

Installationshandbuch für NSX-T Data Center

Geändert am 28. FEBRUAR 2020
VMware NSX-T Data Center 2.4



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

Inhalt

NSX-T Data Center-Installationshandbuch	7
1 Übersicht über NSX-T Data Center	8
Wichtige Konzepte	9
Übersicht über NSX Manager	12
2 Workflows für die Installation von NSX-T Data Center	16
NSX-T Data Center-Workflow für vSphere	16
NSX-T Data Center-Installations-Workflow für KVM	17
NSX-T Data Center-Konfigurations-Workflow für Bare-Metal-Server	18
3 Vorbereitung für die Installation	19
Systemvoraussetzungen	19
Systemanforderungen für NSX Manager-VM	19
Systemanforderungen für NSX Edge-VM	22
Anforderungen der NSX Edge-Bare-Metal-Bereitstellung	23
Bare Metal Server-Systemanforderungen	26
Bare Metal Linux-Container-Anforderungen	26
Ports und Protokolle	26
Von NSX Manager verwendete TCP- und UDP-Ports	28
Von NSX Edge verwendete TCP- und UDP-Ports	29
Von ESXi, KVM-Hosts und Bare-Metal-Server verwendete TCP- und UDP-Ports	30
Installieren von NSX-T Data Center-Komponenten	31
NSX Manager-Installation	31
NSX Edge-Installation	35
4 Installieren von NSX-T Data Center auf vSphere	39
Installieren Sie NSX Manager und die verfügbaren Appliances	39
Installieren von NSX Manager unter ESXi mithilfe des OVF-Befehlszeilentools	42
Konfigurieren von NSX-T Data Center zum Anzeigen des GRUB-Menü zum Startzeitpunkt	47
Anmeldung beim neu erstellten NSX Manager	48
Hinzufügen eines Compute Managers	48
Bereitstellen von NSX Manager-Knoten zur Bildung eines Clusters über die Benutzeroberfläche	50
Konfigurieren einer virtuellen IP-Adresse (VIP) für einen Cluster	55
Installieren einer NSX Edge unter ESXi mithilfe einer grafischen vSphere-Benutzeroberfläche	56
Installieren von NSX Edge auf ESXi unter Verwendung des OVF-Befehlszeilentools	59

5	Installieren von NSX-T Data Center auf KVM	64
	Einrichten von KVM	64
	Verwalten der Gast-VMs in der KVM-CLI	70
	Installieren von NSX Manager auf KVM	71
	Anmeldung beim neu erstellten NSX Manager	75
	Installieren von Drittanbieterpaketen auf einem KVM-Host	75
	Überprüfung der Open vSwitch-Version auf RHEL KVM-Hosts	77
	Bereitstellen von NSX Manager-Knoten zur Bildung eines Cluster mithilfe der CLI	78
	Installieren von NSX Edge mithilfe einer ISO-Datei oder einer PXE	79
	Installieren von NSX Edge per ISO-Datei als virtuelle Appliance	79
	Installieren von NSX Edge per ISO-Datei auf einer Bare-Metal-Bereitstellung	83
	Installieren von NSX Edge auf PXE-Server	86
6	Konfigurieren des Bare-Metal-Servers zur Verwendung von NSX-T Data Center	92
	Installieren von Drittanbieterpaketen auf einem Bare-Metal-Server	92
	Erstellen der Anwendungsschnittstelle für Bare-Metal Server-Arbeitslasten	94
7	Konfigurieren des NSX Manager-Clusters	96
	Anforderungen des NSX Manager-Clusters	96
	NSX Manager-Clusteranforderungen für eine, zwei und mehrere Sites	97
8	Transportzonen und Transportknoten	100
	Erstellen von Transportzonen	100
	Erstellen eines IP-Pools für Tunnel-Endpoint-IP-Adressen	103
	Erweiterter Datenpfad	104
	Konfigurieren von Profilen	107
	Erstellen eines Uplink-Profiles	107
	Konfigurieren von Network I/O Control-Profilen	111
	Hinzufügen eines NSX Edge-Cluster-Profiles	120
	Hinzufügen eines NSX Edge-Bridge-Profiles	121
	Hinzufügen eines Transportknotenprofils	122
	VMkernel-Migration auf einen N-VDS-Switch	127
	Fehler bei der VMkernel-Migration	133
	Erstellen eines eigenständigen Hosts oder Bare-Metal-Server-Transportknotens	136
	Konfigurieren eines verwalteten Host-Transportknotens	146
	Konfigurieren von ESXi-Hosttransportknoten mit Linkaggregation (LAG)	147
	Vollständig reduzierte NSX-T-Bereitstellung mit vSphere-Cluster	148
	Überprüfen des Transportknotenstatus	159
	Optische Darstellung eines N-VDS	162
	Manuelle Installation von NSX-T Data Center-Kernel-Modulen	163
	Manuelles Installieren von NSX-T Data Center-Kernel-Modulen auf ESXi-Hypervisors	163

Manuelles Installieren von NSX-T Data Center-Kernel-Modulen auf Ubuntu-KVM-Hypervisors	166
Manuelles Installieren von NSX-T Data Center-Kernel-Modulen auf RHEL- und CentOS-KVM-Hypervisors	168
NSX Edge-Netzwerkeinrichtung	169
Erstellen eines NSX Edge-Transportknotens	175
Erstellen eines NSX Edge-Clusters	178
9 Automatische Bereitstellung statusfreier Cluster	180
Allgemeine Aufgaben zum automatischen Bereitstellen statusfreier Cluster	181
Voraussetzungen und unterstützte Versionen	181
Erstellen eines benutzerdefinierten Image-Profiles für statusfreie Hosts	182
Zuordnen des benutzerdefinierten Images zu den Referenz- und Zielhosts	184
Einrichten der Netzwerkkonfiguration auf dem Referenzhost	185
Konfigurieren des Referenzhosts als Transportknoten in NSX-T	186
Extrahieren und Überprüfen des Hostprofils	188
Überprüfen der Hostprofilzuordnung mit dem statusfreien Cluster	189
Aktualisieren der Hostanpassung	190
Auslösen der automatischen Bereitstellung auf Zielhosts	191
Neustarten von Hosts vor der TNP-Anwendung	192
Anwenden von TNP auf einem statusfreien Cluster	192
Neustarten von Hosts nach der TNP-Anwendung	195
Szenarien, in denen sich der statusfreie Host im Zielcluster befindet	196
Szenarien, in denen sich der statusfreie Host außerhalb des Zielclusters befindet	198
Fehlerbehebung für das Host- und Transportknotenprofil	201
10 Deinstallieren von NSX-T Data Center von einem Host-Transportknoten	204
Überprüfen der Host-Netzwerkzuordnungen für die Deinstallation	204
Deinstallieren von NSX-T Data Center von einem vSphere-Cluster	206
Deinstallieren von NSX-T Data Center von einem Host in einem vSphere-Cluster	208
Deinstallieren von NSX-T Data Center von einem eigenständigen Host	209
11 Installieren von NSX Cloud-Komponenten	211
Architektur und Komponenten von NSX Cloud	211
Überblick über das Installieren und Konfigurieren von NSX Cloud-Komponenten für Ihre Public Cloud	213
Workflow für Tag 0 zum Herstellen einer Verbindung von NSX Cloud zu Ihrer Public Cloud	213
Installieren von CSM und Herstellen einer Verbindung zu NSX Manager	214
Installieren von CSM	214
Verbinden von CSM mit NSX Manager	214
(Optional) Proxy-Server konfigurieren	215
(Optional) Einrichten von vIDM für Cloud Service Manager	216
Public Cloud mit lokaler Bereitstellung verbinden	217

Zugriff auf Ports und Protokolle auf CSM für Hybrid-Konnektivität ermöglichen	217
Ihr Microsoft Azure-Netzwerk mit Ihrer lokalen NSX-T Data Center-Bereitstellung verbinden	218
Ihr Amazon Web Services-Netzwerk (AWS-Netzwerk) mit Ihrer lokalen NSX-T Data Center-Bereitstellung verbinden	219
Ihr Public Cloud-Konto hinzufügen	220
Einrichten eines sicheren Zugriffs auf Ihre Microsoft Azure-Bestandsliste	221
Einrichten eines sicheren Zugriffs auf Ihre Microsoft Azure-Bestandsliste	227
Bereitstellen oder Verknüpfen von NSX Public Cloud Gateways	231
Bereitstellen von PCG in einem selbstverwalteten VNet oder einem Transit-VNet	233
Bereitstellen von PCG in einer selbstverwalteten VPC oder Transit-VPC	235
Verknüpfung mit einer Transit-VPC oder einem Transit-VNet	238
Automatisch erstellte logische Entitäten und Cloud-native Sicherheitsgruppen	239
Bereitstellung von PCG aufheben	244
Tags für VMs in der Public Cloud entfernen	245
Quarantäne-Richtlinie deaktivieren, falls aktiviert	246
Vom Benutzer erstellte logische Elemente löschen	247
Bereitstellung aufheben von CSM	247

NSX-T Data Center-Installationshandbuch

Im *Installationshandbuch für NSX-T Data Center* wird beschrieben, wie Sie das VMware NSX-T™ Data Center-Produkt installieren. Zu den bereitgestellten Informationen gehören schrittweise Anleitungen für die Konfiguration sowie empfohlene Vorgehensweisen.

Zielgruppe

Diese Informationen sind für Personen bestimmt, die NSX-T Data Center installieren oder nutzen möchten. Diese Informationen richten sich an erfahrene Systemadministratoren, die mit der Technologie virtueller Maschinen und den Netzwerkvirtualisierungskonzepten vertraut sind.

Technische Veröffentlichungen – 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-T Data Center

1

Auf die gleiche Weise wie mit der Servervirtualisierung virtuelle Maschinen programmgesteuert erstellt und verwaltet werden, lassen sich mit der NSX-T Data Center-Netzwerkvirtualisierung softwarebasierte virtuelle Netzwerke programmgesteuert erstellen und verwalten.

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

NSX-T Data Center implementiert drei separate, aber integrierte Ebenen: Management, Steuerung und Daten. Diese Ebenen werden als eine Reihe von Prozessen, Modulen und Agenten implementiert, die auf zwei Typen von Knoten platziert sind: NSX Manager- und Transportknoten.

- Jeder Knoten hostet einen Management Plane-Agenten.
- NSX Manager-Knoten hosten API-Dienste und die Management Plane-Cluster-Daemons.
- NSX Controller-Knoten hosten die Cluster-Daemons der zentralen Control Plane.
- Transportknoten hosten Daemons der lokalen Control Plane und Weiterleitungs-Engines.

NSX Manager bietet Clusterunterstützung für drei Knoten, wobei Richtlinienmanager-, Verwaltungs- und zentrale Steuerungsdienste in einem Knotencluster zusammengeführt werden. NSX Manager-Cluster stellen Hochverfügbarkeit der Benutzeroberfläche und API bereit. Die Konvergenz der Verwaltungs- und Control Plane-Knoten verringert die Anzahl virtueller Appliances, die vom NSX-T Data Center-Administrator bereitgestellt und verwaltet werden müssen.

Die NSX Manager-Appliance ist in drei unterschiedlichen Größen für die verschiedenen Bereitstellungsszenarien verfügbar. Eine kleine Appliance für Test- oder Proof-of-Concept-Bereitstellungen. Eine mittlere Appliance für Bereitstellungen mit bis zu 64 Hosts und eine große Appliance für Kunden, die Bereitstellungen in sehr großen Umgebung durchführen. Weitere Informationen finden Sie unter [Systemanforderungen für NSX Manager-VM](#) und im Tool [Maximalwerte für die Konfiguration](#).

Dieses Kapitel enthält die folgenden Themen:

- [Wichtige Konzepte](#)

■ Übersicht über NSX Manager

Wichtige Konzepte

Die allgemeinen NSX-T Data Center-Konzepte, die in der Dokumentation und auf der Benutzeroberfläche verwendet werden.

Compute Manager	Ein Compute Manager ist eine Anwendung, die Ressourcen wie Hosts und virtuelle Maschinen verwaltet. Ein Beispiel ist vCenter Server.
Control Plane	Berechnet den Laufzeitzustand anhand der Konfiguration aus der Management Plane, verteilt Topologie-Informationen, die von den Data Plane-Elementen gemeldet werden, und überträgt die zustandslose Konfiguration an Weiterleitungs-Engines.
Data Plane	Führt die zustandslose Weiterleitung oder Transformation von Paketen anhand von Tabellen durch, die von der Control Plane aufgefüllt werden. Die Data Plane meldet Topologie-Informationen an die Control Plane und pflegt Statistiken auf Paketebene.
Externes Netzwerk	Ein physisches Netzwerk oder VLAN, das nicht von NSX-T Data Center verwaltet wird. Sie können Ihr logisches Netzwerk oder Overlay-Netzwerk über NSX Edge mit einem externen Netzwerk verknüpfen. Beispiel: Ein physisches Netzwerk in einem Kundendatencenter oder ein VLAN in einer physischen Umgebung.
Fabric-Knoten	Host, der bei der NSX-T Data Center-Management Plane registriert wurde und auf dem NSX-T Data Center-Module installiert sind. Damit ein Hypervisor-Host oder NSX Edge Teil des NSX-T Data Center-Overlays werden kann, muss er der NSX-T Data Center-Fabric hinzugefügt werden.
logischer Port Egress (ausgehend)	Ausgehender Netzwerkdatenverkehr, der die VM oder das logische Netzwerk verlässt, wird als Egress bezeichnet, weil der Datenverkehr das virtuelle Netzwerk verlässt und in das Datencenter eintritt.
logischer Port Ingress (eingehend)	Eingehender Netzwerkdatenverkehr, der das Datencenter verlässt und in die VM eintritt, wird als Ingress-Datenverkehr bezeichnet.
Logischer Router	NSX-T Data Center-Routing-Einheit
Logischer Router Port	Logischer Netzwerkport, mit dem Sie einen logischen Switch-Port oder einen Uplink-Port zu einem physischen Netzwerk verknüpfen können
Logischer Switch	Einheit, die virtuelles Layer 2-Switching für VM-Schnittstellen und Gateway-Schnittstellen bereitstellt. Ein logischer Switch bietet Mandantennetzwerk-Administratoren das logische Äquivalent eines physischen Layer 2-Switches, sodass Sie mehrere VMs mit einer gemeinsamen Broadcast-Domäne verbinden können. Ein logischer Switch ist eine logische Einheit, die von der physischen Hypervisor-Infrastruktur unabhängig ist und viele

Hypervisors umspannt, sodass VMs unabhängig von ihrer physischen Position verbunden werden.

In einer Cloud mit mehreren Mandanten kann es viele logische Switches auf derselben Hypervisor-Hardware geben, wobei jedes Layer 2-Segment von den anderen isoliert ist. Logische Switches können anhand von logischen Routern verbunden werden und logische Router können Uplink-Ports bereitstellen, die mit dem externen physischen Netzwerk verbunden sind.

Port für den logischen Switch	Verknüpfungspunkt für einen logischen Switch, mit dem eine Verbindung zu einer Netzwerkschnittstelle einer virtuellen Maschine oder zu einer logischen Router-Schnittstelle hergestellt werden kann. Der logische Switch Port meldet das angewendete Switching-Profil, den Portstatus und den Linkstatus.
Management Plane	Liefert einen einzelnen API-Einstiegspunkt in das System, speichert die Benutzerkonfiguration, verarbeitet Benutzerabfragen und führt Betriebsaufgaben auf allen Management-, Controller- und Data Plane-Knoten im System aus. Die Management Plane ist außerdem für das Abfragen, Ändern und Speichern der Benutzerkonfiguration zuständig.
NSX Edge-Cluster	Sammlung aus NSX Edge-Knoten-Appliances mit denselben Einstellungen wie Protokolle für die High Availability-Überwachung.
NSX Edge-Knoten	Komponente, deren Funktionsziel es ist, Rechenleistung für die IP-Routing- und IP-Dienstfunktionen bereitzustellen.
NSX-verwalteter Virtual Distributed Switch oder KVM Open vSwitch	<p>Der NSX-verwaltete Virtual Distributed Switch (N-VDS, vormals Host-Switch) oder OVS wird für freigegebene NSX Edge- und Computing-Cluster verwendet. N-VDS ist für die Konfiguration des Overlay-Datenverkehrs erforderlich.</p> <p>Ein N-VDS verfügt über zwei Modi: „Standard“ und „Optimierter Datenpfad“. Ein N-VDS mit optimiertem Datenpfad hat das Leistungsvermögen, NFV-Arbeitslasten (Network Functions Virtualization) zu unterstützen.</p>
NSX Manager	Knoten, der die API-Dienste, die Management Plane und die Agent-Dienste hostet. NSX Manager ist eine Appliance, die im Installationspaket von NSX-T Data Center enthalten ist. Sie können die Appliance mit der Rolle „nsx-manager“, „nsx-controller“ oder „nsx-cloud-service-manager“ bereitstellen. Die Appliance unterstützt derzeit nur jeweils eine Rolle gleichzeitig.
NSX Manager-Cluster	Ein Cluster aus NSX Managern, die Hochverfügbarkeit bereitstellen können.
Open vSwitch (OVS)	Open Source-Software-Switch, der als virtueller Switch in XenServer, Xen, KVM und anderen Linux-basierten Hypervisors fungiert.

