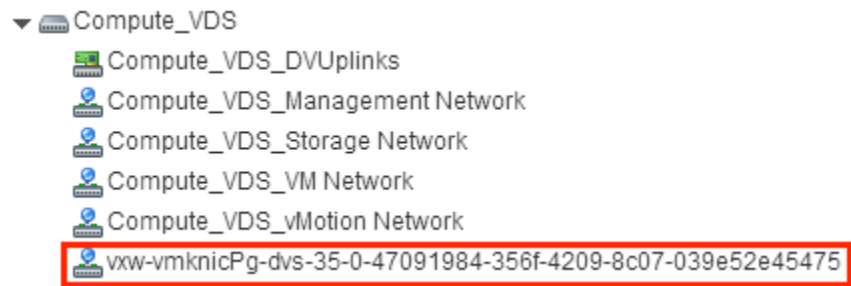
OK Cancel

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.

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 des Segment-ID-Pools und des Multicast-Adressbereichs

14

VXLAN-Segmente werden zwischen den VXLAN-Tunnelendpunkten (VTEPs) erstellt. Ein Hypervisor-Host ist ein Beispiel für einen typischen VTEP. Jeder VXLAN-Tunnel verfügt über eine Segment-ID. Sie müssen für jeden 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.

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.

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 beim vSphere Web Client an.
- 2 Wechseln Sie zu **Home > Networking & Security > Installation** und wählen Sie die Registerkarte **Vorbereitung des logischen Netzwerks (Logical Network Preparation)** aus.
- 3 Klicken Sie auf **Segment-ID > Bearbeiten (Segment ID > Edit)**.
- 4 Geben Sie einen Bereich für die Segment-IDs ein, z. B. **5000–5999**.
- 5 (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.

Hinzufügen einer Transportzone

15

Eine Transportzone steuert, welche Hosts ein logischer Switch erreichen kann. Sie kann einen oder mehrere vSphere-Cluster umfassen. Transportzonen bestimmen, welche Cluster und damit auch welche VMs bei der Verwendung eines bestimmten Netzwerks teilnehmen können.

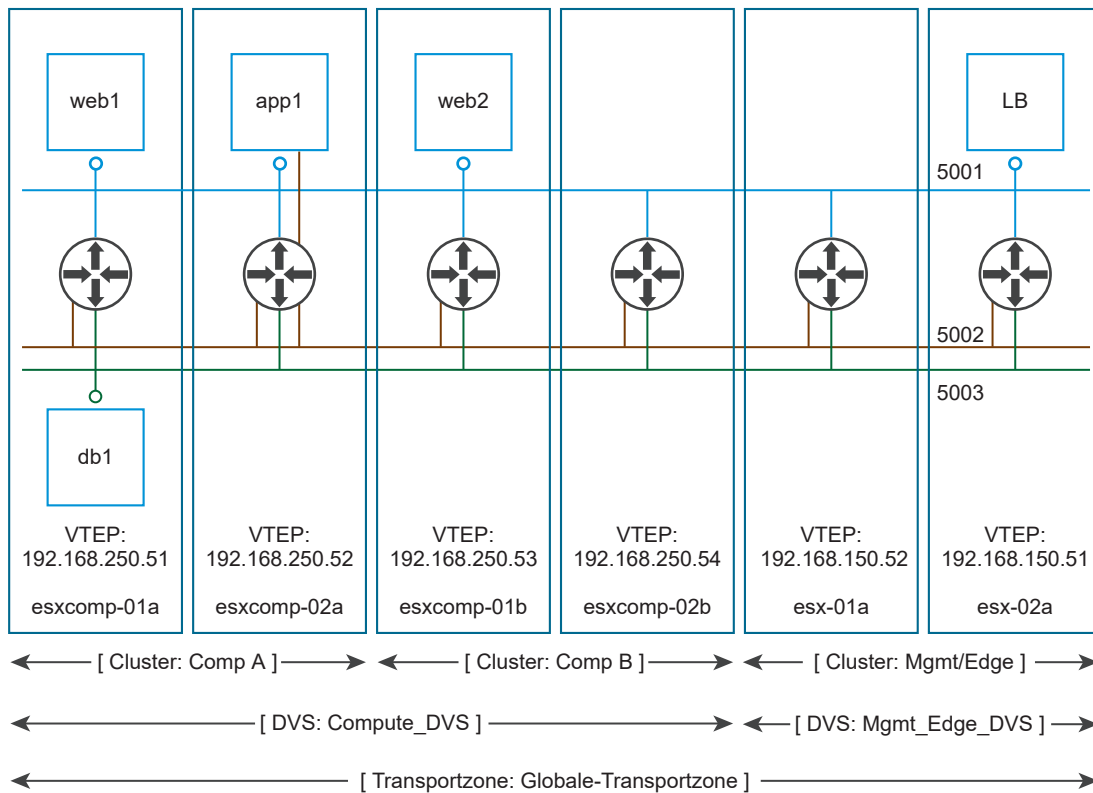
Eine NSX-Umgebung kann je nach Ihren Anforderungen mindestens eine Transportzone enthalten. Ein Hostcluster kann zu mehreren Transportzonen gehören. Ein logischer Switch kann jeweils nur zu einer Transportzone gehören.

NSX lässt nicht die Verbindung von VMs zu, die sich in unterschiedlichen Transportzonen befinden. Die Spannweite eines logischen Switches ist auf eine Transportzone begrenzt, sodass sich virtuelle Maschinen in unterschiedlichen Transportzonen nicht im selben Schicht 2-Netzwerk befinden können. Ein Distributed Logical Router kann keine Verbindung zu logischen Switches herstellen, die sich in unterschiedlichen Transportzonen befinden. Nachdem Sie den ersten logischen Switch verbunden haben, ist die Auswahl von weiteren logischen Switches auf diejenigen begrenzt, die sich in derselben Transportzone befinden.

Mit den folgenden Richtlinien können Sie die Transportzonen entwerfen.

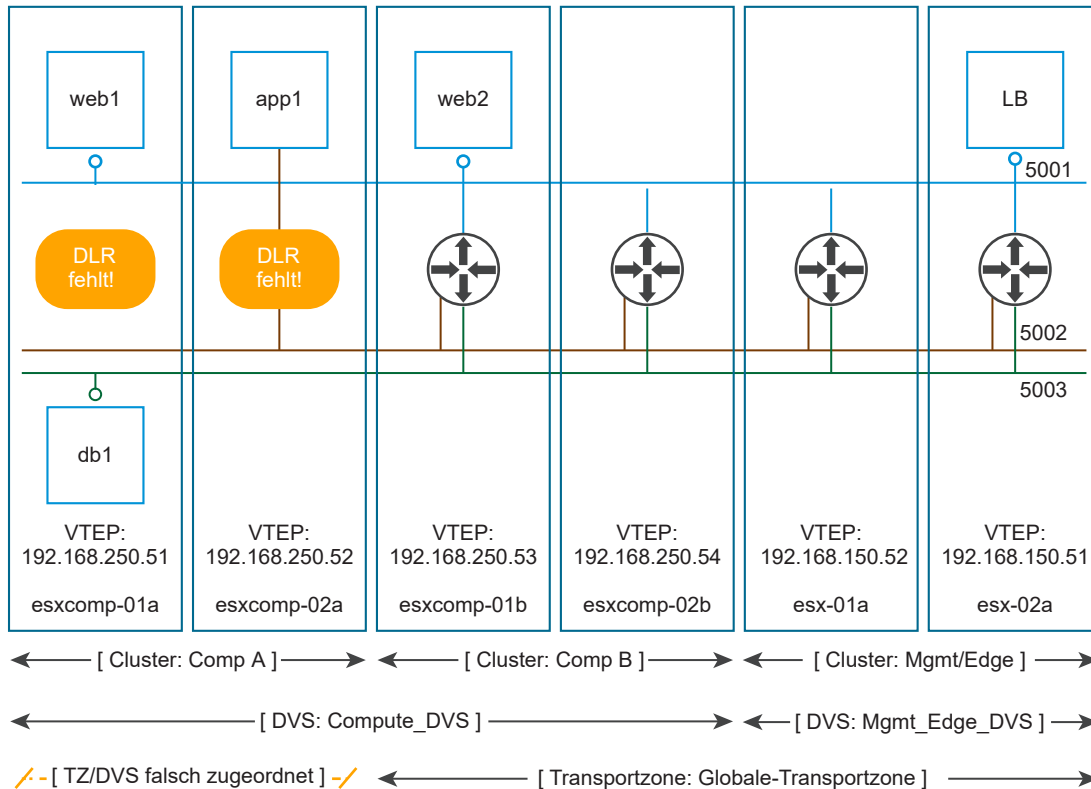
- Wenn ein Cluster Schicht 3-Konnektivität erfordert, muss sich der Cluster in einer Transportzone befinden, die auch einen Edge-Cluster enthält, d. h. einen Cluster mit Schicht 3-Edge-Geräten (Distributed Logical Router und Edge Services Gateways).
- Angenommen, Sie haben zwei Cluster, einen für Webdienste und einen anderen für Anwendungsdienste. Für VXLAN-Konnektivität zwischen den VMs in diesen zwei Clustern müssen beide Cluster in der Transportzone enthalten sein.
- Beachten Sie, dass alle logischen Switches, die in der Transportzone enthalten sind, für alle VMs innerhalb der Cluster verfügbar und sichtbar sind, die in der Transportzone enthalten sind. Wenn ein Cluster gesicherte Umgebungen enthält, möchten Sie ihn möglicherweise nicht für VMs in anderen Clustern verfügbar machen. Sie können stattdessen den sicheren Cluster in einer isolierteren Transportzone ablegen.
- Die Spannweite des vSphere Distributed Switch (VDS oder DVS) sollte der Spannweite der Transportzone entsprechen. Stellen Sie beim Erstellen von Transportzonen in Multi-Cluster-VDS-Konfigurationen sicher, dass alle Cluster in dem ausgewählten VDS in der Transportzone enthalten sind. Dadurch wird sichergestellt, dass der DLR in allen Clustern verfügbar ist, in denen auch VDS dvPortgroups verfügbar sind.

Das folgende Diagramm zeigt eine Transportzone, die korrekt an der VDS-Begrenzung ausgerichtet ist.



Wenn Sie die bewährte Methode nicht befolgen, sollten Sie Folgendes beachten: Wenn ein VDS mehr als einen Hostcluster umfasst und die Transportzone nur einen (oder eine Teilmenge) dieser Cluster enthält, können alle in dieser Transportzone enthaltenen logischen Switches auf VMs innerhalb aller Cluster zugreifen, die von dem VDS umfasst werden. Mit anderen Worten, die Transportzone kann nicht die Spannweite der logischen Switches auf eine Teilmenge der Cluster beschränken. Wenn dieser logische Switch zu einem späteren Zeitpunkt mit einem DLR verbunden wird, müssen Sie sicherstellen, dass die Router-Instanzen nur in dem Cluster erstellt werden, der in der Transportzone enthalten ist, um Probleme mit Schicht 3 zu vermeiden.

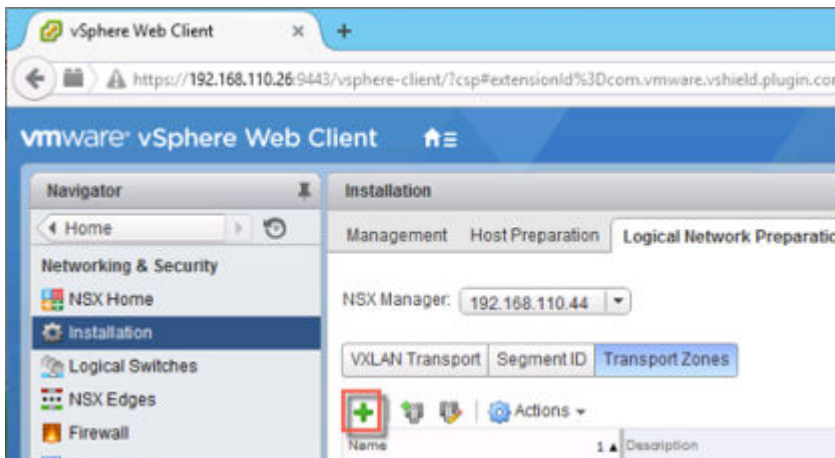
Beispiel: Wenn eine Transportzone nicht an der VDS-Begrenzung ausgerichtet ist, wird der Geltungsbereich der logischen Switches (5001, 5002 und 5003) und die DLR-Instanzen, mit denen diese logischen Switches verbunden sind, getrennt, sodass VMs in Cluster Comp A keinen Zugriff auf die logischen Schnittstellen von DLR (LIFs) haben.



Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Wechseln Sie zu **Home > Networking & Security > Installation** und wählen Sie die Registerkarte **Vorbereitung des logischen Netzwerks (Logical Network Preparation)** aus.
- 3 Klicken Sie auf **Transportzonen (Transport Zones)** und dann auf das Symbol **Neue Transportzone (New Transport Zone)** (+).

Beispiel:



- 4 Geben Sie im Dialogfeld „Neue Transportzone“ einen Namen und eine optionale Beschreibung für die Transportzone ein.
- 5 Wählen Sie den entsprechenden Steuerungskomponenten-Modus aus, je nachdem, ob Sie einen Controller-Knoten in Ihrer Umgebung haben oder Sie Multicast-Adressen verwenden möchten.
 - **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 Kopfendereplikation. 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.
- 6 Wählen Sie die Cluster aus, die zur Transportzone hinzugefügt werden sollen.