Logisches Overlay-Netzwerk	Logisches Netzwerk, das anhand von Layer 2-in-Layer 3-Tunneling implementiert wird, sodass die für VMs sichtbare Topologie von der des physischen Netzwerks entkoppelt wird
Physische Schnittstelle (pNIC)	Netzwerkschnittstelle auf einem physischen Server, auf dem ein Hypervisor installiert ist
Segment	<p>Einheit, die virtuelles Layer 2-Switching für VM-Schnittstellen und Gateway-Schnittstellen bereitstellt. Ein Segment fungiert für Administratoren des Mandantennetzwerks als logisches Äquivalent eines physischen Layer 2-Switches, mit dem mehrere VMs mit einer gemeinsamen Broadcast-Domäne verbunden werden können. Ein Segment ist eine logische Einheit, die von der physischen Hypervisor-Infrastruktur unabhängig ist und viele Hypervisoren umspannt, sodass VMs unabhängig von ihrer physischen Position verbunden werden können. Ein Segment ist auch als logischer Switch bekannt.</p> <p>In einer Cloud mit mehreren Mandanten können zahlreiche Segmente nebeneinander auf derselben Hypervisor-Hardware vorhanden sein, wobei jedes Layer 2-Segment von den anderen isoliert ist. Segmente können mithilfe von Gateways verbunden werden, die Konnektivität mit dem externen physischen Netzwerk bereitstellen können.</p>
Tier-0-Gateway oder logischer Tier-0 Router	Das Tier-0-Gateway auf der Registerkarte Netzwerk und Sicherheit – Erweitert als logischer Tier-0 Router bezeichnet. Er verbindet sich mit dem physischen Netzwerk und kann als Aktiv/Aktiv- oder Aktiv/Standby-Cluster dargestellt werden. Das Tier-0-Gateway führt BGP und Peers mit physischen Routern aus. Im Aktiv/Standby-Modus kann das Gateway auch zustandsbehaftete Dienste bereitstellen.
Tier-1-Gateway oder logischer Tier-1 Router	Das Tier-1-Gateway auf der Registerkarte Netzwerk und Sicherheit – Erweitert als logischer Tier-1 Router bezeichnet. Er verbindet sich mit einem Tier-0-Gateway für Northbound-Konnektivität und einem oder mehreren Overlay-Netzwerken für Southbound-Konnektivität. Bei einem Tier-1-Gateway kann es sich um einen Aktiv/Standby-Cluster handeln, der zustandsbehaftete Dienste bereitstellt.
Transportzone	Sammlung aus Transportknoten, die die maximale Reichweite für logische Switches definiert. Eine Transportzone stellt eine Reihe aus ähnlich bereitgestellten Hypervisoren und die logischen Switches dar, die VMs auf diesen Hypervisoren verbinden.
Transportknoten	Ein Knoten, der an einem NSX-T Data Center-Overlay oder NSX-T Data Center-VLAN-Netzwerk teilnehmen kann. Bei einem KVM-Host können Sie den N-VDS im Voraus konfigurieren oder die Konfiguration von NSX Manager durchführen lassen. Bei einem ESXi-Host wird der N-VDS immer von NSX Manager konfiguriert.

Uplink-Profil

Definiert Richtlinien für die Links von den Hypervisor-Hosts mit logischen NSX-T Data Center-Switches oder von NSX Edge-Knoten mit Top-of-Rack-Switches. Die von Uplink-Profilen definierten Einstellungen können Gruppierungsrichtlinien, Aktiv/Standby-Links, die Transport-VLAN-ID und die MTU-Einstellung umfassen. Das Transport-VLAN, das in den Uplink-Profil-Tags festgelegt ist, überlagert nur den Datenverkehr und die VLAN-ID wird vom TEP-Endpunkt verwendet.

VM-Schnittstelle (vNIC)

Netzwerkschnittstelle auf einer virtuellen Maschine, die Konnektivität zwischen dem virtuellen Gastbetriebssystem und dem Standard-vSwitch oder vSphere Distributed Switch bereitstellt. Die vNIC kann mit einem logischen Port verknüpft werden. Sie können eine vNIC anhand ihrer eindeutigen ID (UUID) identifizieren.

Virtueller Tunnel-Endpoint

Jeder Hypervisor verfügt über einen virtuellen Tunnel-Endpoint (VTEP), der für das Verkapseln des VM-Datenverkehrs innerhalb eines VLAN-Headers und das Weiterleiten des Pakets an einen Ziel-VTEP zur weiteren Verarbeitung verantwortlich ist. Datenverkehr kann an einen anderen VTEP auf einem anderen Host oder an das NSX Edge-Gateway weitergeleitet werden, um auf das physische Netzwerk zuzugreifen.

Übersicht über NSX Manager

NSX Manager bietet eine webbasierte Benutzeroberfläche, auf der Sie die NSX-T-Umgebung verwalten können. Die Anwendung hostet auch den API-Server, der API-Aufrufe verarbeitet.

Die NSX Manager-Webschnittstelle bietet zwei Methoden zum Konfigurieren von Ressourcen.

- Die Richtlinienchnittstelle: Registerkarten **Netzwerk**, **Sicherheit**, **Bestand** sowie **Planen und Fehler beheben**.
- Die erweiterte Schnittstelle: Registerkarte **Registerkarte Netzwerk und Sicherheit – Erweitert**.

Zeitpunkt der Verwendung von Richtlinien- oder erweiterten Schnittstellen

Verwenden Sie konsistent eine Benutzeroberfläche. Es gibt einige Gründe für die Wahl der Benutzeroberfläche.

- Wenn Sie eine neue Umgebung mit NSX-T Data Center 2.4 oder höher einsetzen, ist die Verwendung der neuen richtlinienbasierten Benutzeroberfläche zum Erstellen und Verwalten Ihrer Umgebung in den meisten Fällen die beste Wahl.
 - Einige Funktionen sind in der richtlinienbasierten Benutzeroberfläche nicht verfügbar. Wenn Sie diese Funktionen benötigen, verwenden Sie die erweiterte Benutzeroberfläche für alle Konfigurationen.


- Wenn Sie ein Upgrade auf NSX-T Data Center 2.4 oder höher durchführen, müssen Sie weiterhin Konfigurationsänderungen mithilfe der Benutzerschnittstelle **Netzwerk und Sicherheit – Erweitert** vornehmen.

Tabelle 1-1. Zeitpunkt der Verwendung von Richtlinien- oder erweiterten Schnittstellen

Richtlinienschnittstelle	Erweiterte Schnittstelle
Für die meisten neuen Bereitstellungen sollte die richtlinienbasierte Schnittstelle verwendet werden.	Bereitstellungen, die mithilfe der erweiterten Schnittstelle erstellt wurden, z. B. Upgrades von Versionen, bevor die richtlinienbasierte Schnittstelle vorhanden war.
NSX Cloud-Bereitstellungen	Bereitstellungen, die in andere Plug-ins integriert werden. Beispiel: NSX Container Plug-in, OpenStack und andere Cloud Management-Plattformen.
<p>Netzwerkfunktionen sind nur in der Richtlinienschnittstelle verfügbar:</p> <ul style="list-style-type: none"> ■ DNS-Dienste und -Zonen ■ VPN ■ Weiterleitungsrichtlinien für NSX Cloud 	<p>Netzwerkfunktionen sind nur in der erweiterten Schnittstelle verfügbar:</p> <ul style="list-style-type: none"> ■ Layer 3-Weiterleitung für IPv4 und IPv6 ■ Timer für die Weiterleitung der Aktiv-Benachrichtigung ■ Ändern der IP des internen Transitnetzwerks ■ Unterstützung von VIP HA auf Tier-0 ■ Standby-Verlagerung ■ Routen-Advertisement basierend auf der Auswahl der Tier-1-Präfixe ■ Loopback-Erstellung ■ BGP-Multihop ■ BGP-Quelladressen ■ Statische Routen mit BFD und Schnittstelle als nächster Hop ■ Metadaten-Proxy ■ Der mit einem isolierten Segment verbundene DHCP-Server und die statische Bindung
<p>Sicherheitsfunktionen, die nur in der Richtlinienschnittstelle verfügbar sind:</p> <ul style="list-style-type: none"> ■ Endpoint-Schutz ■ Netzwerk-Introspektion (Ost-West-Service Insertion) ■ Kontextprofile <ul style="list-style-type: none"> ■ L7-Anwendungen ■ FQDN ■ Neue verteilte Firewall und neues Gateway-Firewall-Layout <ul style="list-style-type: none"> ■ Kategorien ■ Automatische Dienstregeln 	<p>Sicherheitsfunktionen, die nur in der erweiterten Schnittstelle verfügbar sind:</p> <ul style="list-style-type: none"> ■ Möglichkeit zur Aktivierung oder Deaktivierung der verteilten Firewall, identitätsbasierten Firewall und Gateway-Firewall ■ Sitzungs-Timer für verteilte Firewall ■ Ausschlusslisten ■ Schwellenwerte von CPU und Arbeitsspeicher ■ Abschnitte für statusfreie Regeln ■ Bridge-Firewall ■ Abschnittssperrung ■ Regel-IDs für verteilte Firewalls ■ Regeln für verteilte Firewalls basierend auf IPs in Quelle und Ziel

Verwenden der Richtlinienschnittstelle

Wenn Sie sich für die Verwendung der Richtlinienschnittstelle entscheiden, verwenden Sie sie, um alle Objekte zu erstellen. Verwenden Sie nicht die erweiterte Schnittstelle, um Objekte zu erstellen.

Sie können die erweiterte Schnittstelle verwenden, um Objekte zu ändern, die in der Richtlinienschnittstelle erstellt wurden. Die Einstellungen für ein mit Richtlinien erstelltes Objekt können einen Link für die **Erweiterte Konfiguration** enthalten. Über diesen Link gelangen Sie zur erweiterten Schnittstelle, in der Sie die Konfiguration feinabstimmen können. Sie können auch mit Richtlinien erstellte Objekte direkt in der erweiterten Schnittstelle anzeigen. Neben Einstellungen, die durch Richtlinien verwaltet werden, aber in der erweiterten Schnittstelle sichtbar sind, wird dieses Symbol angezeigt: . Sie können sie nicht über die erweiterte-Benutzeroberfläche ändern.

Wo Sie die Richtlinienschnittstellen und erweiterten Schnittstellen finden

Die richtlinienbasierten und erweiterten Schnittstellen werden in verschiedenen Teilen der NSX Manager-Benutzeroberfläche angezeigt und verwenden verschiedene API-URLs.

Tabelle 1-2. Richtlinienschnittstellen und erweiterte Schnittstellen

Richtlinienschnittstelle	Erweiterte Schnittstelle
<ul style="list-style-type: none"> ■ Registerkarte Netzwerk ■ Registerkarte Sicherheit ■ Registerkarte Bestand ■ Registerkarte Planen und Fehler beheben 	Registerkarte Netzwerk und Sicherheit – Erweitert
API-URLs, die mit <code>/policy/api</code> beginnen	API-URLs, die mit <code>/api</code> beginnen

Hinweis Die Registerkarte **System** wird für alle Umgebungen verwendet. Wenn Sie Edge-Knoten, Edge-Cluster oder Transportzonen ändern, kann es bis zu 5 Minuten dauern, bis diese Änderungen auf der richtlinienbasierten Benutzeroberfläche sichtbar sind. Mithilfe von `POST /policy/api/v1/infra/sites/default/enforcement-points/default?action=reload` können Sie sofort eine Synchronisation durchführen.

Weitere Informationen zur Verwendung der Richtlinien-API finden Sie im [Einführungshandbuch zur NSX-T-Richtlinien-API](#).

Namen für Objekte, die in den Richtlinien- und erweiterten Schnittstellen erstellt wurden

Die von Ihnen erstellenden Objekte weisen unterschiedliche Namen auf, je nachdem, welche Schnittstelle zur Erstellung verwendet wurde.

Tabelle 1-3. Objektnamen

Mit der Richtlinienschnittstelle erstellte Objekte	Mit der erweiterten Schnittstelle erstellte Objekte
Segment	Logischer Switch
Tier-1-Gateway	Logischer Tier-1 Router
Tier-0-Gateway	Logischer Tier-0 Router
Gruppe	NSGroup, IP-Sets, MAC-Sets
Sicherheitsrichtlinie	Firewallabschnitt

Tabelle 1-3. Objektnamen (Fortsetzung)

Mit der Richtlinienschnittstelle erstellte Objekte	Mit der erweiterten Schnittstelle erstellte Objekte
Regel	Firewallregel
Gateway-Firewall	Edge-Firewall

Workflows für die Installation von NSX-T Data Center

2

Sie können NSX-T Data Center auf vSphere oder KVM-Hosts installieren. Sie können auch einen Bare-Metal-Server für die Verwendung von NSX-T Data Center konfigurieren.

Um Hypervisoren oder Bare Metal zu installieren oder zu konfigurieren, führen Sie die empfohlenen Aufgaben in den Workflows aus.

Dieses Kapitel enthält die folgenden Themen:

- [NSX-T Data Center-Workflow für vSphere](#)
- [NSX-T Data Center-Installations-Workflow für KVM](#)
- [NSX-T Data Center-Konfigurations-Workflow für Bare-Metal-Server](#)

NSX-T Data Center-Workflow für vSphere

Verfolgen Sie mithilfe der Prüfliste den Installationsfortschritt auf einem vSphere-Host.

Führen Sie die einzelnen Verfahren in der empfohlenen Reihenfolge durch.

- 1 Überprüfen der NSX Manager-Installationsanforderungen. Siehe [NSX Manager-Installation](#).
- 2 Konfigurieren der erforderlichen Ports und Protokolle. Siehe [Ports und Protokolle](#).
- 3 Installieren des NSX Manager. Siehe [Installieren Sie NSX Manager und die verfügbaren Appliances](#).
- 4 Anmelden beim neu erstellten NSX Manager. Siehe [Anmeldung beim neu erstellten NSX Manager](#).
- 5 Konfigurieren eines Berechnungsmanagers. Siehe [Hinzufügen eines Compute Managers](#).
- 6 Bereitstellen weiterer NSX Manager-Knoten zum Erstellen eines Clusters. Siehe [Bereitstellen von NSX Manager-Knoten zur Bildung eines Clusters über die Benutzeroberfläche](#).
- 7 Überprüfen der NSX Edge-Installationsanforderungen. Siehe [NSX Edge-Installation](#).
- 8 Installieren von NSX Edges. Weitere Informationen finden Sie unter [Installieren einer NSX Edge unter ESXi mithilfe einer grafischen vSphere-Benutzeroberfläche](#).
- 9 Erstellen eines NSX Edge-Clusters. Siehe [Erstellen eines NSX Edge-Clusters](#).
- 10 Erstellen von Transportzonen. Siehe [Erstellen von Transportzonen](#).
- 11 Erstellen von Hosttransportknoten. Siehe [Erstellen eines eigenständigen Hosts oder Bare-Metal-Server-Transportknotens](#) oder [Konfigurieren eines verwalteten Host-Transportknotens](#).

Auf jedem Host wird ein virtueller Switch erstellt. Die Managementebene sendet die Hostzertifikate an die Steuerungskomponente und überträgt Informationen der Steuerungskomponente an die Hosts. Jeder Host stellt über SSL eine Verbindung zur Steuerungskomponente her und präsentiert sein Zertifikat. Die Steuerungskomponente validiert das Zertifikat anhand des von der Managementebene bereitgestellten Hostzertifikats. Die Controller akzeptieren die Verbindung nach der erfolgreichen Validierung.

Nach der Installation

Wenn die Hosts Transportknoten sind, können Sie jederzeit Transportzonen, logische Switches, logische Router und andere Netzwerkkomponenten über die NSX Manager-Benutzeroberfläche oder -API erstellen. Wenn NSX Edges und Hosts der Verwaltungsebene beitreten, werden die logischen NSX-T Data Center-Einheiten und Konfigurationszustände automatisch an die NSX Edges und Hosts weitergegeben.

Weitere Informationen finden Sie im Dokument *Administratorhandbuch für NSX-T Data Center*.

NSX-T Data Center-Installations-Workflow für KVM

Verfolgen Sie mithilfe der Prüfliste den Installationsfortschritt auf einem KVM-Host.

Führen Sie die einzelnen Verfahren in der empfohlenen Reihenfolge durch.

- 1 Vorbereiten der vSphere-Umgebung. Siehe [Einrichten von KVM](#).
- 2 Überprüfen der NSX Manager-Installationsanforderungen. Siehe [NSX Manager-Installation](#).
- 3 Konfigurieren der erforderlichen Ports und Protokolle. Siehe [Ports und Protokolle](#).
- 4 Installieren des NSX Manager. Siehe [Installieren von NSX Manager auf KVM](#).
- 5 Anmelden beim neu erstellten NSX Manager. Siehe [Anmeldung beim neu erstellten NSX Manager](#).
- 6 Konfigurieren von Drittanbieterpaketen auf einem KVM-Host. Siehe [Installieren von Drittanbieterpaketen auf einem KVM-Host](#).
- 7 Bereitstellen weiterer NSX Manager-Knoten zum Erstellen eines Clusters. Siehe [Bereitstellen von NSX Manager-Knoten zur Bildung eines Cluster mithilfe der CLI](#).
- 8 Überprüfen der NSX Edge-Installationsanforderungen. Siehe [NSX Edge-Installation](#).
- 9 Installieren von NSX Edges. Weitere Informationen finden Sie unter [Installieren von NSX Edge mithilfe einer ISO-Datei oder einer PXE](#).
- 10 Erstellen eines NSX Edge-Clusters. Siehe [Erstellen eines NSX Edge-Clusters](#).
- 11 Erstellen von Transportzonen. Siehe [Erstellen von Transportzonen](#).
- 12 Erstellen von Hosttransportknoten. Siehe [Erstellen eines eigenständigen Hosts oder Bare-Metal-Server-Transportknotens](#).

Auf jedem Host wird ein virtueller Switch erstellt. Die Managementebene sendet die Hostzertifikate an die Steuerungskomponente und überträgt Informationen der Steuerungskomponente an die Hosts. Jeder Host stellt über SSL eine Verbindung zur Steuerungskomponente her und präsentiert sein Zertifikat. Die Steuerungskomponente validiert das Zertifikat anhand des von der Managementebene bereitgestellten Hostzertifikats. Die Controller akzeptieren die Verbindung nach der erfolgreichen Validierung.

Nach der Installation

Wenn die Hosts Transportknoten sind, können Sie jederzeit Transportzonen, logische Switches, logische Router und andere Netzwerkkomponenten über die NSX Manager-Benutzeroberfläche oder -API erstellen. Wenn NSX Edges und Hosts der Verwaltungsebene beitreten, werden die logischen NSX-T Data Center-Einheiten und Konfigurationszustände automatisch an die NSX Edges und Hosts weitergegeben.

Weitere Informationen finden Sie im Dokument *Administratorhandbuch für NSX-T Data Center*.

NSX-T Data Center-Konfigurations-Workflow für Bare-Metal-Server

Verfolgen Sie mithilfe der Prüfliste den Fortschritt, wenn Sie einen Bare-Metal-Server zur Verwendung von NSX-T Data Center konfigurieren.

Führen Sie die einzelnen Verfahren in der empfohlenen Reihenfolge durch.

- 1 Überprüfen der Bare-Metal-Anforderungen. Siehe [Bare Metal Server-Systemanforderungen](#).
- 2 Konfigurieren der erforderlichen Ports und Protokolle. Siehe [Ports und Protokolle](#).
- 3 Installieren des NSX Manager. Siehe [Installieren von NSX Manager auf KVM](#).
- 4 Konfigurieren von Drittanbieterpaketen auf dem Bare-Metal-Server. Siehe [Installieren von Drittanbieterpaketen auf einem Bare-Metal-Server](#).
- 5 Erstellen von Hosttransportknoten. Siehe [Erstellen eines eigenständigen Hosts oder Bare-Metal-Server-Transportknotens](#).

Auf jedem Host wird ein virtueller Switch erstellt. Die Managementebene sendet die Hostzertifikate an die Steuerungskomponente und überträgt Informationen der Steuerungskomponente an die Hosts. Jeder Host stellt über SSL eine Verbindung zur Steuerungskomponente her und präsentiert sein Zertifikat. Die Steuerungskomponente validiert das Zertifikat anhand des von der Managementebene bereitgestellten Hostzertifikats. Die Controller akzeptieren die Verbindung nach der erfolgreichen Validierung.

- 6 Erstellen einer Anwendungsschnittstelle für Arbeitslasten des Bare-Metal-Servers. Siehe [Erstellen der Anwendungsschnittstelle für Bare-Metal Server-Arbeitslasten](#).

Vorbereitung für die Installation

3

Stellen Sie vor der NSX-T Data Center-Installation sicher, dass Ihre Umgebung vorbereitet ist.

Dieses Kapitel enthält die folgenden Themen:

- [Systemvoraussetzungen](#)
- [Ports und Protokolle](#)
- [Installieren von NSX-T Data Center-Komponenten](#)

Systemvoraussetzungen

Vor der Installation von NSX-T Data Center muss die Umgebung bestimmte Hardware- und Ressourcenanforderungen erfüllen.

Systemanforderungen für NSX Manager-VM

Stellen Sie vor der Installation von NSX Manager sicher, dass die Umgebung die unterstützten Anforderungen erfüllt.

Hypervisor-Hostanforderungen für Transportknoten

Hypervisor	Version	CPU-Kerne	Arbeitsspeicher
vSphere	Unterstützte vSphere-Version	4	16 GB
CentOS Linux-KVM	7,4	4	16 GB
Red Hat Enterprise Linux(RHEL)-KVM	7.6, 7.5 und 7.4	4	16 GB
SUSE Linux Enterprise Server-KVM	12 SP3, SP4	4	16 GB
Ubuntu KVM	18.04 und 16.04.2 LTS	4	16 GB

Tabelle 3-1. Unterstützte Hosts für NSX Manager

Beschreibung der Unterstützung	Hypervisor
ESXi	Die unterstützten Hosts finden Sie in der VMware-Produktkompatibilitätsmatrix .
KVM	RHEL 7.4 und Ubuntu 16.04 LTS

Für ESXi-Hosts unterstützt NSX-T Data Center Hostprofile und Auto Deploy-Funktionen auf vSphere 6.7 U1 oder später. Weitere Informationen finden Sie unter *Grundlegendes zu vSphere Auto Deploy* in *VMware ESXi-Installation und -Einrichtung*.

Vorsicht Unter RHEL kann der Befehl `yum update` die Kernel-Version aktualisieren und die Kompatibilität mit NSX-T Data Center entfernen. Deaktivieren Sie das automatische Kernel-Update, wenn Sie `yum update` ausführen. Stellen Sie außerdem nach dem Ausführen des Befehls `yum install` sicher, dass NSX-T Data Center die Kernel-Version unterstützt.

Netzwerkanforderungen für Hypervisor-Hosts

Hypervisor-Hosts, auf denen NSX-T Data Center ausgeführt wird, müssen über eine kompatible Netzwerkkarte verfügen. Informationen zu unterstützten Netzwerkkarten finden Sie im [VMware-Kompatibilitätshandbuch](#).

Tipp Nutzen Sie folgende Kriterien, um im Kompatibilitätshandbuch schnell kompatible Karten zu identifizieren:

- Wählen Sie unter **E/A-Gerätetyp Netzwerk** aus.
- Um optional die unterstützte GENEVE-Kapselung zu verwenden, wählen Sie unter **Funktionen** die GENEVE-Optionen aus.
- Um optional den erweiterten Datenpfad zu verwenden, wählen Sie **N-VDS Erweiterter Datenpfad** aus.

NIC-Treiber mit erweitertem Datenpfad

Laden Sie die unterstützten NIC-Treiber von der Seite [My VMware](#) herunter.

NIC-Karte	NIC-Treiber
Intel 82599	ixgben 1.1.0.26-1OEM.670.0.0.7535516
Intel(R) Ethernet Controller X710 for 10GbE SFP+	i40en 1.2.0.0-1OEM.670.0.0.8169922
Intel(R) Ethernet Controller XL710 for 40GbE QSFP+	

NSX Manager-VM-Ressourcenanforderungen

Die Größe der virtuellen Thin-Festplatte beträgt 3,8 GB und die Größe der virtuellen Thick-Festplatte 200 GB.

Appliance-Größe	Arbeitsspeicher	vCPU	Festplattenspeicher	VM-Hardwareversion
NSX Manager Sehr klein	8 GB	2	200 GB	10 oder höher
NSX Manager Kleine VM	16 GB	4	200 GB	10 oder höher
NSX Manager Mittlere VM	24 GB	6	200 GB	10 oder höher
NSX Manager Große VM	48 GB	12	200 GB	10 oder höher

Hinweis Ab NSX-T 2.4 bietet der NSX Manager mehrere Rollen, die zuvor separate Appliances erforderten. Dazu gehören die Richtlinienrolle, die Rolle der Management Plane und die Rolle der zentralen Control Plane. Die Rolle der zentralen Control Plane wurde zuvor von der NSX Controller-Appliance bereitgestellt.

- Die Ressourcenanforderungen für sehr kleine NSX Manager-VMs gelten nur für den Cloud Service Manager.
- Die kleine NSX Manager-VM-Appliance-Größe ist nur für Test- oder Proof-of-Concept-Bereitstellungen geeignet und darf nicht in der Produktion angewendet werden.
- Die mittlere NSX Manager-VM-Appliance-Größe ist für typische Produktionsumgebungen geeignet und kann bis zu 64 Hypervisoren unterstützen.
- Die große NSX Manager-VM-Appliance-Größe ist für große Bereitstellungen mit mehr als 64 Hypervisoren konzipiert.

Um die maximale Skalierung unter Verwendung der großen NSX Manager-VM-Appliance zu erhalten, wechseln Sie zum Tool VMware Configuration Maximums unter <https://configmax.vmware.com/guest>, und wählen Sie NSX-T Data Center aus der Produktliste aus.

NSX Manager-Browserunterstützung

Die folgenden Browser werden für die Arbeit mit NSX Manager empfohlen.

Browser	Windows 10	Mac OS X 10.13, 10.14	Ubuntu 18.04
Google Chrome 76	Ja	Ja	Ja
Mozilla Firefox 68	Ja	Ja	Ja

Browser	Windows 10	Mac OS X 10.13, 10.14	Ubuntu 18.04
Microsoft Edge 44	Ja		
Apple Safari 12		Ja	

Hinweis

- Internet Explorer wird nicht unterstützt.
- Die unterstützte Mindestauflösung des Browsers beträgt 1280 x 800 Pixel.
- Sprachunterstützung: NSX Manager wurde in mehrere Sprachen lokalisiert: Englisch, Deutsch, Französisch, Japanisch, Chinesisch (vereinfacht), Koreanisch, Chinesisch (traditionell) und Spanisch. Da die NSX Manager-Lokalisierung jedoch die Browser-Spracheinstellungen verwendet, müssen Sie sicherstellen, dass Ihre Einstellungen mit der gewünschten Sprache übereinstimmen. Es gibt innerhalb der NSX Manager-Benutzeroberfläche selbst keine Möglichkeit, die Sprache einzustellen.

Anforderungen an die Netzwerklatenz

Die maximale Netzwerklatenz zwischen NSX Managern in einem NSX Manager-Cluster beträgt 10 ms.

Die maximale Netzwerklatenz zwischen NSX Managern und Transportknoten beträgt 150 ms.

Speicheranforderungen

- Die maximale Latenz für den Festplattenzugriff liegt unter 10 ms.
- Es wird empfohlen, NSX Manager auf einem freigegebenen Speicher zu platzieren.
- Der Speicher sollte hoch verfügbar sein, um einen Speicherausfall zu vermeiden, der dazu führt, dass alle NSX Manager-Dateisysteme in den schreibgeschützten Modus versetzt werden.

Informationen zur optimalen Gestaltung einer hoch verfügbaren Speicherlösung finden Sie in der Dokumentation zu Ihrer Speichertechnologie.

Systemanforderungen für NSX Edge-VM

Stellen Sie vor der Installation von NSX Edge sicher, dass die Umgebung die unterstützten Anforderungen erfüllt.

NSX Edge-Knoten werden nur auf ESXi-basierten Hosts mit Intel-basierten Chipsätzen unterstützt. Andernfalls kann der EVC-Modus von vSphere verhindern, dass NSX Edge-Knoten gestartet werden, wobei eine Fehlermeldung in der Konsole angezeigt wird.

Hinweis Nur VMXNET 3-vNIC wird für die NSX Edge-VM unterstützt.

NSX Cloud-Hinweis Wenn Sie NSX Cloud verwenden, wird NSX Public Cloud Gateway (PCG) für jede unterstützte Public Cloud in einer einzelnen Standardgröße bereitgestellt. Einzelheiten dazu finden Sie unter [Bereitstellen oder Verknüpfen von NSX Public Cloud Gateways](#).

NSX Edge-VM-Ressourcenanforderungen

Appliance-Größe	Arbeitsspeicher	vCPU	Festplattenspeicher	VM-Hardwareversion
NSX Edge Klein	4 GB	2	200 GB	11 oder höher (vSphere 6.0 oder höher)
NSX Edge Mittel	8 GB	4	200 GB	11 oder höher (vSphere 6.0 oder höher)
NSX Edge Groß	32 GB	8	200 GB	11 oder höher (vSphere 6.0 oder höher)

Hinweis

- Die kleine NSX Edge-VM-Appliance-Größe eignet sich für Test- oder Proof-of-Concept-Bereitstellungen.
- Die mittlere NSX Edge-Appliance-Größe ist für typische Produktionsumgebungen geeignet.
- Die große NSX Edge-Appliance-Größe ist für Umgebungen mit Load Balancing konzipiert. Weitere Informationen finden Sie unter [Skalieren von Load Balancer-Ressourcen](#) im *Administratorhandbuch für NSX-T Data Center*.

CPU-Anforderungen für NSX Edge-VM

Zur Unterstützung von DPDK muss die zugrundeliegende Plattform die folgenden Anforderungen erfüllen:

- CPU muss über die AESNI-Funktionalität verfügen.
- CPU muss Unterstützung für umfangreiche Seiten (1 GB) bieten.

Hardware	Typ
CPU	<ul style="list-style-type: none"> ■ Intel Xeon E7-xxxx (CPU-Generation Westmere-EX und höher) ■ Intel Xeon 56xx (Westmere-EP) ■ Intel Xeon E5-xxxx (CPU-Generation Sandy Bridge und höher) ■ Intel Xeon Platinum (alle Generationen) ■ Intel Xeon Gold (alle Generationen) ■ Intel Xeon Silver (alle Generationen) ■ Intel Xeon Bronze (alle Generationen)

Anforderungen der NSX Edge-Bare-Metal-Bereitstellung

Stellen Sie vor der Konfiguration der NSX Edge-Bare-Metal-Bereitstellung sicher, dass die Umgebung die unterstützten Anforderungen erfüllt.

NSX Edge-Knoten werden nur auf ESXi-basierten Hosts mit Intel-basierten Chipsätzen unterstützt. Andernfalls kann der EVC-Modus von vSphere verhindern, dass Edge-Knoten gestartet werden, und es wird eine Fehlermeldung in der Konsole angezeigt.

Arbeitsspeicher-, CPU- und Festplattenanforderungen für NSX Edge-Bare-Metal-Bereitstellungen

Arbeitsspeicher	CPU-Kerne	Festplattenspeicher
32 GB	8	200 GB

DPDK CPU-Anforderungen für NSX Edge-Bare-Metal-Bereitstellungen

Zur Unterstützung von DPDK muss die zugrundeliegende Plattform die folgenden Anforderungen erfüllen:

- CPU muss über die AES-NI-Funktionalität verfügen.
- CPU muss Unterstützung für umfangreiche Seiten (1 GB) bieten.

Hardware	Typ
CPU	<ul style="list-style-type: none"> ■ Intel Xeon E7-xxxx (CPU-Generation Westmere-EX und höher) ■ Intel Xeon 56xx (Westmere-EP) ■ Intel Xeon E5-xxxx (CPU-Generation Sandy Bridge und höher) ■ Intel Xeon Platinum (alle Generationen) ■ Intel Xeon Gold (alle Generationen) ■ Intel Xeon Silver (alle Generationen) ■ Intel Xeon Bronze (alle Generationen)

Hardwareanforderungen für NSX Edge-Bare-Metal-Bereitstellungen

Stellen Sie sicher, dass die NSX Edge-Bare-Metal-Hardware in dieser URL <https://certification.ubuntu.com/server/models/?release=18.04%20LTS&category=Server> aufgeführt ist. Wenn die Hardware nicht aufgeführt ist, werden der Speicher, der Videoadapter oder die Komponenten der Hauptplatine auf der NSX Edge-Appliance unter Umständen nicht ordnungsgemäß ausgeführt.