Beispiel:

New Transport Zone

Name:

Description:

Replication mode:

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

Select clusters that will be part of the Transport Zone

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

OK Cancel

Nächste Schritte

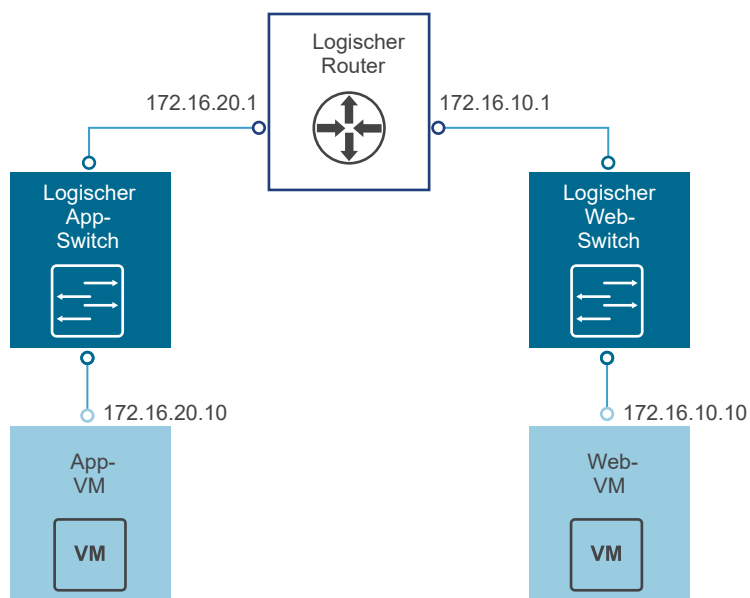
Da Sie nun über eine Transportzone verfügen, können Sie logische Switches hinzufügen.

Hinzufügen eines logischen Switch

16

Ein logischer NSX for vSphere-Switch bildet die Switching-Funktionalität (Unicast, Multicast, Broadcast) in einer virtuellen Umgebung ab, die vollständig von der zugrunde liegenden physischen Hardware entkoppelt ist. Logische Switches sind mit VLANs insofern vergleichbar, da sie Netzwerkverbindungen bereitstellen, an die virtuelle Maschinen angefügt werden können. Die VMs können dann über VXLAN miteinander kommunizieren, wenn sie mit dem gleichen logischen Switch verbunden sind. Jeder logische Switch hat eine Segment-ID, wie eine VLAN-ID. Im Gegensatz zu VLAN-IDs kann er aber bis zu 16 Millionen Segment-IDs enthalten.

Wenn Sie logische Switches hinzufügen, ist es wichtig, eine bestimmte Topologie zu berücksichtigen, die Sie erstellen. Beispiel: Die folgende einfache Topologie zeigt zwei logische Switches, die mit einem einzelnen Distributed Logical Router (DLR) verbunden sind. In diesem Diagramm ist jeder logische Switch mit einer einzelnen VM verbunden. Die beiden VMs können sich auf verschiedenen Hosts oder auf demselben Host, in verschiedenen Hostclustern oder im selben Hostcluster befinden. Wenn ein DLR die VMs nicht trennt, können sich die zugrunde liegenden IP-Adressen, die in den VMs konfiguriert sind, im selben Subnetz befinden. Wenn ein DLR diese trennt, müssen sich die IP-Adressen in den VMs in verschiedenen Subnetzen befinden (wie im Beispiel gezeigt).



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.

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. Es kann sinnvoll sein, den MAC-Lernvorgang zu aktivieren, wenn Sie virtuelle Netzwerkkarten verwenden, die VLAN-Trunking vornehmen.

Voraussetzungen

- vSphere Distributed Switches müssen konfiguriert werden.
- NSX Manager muss installiert werden.
- Controller müssen bereitgestellt werden.
- Hostcluster müssen für NSX vorbereitet werden.
- VXLAN muss konfiguriert werden.
- Ein Segment-ID-Pool muss konfiguriert werden.
- Eine Transportzone muss erstellt werden.

Verfahren



- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Wechseln Sie zu **Home > Netzwerk und Sicherheit > Logische Switches (Home > Networking & Security > Logical Switches)**:
- 3 Klicken Sie auf **Neuer logischer Switch (New Logical Switch) (+)**.
- 4 Geben Sie einen Namen und eine optionale Beschreibung für den logischen Switch ein.
- 5 Wählen Sie die Transportzone aus, in der Sie den logischen Switch erstellen möchten.

Standardmäßig übernimmt der logische Switch den Steuerungskomponenten-Modus der Replikation aus der Transportzone.

- 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 **IP-Erkennung aktivieren (Enable IP Discovery)**, um die ARP-Unterdrückung zu aktivieren.
- 8 (Optional) Klicken Sie auf **MAC-Lernvorgang aktivieren (Enable MAC learning)**.
- 9 Fügen Sie eine virtuelle Maschine an den logischen Switch an, indem Sie den Switch auswählen und auf **Virtuelle Maschine hinzufügen (Add Virtual Machine)** () klicken.
- 10 Wählen Sie eine oder mehrere virtuelle Maschinen aus und klicken Sie auf die Schaltfläche mit dem Pfeil nach rechts ().

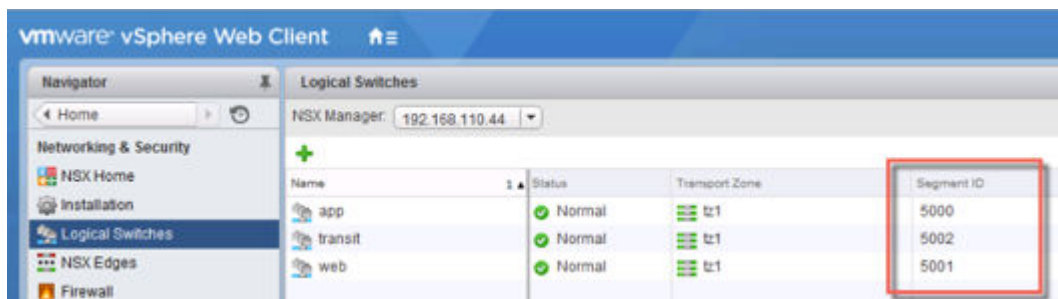
Die virtuellen Maschinen werden von „Verfügbare Objekte“ nach „Ausgewählte Objekte“ verschoben.

- 11 Klicken Sie auf **Weiter (Next)** und wählen Sie eine vNIC für jede virtuelle Maschine aus. Klicken Sie auf **Beenden (Finish)**.

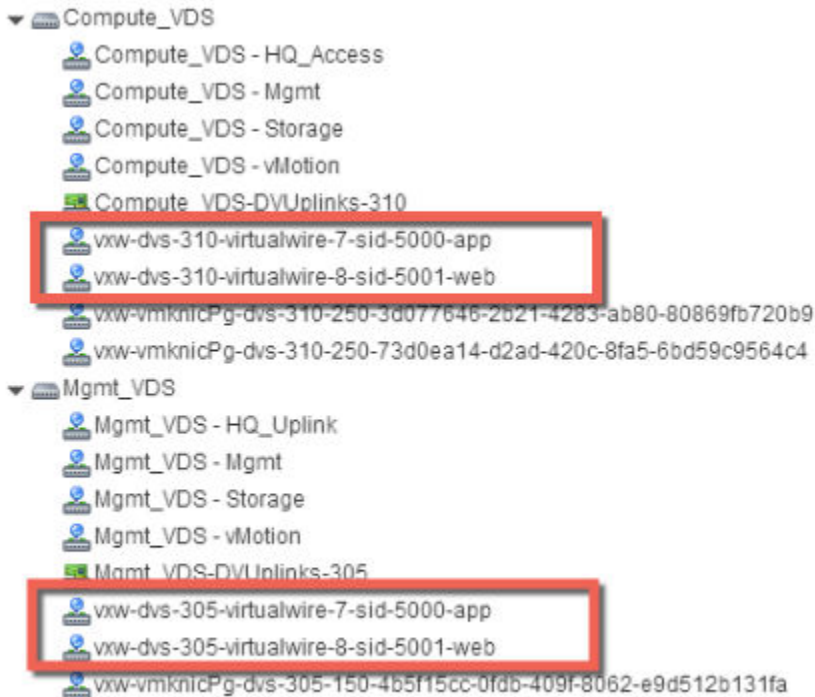
Ergebnisse

Jeder logische Switch, den Sie erstellen, empfängt eine ID aus dem Segment-ID-Pool, und es wird eine virtuelle Leitung erstellt. Eine virtuelle Leitung ist eine dvPortgroup, die in jedem vSphere Distributed Switch erstellt wird. Der Deskriptor der virtuellen Leitung enthält den Namen des logischen Switch und die Segment-ID des logischen Switch. Zugewiesene Segment-IDs werden an verschiedenen Stellen angezeigt (siehe folgende Beispiele).

In **Home > Netzwerk und Sicherheit > Logische Switches (Home > Networking & Security > Logical Switches)**:

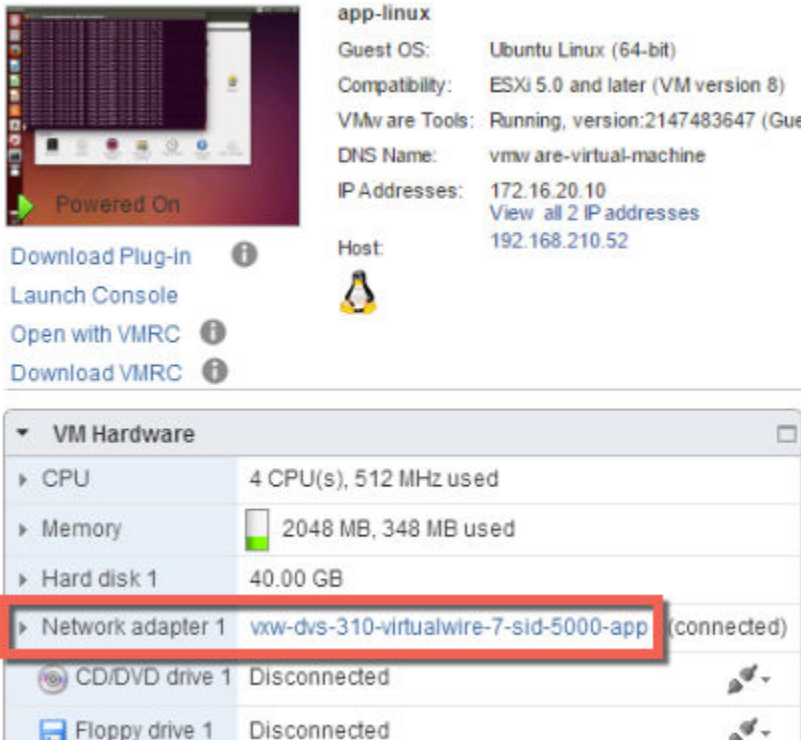


In **Home > Netzwerk (Home > Networking)**:



Hinweis: Die virtuellen Leitungen werden auf beiden vSphere Distributed Switches, Compute_VDS und Mgmt_VDS, erstellt. Grund dafür ist, dass beide dieser vSphere Distributed Switches Mitglieder der Transportzone sind, die dem Internet und den logischen Switches der Apps zugeordnet ist.

In **Home > Hosts und Clusters > VM > Übersicht (Home > Hosts and Clusters > VM > Summary)**:



Melden Sie sich bei den Hosts an, auf denen die VMs ausgeführt werden, die an den logischen Switch angefügt sind, und führen Sie die folgenden Befehle aus, um die lokale VXLAN-Konfiguration und Statusinformationen anzuzeigen.

- Zeigt hostspezifische VXLAN-Informationen an.

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

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

Hinweis Wenn mit dem `esxcli network vswitch dvs vmware vxlan`-Befehl die Fehlermeldung „Unbekannter Befehl oder Namespace“ angezeigt wird, führen Sie den `/etc/init.d/hostd restart`-Befehl auf dem Host aus und versuchen Sie es anschließend erneut.

Der VDS-Name zeigt den vSphere Distributed Switch an, an den der Host angefügt ist.

Die Segment-ID ist das von VXLAN verwendete IP-Netzwerk.

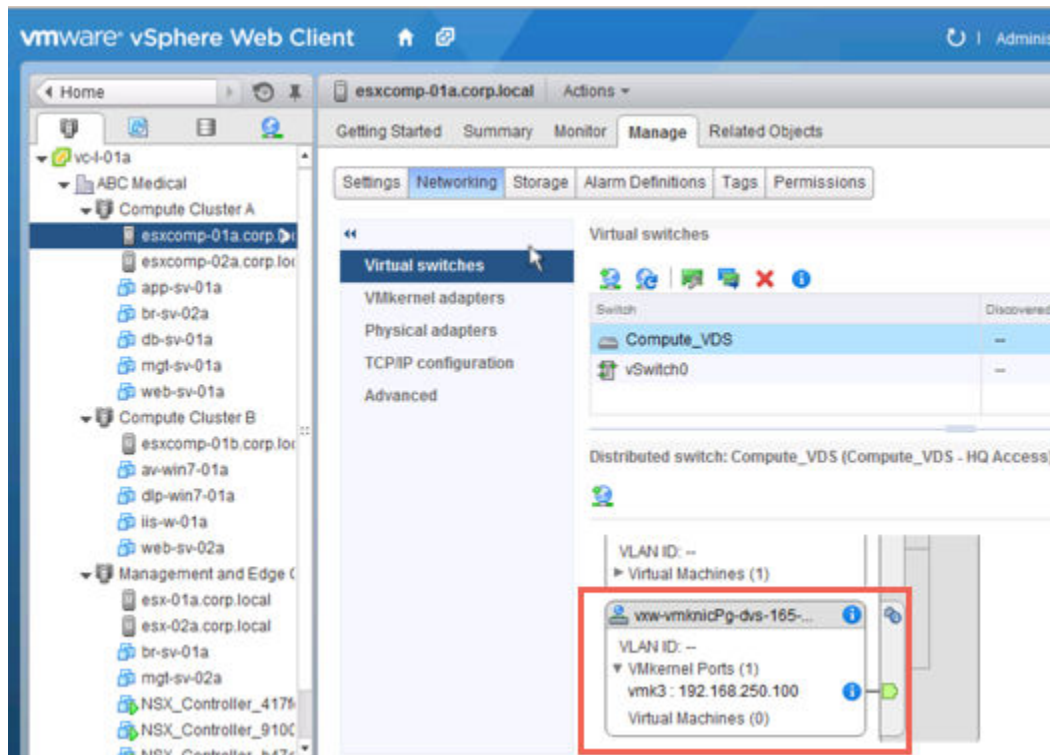
Die Gateway-ID ist die von VXLAN verwendete Gateway-IP-Adresse.

Die Gateway-MAC-Adresse lautet weiterhin `ff:ff:ff:ff:ff:ff`.

Die Netzwerkanzahl lautet weiterhin 0, es sei denn, ein DLR wird an den logischen Switch angefügt.

Die Vmknics-Anzahl sollte mit der Anzahl der an den logischen Switch angefügten VMs übereinstimmen.

- Testen Sie die Konnektivität der IP-VTEP-Schnittstelle und stellen Sie sicher, dass die MTU erhöht wurde, um die VXLAN-Kapselung zu unterstützen. Pinggen Sie die IP-Adresse der vmknics-Schnittstelle, die Sie auf der Seite **Verwalten > Netzwerk > Virtuelle Switches (Manage > Networking > Virtual switches)** des Hosts im vCenter Web Client finden.



Das Flag -d legt das DF-Bit („don't-fragment“) für IPv4-Pakete fest. Das Flag -s legt die Paketgröße fest.

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

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

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

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

Nächste Schritte

Erstellen Sie einen logischen (verteilten) Router und fügen Sie diesen an die logischen Switches an, um die Konnektivität zwischen den virtuellen Maschinen zu aktivieren, die mit verschiedenen logischen Switches verbunden sind.

Hinzufügen eines Distributed Logical Routers

17

Ein verteilter logischer Router (Distributed Logical Router, DLR) ist eine virtuelle Appliance, die die Routing-Steuerungskomponente enthält, und die Datenebene in Kernelmodulen an jeden Hypervisor-Host verteilt. Die Steuerungskomponenten-Funktion des DLR verlässt sich bei der Weiterleitung von Routing-Updates an die Kernelmodule auf den NSX Controller-Cluster.

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>.

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*.

Verfahren

- 1 Navigieren Sie auf vSphere Web Client zu **Start > Netzwerk und Sicherheit > NSX Edges (Home > Networking & Security > NSX Edges)**.
- 2 Klicken Sie auf das Symbol **Hinzufügen (Add)** (+).

- 3 Wählen Sie **Logischer (verteilter) Router (Logical (Distributed) Router)** aus und geben Sie einen Namen für das Gerät ein.

Dieser Name wird in Ihrer vCenter-Bestandsliste angezeigt. Verwenden Sie einen Namen, der über alle logischen Router eines einzelnen Mandanten hinweg eindeutig ist.

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

Sie können optional eine Beschreibung und einen Mandanten eingeben.

Beispiel:

Name and description

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

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

Name: *

Hostname:

Description:

Tenant:

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

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

- 4 (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.

- 5 (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.

- 6 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

- 7 (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.

- 8 (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 EMERGENCY ▼

Set the Edge Control Level Logging

- 9 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...	▼

10 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:

Mgmt_VDS - Mgmt

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

11 Konfigurieren Sie ein Standard-Gateway.

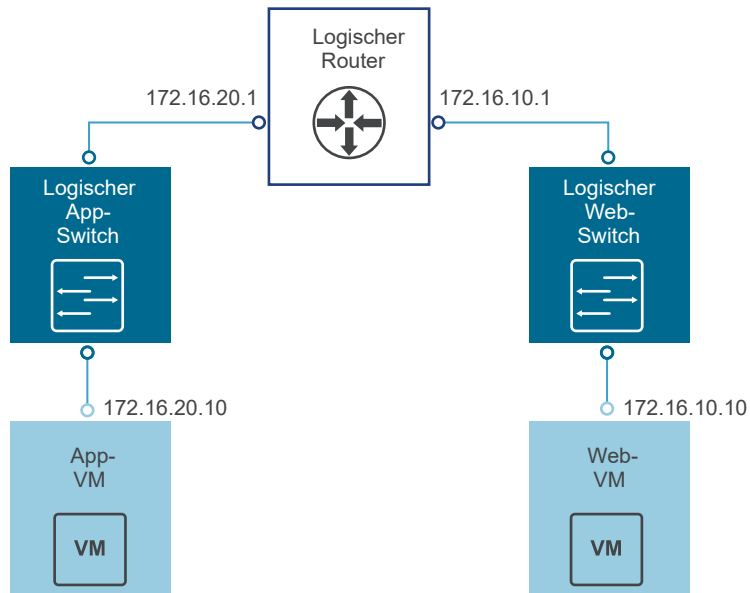
Beispiel:

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

- 12 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 pinggen 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 | vxl  | 0x1389 | 172.16.10.1/24  |
| 13880000000a | vxl  | 0x1388 | 172.16.20.1/24  |
| 138800000002 | vxl  | 0x138a | 192.168.10.2/29 |

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

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

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

VMkernel Routes:

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

- 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.

# Hinzufügen eines Edge Services Gateway

# 18

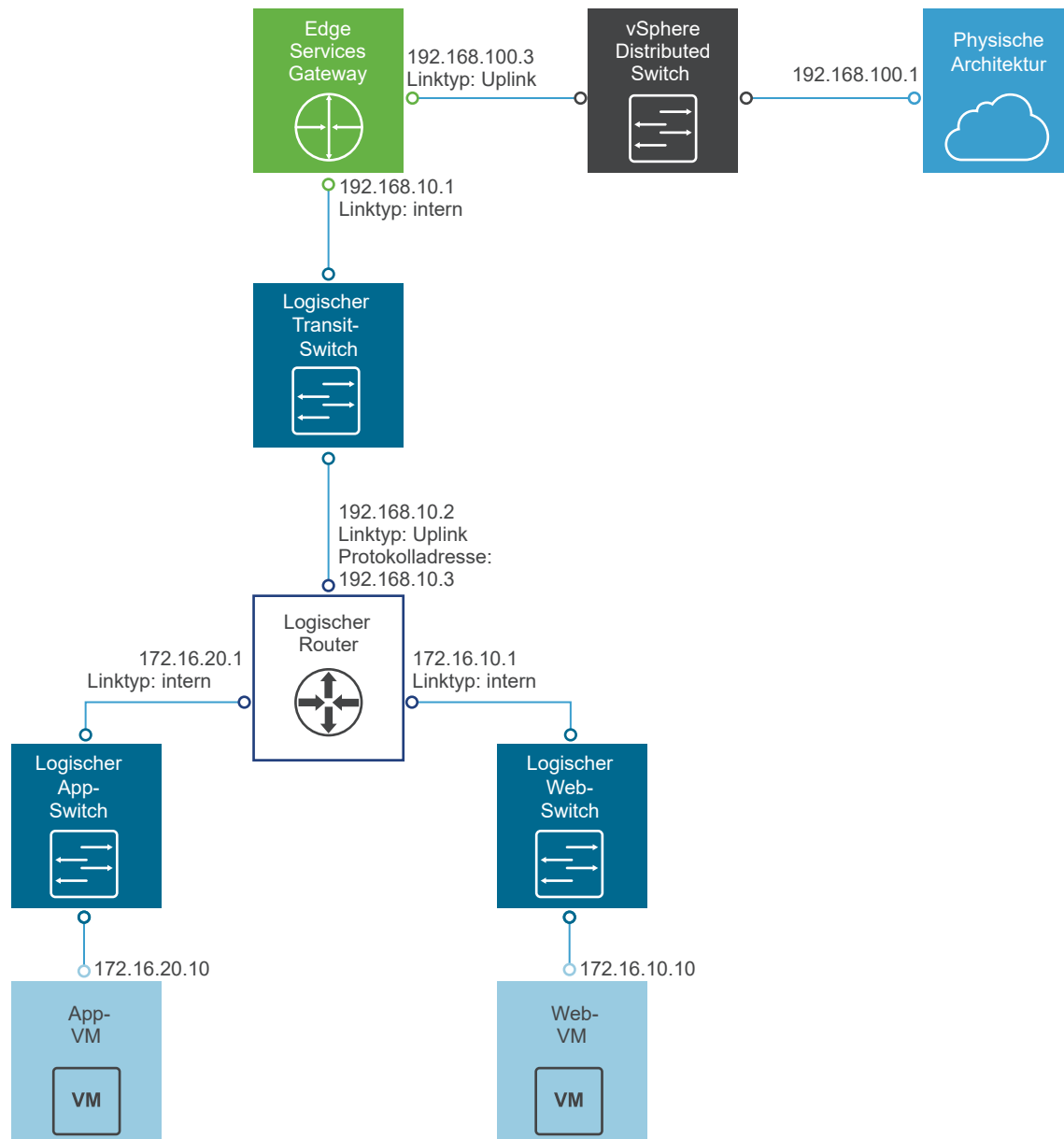
Sie können mehrere virtuelle NSX Edge Services Gateway-Appliances in einem Datacenter installieren. Jede virtuelle NSX Edge-Appliance kann über insgesamt zehn Uplink- und interne Netzwerkschnittstellen verfügen. Die internen Schnittstellen werden mit gesicherten Portgruppen verbunden und dienen als das Gateway für alle geschützten virtuellen Maschinen in der Portgruppe. Das Subnetz, das der internen Schnittstelle zugewiesen ist, kann ein öffentlich gerouteter IP-Adressbereich, 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.

In der folgenden Liste wird die Unterstützung von Funktionen nach Schnittstellenart (intern und Uplink) in einem ESG beschrieben.

- DHCP: wird nicht in einer Uplink-Schnittstelle unterstützt.
- DNS-Weiterleitung: wird nicht in einer Uplink-Schnittstelle unterstützt.
- HA: wird nicht in einer Uplink-Schnittstelle unterstützt, erfordert mindestens eine interne Schnittstelle.
- SSL VPN: Listener-IP muss zur Uplink-Schnittstelle gehören.
- IPSec-VPN: Listener-IP muss zur Uplink-Schnittstelle gehören.
- L2 VPN: Es können nur interne Netzwerke ausgeweitet werden.

Die folgende Abbildung zeigt eine Beispieltopologie mit einer Uplink-Schnittstelle von ESG, die mit der physischen Infrastruktur durch den vSphere Distributed Switch verbunden ist, und der internen Schnittstelle von ESG, die mit einem NSX Logical Router durch einen NSX Logical Transit Switch verbunden ist.



Mehrere externe IP-Adressen können für Load-Balancing-, Site-to-Site-VPN- und NAT-Dienste konfiguriert werden.

### Voraussetzungen

- Ihnen muss die Rolle „Enterprise-Administrator“ oder „NSX-Administrator“ zugewiesen worden sein.
- Stellen Sie sicher, dass der Ressourcenpool genug Kapazität für die Bereitstellung der virtuellen Edge Services Gateway (ESG)-Appliance aufweist. Weitere Informationen dazu finden Sie unter [Systemvoraussetzungen für NSX](#).
- Stellen Sie sicher, dass die Hostcluster, auf denen die NSX Edge-Appliance installiert wird, für NSX vorbereitet ist. Informationen dazu erhalten Sie unter „Vorbereiten der Hostcluster für NSX“ in der Dokumentation *Installationshandbuch für NSX*.

## Verfahren

- 1 Navigieren Sie in vCenter zu **Home > Networking & Security > NSX Edges** und klicken Sie auf das Symbol **Hinzufügen (Add)** (+).

- 2 Wählen Sie **Edge Services Gateway** aus und geben Sie einen Namen für das Gerät ein.

Dieser Name wird in Ihrer vCenter-Bestandsliste angezeigt. Der Name muss über alle ESGs 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 auch eine Beschreibung und einen Mandanten eingeben und „High Availability“ aktivieren.

Beispiel:

The screenshot shows the 'New NSX Edge' configuration window. On the left, a sidebar lists steps: 1 Name and description (selected), 2 Settings, 3 Configure deployment, 4 Configure interfaces, 5 Default gateway settings, 6 Firewall and HA, and 7 Ready to complete. The main area is titled 'Name and description'. Under 'Install Type', 'Edge Services Gateway' is selected with a radio button, and 'Logical (Distributed) Router' is unselected. Below this, the 'Name' field is populated with 'ESG-1', while 'Hostname' and 'Description' are empty. The 'Tenant' field is also empty. At the bottom, the 'Deploy NSX Edge' checkbox is checked, and the 'Enable High Availability' checkbox is unchecked. Navigation buttons 'Back', 'Next', 'Finish', and 'Cancel' are at the bottom right.

- 3 Geben Sie ein Kennwort für das ESG ein und bestätigen Sie es.

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
- 4 (Optional) Aktivieren Sie SSH, hohe Verfügbarkeit, automatische Regelgenerierung und FIPS-Modus, und legen Sie die Protokollierungsebene fest.

Wenn Sie die automatische Regelerstellung nicht aktivieren, müssen Sie die Firewall-, NAT- und Routing-Konfiguration manuell hinzufügen, um den Steuerungsdatenverkehr für bestimmte NSX Edge-Dienste wie beispielsweise Load Balancing, VPN zu ermöglichen. Die Option „Automatische Regelerstellung“ erstellt keine Regeln für Datenkanal-Datenverkehr.

Standardmäßig sind SSH und High Availability deaktiviert und die automatische Regelerstellung ist aktiviert.

Der FIPS-Modus ist standardmäßig deaktiviert.

Als Protokollierungsebene ist standardmäßig „Notfall“ eingestellt.

Beispiel:

**New NSX Edge**

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

**Settings**

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

User Name: \* admin

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

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

☒ Enable SSH access

☒ Enable FIPS mode

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

Edge Control Level Logging **EMERGENCY**

[Set the Edge Control Level Logging](#)

Back Next Finish Cancel

- 5 Wählen Sie die Größe der NSX Edge-Instanz basierend auf den Systemressourcen aus.

Das **große (Large)**NSX Edge verfügt über mehr CPU, Arbeitsspeicher und Festplattenspeicher als das **kompakte (Compact)**NSX Edge und unterstützt eine größere Anzahl an gleichzeitigen SSL VPN-Plus-Benutzern. Das **sehr große (X-Large)**NSX Edge eignet sich für Umgebungen, die über einen Load Balancer mit Millionen von gleichzeitig ausgeführten Sitzungen verfügen. Das Quad Large NSX Edge wird bei hohem Durchsatz empfohlen und benötigt eine hohe Verbindungsrate.