Netzwerkkartenanforderungen für NSX Edge-Bare-Metal-Bereitstellungen

Typ der Netzwerkkarte	Beschreibung	ID des PCI-Geräts
Intel XXV710	I40E_DEV_ID_25G_B	0x158A
	I40E_DEV_ID_25G_SFP28	0x158B
Intel X520/Intel 82599	IXGBE_DEV_ID_82599_KX4	0x10F7
	IXGBE_DEV_ID_82599_KX4_MEZZ	0x1514
	IXGBE_DEV_ID_82599_KR	0x1517
	IXGBE_DEV_ID_82599_COMBO_BACK	0x10F8
	PLANE	0x000C
	IXGBE_SUBDEV_ID_82599_KX4_KR_	0x10F9
	MEZZ	0x10FB
	IXGBE_DEV_ID_82599_CX4	0x11A9
	IXGBE_DEV_ID_82599_SFP	0x1F72
	IXGBE_SUBDEV_ID_82599_SFP	0x17D0
	IXGBE_SUBDEV_ID_82599_RNDC	0x0470
	IXGBE_SUBDEV_ID_82599_560FLR	0x1507
	IXGBE_SUBDEV_ID_82599_ECNA_DP	0x154D
	IXGBE_DEV_ID_82599_SFP_EM	0x154A
	IXGBE_DEV_ID_82599_SFP_SF2	0x1558
	IXGBE_DEV_ID_82599_SFP_SF_QP	0x1557
	IXGBE_DEV_ID_82599_QSFP_SF_QP	0x10FC
	IXGBE_DEV_ID_82599EN_SFP	0x151C
	IXGBE_DEV_ID_82599_XAUI_LOM	
	IXGBE_DEV_ID_82599_T3_LOM	
Intel X540	IXGBE_DEV_ID_X540T	0x1528
	IXGBE_DEV_ID_X540T1	0x1560
Intel X550	IXGBE_DEV_ID_X550T	0x1563
	IXGBE_DEV_ID_X550T1	0x15D1
Intel X710	I40E_DEV_ID_SFP_X710	0x1572
	I40E_DEV_ID_KX_C	0x1581
	I40E_DEV_ID_10G_BASE_T	0x1586
Intel XL710	I40E_DEV_ID_KX_B	0x1580
	I40E_DEV_ID_QSFP_A	0x1583
	I40E_DEV_ID_QSFP_B	0x1584
	I40E_DEV_ID_QSFP_C	0x1585
Cisco VIC 1387	Cisco UCS Virtual Interface Card 1387	0x0043

Bare Metal Server-Systemanforderungen

Bevor Sie den Bare Metal Server konfigurieren, stellen Sie sicher, dass Ihr Server die unterstützten Anforderungen erfüllt.

Wichtig Der Benutzer, der die Installation durchführt, benötigt möglicherweise sudo-Befehlsberechtigungen für einige der Verfahren. Siehe [Installieren von Drittanbieterpaketen auf einem Bare-Metal-Server](#).

Bare Metal Server-Anforderungen

Betriebssystem	Version	CPU-Kerne	Arbeitsspeicher
CentOS Linux	7,4	4	16 GB
Red Hat Enterprise Linux (RHEL)	7.5 und 7.4	4	16 GB
SUSE Linux Enterprise Server	12 SP3	4	16 GB
Ubuntu	18.04 und 16.04.2 LTS	4	16 GB

Bare Metal Linux-Container-Anforderungen

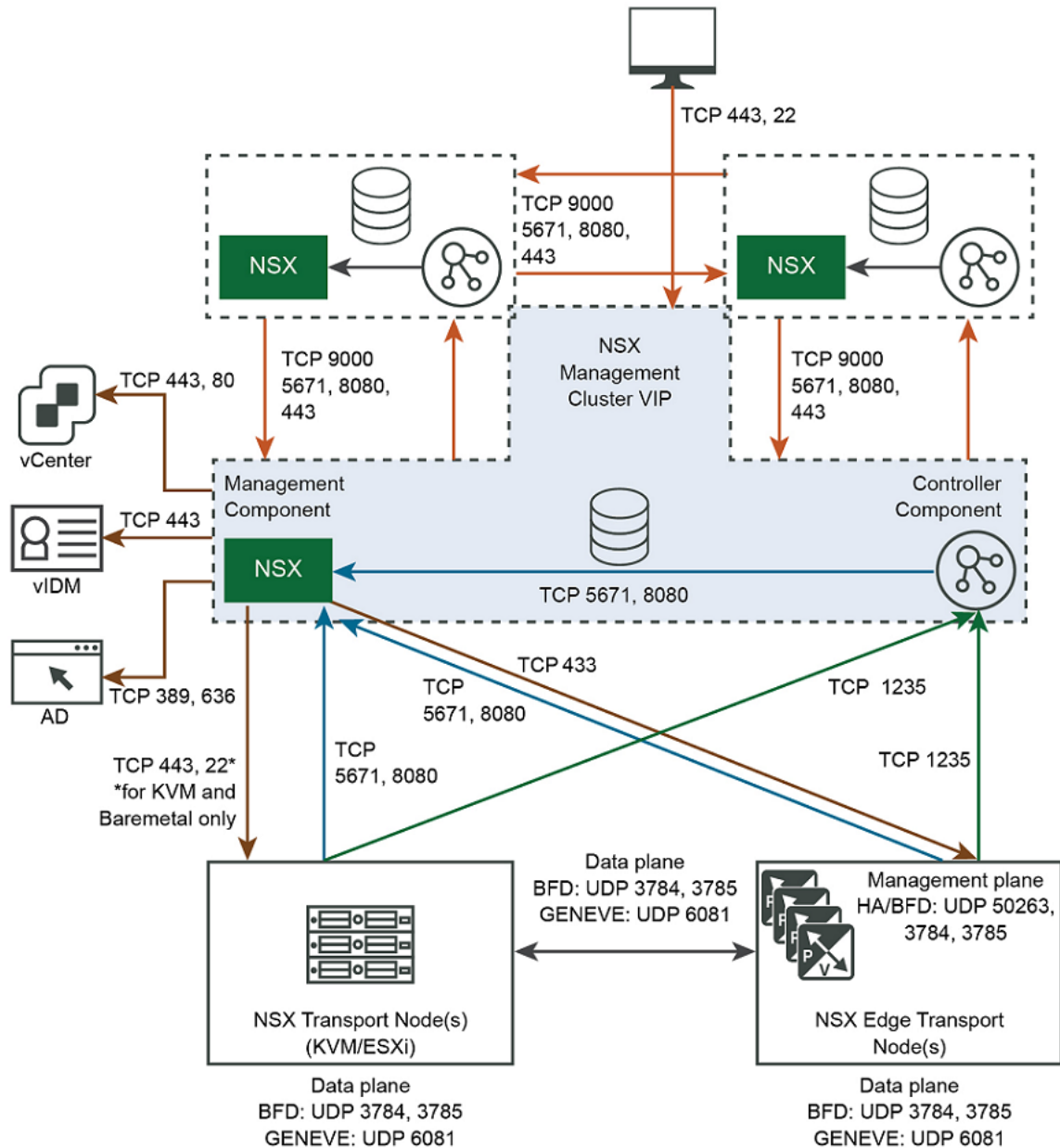
Informationen zu den Bare Metal Linux-Container-Anforderungen finden Sie im *NSX-T Container Plug-In für OpenShift – Installations- und Administratorhandbuch*.

Ports und Protokolle

Ports und Protokolle ermöglichen Kommunikationspfade zwischen Knoten in NSX-T Data Center. Die Pfade werden gesichert und authentifiziert, und ein Speicherort für die Anmeldedaten wird verwendet, um gegenseitige Authentifizierung einzurichten.

Hinweis Die erforderlichen Ports und Protokolle müssen sowohl auf den physischen als auch auf den Host-Hypervisor-Firewalls offen sein.

Abbildung 3-1. Ports und Protokolle von NSX-T Data Center



Standardmäßig sind alle Zertifikate selbstsignierte Zertifikate. Die northbound-GUI- und API-Zertifikate und privaten Schlüssel können durch Zertifikate mit Signatur einer Zertifizierungsstelle ersetzt werden.

Interne Daemons kommunizieren über die Loopback- oder UNIX-Domänen-Sockets:

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

- ESXi: netcpa, ESX-DP (im Kernel)

Hinweis Um den Zugriff auf NSX-T Data Center-Knoten zu erhalten, müssen Sie SSH auf diesen Knoten aktivieren.

NSX Cloud-Hinweis Eine Liste der Ports, die für die Bereitstellung von NSX Clouderforderlich sind, finden Sie unter [Zugriff auf Ports und Protokolle auf CSM für Hybrid-Konnektivität ermöglichen](#).

Von NSX Manager verwendete TCP- und UDP-Ports

NSX Manager verwendet bestimmte TCP- und UDP-Ports, um mit anderen Komponenten und Produkten zu kommunizieren. Diese Ports müssen in der Firewall offen sein.

Sie können einen API-Aufruf oder einen CLI-Befehl verwenden, um benutzerdefinierte Ports zum Übertragen von Dateien (standardmäßig 22) und zum Exportieren von Syslog-Daten (standardmäßig 514 und 6514) anzugeben. Wenn Sie dies tun, müssen Sie die Firewall entsprechend konfigurieren.

Tabelle 3-2. Von NSX Manager verwendete TCP- und UDP-Ports

Quelle	Ziel	Port	Protokoll	Beschreibung
NSX Manager	Active Directory	389	TCP	Active Directory
NSX Controllers, NSX Edge-Knoten, Transportknoten	NSX Manager	5671	TCP	NSX-Messaging
NSX Controller, NSX Edge-Knoten, Transportknoten, vCenter Server	NSX Manager	8080	TCP	HTTP-Repository für Upgrade-Installation
NSX Manager	NSX Manager	9000	TCP	Interner Datenspeicherzugriff
NSX Manager	DNS-Server	53	TCP	DNS
NSX Manager	DNS-Server	53	UDP	DNS
NSX Manager	NSX Edge	443	TCP	HTTPS
NSX Manager	Management-SCP-Server	22	TCP	SSH (Hochladen von Support-Paketen, Sicherungen und so weiter)
NSX Manager	NTP-Server	123	UDP	NTP
NSX Manager	SNMP-Server	161, 162	TCP	SNMP
NSX Manager	SNMP-Server	161, 162	UDP	SNMP
NSX Manager	Syslog-Server	514	TCP	Syslog
NSX Manager	Syslog-Server	514	UDP	Syslog
NSX Manager	Syslog-Server	6514	TCP	Syslog
NSX Manager	Syslog-Server	6514	UDP	Syslog
NSX Manager	Traceroute-Ziel	3343 4– 3352 3	UDP	Traceroute

Tabelle 3-2. Von NSX Manager verwendete TCP- und UDP-Ports (Fortsetzung)

Quelle	Ziel	Port	Protokoll	Beschreibung
NSX Manager	vCenter Server	80	TCP	NSX Manager zum Berechnen der Manager-Kommunikation (vCenter Server), wenn konfiguriert.
NSX Manager	vCenter Server	443	TCP	NSX Manager zum Berechnen der Manager-Kommunikation (vCenter Server), wenn konfiguriert.
NSX Manager	vIDM	443	TCP	vIDM
NSX Manager	NSX Manager	443	TCP	NSX Manager-zu-NSX Manager-Kommunikation
Verwaltungsclients	NSX Manager	22	TCP	SSH (standardmäßig deaktiviert)
Verwaltungsclients	NSX Manager	443	TCP	NSX-API-Server
SNMP-Server	NSX Manager	161	UDP	SNMP

Von NSX Edge verwendete TCP- und UDP-Ports

NSX Edge verwendet bestimmte TCP- und UDP-Ports, um mit anderen Komponenten und Produkten zu kommunizieren. Diese Ports müssen in der Firewall offen sein.

Sie können einen API-Aufruf oder einen CLI-Befehl verwenden, um benutzerdefinierte Ports zum Übertragen von Dateien (standardmäßig 22) und zum Exportieren von Syslog-Daten (standardmäßig 514 und 6514) anzugeben. Wenn Sie dies tun, müssen Sie die Firewall entsprechend konfigurieren.

Tabelle 3-3. Von NSX Edge verwendete TCP- und UDP-Ports

Quelle	Ziel	Port	Protokoll	Beschreibung
Verwaltungsclients	NSX Edge-Knoten	22	TCP	SSH (standardmäßig deaktiviert)
NSX Agent	NSX Edge-Knoten	5555	TCP	NSX Cloud: Agent der Instanz kommuniziert mit dem NSX Cloud-Gateway.
NSX Edge-Knoten	DNS-Server	53	UDP	DNS
NSX Edge-Knoten	Management-SCP- oder -SSH-Server	22	TCP	SSH (Hochladen von Support-Paketen, Sicherungen und so weiter)
NSX Edge-Knoten	NSX Controller-Knoten	1235	TCP	netcpa
NSX Edge-Knoten	NSX Edge-Knoten	1167	TCP	DHCP-Backend
NSX Edge-Knoten	NSX Edge-Knoten	2480	TCP	Nestdb
NSX Edge-Knoten	NSX Edge-Knoten	6666	TCP	NSX Cloud: lokale NSX Edge-Kommunikation.

Tabelle 3-3. Von NSX Edge verwendete TCP- und UDP-Ports (Fortsetzung)

Quelle	Ziel	Port	Protokoll	Beschreibung
NSX Edge-Knoten	NSX Edge-Knoten	50263	UDP	Hohe Verfügbarkeit
NSX Edge-Knoten	NSX Manager-Knoten	443	TCP	HTTPS
NSX Edge-Knoten	NSX Manager-Knoten	5671	TCP	NSX-Messaging
NSX Edge-Knoten	NSX Manager-Knoten	8080	TCP	NAPI, NSX-T Data Center-Upgrade
NSX Edge-Knoten	NTP-Server	123	UDP	NTP
NSX Edge-Knoten	OpenStack Nova-API-Server	3000–9000	TCP	Metadaten-Proxy
NSX Edge-Knoten	SNMP-Server	161, 162	TCP	SNMP
NSX Edge-Knoten	SNMP-Server	161, 162	UDP	SNMP
NSX Edge-Knoten	Syslog-Server	514	TCP	Syslog
NSX Edge-Knoten	Syslog-Server	514	UDP	Syslog
NSX Edge-Knoten	Syslog-Server	6514	TCP	Syslog
NSX Edge-Knoten	Syslog-Server	6514	UDP	Syslog
NSX Edge-Knoten	Traceroute-Ziel	33434–33523	UDP	Traceroute
NSX Edge-Knoten, Transportknoten	NSX Edge-Knoten	3784, 3785	UDP	BFD zwischen der TEP-IP-Adresse des Transportknotens in den Daten.
SNMP-Server	NSX Edge-Knoten	161	UDP	SNMP

Von ESXi, KVM-Hosts und Bare-Metal-Server verwendete TCP- und UDP-Ports

Für ESXi, KVM-Hosts und Bare-Metal-Server müssen bei Verwendung als Transportknoten bestimmte TCP- und UDP-Ports verfügbar sein.

Tabelle 3-4. Von ESXi- und KVM-Hosts verwendete TCP- und UDP-Ports

Quelle	Ziel	Port	Protokoll	Beschreibung
ESXi-Host	NSX Controller	123 5	TCP	Steuerungskomponente – Kommunikation von LCP zu CCP
ESXi-Host	NSX Manager	567 1	TCP	AMQP-Kommunikationskanal zu NSX Manager

Tabelle 3-4. Von ESXi- und KVM-Hosts verwendete TCP- und UDP-Ports (Fortsetzung)

Quelle	Ziel	Port	Protokoll	Beschreibung
ESXi-Host	NSX Manager	8080	TCP	Installation und Upgrade des HTTP-Repositorys
ESXi und KVM-Host	NSX Manager	443	TCP	Verwaltungs- und Bereitstellungsverbindung
ESXi und KVM-Host	NSX Manager	443	TCP	Installation und Upgrade des HTTP-Repositorys
GENEVE Terminierungsendpunkt (TEP)	GENEVE Terminierungsendpunkt (TEP)	6081	UDP	Transportnetzwerk
KVM-Host	NSX Manager	5671	TCP	AMQP-Kommunikationskanal zu NSX Manager
KVM-Host	NSX Controller	1235	TCP	Steuerungskomponente – Kommunikation von LCP zu CCP
KVM-Host	NSX Manager	8080	TCP	Installation und Upgrade des HTTP-Repositorys
NSX Manager	ESXi-Host	443	TCP	Verwaltungs- und Bereitstellungsverbindung
NSX Manager	KVM-Host	443	TCP	Verwaltungs- und Bereitstellungsverbindung
ESXi und KVM-Host	Syslog-Server	514	TCP	Syslog
ESXi und KVM-Host	Syslog-Server	514	UDP	Syslog
ESXi und KVM-Host	Syslog-Server	6514	TCP	Syslog
ESXi und KVM-Host	Syslog-Server	6514	UDP	Syslog
NSX-T Data Center-Transportknoten	NSX-T Data Center-Transportknoten	3784, 3785	UDP	BFD-Sitzung zwischen TEPs, im Datenpfad unter Verwendung der TEP-Schnittstelle

Installieren von NSX-T Data Center-Komponenten

Sie müssen die Hauptkomponenten NSX Manager und NSX Edge zur Verwendung von NSX-T Data Center installieren.