Weitere Informationen dazu finden Sie unter [Systemvoraussetzungen für NSX](#).

- 6 Erstellen Sie eine Edge-Appliance.

Geben Sie die Einstellungen für die virtuelle ESG-Appliance ein, die zur vCenter-Bestandsliste hinzugefügt wird. Wenn Sie bei der Installation von NSX Edge keine Appliance hinzufügen, bleibt NSX Edge so lange im Offline-Modus, bis Sie eine Appliance hinzugefügt haben.

Wenn HA aktiviert ist, können Sie zwei Appliances hinzufügen. Wenn Sie eine einzelne Appliance hinzufügen, repliziert NSX Edge deren Konfiguration für die Standby-Appliance und stellt sicher, dass sich die zwei virtuellen HA-NSX Edge-Maschinen auch dann nicht auf demselben ESX-Host befinden, wenn Sie DRS und vMotion verwendet haben (es sei denn, Sie migrieren sie per vMotion manuell auf denselben Host). Damit HA ordnungsgemäß funktioniert, müssen Sie beide Appliances in einem gemeinsam verwendeten Datenspeicher bereitstellen.

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... ▼

- 7 Wählen Sie **NSX Edge bereitstellen (Deploy NSX Edge)** aus, um den Edge in einem bereitgestellten Modus hinzuzufügen. Sie müssen Appliances und Schnittstellen für die Edge-Instanz konfigurieren, bevor sie bereitgestellt werden kann.

- 8 Konfigurieren Sie Schnittstellen.

Auf ESGs werden sowohl IPv4- als auch IPv6-Adressen unterstützt.

Sie müssen mindestens eine interne Schnittstelle hinzufügen, damit HA funktioniert.

Eine Schnittstelle kann über mehrere nicht überlappende Subnetze verfügen.

Wenn Sie mehr als eine IP-Adresse für eine Schnittstelle eingeben, können Sie die primäre IP-Adresse auswählen. Eine Schnittstelle kann eine primäre und mehrere sekundäre IP-Adressen aufweisen. NSX Edge betrachtet die primäre IP-Adresse als Quelladresse für lokal generierten Datenverkehr, wie z. B. Remote-Syslog- und Operator-initiierte Pings.

Sie müssen der Schnittstelle zuerst eine IP-Adresse hinzufügen, bevor Sie sie für jede beliebige Funktionskonfiguration verwenden können.

Sie können auch die MAC-Adresse für die Schnittstelle hinzufügen.

Wenn Sie die MAC-Adresse später mithilfe des API-Aufrufs ändern, müssen Sie das Edge nach der Änderung der MAC-Adresse erneut bereitstellen.

Wenn HA aktiviert ist, können Sie optional zwei Verwaltungs-IP-Adressen im CIDR-Format eingeben. Die Taktsignale der zwei virtuellen NSX Edge-HA-Maschinen werden über diese Verwaltungs-IP-Adressen übertragen. Die Verwaltungs-IP-Adressen müssen sich in demselben L2/Subnetz befinden und müssen untereinander kommunizieren können.

Sie können auch den MTU-Wert ändern.

Aktivieren Sie Proxy-ARP, wenn das ESG ARP-Anforderungen beantworten soll, die für andere Maschinen bestimmt sind. Dies ist dann zum Beispiel hilfreich, wenn Sie über dasselbe Subnetz auf beiden Seiten einer WAN-Verbindung verfügen.

Aktivieren Sie die ICMP-Umleitung, um Routing-Informationen an Hosts weiterzuleiten.

Aktivieren Sie umgekehrte Pfadfilter, um zu die Erreichbarkeit der Quelladresse in weitergeleiteten Paketen zu überprüfen. Im aktivierten Modus muss das Paket auf der Schnittstelle empfangen werden, die der Router zum Weiterleiten des Rückgabepakets verwenden würde. Im Loose-Modus muss die Quelladresse in der Routing-Tabelle angezeigt werden.

Konfigurieren Sie Fence-Parameter, wenn Sie IP- und MAC-Adressen über verschiedene umgrenzende Umgebungen hinweg wiederverwenden möchten. In einer Cloud-Verwaltungsplattform (Cloud Management Platform, CMP) können Sie mit Fencing mehrere Cloud-Instanzen gleichzeitig mit denselben IP- und MAC-Adressen ausführen, die vollständig isoliert oder „umgrenzt“ sind.

Beispiel:



**Edit NSX Edge Interface** ?

VNIC#: 1

Name: \* Internal

Type: ☒ Internal ☐ Uplink

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

Connectivity Status: ☒ Connected ☐ Disconnected

Configure subnets

+ / ✖

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

MAC Addresses:

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

MTU:

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

Fence Parameters:

Example: ethernet0.filter1.param1=1

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

Das folgende Beispiel zeigt zwei Schnittstellen. Eine Schnittstelle, die das ESG mit der Außenwelt durch eine Uplink-Portgroup in einem vSphere Distributed Switch verbindet, und eine zweite Schnittstelle, die das ESG mit einem Logical Transit Switch verbindet, an den auch ein Distributed Logical Router angefügt ist.

**New NSX Edge**

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

**Configure interfaces**

Configure interfaces of this NSX Edge

+ ✎ ✕

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

Back Next Finish Cancel

## 9 Konfigurieren Sie ein Standard-Gateway.

Sie können den MTU-Wert bearbeiten, er darf jedoch nicht höher als der konfigurierte MTU-Wert für die Schnittstelle sein.

Beispiel:

**New NSX Edge**

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

**Default gateway settings**

☒ Configure Default Gateway

vNIC: \* uplink

Gateway IP: \* 192.168.100.2

MTU: 1500

Back Next Finish Cancel

**10** Konfigurieren Sie die Firewallrichtlinie, die Protokollierung und HA-Parameter.

**Vorsicht** Wenn Sie keine Firewallrichtlinie konfigurieren, ist die Standardrichtlinie gesetzt, um jeglichen Datenverkehr zu verweigern.

Standardmäßig sind Protokolle auf allen neuen NSX Edge-Appliances aktiviert. Die Standardprotokollierungsebene ist HINWEIS. Wenn Protokolle lokal im ESG gespeichert sind, werden durch die Protokollierung möglicherweise zu viele Protokolle generiert und die Leistung von NSX Edge wird beeinträchtigt. Aus diesem Grund ist es empfehlenswert, Remote-Syslog-Server zu konfigurieren und alle Protokolle an eine zentrale Stelle zur Analyse und Überwachung weiterzuleiten.

Wenn Sie High Availability aktiviert haben, vervollständigen Sie den HA-Bereich. Standardmäßig wählt HA automatisch eine interne Schnittstelle aus und weist automatisch verbindungslokale IP-Adressen zu. NSX Edge unterstützt zwei virtuelle Maschinen für High Availability und beide Maschinen werden mithilfe von Benutzerkonfigurationen auf dem neuesten Stand gehalten. Falls ein Taktsignalfehler auf der primären virtuellen Maschine auftritt, wird der Zustand der sekundären

virtuellen Maschine in „aktiv“ geändert. Folglich ist immer eine virtuelle NSX Edge-Maschine im Netzwerk aktiv. NSX Edge repliziert die Konfiguration der primären Appliance für die Standby-Appliance und stellt sicher, dass sich die zwei virtuellen HA-NSX Edge-Maschinen auch dann nicht auf demselben ESX-Host befinden, wenn Sie DRS und vMotion verwendet haben. Zwei virtuelle Maschinen werden auf vCenter in demselben Ressourcenpool und Datenspeicher wie die von Ihnen konfigurierte Appliance bereitgestellt. Die IP-Adressen von lokalen Links werden virtuellen HA-Maschinen in der NSX Edge HA zugewiesen, damit sie untereinander kommunizieren können. Wählen Sie die interne Schnittstelle aus, für die HA-Parameter konfiguriert werden sollen. Wenn Sie BELIEBIG für die Schnittstelle auswählen, aber keine internen Schnittstellen konfiguriert sind, wird auf der Benutzeroberfläche ein Fehler angezeigt. Zwei Edge-Appliances werden erstellt, aber da keine interne Schnittstelle konfiguriert ist, bleibt die neue Edge-Appliance im Standby-Modus und HA wird deaktiviert. Sobald eine interne Schnittstelle konfiguriert ist, wird HA in der Edge-Appliance aktiviert. Geben Sie den Zeitraum (in Sekunden) ein, nach dem die primäre Appliance als inaktiv betrachtet wird und die Backup-Appliance die Arbeit übernimmt, falls die Backup-Appliance kein Taktsignal von der primären Appliance erhält. Das Standardintervall beträgt 15 Sekunden. Sie können auch zwei Verwaltungs-IP-Adressen im CIDR-Format eingeben, die die IP-Adressen der lokalen Links überschreiben, die den virtuellen HA-Maschinen zugewiesen sind. Vergewissern Sie sich, dass sich die Verwaltungs-IP-Adressen nicht mit den IP-Adressen überschneiden, die für andere Schnittstellen verwendet wurden, und dass sie das Routing des Netzwerkdatenverkehrs nicht stören. Sie sollten keine IP-Adresse verwenden, die an einer anderen Stelle im Netzwerk existiert, auch wenn das Netzwerk nicht direkt mit dem NSX Edge verbunden ist.

Beispiel:

**New NSX Edge**

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

### Firewall and HA

☒ **Configure Firewall default policy**

Default Traffic Policy: ☒ Accept ☐ Deny

Logging: ☐ Enable ☒ Disable

#### Configure HA parameters

Configuring HA parameters is mandatory for HA to work.

vNIC: \* internal

Declare Dead Time: 15 (seconds)

Management IPs:

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

Back Next Finish Cancel

## Ergebnisse

Nach der Bereitstellung von ESG navigieren Sie zur Ansicht „Hosts und Cluster“ und öffnen Sie die Konsole der virtuellen Edge-Appliance. Stellen Sie in der Konsole sicher, dass Sie die verbundenen Schnittstellen pingen können.

## 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*.

Sie können jetzt Routing konfigurieren, um die Konnektivität von externen Geräten zu Ihren VMs zu ermöglichen.

# Konfigurieren von OSPF auf einem logischen (Distributed) Router

# 19

Durch das Konfigurieren von OSPF auf einem logischen Router wird VM-Konnektivität über logische Router hinweg und von logischen Routern zu Edge Services Gateways (ESGs) aktiviert.

OSPF-Routing-Richtlinien bieten einen dynamischen Vorgang des Datenverkehrs-Load-Balancer zwischen Routen mit gleichen Kosten.

Ein OSPF-Netzwerk wird in Routing-Areas unterteilt, um den Datenverkehrsfluss zu optimieren und die Größe der Routing-Tabellen zu begrenzen. Eine Area ist eine logische Sammlung von OSPF-Netzwerken, Routern und Links, die über dieselbe Area-Identifikation verfügen.

Areas werden anhand einer Area-ID identifiziert.

## Voraussetzungen

Es muss eine Router-ID konfiguriert werden, wie unter [OSPF wird im logischen \(verteilten\) Router konfiguriert](#) dargestellt.

Wenn Sie eine Router-ID aktivieren, wird das Feld standardmäßig mit der Uplink-Schnittstelle des logischen Routers ausgefüllt.

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf einen logischen Router.
- 4 Klicken Sie auf **Routing** und anschließend auf **OSPF**.
- 5 Aktivieren Sie OSPF.
  - a Klicken Sie auf **Bearbeiten (Edit)** in der oberen rechten Ecke des Fensters und dann auf **OSPF aktivieren (Enable OSPF)**.
  - b Geben Sie in **Weiterleitungsadresse (Forwarding Address)** eine IP-Adresse ein, die von dem Router-Datenpfad-Modul in den Hosts verwendet wird, um Datenpfadpakete weiterzuleiten.
  - c Geben Sie in **Protokolladresse (Protocol Address)** eine eindeutige IP-Adresse innerhalb desselben Subnetzes wie in **Weiterleitungsadresse (Forwarding Address)** ein. Die Protokolladresse wird vom Protokoll zum Gestalten benachbarter Bereiche mit den Peers verwendet.

## 6 Konfigurieren Sie die OSPF-Areas.

- a Sie können auch die „Not-So-Stubby-Area“ (NSSA) 51 löschen, die standardmäßig konfiguriert wird.
- b Klicken Sie in **Area Definitions** auf das Symbol **Hinzufügen (Add)**.
- c Geben Sie eine Area-ID ein. NSX Edge unterstützt eine Area-ID in Form einer Dezimalzahl. Gültige Werte sind 0 bis 4294967295.
- d Wählen Sie unter **Typ (Type)** die Option **Normal** oder **NSSA** aus.

NSSAs verhindert das Überfluten von AS-externen Verbindungsstatus-Ankündigungen (LSAs) in NSSAs. Sie verwenden das Standardrouting zu externen Zielen. Daher müssen NSSAs am Rand einer OSPF-Routing-Domäne abgelegt werden. NSSA kann externe Routen in die OSPF-Routing-Domäne importieren, sodass der Transit-Dienst für kleine Routing-Domänen bereitgestellt wird, die nicht Teil der OSPF-Routing-Domäne sind.

## 7 (Optional) Wählen Sie den Typ der **Authentifizierung (Authentication)**. OSPF führt die Authentifizierung auf der Area-Ebene aus.

Daher müssen alle Router innerhalb einer Area über dieselbe Authentifizierung und das entsprechend konfigurierte Kennwort verfügen. Damit die MD5-Authentifizierung funktionieren kann, müssen sowohl der Empfangs- als auch der Übertragungsrouten über denselben MD5-Schlüssel verfügen.

- a **Keine (None)**: Keine Authentifizierung ist erforderlich; dies ist der Standardwert.
- b **Kennwort (Password)**: Bei dieser Authentifizierungsmethode wird ein Kennwort im übertragenen Paket eingeschlossen.
- c **MD5**: Diese Authentifizierungsmethode verwendet die MD5-Verschlüsselung (Message Digest Type 5). Ein MD5-Prüfsummenwert ist im übertragenen Paket eingeschlossen.
- d Geben Sie für den Authentifizierungstyp **Kennwort (Password)** oder **MD5** das Kennwort bzw. den MD5-Schlüssel ein.