NSX Manager-Installation

NSX Manager bietet eine grafische Benutzeroberfläche (GUI) und REST-APIs zum Erstellen, Konfigurieren und Überwachen von NSX-T Data Center-Komponenten wie logischen Switches, logischen Routern und Firewalls.

NSX Manager stellt eine Systemansicht bereit und ist die Managementkomponente von NSX-T Data Center.

Für Hochverfügbarkeit unterstützt NSX-T Data Center einen Verwaltungscluster mit drei NSX Managern. Es empfiehlt sich, für eine Produktionsumgebung einen Verwaltungscluster bereitzustellen. Für eine Proof-of-Concept-Umgebung können Sie einen einzelnen NSX Manager bereitstellen.

Anforderung an die NSX Manager-Bereitstellung, -Plattform und -Installation

In der folgenden Tabelle sind die Anforderungen für NSX Manager-Bereitstellung, -Plattform und -Installation aufgeführt.

Anforderungen	Beschreibung
Unterstützte Bereitstellungsmethoden	<ul style="list-style-type: none"> ■ OVA/OVF ■ QCOW2
Unterstützte Plattformen	<p>Siehe Systemanforderungen für NSX Manager-VM.</p> <p>Es wird empfohlen, unter ESXi die NSX Manager-Appliance auf freigegebenem Speicher zu installieren.</p>
IP-Adresse	Ein NSX Manager muss eine statische IP-Adresse aufweisen. Sie können die IP-Adresse nach der Installation nicht mehr ändern.
Kennwort für NSX-T Data Center-Appliance	<ul style="list-style-type: none"> ■ mindestens 12 Zeichen ■ mindestens ein Kleinbuchstabe ■ mindestens ein Großbuchstabe ■ mindestens eine Zahl ■ mindestens ein Sonderzeichen ■ mindestens fünf unterschiedliche Zeichen ■ keine Wörterbuchwörter ■ keine Palindrome ■ mehr als vier monotone Zeichenfolgen ist nicht zulässig
Hostname	<p>Geben Sie beim Installieren von NSX Manager einen Hostnamen an, der keine ungültigen Zeichen wie z. B. einen Unterstrich enthält. Wenn der Hostname ein ungültiges Zeichen enthält, wird der Hostname nach der Bereitstellung auf nsx-manager festgelegt.</p> <p>Weitere Informationen zu Hostnamenbeschränkungen finden Sie unter https://tools.ietf.org/html/rfc952 und https://tools.ietf.org/html/rfc1123.</p>
VMware Tools	Auf der unter ESXi ausgeführten NSX Manager-VM sind VMware Tools installiert. Entfernen oder aktualisieren Sie VMTools nicht.

Anforderungen	Beschreibung
System	<ul style="list-style-type: none"> ■ Stellen Sie sicher, dass die Systemanforderungen erfüllt sind. Siehe Systemvoraussetzungen. ■ Stellen Sie sicher, dass die erforderlichen Ports geöffnet sind. Siehe Ports und Protokolle. ■ Stellen Sie sicher, dass auf dem ESXi-Host ein Datenspeicher konfiguriert und verfügbar ist. ■ 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 haben, die von NSX Manager verwendet werden. ■ Erstellen Sie das Ziel-VM-Portgruppennetzwerk, wenn noch keines vorhanden ist. Platzieren Sie die NSX-T Data Center-Appliances in einem VM-Verwaltungsnetzwerk. Wenn Sie über mehrere Verwaltungsnetzwerke verfügen, können Sie statische Routen von der NSX-T Data Center-Appliance zu den anderen Netzwerken hinzufügen. ■ Planen Sie Ihr IPv4 oder IPv6-IP-Adressschema für NSX Manager.
OVF-Berechtigungen	<p>Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Bereitstellen einer OVF-Vorlage auf dem ESXi-Host verfügen.</p> <p>Ein Managementtool, das OVF-Vorlagen wie vCenter Server oder den vSphere-Client bereitstellen kann. Das OVF-Bereitstellungstool muss Konfigurationsoptionen für manuelle Konfiguration unterstützen.</p> <p>Die Version des OVF-Tools muss 4.0 oder höher sein.</p>
Client-Plug-In	Das Client-Integrations-Plug-In muss installiert sein.

Hinweis Wenn Sie NSX Manager neu installieren, neu starten oder das **admin**-Kennwort bei der ersten Anmeldung geändert haben, kann der NSX Manager-Start einige Minuten dauern.

NSX Manager-Installationsszenarien

Wichtig Wenn Sie NSX Manager über eine OVA- oder OVF-Datei installieren (entweder über den vSphere Client oder die Befehlszeile), werden OVA-/OVF-Eigenschaftswerte wie Benutzernamen, Kennwörter oder IP-Adressen erst beim Einschalten der virtuellen Maschine validiert.

- Wenn Sie einen Benutzernamen für den **admin**- oder **audit**-Benutzer angeben, muss der Name eindeutig sein. Wenn Sie den gleichen Namen angeben, wird er ignoriert, und die Standardnamen (**admin** und **audit**) werden verwendet.
- Wenn das Kennwort für den **admin**-Benutzer die Komplexitätsanforderungen nicht erfüllt, müssen Sie sich bei NSX Manager über SSH oder bei der Konsole als **admin**-Benutzer mit dem Kennwort **vmware** anmelden. Sie werden aufgefordert, das Kennwort zu ändern.
- Wenn das Kennwort für den **audit**-Benutzer nicht die Anforderungen an die Komplexität erfüllt, wird das Benutzerkonto deaktiviert. Um das Konto zu aktivieren, melden Sie sich bei NSX Manager über SSH oder an der Konsole als **admin**-Benutzer an, und führen Sie den Befehl **set user audit** aus, um das Kennwort des **audit**-Benutzers festzulegen (das aktuelle Kennwort ist leer).

- Wenn das Kennwort für den **root**-Benutzer die Komplexitätsanforderungen nicht erfüllt, müssen Sie sich bei NSX Manager über SSH oder an der Konsole als **root**-Benutzer mit dem Kennwort **vmware** anmelden. Sie werden aufgefordert, das Kennwort zu ändern.

Vorsicht Änderungen, die am NSX-T Data Center vorgenommen werden, während Sie mit den **root**-Benutzeranmeldedaten angemeldet sind, können zu Systemausfällen führen und sich möglicherweise auf Ihr Netzwerk auswirken. Sie können Änderungen unter Verwendung der **root**-Benutzeranmeldedaten nur mithilfe des Teams von VMware Support vornehmen.

Hinweis Die Kerndienste der Appliance werden erst gestartet, wenn ein Kennwort mit ausreichender Komplexität festgelegt wurde.

Nach der Bereitstellung von NSX Manager über eine OVA-Datei können Sie die IP-Einstellungen der VM nicht durch Ausschalten der VM und Bearbeiten der OVA-Einstellungen in vCenter Server ändern.

Konfigurieren von NSX Manager für den Zugriff durch den DNS-Server

Standardmäßig greifen Transportknoten basierend auf ihren IP-Adressen auf NSX Manager zu. Dies kann jedoch auch auf den DNS-Namen der NSX Manager basieren.

Durch Aktivieren der FQDN-Nutzung (DNS) auf NSX Managern kann sich die IP-Adresse der Manager ändern, ohne dass sich dies auf die Transportknoten auswirkt.

Sie aktivieren die FQDN-Nutzung, indem Sie die FQDNs der NSX Manager veröffentlichen.

Hinweis Die Aktivierung der FQDN-Nutzung (DNS) auf NSX Managern ist für Multisite Lite und NSX Cloud und Bereitstellungen erforderlich. (Für alle anderen Bereitstellungstypen ist sie optional.) Weitere Informationen finden Sie unter *Bereitstellung von NSX-T Data Center für mehrere Sites* im *Administratorhandbuch für NSX-T Data Center* und [Kapitel 11 Installieren von NSX Cloud-Komponenten](#) in diesem Handbuch.

Veröffentlichen der FQDNs der NSX Manager

Nach der Installation der Hauptkomponenten von NSX-T Data Center und der Installation von CSM richten Sie zur Aktivierung von NAT unter Verwendung des FQDN die Einträge für die Suche und die umgekehrte Suche im NSX-T-DNS-Server in Ihrer Bereitstellung ein.

Zusätzlich müssen Sie unter Verwendung der NSX-T-API die Veröffentlichung der NSX Manager-FQDNs aktivieren.

Beispielanforderung: PUT `https://<nsx-mgr>/api/v1/configs/management`

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

Beispielantwort:

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

Weitere Informationen finden Sie unter *Handbuch für die NSX-T Data Center-API*.

Hinweis Validieren Sie nach dem Veröffentlichen der FQDNs den Zugriff durch die Transportknoten wie im nächsten Abschnitt beschrieben.

Validieren des Zugriffs über den FQDN durch Transportknoten

Stellen Sie nach dem Veröffentlichen der FQDNs der NSX Manager sicher, dass die Transportknoten erfolgreich auf die NSX Manager zugreifen.

Melden Sie sich mithilfe von SSH bei einem Transportknoten an, z. B. einem Hypervisor oder einem Edge-Knoten, und führen Sie den CLI-Befehl `get controllers` aus.

Beispielantwort:

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

NSX Edge-Installation

NSX Edge liefert Routing-Dienste und Konnektivität zu Netzwerk-NSX Edges, die sich außerhalb der NSX-T Data Center-Bereitstellung befinden. Ein NSX Edge ist erforderlich, wenn Sie einen Tier-0- oder Tier-1-Router mit zustandsbehafteten Diensten wie Netzwerkadressübersetzung (Network Address Translation, NAT), VPN usw. bereitstellen möchten.

Hinweis Pro NSX Edge-Knoten kann nur ein Tier-0-Router vorhanden sein. Allerdings können mehrere Tier-1-Lastrouter auf einem NSX Edge-Knoten gehostet werden. NSX Edge-VMs unterschiedlicher Größe können im selben Cluster kombiniert werden. Es wird jedoch nicht empfohlen.

Tabelle 3-5. Anforderung an die NSX Edge-Bereitstellung, -Plattformen und -Installation

Anforderungen	Beschreibung
Unterstützte Bereitstellungsmethoden	<ul style="list-style-type: none"> ■ OVA/OVF ■ ISO mit PXE ■ ISO ohne PXE
Unterstützte Plattformen	<p>NSX Edge wird nur auf ESXi oder in Bare-Metal-Bereitstellungen unterstützt.</p> <p>Auf KVM wird NSX Edge nicht unterstützt.</p>
PXE-Installation	Die Kennwort-Zeichenfolge muss mit dem sha-512-Algorithmus für das Kennwort des root und admin-Benutzers verschlüsselt werden.

Tabelle 3-5. Anforderung an die NSX Edge-Bereitstellung, -Plattformen und -Installation (Fortsetzung)

Anforderungen	Beschreibung
Kennwort für NSX-T Data Center-Appliance	<ul style="list-style-type: none"> ■ mindestens 12 Zeichen ■ mindestens ein Kleinbuchstabe ■ mindestens ein Großbuchstabe ■ mindestens eine Zahl ■ mindestens ein Sonderzeichen ■ mindestens fünf unterschiedliche Zeichen ■ keine Wörterbuchwörter ■ keine Palindrome ■ mehr als vier monotone Zeichenfolgen ist nicht zulässig
Hostname	Geben Sie beim Installieren von NSX Edge einen Hostnamen an, der keine ungültigen Zeichen wie z. B. einen Unterstrich enthält. Wenn der Hostname ein ungültiges Zeichen enthält, wird der Hostname nach der Bereitstellung auf localhost festgelegt. Weitere Informationen zu Hostnamenbeschränkungen finden Sie unter https://tools.ietf.org/html/rfc952 und https://tools.ietf.org/html/rfc1123 .
VMware Tools	Auf der unter ESXi ausgeführten NSX Edge-VM sind VMware Tools installiert. Entfernen oder aktualisieren Sie VMTtools nicht.
System	Stellen Sie sicher, dass die Systemanforderungen erfüllt sind. Siehe Systemanforderungen für NSX Edge-VM .
Ports	Stellen Sie sicher, dass die erforderlichen Ports geöffnet sind. Siehe Ports und Protokolle .
IP-Adressen	Wenn Sie über mehrere Verwaltungsnetzwerke verfügen, können Sie statische Routen von der NSX-T Data Center-Appliance zu den anderen Netzwerken hinzufügen. Planen Sie Ihr IPv4- oder IPv6-IP-Adressschema für NSX Edge.
OVF-Vorlage	<ul style="list-style-type: none"> ■ Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Bereitstellen einer OVF-Vorlage auf dem ESXi-Host verfügen. ■ Stellen Sie sicher, dass Hostnamen keine Unterstriche enthalten. Andernfalls wird der Hostname auf <i>nsx-manager</i> gesetzt. ■ Ein Managementtool, das OVF-Vorlagen wie vCenter Server oder den vSphere-Client bereitstellen kann. Das OVF-Bereitstellungstool muss Konfigurationsoptionen für eine manuelle Konfiguration unterstützen. ■ Das Client-Integrations-Plug-In muss installiert sein.
NTP-Server	Auf allen NSX Edge-Servern in einem Edge-Cluster muss derselbe NTP-Server konfiguriert sein.

NSX Edge-Installationsszenarien

Wichtig Wenn Sie NSX Edge über eine OVA- oder OVF-Datei installieren (entweder per vSphere-Webclient oder Befehlszeile), werden OVA/OVF-Eigenschaftswerte wie Benutzernamen, Kennwörter oder IP-Adressen erst beim Einschalten der virtuellen Maschine validiert.

- Wenn Sie einen Benutzernamen für den **admin**- oder **audit**-Benutzer angeben, muss der Name eindeutig sein. Wenn Sie den gleichen Namen angeben, wird er ignoriert, und die Standardnamen (**admin** und **audit**) werden verwendet.
- Wenn das Kennwort für den **admin**-Benutzer die Komplexitätsanforderungen nicht erfüllt, müssen Sie sich bei NSX Edge über SSH oder bei der Konsole als **admin**-Benutzer mit dem Kennwort **vmware** anmelden. Sie werden aufgefordert, das Kennwort zu ändern.
- Wenn das Kennwort für den **audit**-Benutzer nicht die Anforderungen an die Komplexität erfüllt, wird das Benutzerkonto deaktiviert. Um das Konto zu aktivieren, melden Sie sich bei NSX Edge über SSH oder an der Konsole als **admin**-Benutzer an, und führen Sie den Befehl **set user audit** aus, um das Kennwort des **audit**-Benutzers festzulegen (das aktuelle Kennwort ist leer).
- Wenn das Kennwort für den **root**-Benutzer die Komplexitätsanforderungen nicht erfüllt, müssen Sie sich bei NSX Edge über SSH oder an der Konsole als **root**-Benutzer mit dem Kennwort **vmware** anmelden. Sie werden aufgefordert, das Kennwort zu ändern.

Vorsicht Änderungen, die am NSX-T Data Center vorgenommen werden, während Sie mit den **root**-Benutzeranmeldedaten angemeldet sind, können zu Systemausfällen führen und sich möglicherweise auf Ihr Netzwerk auswirken. Sie können Änderungen unter Verwendung der **root**-Benutzeranmeldedaten nur mithilfe des Teams von VMware Support vornehmen.

Hinweis Die Kerndienste der Appliance werden erst gestartet, wenn ein Kennwort mit ausreichender Komplexität festgelegt wurde.

Nach der Bereitstellung von NSX Edge über eine OVA-Datei können Sie die IP-Einstellungen der VM nicht durch Ausschalten der VM und Bearbeiten der OVA-Einstellungen in vCenter Server ändern.

Verbinden von NSX Edge mit der Managementebene

Durch Verbinden der NSX Edges mit der Managementebene wird sichergestellt, dass NSX Manager und die NSX Edges miteinander kommunizieren können.

Voraussetzungen

Vergewissern Sie sich, dass Sie über Administratorberechtigungen zur Anmeldung bei den NSX Edges und der NSX Manager-Appliance verfügen.

Verfahren

- 1 Öffnen Sie eine SSH-Sitzung mit der NSX Manager-Appliance.
- 2 Öffnen Sie eine SSH-Sitzung mit NSX Edge.

- 3 Führen Sie den Befehl `get certificate api thumbprint` auf der NSX Manager-Appliance aus.

Die Befehlsausgabe besteht aus einer Reihe von alphanumerischen Zeichen, die für diesen NSX Manager eindeutig sind.

Beispiel:

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

- 4 Führen Sie auf NSX Edge den Befehl **join management-plane** aus.

Geben Sie die folgenden Informationen an:

- Hostname oder IP-Adresse von NSX Manager mit einer optionalen Portnummer
- NSX Manager-Benutzername
- Zertifikatsfingerabdruck von NSX Manager
- NSX Manager-Kennwort

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

Wiederholen Sie diesen Befehl auf jedem NSX Edge-Knoten.

- 5 Überprüfen Sie das Ergebnis, indem Sie den Befehl `get managers` auf den NSX Edges ausführen.

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

- 6 Wählen Sie auf der NSX Manager-Benutzeroberfläche die Seite **System > Fabric > Knoten > Edge-Transportknoten** aus.

Die NSX Manager-Konnektivität muss „Aktiv“ sein. Wenn die NSX Manager-Konnektivität nicht „Aktiv“ ist, aktualisieren Sie das Browserfenster.

Nächste Schritte

Fügen Sie NSX Edge als Transportknoten hinzu. Siehe [Erstellen eines NSX Edge-Transportknotens](#).

Installieren von NSX-T Data Center auf vSphere

4

Sie können die NSX-T Data Center-Komponenten NSX Manager und NSX Edge mithilfe der Benutzeroberfläche oder Befehlszeilenschnittstelle (CLI) installieren.

Stellen Sie sicher, dass Sie über die unterstützte vSphere-Version verfügen. Weitere Informationen finden Sie unter [vSphere-Unterstützung](#).

Dieses Kapitel enthält die folgenden Themen:

- [Installieren Sie NSX Manager und die verfügbaren Appliances](#)
- [Installieren einer NSX Edge unter ESXi mithilfe einer grafischen vSphere-Benutzeroberfläche](#)

Installieren Sie NSX Manager und die verfügbaren Appliances

Sie können den vSphere Client verwenden, um den NSX Manager oder den Cloud Service Manager als virtuelle Appliance bereitzustellen.

Cloud Service Manager ist eine virtuelle Appliance, die NSX-T Data Center-Komponenten verwendet und in Ihre Public Cloud integriert.

Voraussetzungen

- Stellen Sie sicher, dass die Systemanforderungen erfüllt sind. Siehe [Systemvoraussetzungen](#).
- Stellen Sie sicher, dass die erforderlichen Ports geöffnet sind. Siehe [Ports und Protokolle](#).
- Stellen Sie sicher, dass auf dem ESXi-Host ein Datenspeicher konfiguriert und verfügbar ist.
- 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 haben, die von NSX Manager verwendet werden.
- Erstellen Sie das Ziel-VM-Portgruppennetzwerk, wenn noch keines vorhanden ist. Platzieren Sie die NSX-T Data Center-Appliances in einem VM-Verwaltungsnetzwerk.

Wenn Sie über mehrere Verwaltungsnetzwerke verfügen, können Sie statische Routen von der NSX-T Data Center-Appliance zu den anderen Netzwerken hinzufügen.
- Planen Sie Ihr IPv4 oder IPv6-IP-Adressschema für NSX Manager.

Verfahren

- 1 Suchen Sie im VMware-Download-Portal nach der NSX-T Data Center-OVA-Datei.
Kopieren Sie die Download-URL oder laden Sie die OVA-Datei herunter.
- 2 Wählen Sie im vSphere Client den Host aus, auf dem NSX-T Data Center installiert werden soll.
- 3 Wählen Sie im Kontextmenü die Option **OVF-Vorlage bereitstellen** aus, um den Installationsassistenten zu starten.
- 4 Geben Sie die URL der herunterzuladenden OVA-Datei ein oder navigieren Sie zur OVA-Datei.
- 5 Geben Sie einen Namen für die NSX Manager-VM ein.
Der eingegebene Name wird in der vSphere-Bestandsliste angezeigt.
- 6 Wählen Sie eine Computing-Ressource für die NSX Manager-Appliance aus.
 - ◆ Für die Installation auf einem von vCenter verwalteten ESXi-Host wählen Sie einen Host aus, auf dem die NSX Manager-Appliance bereitgestellt werden soll.
 - ◆ Für die Installation auf einem eigenständigen ESXi-Host wählen Sie den Host aus, auf dem die NSX Manager-Appliance bereitgestellt werden soll.
- 7 Überprüfen Sie die Details der OVF-Vorlage.
- 8 Reservieren Sie Arbeitsspeicher für die NSX Manager-Appliance, um eine optimale Leistung zu erreichen.

Legen Sie die Reservierung so fest, dass NSX Manager über ausreichend Arbeitsspeicher verfügt, um eine effiziente Ausführung sicherzustellen. Siehe [Systemanforderungen für NSX Manager-VM](#).
- 9 Wählen Sie einen Datenspeicher für die Dateien der NSX Manager-Appliance aus.
- 10 Wählen Sie ein Zielnetzwerk für jedes Quellnetzwerk aus.
- 11 Wählen Sie die Portgruppe oder das Zielnetzwerk für NSX Manager.
- 12 Geben Sie die System-Root-, CLI-Admin- und Audit-Kennwörter für die NSX Manager ein.
Ihre Kennwörter müssen den Einschränkungen zur Kennwortkomplexität entsprechen.
 - mindestens 12 Zeichen
 - mindestens ein Kleinbuchstabe
 - mindestens ein Großbuchstabe
 - mindestens eine Zahl
 - mindestens ein Sonderzeichen
 - mindestens fünf unterschiedliche Zeichen
 - keine Wörterbuchwörter
 - keine Palindrome
 - mehr als vier monotone Zeichenfolgen ist nicht zulässig

13 Geben Sie den Hostnamen des NSX Manager ein.

Hinweis Der Hostname muss ein gültiger Domänenname sein. Stellen Sie sicher, dass jeder Teil des Hostnamens (Domäne/Unterdomäne), der per Punkt getrennt ist, mit einem alphabetischen Zeichen beginnen muss.

14 Akzeptieren Sie die **NSX Manager**-Standardrolle für VM.

Wählen Sie die **nsx-cloud-service-manager**-Rolle aus dem Dropdown-Menü aus, um die NSX Cloud-Appliance zu installieren.

15 Geben Sie das Standard-Gateway, die IPv4-Adresse und Netzmaske des Verwaltungsnetzwerks, die DNS- und NTP-IP-Adresse ein.**16** Aktivieren Sie SSH und gewähren Sie die Root-SSH-Anmeldung an der NSX Manager-Befehlszeile.
Standardmäßig sind diese Optionen aus Sicherheitsgründen deaktiviert.**17** Stellen Sie sicher, dass die gesamte Spezifikation der benutzerdefinierten OVF-Vorlage korrekt ist, und klicken Sie auf **Beenden**, um die Installation zu starten.

Die Installation kann 7 bis 8 Minuten dauern.

18 Öffnen Sie über den vSphere Client die VM-Konsole von NSX Manager, um den Startvorgang zu verfolgen.**19** Melden Sie sich nach dem Start von NSX Manager als Administrator bei der CLI an und führen Sie den Befehl `get interface eth0` aus, um zu überprüfen, ob die IP-Adresse erwartungsgemäß angewendet wurde.**20** Geben Sie den Befehl `get services` ein, um sicherzustellen, dass alle Dienste ausgeführt werden.
Wenn die Dienste nicht ausgeführt werden, warten Sie, bis alle Dienste gestartet wurden.

Hinweis Die folgenden Dienste werden nicht standardmäßig ausgeführt: `liagent`, `migration-coordinator` und `snmp`. Sie können sie wie folgt starten:

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

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

21 Stellen Sie sicher, dass Ihr NSX Manager über die erforderliche Konnektivität verfügt.

Stellen Sie sicher, dass Sie die folgenden Aufgaben ausführen können.

- Führen Sie für Ihren NSX Manager von einer anderen Maschine aus einen Ping-Vorgang aus.
- Der NSX Manager kann einen Ping-Vorgang für das zugehörige Standard-Gateway ausführen.
- Der NSX Manager kann mithilfe der Verwaltungsschnittstelle einen Ping-Vorgang für die Hypervisor-Hosts ausführen, die sich im selben Netzwerk wie der NSX Manager befinden.

- Der NSX Manager kann einen Ping-Vorgang für den zugehörigen DNS-Server und NTP-Server ausführen.
- Wenn Sie SSH aktiviert haben, stellen Sie sicher, dass Sie eine SSH-Verbindung zu NSX Manager herstellen können.

Wenn keine Konnektivität hergestellt werden kann, stellen Sie sicher, dass sich der Netzwerkadapter der virtuellen Appliance im richtigen Netzwerk oder VLAN befindet.

Nächste Schritte

Melden Sie sich über einen unterstützten Webbrowser beim NSX Manager an. Siehe [Anmeldung beim neu erstellten NSX Manager](#).

Installieren von NSX Manager unter ESXi mithilfe des OVF-Befehlszeilentools

Wenn Sie die Installation von NSX Manager automatisieren oder CLI dazu verwenden möchten, können Sie dazu das VMware OVF-Tool verwenden. Dabei handelt es sich um ein Befehlszeilendienstprogramm.

Standardmäßig sind `nsx_isSshEnabled` und `nsx_allowSSHRootLogin` aus Sicherheitsgründen deaktiviert. Wenn diese Optionen deaktiviert sind, können Sie SSH nicht verwenden oder sich nicht bei der NSX Manager-Befehlszeile anmelden. Wenn Sie `nsx_isSshEnabled` aktivieren, nicht jedoch `nsx_allowSSHRootLogin`, können Sie eine SSH-Verbindung mit NSX Manager herstellen, sich aber nicht als Root anmelden.

Voraussetzungen

- Stellen Sie sicher, dass die Systemanforderungen erfüllt sind. Siehe [Systemvoraussetzungen](#).
- Stellen Sie sicher, dass die erforderlichen Ports geöffnet sind. Siehe [Ports und Protokolle](#).
- Stellen Sie sicher, dass auf dem ESXi-Host ein Datenspeicher konfiguriert und verfügbar ist.
- 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 haben, die von NSX Manager verwendet werden.
- Erstellen Sie das Ziel-VM-Portgruppennetzwerk, wenn noch keines vorhanden ist. Platzieren Sie die NSX-T Data Center-Appliances in einem VM-Verwaltungsnetzwerk.

Wenn Sie über mehrere Verwaltungsnetzwerke verfügen, können Sie statische Routen von der NSX-T Data Center-Appliance zu den anderen Netzwerken hinzufügen.

- Planen Sie Ihr IPv4 oder IPv6-IP-Adressschema für NSX Manager.

Verfahren

- 1 Führen Sie den Befehl `ovftool` mit den richtigen Parametern aus.

Der Prozess hängt davon ab, ob der Host eigenständig ist oder von vCenter Server verwaltet wird.

- Bei einem eigenständigen Host:
 - Windows-Beispiel:

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

Hinweis Der obige Windows-Codeblock verwendet den umgekehrten Schrägstrich (\), um die Fortsetzung der Befehlszeile anzugeben. Lassen Sie bei der eigentlichen Verwendung den umgekehrten Schrägstrich weg und setzen Sie den gesamten Befehl in eine einzelne Zeile.

Hinweis Im obigen Beispiel ist 10.168.110.51 die IP-Adresse der Hostmaschine, auf der NSX Manager bereitgestellt werden soll.

- Linux-Beispiel:

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

```

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

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

mgresxhost01="192.168.110.113"

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

```

Das Ergebnis sollte etwa wie folgt aussehen:

```

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

```

- Bei einem von vCenter Server verwalteten Host:
 - Windows-Beispiel:

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

Hinweis Der obige Windows-Codeblock verwendet den umgekehrten Schrägstrich (\), um die Fortsetzung der Befehlszeile anzugeben. Lassen Sie bei der eigentlichen Verwendung den umgekehrten Schrägstrich weg und setzen Sie den gesamten Befehl in eine einzelne Zeile.

- Linux-Beispiel:

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

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

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

```

logLevel="trivia"

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

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

```

Das Ergebnis sollte etwa wie folgt aussehen:

```

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

```

- 2 Reservieren Sie Arbeitsspeicher für die NSX Manager-Appliance, um eine optimale Leistung zu erreichen.

Legen Sie die Reservierung so fest, dass NSX Manager über ausreichend Arbeitsspeicher verfügt, um eine effiziente Ausführung sicherzustellen. Siehe [Systemanforderungen für NSX Manager-VM](#).

- 3 Öffnen Sie über den vSphere Client die VM-Konsole von NSX Manager, um den Startvorgang zu verfolgen.
- 4 Melden Sie sich nach dem Start von NSX Manager als Administrator bei der CLI an und führen Sie den Befehl `get interface eth0` aus, um zu überprüfen, ob die IP-Adresse erwartungsgemäß angewendet wurde.
- 5 Stellen Sie sicher, dass Ihr NSX Manager über die erforderliche Konnektivität verfügt.

Stellen Sie sicher, dass Sie die folgenden Aufgaben ausführen können.

- Führen Sie für Ihren NSX Manager von einer anderen Maschine aus einen Ping-Vorgang aus.
- Der NSX Manager kann einen Ping-Vorgang für das zugehörige Standard-Gateway ausführen.
- Der NSX Manager kann mithilfe der Verwaltungsschnittstelle einen Ping-Vorgang für die Hypervisor-Hosts ausführen, die sich im selben Netzwerk wie der NSX Manager befinden.
- Der NSX Manager kann einen Ping-Vorgang für den zugehörigen DNS-Server und NTP-Server ausführen.
- Wenn Sie SSH aktiviert haben, stellen Sie sicher, dass Sie eine SSH-Verbindung zu NSX Manager herstellen können.

Wenn keine Konnektivität hergestellt werden kann, stellen Sie sicher, dass sich der Netzwerkadapter der virtuellen Appliance im richtigen Netzwerk oder VLAN befindet.

Nächste Schritte

Melden Sie sich über einen unterstützten Webbrowser beim NSX Manager an. Siehe [Anmeldung beim neu erstellten NSX Manager](#).

Konfigurieren von NSX-T Data Center zum Anzeigen des GRUB-Menü zum Startzeitpunkt

Die Konfiguration der NSX-T Data Center-Appliance, um das GRUB-Menü zum Startzeitpunkt anzuzeigen, ist erforderlich, um das Root-Kennwort der NSX-T Data Center-Appliance zurückzusetzen.

Wichtig Wenn die Konfiguration nach der Bereitstellung der Appliance nicht durchgeführt wird und Sie das Root-, Admin- oder Überwachungskennwort vergessen, ist ein Zurücksetzen nicht möglich.

Verfahren

- 1 Melden Sie sich bei der VM als Root-Benutzer an.
- 2 Ändern Sie den Wert für den Parameter `GRUB_HIDDEN_TIMEOUT` in der Datei `/etc/default/grub`.
`GRUB_HIDDEN_TIMEOUT=2`
- 3 (Optional) Ändern Sie das GRUB-Kennwort in der Datei `/etc/grub.d/40_custom`.
Das Standardkennwort lautet `VMware1`.

4 Aktualisieren Sie die GRUB-Konfiguration.

update-grub

Anmeldung beim neu erstellten NSX Manager

Nach der Installation von NSX Manager können Sie weitere Installationsaufgaben mithilfe der Benutzeroberfläche ausführen.

Nach der Installation von NSX Manager können Sie dem Programm zur Verbesserung der Benutzerfreundlichkeit für NSX-T Data Center beitreten. Unter „Programm zur Verbesserung der Benutzerfreundlichkeit“ im *Administratorhandbuch für NSX-T Data Center* finden Sie weitere Informationen dazu, wie Sie am Programm teilnehmen und sich später wieder abmelden können.

Voraussetzungen

Stellen Sie sicher, dass NSX Manager installiert ist. Siehe [Installieren Sie NSX Manager und die verfügbaren Appliances](#).

Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
Die Nutzungsbedingungen werden angezeigt.
- 2 Lesen und akzeptieren Sie die Bedingungen der Endbenutzer-Lizenzvereinbarung.
- 3 Geben Sie an, ob Sie dem Programm zur Verbesserung der Benutzerfreundlichkeit beitreten möchten.
- 4 Klicken Sie auf **Speichern**

Hinzufügen eines Compute Managers

Ein Compute Manager, z. B. vCenter Server, ist eine Anwendung, die Ressourcen wie Hosts und virtuelle Maschinen verwaltet.

NSX-T Data Center fragt Compute Manager ab, um Informationen zu Änderungen wie hinzugefügten oder entfernten Hosts oder virtuellen Maschinen zu erhalten, und aktualisiert die Bestandsliste entsprechend. Optional haben Sie die Möglichkeit, einen Compute Manager hinzuzufügen, denn NSX-T Data Center erhält die Bestandslisteninformationen auch ohne Compute Manager, zum Beispiel von eigenständigen Hosts und VMs.