---

### Wichtig

- Wenn NSX Edge mit aktiviertem OSPF Graceful Restart für HA konfiguriert ist und MD5 für die Authentifizierung verwendet wird, kann OSPF nicht ordnungsgemäß neu gestartet werden. Nachbarschaften werden erst nach dem Kulanzzzeitraum auf den OSPF-Hilfsknoten gebildet.
  - Bei aktiviertem FIPS-Modus können Sie die **MD5**-Authentifizierung nicht konfigurieren.
  - NSX for vSphere verwendet immer einen Schlüssel-ID-Wert von 1. Jedes Gerät, das nicht von NSX for vSphere verwaltet wird und als Peer eines Edge Services Gateways oder logischen verteilten Routers fungiert, muss für die Verwendung einer Schlüssel-ID mit dem Wert 1 konfiguriert werden, wenn MD5-Authentifizierung verwendet wird. Andernfalls kann keine OSPF-Sitzung hergestellt werden.
-



**8** Ordnen Sie die Schnittstellen den Areas :zu.

- a Klicken Sie in **Zuordnung von Area zu Schnittstelle (Area to Interface Mapping)** auf das Symbol **Hinzufügen (Add)**, um die Schnittstelle zuzuordnen, die zur OSPF-Area gehört.
- b Wählen Sie die Schnittstelle, die Sie zuordnen möchten, und der OSPF-Area, der sie zugeordnet werden soll.

**9** (Optional) Bearbeiten Sie bei Bedarf die standardmäßigen OSPF -Einstellungen.

In den meisten Fällen wird empfohlen, die standardmäßigen OSPF-Einstellungen beizubehalten. Wenn Sie Änderungen an den Einstellungen vornehmen, stellen Sie sicher, dass die OSPF-Peers dieselben Einstellungen verwenden.

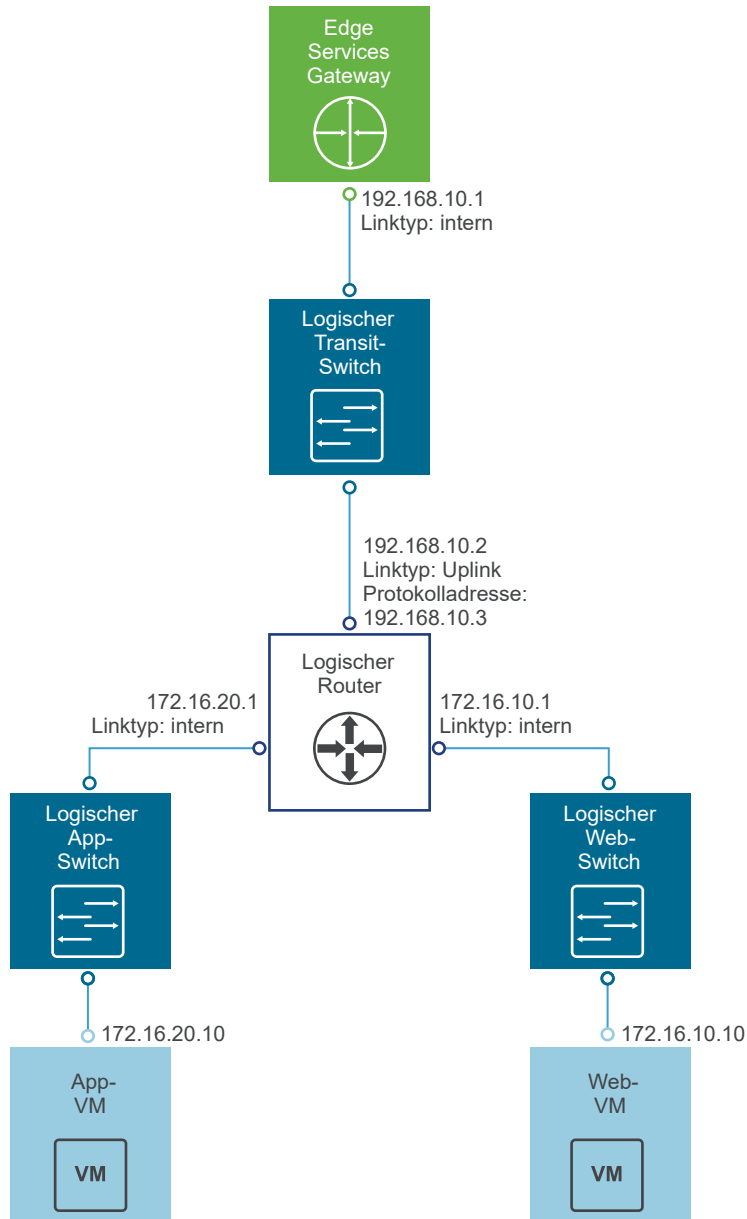
- a **Hallo-Intervall (Hello Interval)** zeigt das Standardintervall zwischen Hallo-Paketen an, die über die Schnittstelle gesendet werden.
- b **Ausfallintervall (Dead Interval)** zeigt das Standardintervall an, während dessen mindestens ein Hallo-Paket von einem Nachbarn empfangen werden muss, bevor der Router den Nachbarn als ausgefallen einstuft.
- c **Priorität (Priority)** zeigt die Standardpriorität der Schnittstelle an. Die Schnittstelle mit der höchsten Priorität ist der festgelegte Router.
- d **Kosten (Cost)** einer Schnittstelle zeigt den Standard-Overhead an, der für das Senden von Paketen über die Schnittstelle erforderlich ist. Die Kosten einer Schnittstelle sind umgekehrt proportional zur Bandbreite dieser Schnittstelle. Je größer die Bandbreite ist, desto geringer sind die Kosten.

**10** Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.

## Beispiel: OSPF wird im logischen (verteilten) Router konfiguriert

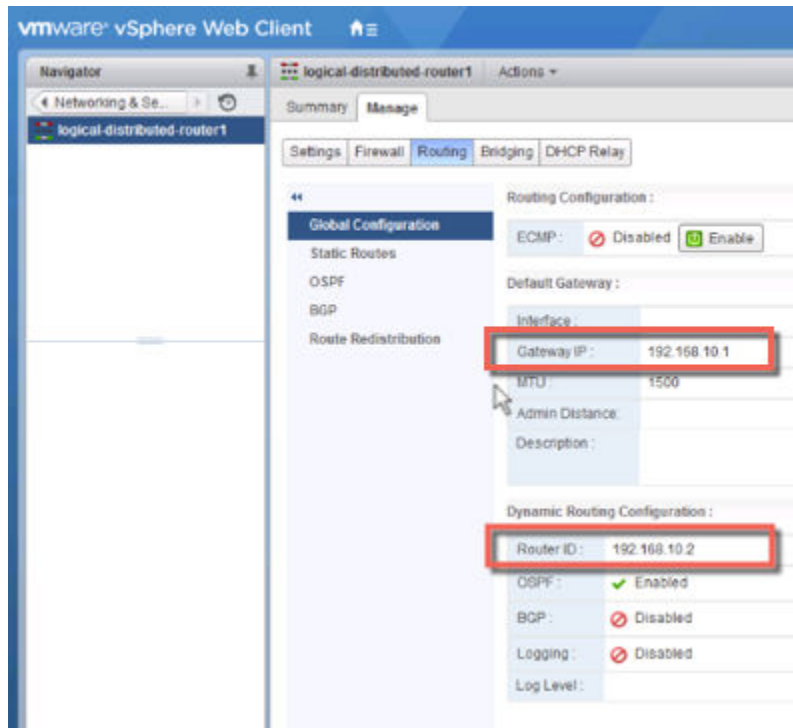
Ein einfaches NSX for vSphere-Szenario, bei dem OSPF verwendet wird, ist, wenn ein logischer Router (DLR) und ein Edge Services Gateway (ESG) OSPF-Nachbarn sind, wie hier gezeigt.

Abbildung 19-1. NSX for vSphere-Topologie

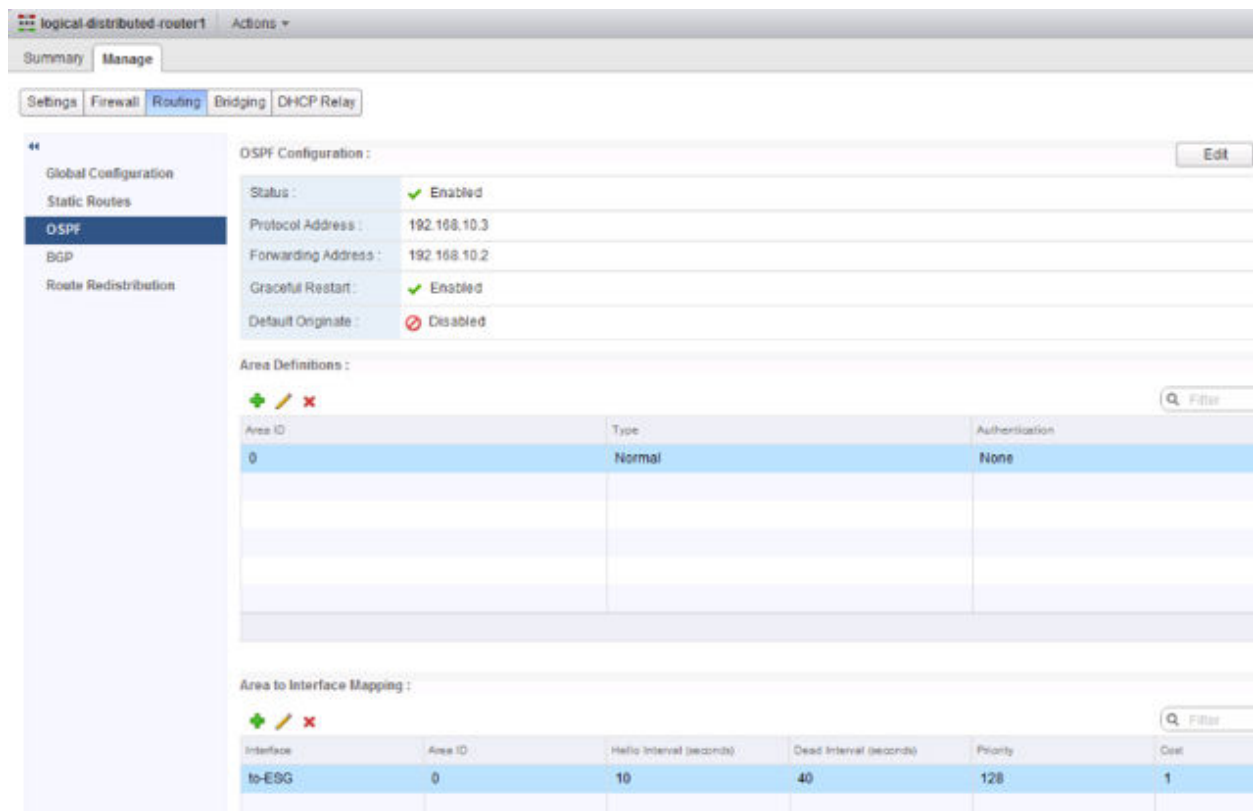


Im folgenden Bildschirm ist das Standard-Gateway des logischen Routers die IP-Adresse der internen Schnittstelle von ESG (192.168.10.1).

Die Router-ID ist die Uplink-Schnittstelle des logischen Routers – in anderen Worten, die IP-Adresse, die ESG gegenüberliegt (192.168.10.2).



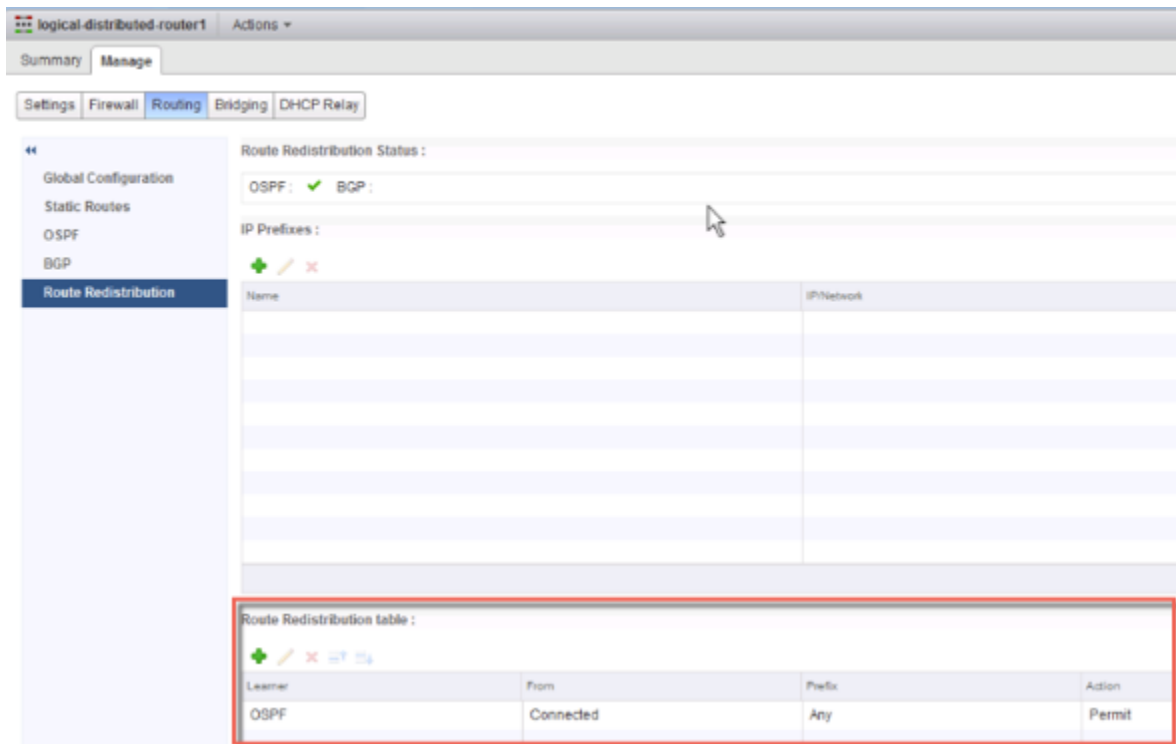
Die Konfiguration des logischen Routers verwendet 192.168.10.2 als Weiterleitungsadresse. Die Protokolladresse kann eine beliebige IP-Adresse sein, die sich im selben Subnetz befindet und an keiner anderen Stelle verwendet wird. In diesem Fall ist 192.168.10.3 konfiguriert. Die konfigurierte Area-ID ist 0, und die Uplink-Schnittstelle (die Schnittstelle, die ESG gegenüberliegt) wird dieser Area zugeordnet.



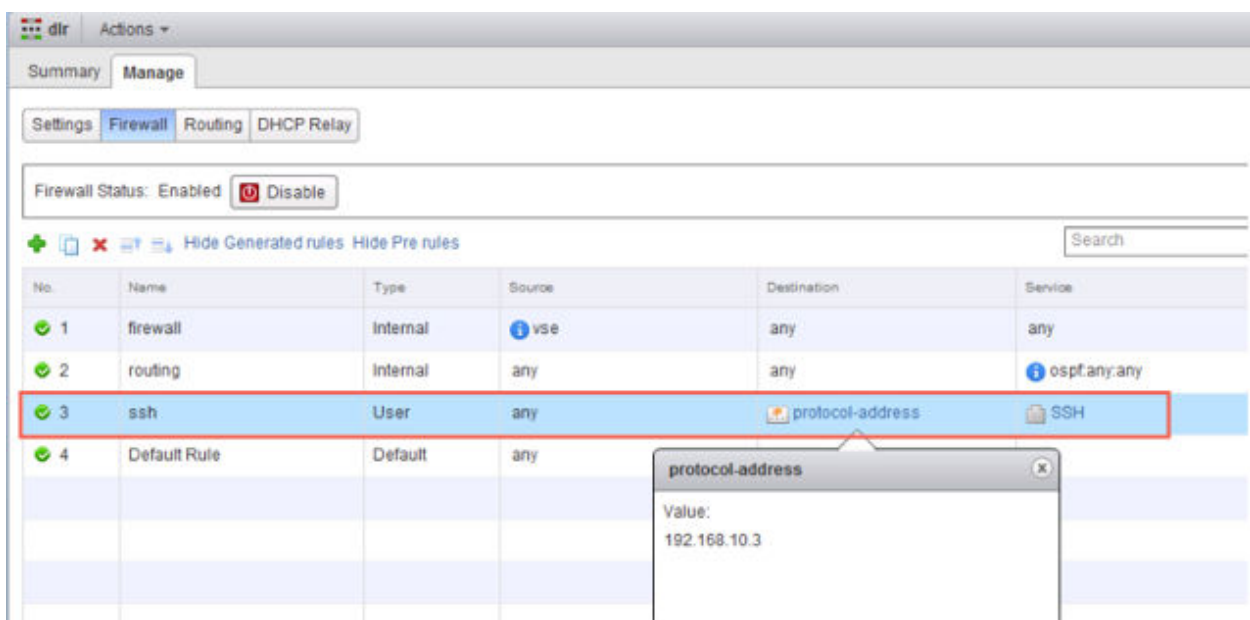
## Nächste Schritte

Stellen Sie sicher, dass durch die Route Redistribution und die Firewallkonfiguration die richtigen Routen angekündigt werden können.

In diesem Beispiel werden die verbundenen Routen (172.16.10.0/24 und 172.16.20.0/24) nach OSPF angekündigt.



Wenn Sie SSH beim Erstellen des logischen Routers aktiviert haben, müssen Sie auch einen Firewallfilter konfigurieren, der SSH zur Protokolladresse des logischen Routers zulässt. Beispiel:



# Konfigurieren von OSPF in einem Edge Services Gateway

# 20

Durch das Konfigurieren von OSPF in einem Edge Services Gateway (ESG) kann das ESG lernen und Routen ankündigen. Der gängigste Einsatzbereich von OSPF in einer ESG ist die Verknüpfung zwischen dem ESG und einem logischen (Distributed) Router. Dadurch kann das ESG in Bezug auf die logischen Schnittstellen (LIFs) lernen, die mit dem logischen Router verbunden sind. Dieses Ziel kann mit OSPF, IS-IS, BGP oder statischem Routing erreicht werden.

OSPF-Routing-Richtlinien bieten einen dynamischen Vorgang des Datenverkehrs-Load-Balancer zwischen Routen mit gleichen Kosten.

Ein OSPF-Netzwerk wird in Routing-Areas unterteilt, um den Datenverkehrsfluss zu optimieren und die Größe der Routing-Tabellen zu begrenzen. Eine Area ist eine logische Sammlung von OSPF-Netzwerken, Routern und Links, die über dieselbe Area-Identifikation verfügen.

Areas werden anhand einer Area-ID identifiziert.

## Voraussetzungen

Es muss eine Router-ID konfiguriert werden, wie unter [OSPF wird in einem Edge Services Gateway konfiguriert](#) dargestellt.

Wenn Sie eine Router-ID aktivieren, wird das Feld standardmäßig mit der IP-Adresse der Uplink-Schnittstelle von ESG ausgefüllt.

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf ein ESG.
- 4 Klicken Sie auf **Routing** und anschließend auf **OSPF**.
- 5 Aktivieren Sie OSPF.
  - a Klicken Sie auf **Bearbeiten (Edit)** in der oberen rechten Ecke des Fensters und dann auf **OSPF aktivieren (Enable OSPF)**.
  - b (Optional) Klicken Sie auf **Graceful Restart aktiviert (Enable Graceful Restart)**, damit die Paketweiterleitung beim Neustart von OSPF-Diensten nicht unterbrochen wird.
  - c (Optional) Klicken Sie auf **Default Originate aktiviert (Enable Default Originate)**, damit sich ESG selbst als ein Standard-Gateway bei seinen Peers ankündigen kann.

## 6 Konfigurieren Sie die OSPF-Areas.

- a (Optional) Löschen Sie die „Not-So-Stubby-Area“ (NSSA) 51, die standardmäßig konfiguriert wird.
- b Klicken Sie in **Area Definition (Area Definitions)** auf das Symbol **Hinzufügen (Add)**.
- c Geben Sie eine Area-ID ein. NSX Edge unterstützt eine Area-ID in Form einer IP-Adresse oder Dezimalzahl.
- d Wählen Sie unter **Typ (Type)** die Option **Normal** oder **NSSA** aus.

NSSAs verhindert das Überfluten von AS-externen Verbindungsstatus-Ankündigungen (LSAs) in NSSAs. Sie verwenden das Standardrouting zu externen Zielen. Daher müssen NSSAs am Rand einer OSPF-Routing-Domäne abgelegt werden. NSSA kann externe Routen in die OSPF-Routing-Domäne importieren, sodass der Transit-Dienst für kleine Routing-Domänen bereitgestellt wird, die nicht Teil der OSPF-Routing-Domäne sind.

- 7 (Optional) Wenn Sie für den Typ **NSSA** auswählen, wird das Feld **NSSA-Konvertierungsrolle (NSSA Translator Role)** angezeigt. Aktivieren Sie das Kontrollkästchen **Immer (Always)**, um Typ-7-LSAs in Typ-5-LSAs zu konvertieren. Alle Typ-7-LSAs werden durch den NSSA-Typ in Typ-5-LSAs konvertiert.

- 8 (Optional) Wählen Sie den Typ der **Authentifizierung (Authentication)**. OSPF führt die Authentifizierung auf der Area-Ebene aus.

Daher müssen alle Router innerhalb einer Area über dieselbe Authentifizierung und das entsprechend konfigurierte Kennwort verfügen. Damit die MD5-Authentifizierung funktionieren kann, müssen sowohl der Empfangs- als auch der Übertragungsrouten über denselben MD5-Schlüssel verfügen.

- a **Keine (None)**: Keine Authentifizierung ist erforderlich; dies ist der Standardwert.
- b **Kennwort (Password)**: Bei dieser Authentifizierungsmethode wird ein Kennwort im übertragenen Paket eingeschlossen.
- c **MD5**: Diese Authentifizierungsmethode verwendet die MD5-Verschlüsselung (Message Digest Type 5). Ein MD5-Prüfsummenwert ist im übertragenen Paket eingeschlossen.
- d Geben Sie für den Authentifizierungstyp **Kennwort (Password)** oder **MD5** das Kennwort bzw. den MD5-Schlüssel ein.

---

### Hinweis

- Bei aktiviertem FIPS-Modus können Sie die **MD5**-Authentifizierung nicht konfigurieren.
  - NSX verwendet immer einen Schlüssel-ID-Wert von 1. Jedes Nicht-NSX-Gerät mit einem Peering mit einem NSX Edge oder einem Distributed Logical Router muss für die Verwendung eines Schlüssel-ID-Werts von 1 konfiguriert sein, wenn die MD5-Authentifizierung verwendet wird. Ansonsten wird keine OSPF-Sitzung eingerichtet.
-

**9** Ordnen Sie die Schnittstellen den Areas :zu.

- a Klicken Sie in **Zuordnung von Area zu Schnittstelle (Area to Interface Mapping)** auf das Symbol **Hinzufügen (Add)**, um die Schnittstelle zuzuordnen, die zur OSPF-Area gehört.
- b Wählen Sie die Schnittstelle, die Sie zuordnen möchten, und der OSPF-Area, der sie zugeordnet werden soll.

**10** (Optional) Bearbeiten Sie die standardmäßigen OSPF -Einstellungen.

In den meisten Fällen wird empfohlen, die standardmäßigen OSPF-Einstellungen beizubehalten. Wenn Sie Änderungen an den Einstellungen vornehmen, stellen Sie sicher, dass die OSPF-Peers dieselben Einstellungen verwenden.

- a **Hallo-Intervall (Hello Interval)** zeigt das Standardintervall zwischen Hallo-Paketen an, die über die Schnittstelle gesendet werden.
- b **Ausfallintervall (Dead Interval)** zeigt das Standardintervall an, während dessen mindestens ein Hallo-Paket von einem Nachbarn empfangen werden muss, bevor der Router den Nachbarn als ausgefallen einstuft.
- c **Priorität (Priority)** zeigt die Standardpriorität der Schnittstelle an. Die Schnittstelle mit der höchsten Priorität ist der festgelegte Router.
- d **Kosten (Cost)** einer Schnittstelle zeigt den Standard-Overhead an, der für das Senden von Paketen über die Schnittstelle erforderlich ist. Die Kosten einer Schnittstelle sind umgekehrt proportional zur Bandbreite dieser Schnittstelle. Je größer die Bandbreite ist, desto geringer sind die Kosten.

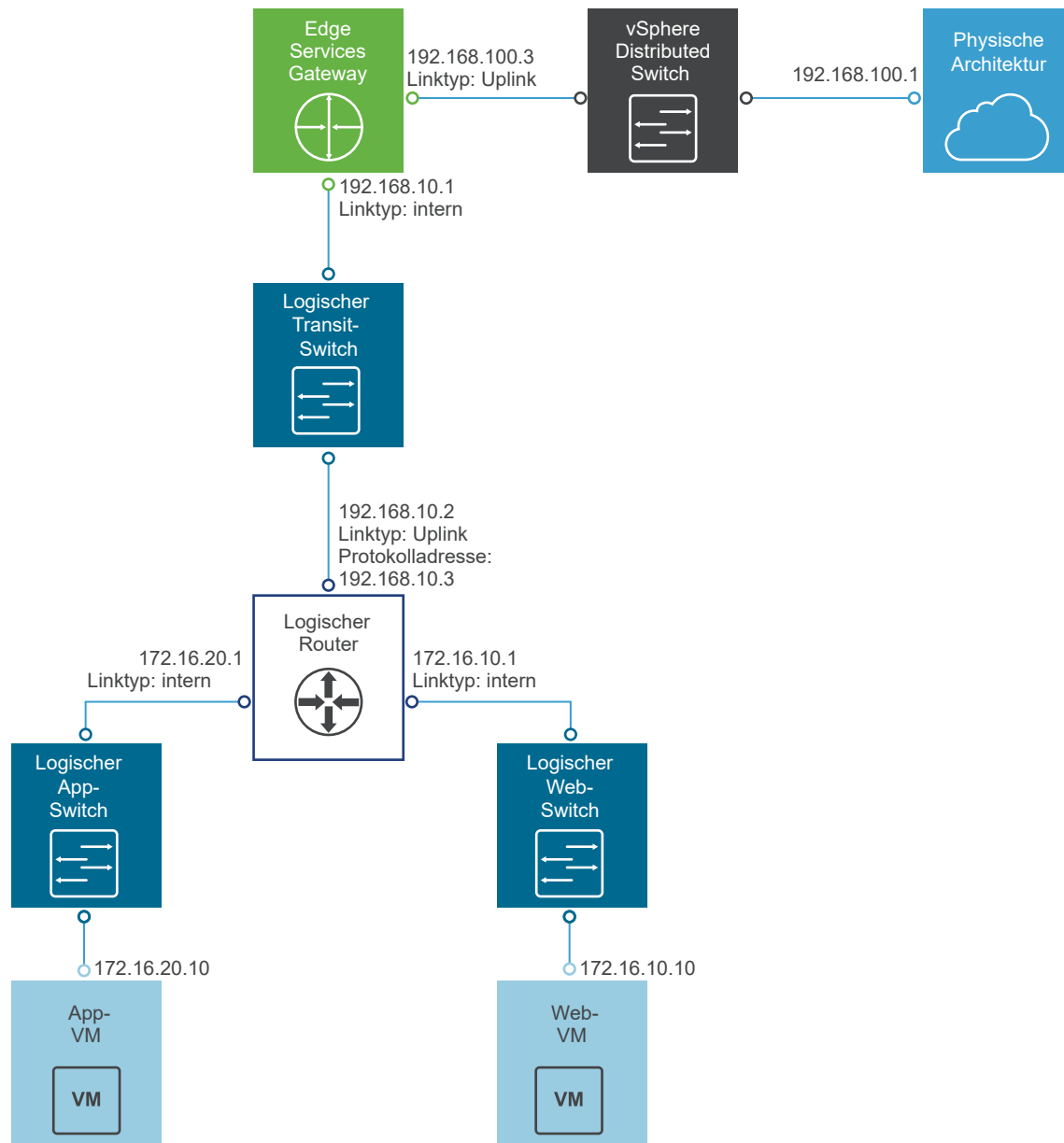
**11** Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.**12** Stellen Sie sicher, dass durch die Route Redistribution und die Firewallkonfiguration die richtigen Routen angekündigt werden können.