Wenn Sie einen vCenter Server-Compute Manager hinzufügen, müssen Sie die Anmeldedaten eines vCenter Server-Benutzers angeben. Sie können die Anmeldedaten des vCenter Server-Administrators angeben oder eine Rolle und einen Benutzer speziell für NSX-T Data Center erstellen und die Anmeldedaten dieses Benutzers angeben. Diese Rolle muss über die folgenden vCenter Server-Berechtigungen verfügen:

Extension.Register extension

Extension.Unregister extension

Extension.Update extension
Sessions.Message
Sessions.Validate session
Sessions.View and stop sessions
Host.Configuration.Maintenance
Host.Local Operations.Create virtual machine
Host.Local Operations.Delete virtual machine
Host.Local Operations.Reconfigure virtual machine
Tasks
Scheduled task
Global.Cancel task
Permissions.Reassign role permissions
Resource.Assign vApp to resource pool
Resource.Assign virtual machine to resource pool
Virtual Machine.Configuration
Virtual Machine.Guest Operations
Virtual Machine.Provisioning
Virtual Machine.Inventory
Network.Assign network
vApp

Weitere Informationen zu vCenter Server-Rollen und -Berechtigungen finden Sie im Dokument *vSphere-Sicherheit*.

Voraussetzungen

- Stellen Sie sicher, dass Sie die unterstützte vSphere-Version verwenden. Siehe [Unterstützte vSphere-Version](#).
- IPv6- und IPv4-Kommunikation mit vCenter Server.
- Stellen Sie sicher, dass Sie die empfohlene Anzahl an Compute Managern verwenden. Siehe <https://configmax.vmware.com/home>.

Hinweis NSX-T Data Center unterstützt nicht die Registrierung desselben vCenter Server mit mehr als einem NSX Manager.

Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **System > Fabric > Compute Managers > Hinzufügen** aus.

3 Vervollständigen Sie die Details zum Compute Manager.

Option	Beschreibung
Name und Beschreibung	Geben Sie den Namen zum Identifizieren von vCenter Server ein. Sie können optional spezielle Details wie z. B. die Anzahl Cluster in vCenter Serverbeschreiben.
Domänenname/IP-Adresse	Geben Sie die IP-Adresse für vCenter Server ein.
Typ	Behalten Sie die Standardoption bei.
Benutzername und Kennwort	Geben Sie die vCenter Server-Anmeldedaten ein.
Fingerabdruck	Geben Sie den Wert für den vCenter Server-SHA-256-Fingerabdruckalgorithmus ein.

Wenn Sie den Fingerabdruckwert leer lassen, werden Sie aufgefordert, den vom Server bereitgestellten Fingerabdruck zu akzeptieren.

Nachdem Sie den Fingerabdruck akzeptiert haben, dauert es einige Sekunden, bis NSX-T Data Center die vCenter Server-Ressourcen ermittelt und registriert.

4 Wenn sich das Symbol „Fortschritt“ von **In Bearbeitung** in **Nicht registriert** ändert, führen Sie die folgenden Schritte aus, um den Fehler zu beheben.

- a Wählen Sie die Fehlermeldung und klicken Sie auf **Beheben**. Eine mögliche Fehlermeldung lautet:

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

- b Geben Sie die vCenter Server-Anmeldedaten ein und klicken Sie auf **Beheben**.

Wenn eine bestehende Registrierung vorhanden ist, wird sie ersetzt.

Ergebnisse

Es dauert einige Zeit, um den Compute Manager bei vCenter Server zu registrieren und bis der Verbindungsstatus als Aktiv angezeigt wird.

Sie können auf den Namen des Compute Managers klicken, um Details anzuzeigen, den Compute Manager zu bearbeiten oder um Tags zu verwalten, die für den Compute Manager gelten.

Bereitstellen von NSX Manager-Knoten zur Bildung eines Clusters über die Benutzeroberfläche

Sie können für hohe Verfügbarkeit und Zuverlässigkeit mehrere NSX Manager-Knoten bereitstellen.

Nachdem die neuen Knoten bereitgestellt wurden, stellen diese Knoten eine Verbindung zum NSX Manager-Knoten her, um einen Cluster zu bilden. Die empfohlene Anzahl von geclusterten NSX Manager-Knoten beträgt drei.

Hinweis Eine Bereitstellung mehrerer NSX Manager-Knoten mithilfe der Benutzeroberfläche wird nur auf von vCenter Server verwalteten ESXi-Hosts unterstützt.

Alle Repository-Details und das Kennwort des ersten bereitgestellten NSX Manager-Knotens werden mit den neu bereitgestellten Knoten im Cluster synchronisiert.

Voraussetzungen

- Stellen Sie sicher, dass ein NSX Manager-Knoten installiert ist. Siehe [Installieren Sie NSX Manager und die verfügbaren Appliances](#).
- Stellen Sie sicher, dass der Berechnungsmanager konfiguriert ist. Siehe [Hinzufügen eines Compute Managers](#).
- Stellen Sie sicher, dass die Systemanforderungen erfüllt sind. Siehe [Systemvoraussetzungen](#).
- Stellen Sie sicher, dass die erforderlichen Ports geöffnet sind. Siehe [Ports und Protokolle](#).
- Stellen Sie sicher, dass auf dem ESXi-Host ein Datenspeicher konfiguriert und verfügbar ist.
- 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 haben, die von NSX Manager verwendet werden.
- Erstellen Sie das Ziel-VM-Portgruppennetzwerk, wenn noch keines vorhanden ist. Platzieren Sie die NSX-T Data Center-Appliances in einem VM-Verwaltungsnetzwerk.

Wenn Sie über mehrere Verwaltungsnetzwerke verfügen, können Sie statische Routen von der NSX-T Data Center-Appliance zu den anderen Netzwerken hinzufügen.

Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **System > Appliances > Übersicht > Knoten hinzufügen** aus.
- 3 Geben Sie die üblichen Attributdetails von NSX Manager an.

Option	Beschreibung
Berechnungsmanager	Der registrierte Ressourcenberechnungsmanager wird mit Daten befüllt.
SSH aktivieren	Schalten Sie die Schaltfläche um, um eine SSH-Anmeldung am neuen NSX Manager-Knoten zu ermöglichen.
Root-Zugriff aktivieren	Schalten Sie die Schaltfläche um, um den Root-Zugriff auf den neuen NSX Manager-Knoten zu ermöglichen.

Option	Beschreibung
CLI-Benutzername und Kennwortbestätigung	<p>Legen Sie das CLI-Kennwort und die Kennwortbestätigung für den neuen Knoten fest.</p> <p>Ihr Kennwort muss den Einschränkungen zur Kennwortkomplexität entsprechen.</p> <ul style="list-style-type: none"> ■ mindestens 12 Zeichen ■ mindestens ein Kleinbuchstabe ■ mindestens ein Großbuchstabe ■ mindestens eine Zahl ■ mindestens ein Sonderzeichen ■ mindestens fünf unterschiedliche Zeichen ■ keine Wörterbuchwörter ■ keine Palindrome ■ mehr als vier monotone Zeichenfolgen ist nicht zulässig <p>Der CLI-Benutzername ist bereits auf Admin festgelegt.</p>
Root-Kennwort und Kennwortbestätigung	<p>Legen Sie das Root-Kennwort und die Kennwortbestätigung für den neuen Knoten fest.</p> <p>Ihr Kennwort muss den Einschränkungen zur Kennwortkomplexität entsprechen.</p> <ul style="list-style-type: none"> ■ mindestens 12 Zeichen ■ mindestens ein Kleinbuchstabe ■ mindestens ein Großbuchstabe ■ mindestens eine Zahl ■ mindestens ein Sonderzeichen ■ mindestens fünf unterschiedliche Zeichen ■ keine Wörterbuchwörter ■ keine Palindrome ■ mehr als vier monotone Zeichenfolgen ist nicht zulässig
DNS-Server	Geben Sie die IP-Adresse des DNS-Servers ein, der im vCenter Server verfügbar ist.
NTP-Server	Geben Sie die IP-Adresse des NTP-Servers ein.

4 Geben Sie die Knotendetails zu NSX Manager ein.

Option	Beschreibung
Name	Geben Sie einen Namen für den NSX Manager-Knoten ein.
Cluster	Weisen Sie über das Dropdown-Menü den Cluster zu, dem der Knoten beitreten wird.
Ressourcenpool oder Host	Weisen Sie aus dem Dropdown-Menü entweder einen Ressourcenpool oder einen Host für den Knoten zu.
Datenspeicher	Wählen Sie einen Datenspeicher für die Knoten-Dateien aus dem Dropdown-Menü aus.
Netzwerk	Wählen Sie aus dem Dropdown-Menü das Netzwerk aus.
Verwaltungs-IP/Netmask	Geben Sie die IP-Adresse und Netzmaske ein.
Verwaltungs-Gateway	Geben Sie die Gateway-IP-Adresse ein.

- 5 (Optional) Klicken Sie auf **Neuer Knoten** und konfigurieren Sie einen anderen Knoten.

Wiederholen Sie die Schritte 3 bis 4.

- 6 Klicken Sie auf **Fertigstellen**.

Die neuen Knoten werden bereitgestellt. Sie können den Bereitstellungsvorgang auf der Seite **System > Appliances > Übersicht** oder dem vCenter Server nachverfolgen.

- 7 Warten Sie 10 bis 15 Minuten, bis die Bereitstellung, die Bildung von Clustern und die Repository-Synchronisierung abgeschlossen sind.

Alle Repository-Details und das Kennwort des ersten bereitgestellten NSX Manager-Knotens werden mit den neu bereitgestellten Knoten im Cluster synchronisiert.

- 8 Melden Sie sich nach dem Start von NSX Manager als Administrator bei der CLI an und führen Sie den Befehl `get interface eth0` aus, um zu überprüfen, ob die IP-Adresse erwartungsgemäß angewendet wurde.

- 9 Geben Sie den Befehl `get services` ein, um sicherzustellen, dass alle Dienste ausgeführt werden.

Wenn die Dienste nicht ausgeführt werden, warten Sie, bis alle Dienste gestartet wurden.

Hinweis Die folgenden Dienste werden nicht standardmäßig ausgeführt: `liagent`, `migration-coordinator` und `snmp`. Sie können sie wie folgt starten:

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

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

- 10 Melden Sie sich am ersten bereitgestellten NSX Manager-Knoten an und geben Sie den Befehl `get cluster status` ein, um sicherzustellen, dass die Knoten erfolgreich zum Cluster hinzugefügt werden.

- 11 Stellen Sie sicher, dass Ihr NSX Manager über die erforderliche Konnektivität verfügt.

Stellen Sie sicher, dass Sie die folgenden Aufgaben ausführen können.

- Führen Sie für Ihren NSX Manager von einer anderen Maschine aus einen Ping-Vorgang aus.
- Der NSX Manager kann einen Ping-Vorgang für das zugehörige Standard-Gateway ausführen.
- Der NSX Manager kann mithilfe der Verwaltungsschnittstelle einen Ping-Vorgang für die Hypervisor-Hosts ausführen, die sich im selben Netzwerk wie der NSX Manager befinden.
- Der NSX Manager kann einen Ping-Vorgang für den zugehörigen DNS-Server und NTP-Server ausführen.
- Wenn Sie SSH aktiviert haben, stellen Sie sicher, dass Sie eine SSH-Verbindung zu NSX Manager herstellen können.

Wenn keine Konnektivität hergestellt werden kann, stellen Sie sicher, dass sich der Netzwerkadapter der virtuellen Appliance im richtigen Netzwerk oder VLAN befindet.

Nächste Schritte

Konfigurieren Sie NSX Edge. Siehe [Installieren einer NSX Edge unter ESXi mithilfe einer grafischen vSphere-Benutzeroberfläche](#).

Bereitstellen von NSX Manager-Knoten zur Bildung eines Cluster mithilfe der CLI

Durch Verknüpfen des NSX Manager zur Bildung eines Clusters über die CLI wird sichergestellt, dass alle NSX Manager-Knoten im Cluster miteinander kommunizieren können.

Voraussetzungen

Die Installation von NSX-T Data Center-Komponenten muss abgeschlossen sein.

Verfahren

- 1 Öffnen Sie eine SSH-Sitzung für den ersten bereitgestellten NSX Manager-Knoten.
- 2 Melden Sie sich mit den Anmeldedaten des Administrators an.
- 3 Führen Sie auf dem NSX Manager-Knoten den Befehl `get certificate api thumbprint` aus.
Die Befehlsausgabe besteht aus einer Reihe von Zahlen, die für diesen NSX Manager eindeutig sind.
- 4 Führen Sie den Befehl `get cluster config` aus, um die Kennung des ersten bereitgestellten NSX Manager-Clusters zu erhalten.
- 5 Fügen Sie den NSX Manager-Knoten zum Cluster hinzu.

Hinweis Sie müssen den Verknüpfungsbefehl für den neu bereitgestellte NSX Manager-Knoten ausführen.

Geben Sie die folgenden NSX Manager-Informationen an:

- Hostname oder IP-Adressen des Knoten, dem Sie beitreten möchten
- Cluster-ID
- Benutzername
- Kennwort
- Zertifikatfingerabdruck

Sie können den CLI-Befehl oder den API-Aufruf verwenden.

- CLI-Befehl

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

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

Der Vorgang zur Verknüpfung und Cluster-Stabilisierung dauert möglicherweise 10 bis 15 Minuten.

- 6 Fügen Sie den dritten NSX Manager-Knoten zum Cluster hinzu.

Wiederholen Sie Schritt 5.

- 7 Überprüfen Sie den Cluster-Status, indem Sie den Befehl `get cluster status` auf Ihren Hosts ausführen.
- 8 Wählen Sie **System > Appliances > Übersicht** und überprüfen Sie die Cluster-Konnektivität.

Nächste Schritte

Erstellen Sie eine Transportzone. Siehe [Erstellen eines eigenständigen Hosts oder Bare-Metal-Server-Transportknotens](#).

Konfigurieren einer virtuellen IP-Adresse (VIP) für einen Cluster

Um Fault Tolerance und Hochverfügbarkeit für NSX Manager-Knoten bereitzustellen, weisen Sie einem Mitglied des NSX-T-Clusters eine virtuelle IP-Adresse (VIP) zu.

NSX Manager eines Clusters werden Teil einer HTTPS-Gruppe zum Bearbeiten von API- und Benutzeroberflächenanforderungen. Der Leader-Knoten des Clusters übernimmt die Zuständigkeit für die Set-VIP des Clusters, um alle API- und UI-Anforderungen zu bedienen. Alle API- und UI-Anforderungen, die von Clients eingehen, werden an den Leader-Knoten weitergeleitet.

Hinweis Bei der Zuweisung virtueller IP-Adressen müssen alle NSX Manager-VMs im Cluster im selben Subnetz konfiguriert werden.

Wenn der Leader-Knoten, der für die VIP zuständig ist, nicht verfügbar ist, wählt NSX-T einen neuen Leader aus. Der neue Leader ist für die VIP zuständig. Er sendet ein Gratuitous ARP-Paket, um die neue VIP-zu-Mac-Adresszuordnung anzukündigen. Nach der Auswahl eines neuen Leader-Knotens werden neue API- und Benutzeroberflächenanforderungen an den neuen Leader-Knoten gesendet.

Das Failover der VIP auf einen neuen Leader-Knoten des Clusters kann einige Minuten dauern. Wenn das VIP-Failover auf einen neuen Leader-Knoten durchgeführt wird, weil der vorherige Leader-Knoten nicht mehr verfügbar war, müssen die Anmeldedaten erneut authentifiziert werden, damit API-Anforderungen an den neuen Leader-Knoten weitergeleitet werden.

Hinweis Die VIP ist nicht als Load Balancer vorgesehen und kann nicht verwendet werden, wenn Sie die vIDM **Integration des externen Load Balancers** unter **System > Benutzer > Konfiguration** aktivieren. Richten Sie keine VIP ein, wenn Sie den externen Load Balancer von vIDM verwenden möchten. Weitere Informationen finden Sie unter [Konfigurieren der VMware Identity Manager-Integration im Administratorhandbuch für NSX-T Data Center](#).

Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wechseln Sie zu **System > Übersicht**.

- 3 Klicken Sie im Feld „Virtuelle IP“ auf **Bearbeiten**.
- 4 Geben Sie die VIP für den Cluster ein. Stellen Sie sicher, dass die VIP Teil desselben Subnetzes wie die anderen Verwaltungsknoten ist.
- 5 Klicken Sie auf **Speichern**.
- 6 Um den Clusterstatus und den API-Führer der HTTPS-Gruppe zu überprüfen, geben Sie den NSX Manager-CLI-Befehl `get cluster status verbose` in die NSX Manager-Konsole oder über SSH ein.