## Beispiel: OSPF wird in einem Edge Services Gateway konfiguriert

Ein einfaches NSX-Szenario, bei dem OSPF verwendet wird, liegt vor, wenn wie hier dargestellt ein logischer Router und ein Edge Services Gateway OSPF-Nachbarn sind.

Das ESG kann mit der Außenwelt durch eine Bridge, einen physischen Router (oder wie hier gezeigt) durch eine Uplink-Portgruppe in einem vSphere Distributed Switch verbunden werden.

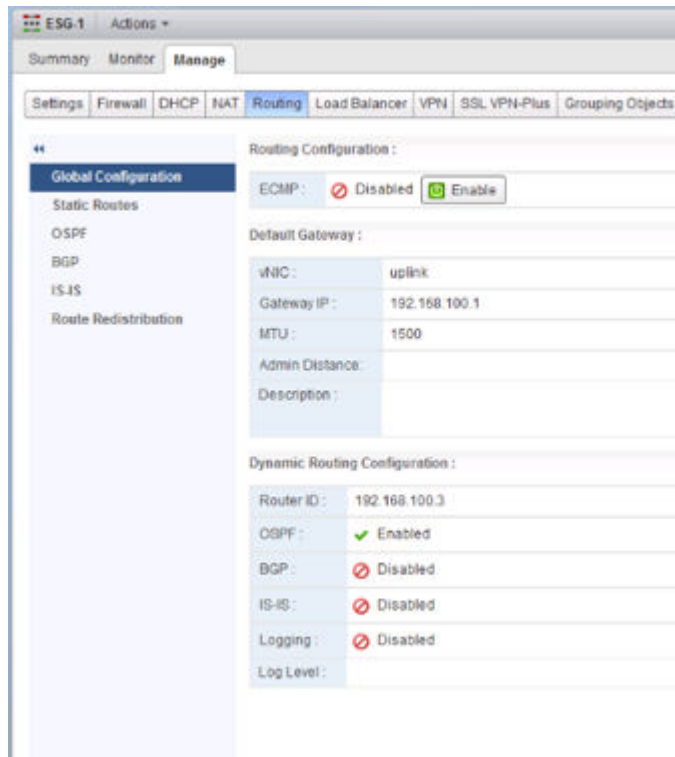
Abbildung 20-1. NSX-Topologie



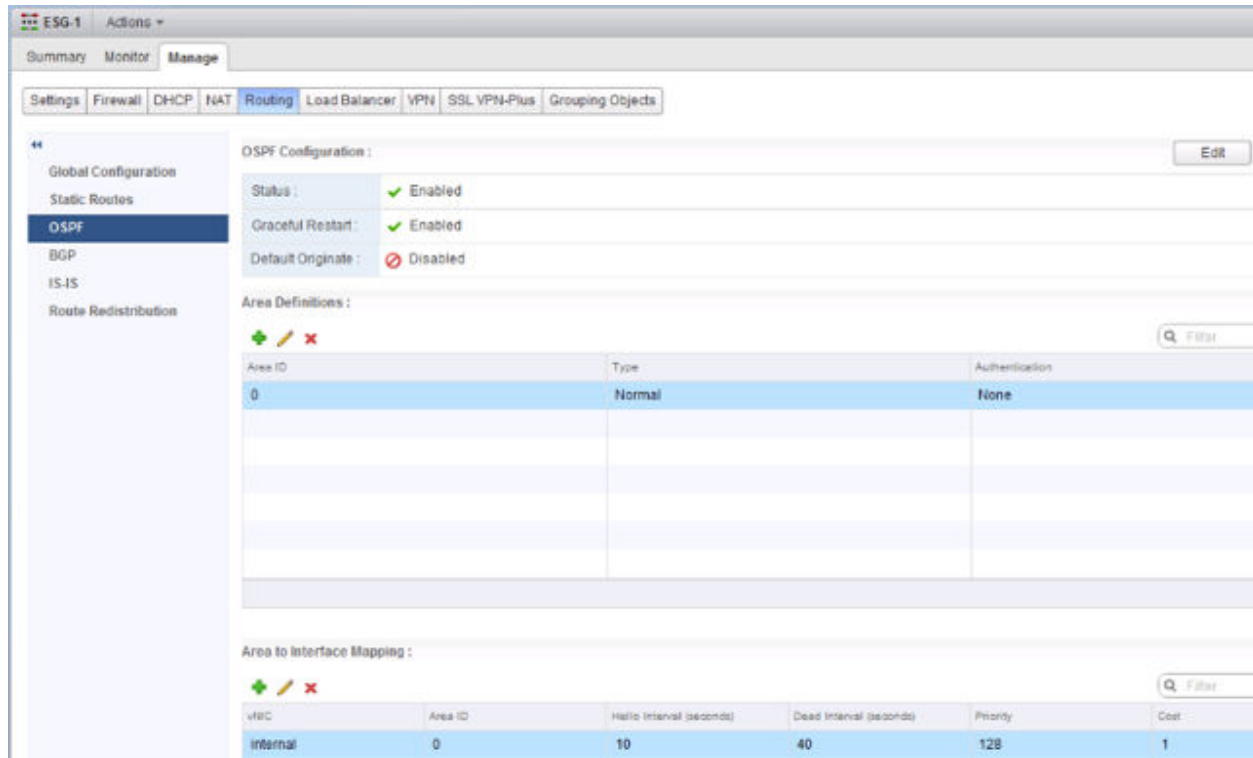
Im folgenden Bildschirm ist das Standard-Gateway von ESG die Uplink-Schnittstelle von ESG zu seinem externen Peer.

Die Router-ID ist die IP-Adresse der Uplink-Schnittstelle von ESG – in anderen Worten, die IP-Adresse, die seinem externen Peer gegenüberliegt.





Die konfigurierte Area-ID ist 0, und die interne Schnittstelle (die Schnittstelle, die dem logischen Router gegenüberliegt) wird der Area zugeordnet.



Die verbundenen Routen werden erneut in OSPF verteilt, sodass der OSPF-Nachbar (der logische Router) Informationen über das Uplink-Netzwerk von ESG abrufen kann.

Summary Monitor Manage

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

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

Route Redistribution States :

OSPF ☒ ISIS ☐ BGP ☐

IP Prefixes :

+ - ✎ ✖

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

Route Redistribution table :

+ - ✎ ✖

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

**Hinweis** Zusätzlich kann OSPF zwischen dem ESG und seinem externen Peer-Router konfiguriert werden, aber üblicherweise verwendet dieser Link BGP für die Routen-Ankündigung.

Stellen Sie sicher, dass das ESG die externen Routen von OSPF von dem logischen Router abrufen kann.

```

NSX-edge-7-0> show ip route

Codes: 0 - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

Total number of routes: 5

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

```

Um die Konnektivität zu überprüfen, stellen Sie sicher, dass ein externes Gerät in der physischen Architektur die VMs pingen kann.

Beispiel:

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

```

Pinging 172.16.10.10 with 32 bytes of data:
Reply from 172.16.10.10: bytes=32 time=5ms TTL=61
Reply from 172.16.10.10: bytes=32 time=1ms TTL=61

```

```

Ping statistics for 172.16.10.10:
 Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
 Minimum = 1ms, Maximum = 5ms, Average = 3ms

```

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

```

Pinging 172.16.20.10 with 32 bytes of data:
Reply from 172.16.20.10: bytes=32 time=2ms TTL=61
Reply from 172.16.20.10: bytes=32 time=1ms TTL=61

```

```

Ping statistics for 172.16.20.10:
 Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
 Minimum = 1ms, Maximum = 2ms, Average = 1ms

```

# Installieren von Guest Introspection auf Hostclustern

# 21

Durch die automatische Installation von Guest Introspection werden auf jedem Host im Cluster ein neuer VIB und eine neue Dienst-VM installiert. Guest Introspection ist für Activity Monitoring und verschiedene Drittanbieter-Sicherheitslösungen erforderlich.

---

**Hinweis** Sie können eine Dienst-VM (Service VM, SVM) nicht mithilfe von vMotion/SvMotion migrieren. Die Dienst-VMs müssen für eine korrekte Ausführung auf dem Host verbleiben, auf dem sie bereitgestellt wurden.

---

## Voraussetzungen

Die folgenden Installationsanweisungen setzen voraus, dass Sie über folgendes System verfügen:

- Ein Datacenter mit unterstützten Versionen von vCenter Server und ESXi, die auf jedem Host im Cluster installiert sein müssen.
- Falls die Hosts in Ihren Clustern von der vCenter Server-Version 5.0 auf 5.5 aktualisiert wurden, dann müssen Sie auf diesen Hosts die Ports 80 und 443 öffnen.
- Die Hosts in dem Cluster, in dem Sie Guest Introspection installieren möchten, wurden für NSX vorbereitet. Informationen dazu erhalten Sie unter „Vorbereiten der Hostcluster für NSX“ in der Dokumentation *Installationshandbuch für NSX*. Guest Introspection kann nicht auf eigenständigen Hosts installiert werden. Wenn Sie NSX für das Bereitstellen und Verwalten von Guest Introspection nur für die Antivirenfunktion verwenden, müssen Sie die Hosts nicht für NSX vorbereiten. Mit der NSX für vShield Endpoint-Lizenz ist dies nicht möglich.
- NSX Manager ist installiert und wird ausgeführt.
- Stellen Sie sicher, dass die NSX Manager und die vorbereiteten Hosts, auf denen die Guest Introspection-Dienste ausgeführt werden, mit demselben NTP-Server verknüpft sind und dass die Zeit synchronisiert ist. Andernfalls sind VMs möglicherweise nicht durch Antivirendienste geschützt, auch wenn der Status des Clusters für Guest Introspection und alle Drittanbieterdienste grün angezeigt wird.

Wird ein NTP-Server hinzugefügt, empfiehlt VMware, Guest Introspection und alle Drittanbieterdienste anschließend erneut bereitzustellen.

Wenn Sie der VM des NSX Guest Introspection-Dienstes eine IP-Adresse aus einem IP-Pool zuweisen möchten, erstellen Sie den IP-Pool, bevor Sie NSX Guest Introspection installieren. Informationen dazu finden unter „Arbeiten mit IP-Pools“ im Dokument *Administratorhandbuch für NSX*.

---

**Vorsicht** Guest Introspection verwendet das Subnetz 169.254.x.x, um IP-Adressen intern für den GI-Dienst zuzuweisen. Wenn Sie die IP-Adresse 169.254.1.1 einer beliebigen VMkernel-Schnittstelle eines ESXi-Hosts zuweisen, schlägt die Guest Introspection-Installation fehl. Der GI-Dienst verwendet diese IP-Adresse für die interne Kommunikation.

---

vSphere Fault Tolerance kann nicht zusammen mit Guest Introspection verwendet werden.

## Verfahren

- 1 Klicken Sie auf der Registerkarte **Installation** auf **Dienstbereitstellungen (Service Deployments)**.
- 2 Klicken Sie auf das Symbol **Neue Dienstbereitstellung (New Service Deployment)** (  ).
- 3 Wählen Sie im Dialogfeld „Netzwerk- und Sicherheitsdienste bereitstellen“ die Option **Guest Introspection** aus.
- 4 Wählen Sie unter **Zeitplan angeben (Specify schedule)** (am unteren Rand des Dialogfelds) die Option **Jetzt bereitstellen (Deploy now)** aus, um Guest Introspection sofort nach der Installation bereitzustellen, oder wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- 5 Klicken Sie auf **Weiter (Next)**.
- 6 Wählen Sie das Datacenter und die Cluster aus, in denen Sie Guest Introspection installieren möchten, und klicken Sie auf **Weiter (Next)**.
- 7 Wählen Sie auf der Seite „Speicher- und Verwaltungsnetzwerk auswählen“ den Datenspeicher aus, auf dem Sie den VM-Speicher für den Dienst hinzufügen möchten, oder wählen Sie die Option **Angegeben auf dem Host (Specified on host)** aus. Es wird empfohlen, dass Sie gemeinsame Datenspeicher und Netzwerke anstatt „Angegeben auf dem Host“ verwenden, damit die bereitgestellten Workflows automatisiert werden.

Der ausgewählte Datenspeicher muss auf allen Hosts im ausgewählten Cluster verfügbar sein.

Wenn Sie **Angegeben auf dem Host (Specified on host)** ausgewählt haben, führen Sie die unten genannten Schritte für jeden Host im Cluster aus.

- a Klicken Sie auf der Startseite von vSphere Web Client auf **vCenter** und dann auf **Hosts**.
- b Klicken Sie in der Spalte **Name** auf einen Host und dann auf die Registerkarte **Verwalten (Manage)**.
- c Klicken Sie auf **Agent-VMs (Agent VMs)** und anschließend auf **Bearbeiten (Edit)**.
- d Wählen Sie den Datenspeicher aus und klicken Sie auf **OK**.

- 8 Wählen Sie die verteilte virtuelle Portgruppe aus, in der die Verwaltungsschnittstelle gehostet werden soll. Wenn der Datenspeicher auf **Angegeben auf dem Host (Specified on host)** gesetzt ist, muss das Netzwerk auch auf **Angegeben auf dem Host (Specified on host)** gesetzt sein.

Die ausgewählte Portgruppe muss die Portgruppe des NSX Manager erreichen können und auf allen Hosts im ausgewählten Cluster verfügbar sein.

Wenn Sie **Angegeben auf dem Host (Specified on host)** ausgewählt haben, führen Sie die Teilschritte unter Schritt 7 aus, um ein Netzwerk auf dem Host auszuwählen. Wenn Sie dem Cluster einen (oder mehrere) Hosts hinzufügen, muss vor dem Hinzufügen der Datenspeicher und das Netzwerk für jeden Host festgelegt werden.

- 9 Wählen Sie unter „IP-Zuweisungen“ eine der folgenden Optionen aus:

| Auswählen            | An                                                                                                                                                                                                                          |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DHCP</b>          | Weisen Sie der VM des NSX Guest Introspection-Dienstes eine IP-Adresse über Dynamic Host Configuration Protocol (DHCP) zu. Wählen Sie diese Option aus, wenn Ihre Hosts auf unterschiedlichen Subnetzen untergebracht sind. |
| <b>Einen IP-Pool</b> | Weisen Sie der VM des NSX Guest Introspection-Diensts eine IP-Adresse aus dem ausgewählten IP-Pool zu.                                                                                                                      |

- 10 Klicken Sie auf der Seite „Bereit zum Abschließen“ auf **Weiter (Next)** und anschließend auf **Beenden (Finish)**.
- 11 Überwachen Sie die Bereitstellung, bis **Erfolg (Succeeded)** für die Spalte **Installationsstatus (Installation Status)** angezeigt wird.
- 12 Wenn **Fehlgeschlagen (Failed)** für die Spalte **Installationsstatus (Installation Status)** angezeigt wird, klicken Sie auf das Symbol neben „Fehlgeschlagen“. Es werden alle Bereitstellungsfehler angezeigt. Klicken Sie auf **Auflösen (Resolve)**, um die Fehler zu beheben. In einigen Fällen werden beim Auflösen der Fehler zusätzliche Fehlermeldungen angezeigt. Führen Sie die nötige(n) Aktion(en) aus und klicken Sie wieder auf **Auflösen (Resolve)**.

# Deinstallieren von NSX-Komponenten

# 22

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:

- [Deinstallieren eines Guest Introspection-Moduls](#)
- [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](#)

## Deinstallieren eines Guest Introspection-Moduls

Durch das Deinstallieren von Guest Introspection wird ein VIB aus den Hosts im Cluster und die Dienst-VM aus jedem Host im Cluster entfernt. Guest Introspection ist für die Identitäts-Firewall, die Endpoint-Überwachung und verschiedene Drittanbieter-Sicherheitslösungen erforderlich. Das Deinstallieren von Guest Introspection kann weitreichende Auswirkungen haben.

---

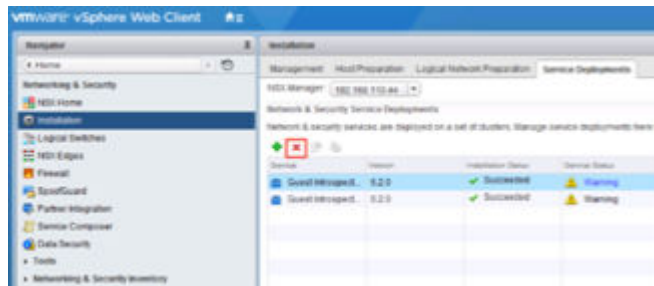
**Vorsicht** Bevor Sie ein Guest Introspection-Modul aus einem Cluster deinstallieren, müssen Sie alle Drittanbieter-Produkte, die Guest Introspection verwenden, auf den Hosts in diesem Cluster deinstallieren. Halten Sie sich dabei an die Anweisungen des Anbieters.

---

Es gibt weniger Schutz für VMs im NSX-Cluster. Sie müssen mit vMotion die virtuellen Maschinen aus dem Cluster verschieben, bevor Sie die Deinstallation durchführen.

So wird Guest Introspection deinstalliert:

- 1 Navigieren Sie in vCenter zu **Home > Networking & Security > Installation** und wählen Sie die Registerkarte **Dienstbereitstellungen (Service Deployments)** aus.
- 2 Wählen Sie die Guest Introspection-Instanz aus und klicken Sie auf das Symbol „Löschen“.
- 3 Löschen Sie sie entweder jetzt oder planen Sie das Löschen für einen späteren Zeitpunkt.



## 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.

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



# 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: [Kapitel 12 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, Guest Introspection 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 (z. B. Controller oder Edges), die direkt aus vCenter von NSX bereitgestellt wurden. Verwenden Sie zum Verwalten und Entfernen von NSX-Appliances immer die Registerkarte **Networking & Security** von vSphere Web Client.

---

### Voraussetzungen

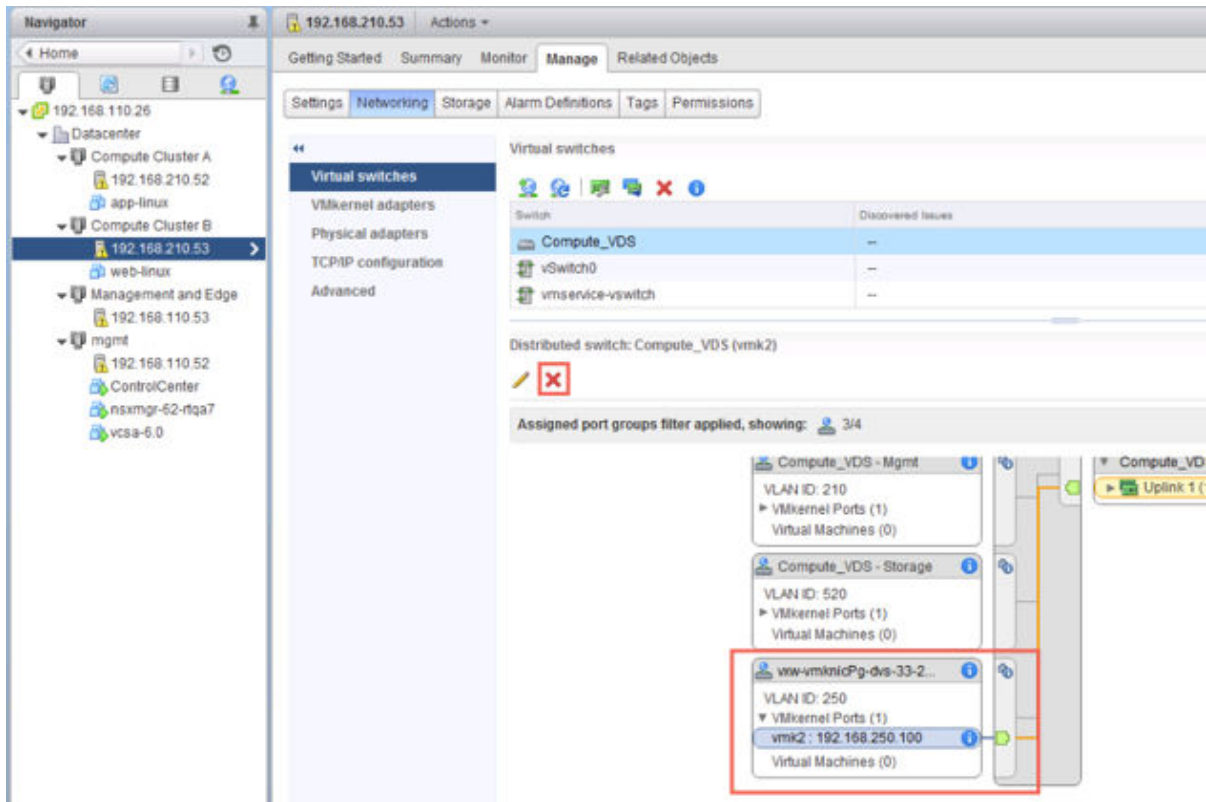
- Ihnen muss die Rolle „Enterprise-Administrator“ oder „NSX-Administrator“ zugewiesen worden sein.
- Entfernen Sie jegliche registrierten Partnerlösungen sowie Endpoint-Dienste, bevor Sie die Hostvorbereitung umkehren, sodass die Dienst-VMs im Cluster ordnungsgemäß entfernt werden.
- Löschen Sie alle 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.

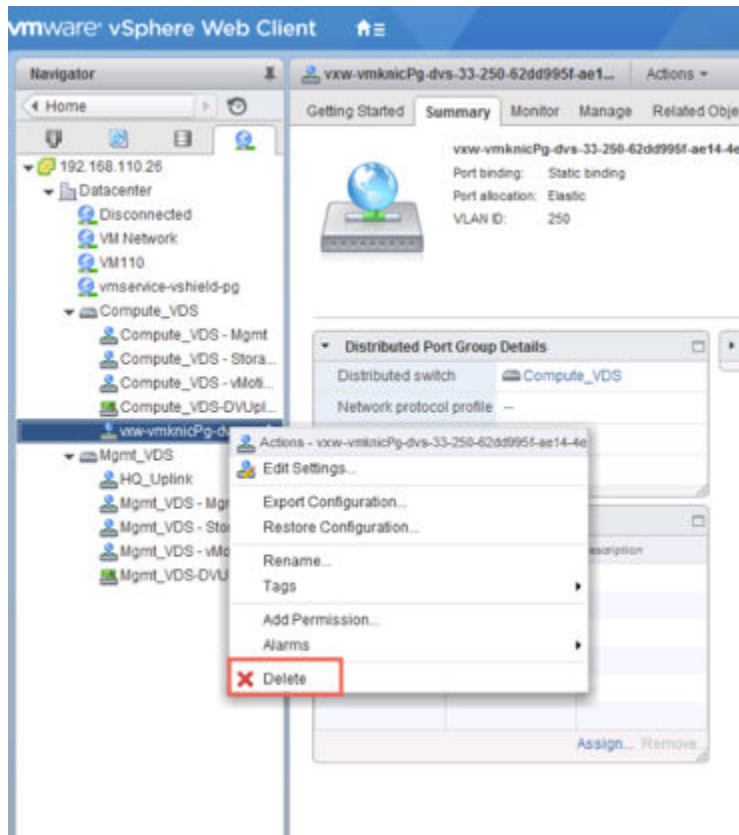
Beispiel:



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

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

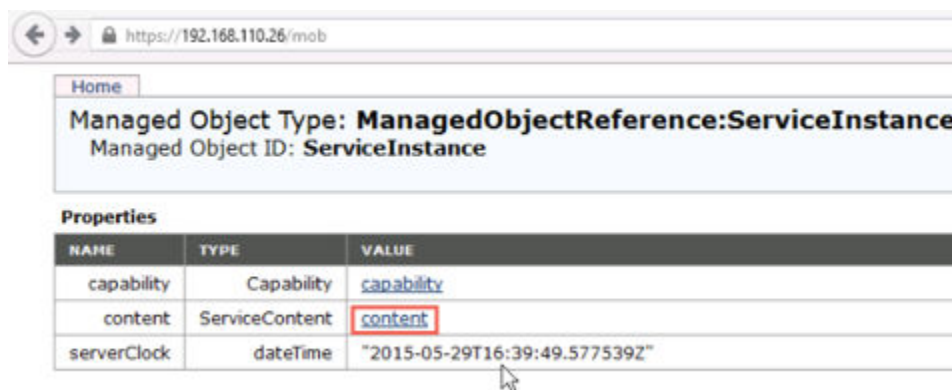
Beispiel:



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</b> (required) | 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                                                     |
|------------------------------------------|------------------------------------------------------------------------|
| <b>Disable BASH Shell</b><br>Disable SSH | <b>BASH Shell is Enabled</b><br>Change current state of the BASH Shell |
| <Up/Down> Select                         | <Enter> Change<br><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:

- VMware vCenter Server für Windows – `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity\`
- VMware vCenter Server Appliance – `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/`

Starten Sie die vCenter Server Appliance neu:

- Melden Sie sich in der vCenter Server Appliance 6.0 bei der vCenter Server-Shell als Root-Benutzer an und führen Sie die folgenden Befehle aus:

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

- Führen Sie dazu in vCenter Server 6.0 auf Windows die nachfolgend aufgeführten Befehle aus.

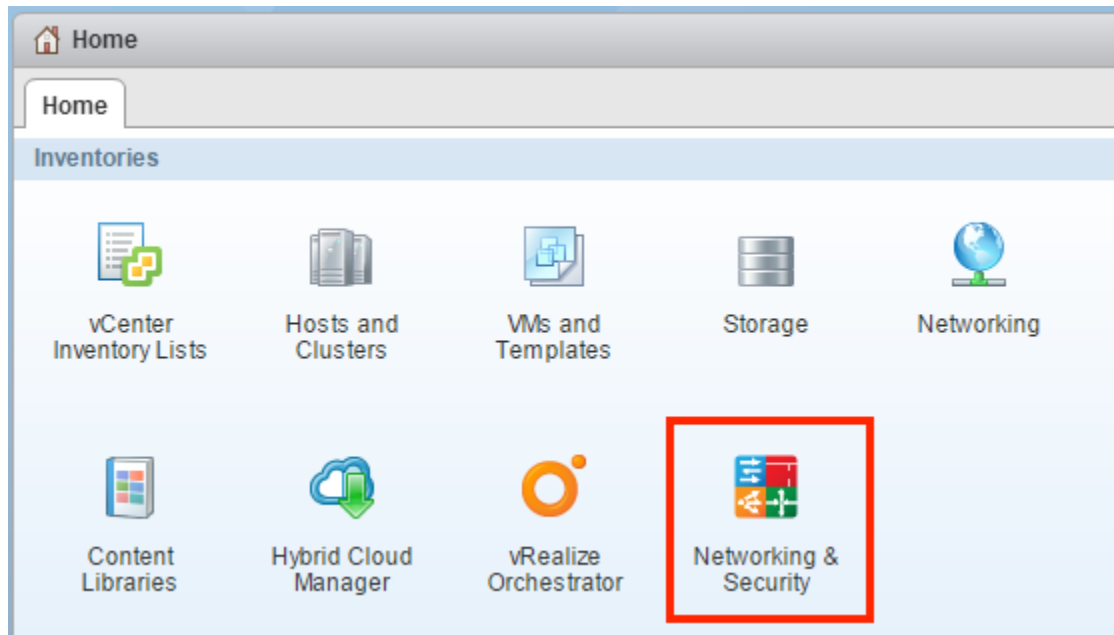
```
cd C:\Program Files\VMware\vCenter Server\bin
service-control --stop vspherewebclientsvc
service-control --start vspherewebclientsvc
```

### 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.