Im Folgenden finden Sie eine Beispielausgabe, in der die Führungslinie fett markiert ist.

```

Group Type: HTTPS
Group Status: STABLE

Members:
  UUID                                FQDN                                IP
STATUS
cdb93642-ccba-fdf4-8819-90bf018cd727    nsx-manager    192.196.197.84
UP
51a13642-929b-8dfc-3455-109e6cc2a7ae    nsx-manager    192.196.198.156
UP
d0de3642-d03f-c909-9cca-312fd22e486b    nsx-manager    192.196.198.54
UP

Leaders:
  SERVICE                                LEADER                                LEASE
VERSION
api                                cdb93642-ccba-fdf4-8819-90bf018cd727    8

```

- 7 Um VIP-Fehler zu beheben, überprüfen Sie die Reverse-Proxy-Protokolle unter `/var/log/proxy/reverse-proxy.log` und die Clustermanager-Protokolle unter `/var/log/cbm/cbm.log` in der NSX Manager-CLI.

Ergebnisse

Alle API-Anforderungen an NSX-T werden an die virtuelle IP-Adresse des Clusters umgeleitet, für die der Leader-Knoten zuständig ist. Der Leader-Knoten leitet die Anforderung dann an die anderen Komponenten der Appliance weiter.

Installieren einer NSX Edge unter ESXi mithilfe einer grafischen vSphere-Benutzeroberfläche

Wenn Sie eine interaktive NSX Edge-Installation bevorzugen, können Sie den vSphere Web Client verwenden.

Wichtig In NSX-T wird vMotion von der NSX Edge-VM nicht unterstützt.

Voraussetzungen

Siehe NSX Edge-Netzwerkanforderungen im Handbuch [NSX Edge-Installation](#).

Verfahren

- 1 Suchen Sie im VMware-Download-Portal nach der OVA-Datei der NSX Edge-Appliance.
Kopieren Sie die Download-URL oder laden Sie die OVA-Datei auf Ihren Computer herunter.
- 2 Wählen Sie im vSphere Client den Host aus, auf dem die NSX Edge-Appliance installiert werden soll.
- 3 Wählen Sie im Kontextmenü die Option **OVF-Vorlage bereitstellen** aus, um den Installationsassistenten zu starten.
- 4 Geben Sie die URL der herunterzuladenden OVA-Datei ein oder navigieren Sie zur gespeicherten OVA-Datei.
- 5 Geben Sie einen Namen für die NSX Edge-VM ein.
Der eingegebene Name wird in der Bestandsliste angezeigt.
- 6 Wählen Sie eine Computing-Ressource für die NSX Edge-Appliance aus.
- 7 Reservieren Sie Arbeitsspeicher für die NSX Edge-Appliance, um eine optimale Leistung zu erreichen.
Legen Sie die Reservierung so fest, dass NSX Edge über ausreichend Arbeitsspeicher verfügt, um eine effiziente Ausführung sicherzustellen. Siehe [Systemanforderungen für NSX Edge-VM](#).
- 8 Überprüfen Sie die Details der OVF-Vorlage.
- 9 Wählen Sie einen Datenspeicher für die Dateien der NSX Edge-Appliance aus.
- 10 Akzeptieren Sie die Standardnetzwerkschnittstelle für die Quelle und das Ziel.
Sie können das Ziel des Standardnetzwerks für die restlichen Netzwerke übernehmen und die Netzwerkkonfiguration ändern, nachdem die NSX Edge bereitgestellt wurde.
- 11 Wählen Sie im Dropdown-Menü die IP-Zuteilung aus.
- 12 Geben Sie die System-Root-, CLI-Admin- und Audit-Kennwörter für die NSX Edge ein.
Ihre Kennwörter müssen den Einschränkungen zur Kennwortkomplexität entsprechen.
 - mindestens 12 Zeichen
 - mindestens ein Kleinbuchstabe
 - mindestens ein Großbuchstabe
 - mindestens eine Zahl
 - mindestens ein Sonderzeichen
 - mindestens fünf unterschiedliche Zeichen
 - keine Wörterbuchwörter
 - keine Palindrome
 - mehr als vier monotone Zeichenfolgen ist nicht zulässig

- 13 Geben Sie das Standard-Gateway, die IPv4-Adresse und Netzmaske des Verwaltungsnetzwerks, die DNS- und NTP-IP-Adresse ein.
- 14 (Optional) Registrieren Sie die NSX Edge mit der Verwaltungsebene, wenn ein NSX Manager zur Verfügung steht.
 - a Geben Sie die IP-Adresse und den Fingerabdruck des übergeordneten NSX Manager-Knotens ein
 - b Führen Sie den API-Aufruf `POST https://<nsx-manager>/api/v1/aaa/registration-token` aus, um das NSX Manager-Token abzurufen.
- 15 Geben Sie den Hostnamen der NSX Edge-VM ein.
- 16 Aktivieren Sie SSH und gewähren Sie Root-SSH-Anmeldung an der NSX Edge-Befehlszeile.
Standardmäßig sind diese Optionen aus Sicherheitsgründen deaktiviert.
- 17 Stellen Sie sicher, dass die gesamte Spezifikation der benutzerdefinierten OVA-Vorlage korrekt ist, und klicken Sie auf **Beenden**, um die Installation zu starten.
Die Installation kann 7 bis 8 Minuten dauern.
- 18 Öffnen Sie die Konsole von NSX Edge, um den Startvorgang zu verfolgen.
Wenn das Konsolenfenster nicht geöffnet wird, stellen Sie sicher, dass Popups zulässig sind.
- 19 Nachdem der NSX Edge gestartet ist, melden Sie sich bei der CLI mit Admin-Anmeldedaten an.

Hinweis Wenn Sie sich nach dem Starten des NSX Edge nicht zum ersten Mal als Administrator anmelden, wird der Datenebenenendienst nicht automatisch auf dem NSX Edge gestartet.

- 20 Führen Sie den Befehl `get interface eth0.<vlan_ID>` aus, um zu überprüfen, ob die IP-Adresse wie erwartet angewendet wurde.

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

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

Hinweis Wenn Sie NSX Edge-VMs auf einem nicht von NSX verwalteten Host erstellen, stellen Sie sicher, dass die MTU-Einstellung auf dem physischen Host-Switch für die Datennetzwerkkarte auf 1600 (statt 1500) festgelegt ist.

- 21 Führen Sie den `get managers`-Befehl aus, um sicherzustellen, dass die NSX Edge registriert ist.

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

22 Stellen Sie sicher, dass die NSX Edge-Appliance über die erforderliche Konnektivität verfügt.

Wenn Sie SSH aktiviert haben, stellen Sie sicher, dass Sie eine SSH-Verbindung zu NSX Edge herstellen können.

- Sie können einen Ping-Vorgang für das NSX Edge ausführen.
- NSX Edge kann einen Ping-Vorgang für das zugehörige Standard-Gateway ausführen.
- Das NSX Edge kann einen Ping-Vorgang für die Hypervisor-Hosts ausführen, die im selben Netzwerk wie NSX Edge sind.
- NSX Edge kann einen Ping-Vorgang für den zugehörigen DNS-Server und NTP-Server ausführen.

23 Beheben Sie Konnektivitätsprobleme.

Hinweis Wenn keine Konnektivität hergestellt werden kann, stellen Sie sicher, dass sich der VM-Netzwerkadapter im richtigen Netzwerk oder VLAN befindet.

Standardmäßig beansprucht der NSX Edge-Datenpfad alle Netzwerkkarten (NICs) von virtuellen Maschinen mit Ausnahme der Management-NIC (derjenigen, die eine IP-Adresse und eine Standardroute aufweist). Wenn Sie eine Netzwerkkarte als Verwaltungsschnittstelle falsch zugewiesen haben, führen Sie die folgenden Schritte aus, um mit DHCP die Verwaltungs-IP-Adresse der korrekten Netzwerkkarte zuzuweisen.

- a Melden Sie sich bei der Befehlszeilenschnittstelle (CLI) an, und geben Sie den Befehl **stop service dataplane** ein.
- b Geben Sie den Befehl **set interface *Schnittstelle* dhcp plane mgmt** ein.
- c Platzieren Sie die *Schnittstelle* im DHCP-Netzwerk und warten Sie, bis dieser *Schnittstelle* eine IP-Adresse zugewiesen wurde.
- d Geben Sie den Befehl **start service dataplane** ein.

Die fp-ethX-Ports des Datenpfads, die für VLAN-Uplink und Tunnel-Overlay verwendet werden, werden mit den Befehlen **get interfaces** und **get physical-port** von NSX Edge angezeigt.

Nächste Schritte

Verbinden Sie NSX Edge mit der Managementebene. Siehe [Verbinden von NSX Edge mit der Managementebene](#).

Installieren von NSX Edge auf ESXi unter Verwendung des OVF-Befehlszeilentools

Wenn Sie die NSX Edge-Installation automatisieren möchten, können Sie dazu das VMware OVF Tool verwenden. Dabei handelt es sich um ein Befehlszeilendienstprogramm.

Voraussetzungen

- Stellen Sie sicher, dass die Systemanforderungen erfüllt sind. Siehe [Systemvoraussetzungen](#).

- Stellen Sie sicher, dass die erforderlichen Ports geöffnet sind. Siehe [Ports und Protokolle](#).
- Stellen Sie sicher, dass auf dem ESXi-Host ein Datenspeicher konfiguriert und verfügbar ist.
- 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 haben, die von NSX Manager verwendet werden.
- Erstellen Sie das Ziel-VM-Portgruppennetzwerk, wenn noch keines vorhanden ist. Platzieren Sie die NSX-T Data Center-Appliances in einem VM-Verwaltungsnetzwerk.

Wenn Sie über mehrere Verwaltungsnetzwerke verfügen, können Sie statische Routen von der NSX-T Data Center-Appliance zu den anderen Netzwerken hinzufügen.

- Planen Sie Ihr IPv4 oder IPv6-IP-Adressschema für NSX Manager.
- Siehe NSX Edge-Netzwerkanforderungen im Handbuch [NSX Edge-Installation](#).
- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Bereitstellen einer OVF-Vorlage auf dem ESXi-Host verfügen.
- Stellen Sie sicher, dass Hostnamen keine Unterstriche enthalten. Andernfalls wird der Hostname auf *localhost* gesetzt.
- OVF Tool Version 4.3 oder höher

Verfahren

- ◆ Führen Sie bei einem eigenständigen Host den `ovftool`-Befehl mit den jeweiligen Parametern aus.

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

```
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-edge
<path/url to nsx component ova>
vi://root:<password>@192.168.110.51
```

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

- ◆ Führen Sie bei einem von vCenter Server verwalteten Host den `ovftool`-Befehl mit den jeweiligen Parametern aus.

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

```
--prop:nsx_hostname=nsx-edge
<path/url to nsx component ova>
vi://administrator@vsphere.local:<password>@192.168.110.24/?ip=192.168.210.53
```

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

- ◆ Reservieren Sie Arbeitsspeicher für die NSX Manager-Appliance, um eine optimale Leistung zu erreichen.

Legen Sie die Reservierung so fest, dass NSX Manager über ausreichend Arbeitsspeicher verfügt, um eine effiziente Ausführung sicherzustellen. Siehe [Systemanforderungen für NSX Manager-VM](#).

- ◆ Öffnen Sie die Konsole von NSX Edge, um den Startvorgang zu verfolgen.
- ◆ Nachdem der NSX Edge gestartet ist, melden Sie sich bei der CLI mit Admin-Anmeldedaten an.
- ◆ Führen Sie den Befehl `get interface eth0.<vlan_ID>` aus, um zu überprüfen, ob die IP-Adresse wie erwartet angewendet wurde.

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

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

Hinweis Wenn Sie NSX Edge-VMs auf einem nicht von NSX verwalteten Host erstellen, stellen Sie sicher, dass die MTU-Einstellung auf dem physischen Host-Switch für die Datennetzkarte auf 1600 (statt 1500) festgelegt ist.

- ◆ Stellen Sie sicher, dass die NSX Edge-Appliance über die erforderliche Konnektivität verfügt.
Wenn Sie SSH aktiviert haben, stellen Sie sicher, dass Sie eine SSH-Verbindung zu NSX Edge herstellen können.
 - Sie können einen Ping-Vorgang für das NSX Edge ausführen.
 - NSX Edge kann einen Ping-Vorgang für das zugehörige Standard-Gateway ausführen.

- Das NSX Edge kann einen Ping-Vorgang für die Hypervisor-Hosts ausführen, die im selben Netzwerk wie NSX Edge sind.
- NSX Edge kann einen Ping-Vorgang für den zugehörigen DNS-Server und NTP-Server ausführen.
- ◆ Beheben Sie Konnektivitätsprobleme.

Hinweis Wenn keine Konnektivität hergestellt werden kann, stellen Sie sicher, dass sich der VM-Netzwerkadapter im richtigen Netzwerk oder VLAN befindet.

Standardmäßig beansprucht der NSX Edge-Datenpfad alle Netzwerkkarten (NICs) von virtuellen Maschinen mit Ausnahme der Management-NIC (derjenigen, die eine IP-Adresse und eine Standardroute aufweist). Wenn Sie eine Netzwerkkarte als Verwaltungsschnittstelle falsch zugewiesen haben, führen Sie die folgenden Schritte aus, um mit DHCP die Verwaltungs-IP-Adresse der korrekten Netzwerkkarte zuzuweisen.

- a Melden Sie sich bei der Befehlszeilenschnittstelle (CLI) an, und geben Sie den Befehl **stop service dataplane** ein.
- b Geben Sie den Befehl **set interface *Schnittstelle* dhcp plane mgmt** ein.
- c Platzieren Sie die *Schnittstelle* im DHCP-Netzwerk und warten Sie, bis dieser *Schnittstelle* eine IP-Adresse zugewiesen wurde.
- d Geben Sie den Befehl **start service dataplane** ein.

Die fp-ethX-Ports des Datenpfads, die für VLAN-Uplink und Tunnel-Overlay verwendet werden, werden mit den Befehlen **get interfaces** und **get physical-port** von NSX Edge angezeigt.

Nächste Schritte

Verbinden Sie NSX Edge mit der Managementebene. Siehe [Verbinden von NSX Edge mit der Managementebene](#).

Installieren von NSX-T Data Center auf KVM

5

NSX-T Data Center unterstützt KVM auf zwei Arten: als Hosttransportknoten und als Host für NSX Manager.

Stellen Sie sicher, dass Sie über die unterstützten KVM-Versionen verfügen. Siehe [Systemanforderungen für NSX Manager-VM](#).

Dieses Kapitel enthält die folgenden Themen:

- [Einrichten von KVM](#)
- [Verwalten der Gast-VMs in der KVM-CLI](#)
- [Installieren von NSX Manager auf KVM](#)
- [Anmeldung beim neu erstellten NSX Manager](#)
- [Installieren von Drittanbieterpaketen auf einem KVM-Host](#)
- [Überprüfung der Open vSwitch-Version auf RHEL KVM-Hosts](#)
- [Bereitstellen von NSX Manager-Knoten zur Bildung eines Cluster mithilfe der CLI](#)
- [Installieren von NSX Edge mithilfe einer ISO-Datei oder einer PXE](#)

Einrichten von KVM

Wenn Sie KVM als Transportknoten oder als Host für eine NSX Manager-Gast-VM einsetzen möchten, KVM aber noch nicht eingerichtet haben, können Sie das hier beschriebene Verfahren verwenden.

Hinweis Das Geneve-Kapselungsprotokoll verwendet UDP-Port 6081. Sie müssen diesem Port in der Firewall auf dem KVM-Host Zugriff gewähren.

Verfahren

- 1 (Nur RHEL) Öffnen Sie die Datei `/etc/yum.conf`.
- 2 Suchen Sie nach der Zeile `exclude`.

- 3 Fügen Sie die Zeile "kernel* redhat-release*" zum Konfigurieren von YUM hinzu, damit nur unterstützte RHEL-Upgrades durchgeführt werden.

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

Schließen Sie auch die für die Container relevanten Module aus, wenn Sie das NSX-T Data Center-Container-Plug-In ausführen möchten, für das bestimmte Kompatibilitätsanforderungen gelten.

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

Zu den unterstützten RHEL-Versionen gehören 7.4 und 7.5.

- 4 Installieren Sie KVM und Bridge-Dienstprogramme.

Linux-Bereitstellung	Befehle
Ubuntu	<pre>apt-get install -y qemu-kvm libvirt-bin ubuntu-vm-builder bridge-utils virtinst virt-manager virt-viewer libguestfs-tools</pre>
RHEL oder CentOS Linux	<pre>yum groupinstall "Virtualization Hypervisor" yum groupinstall "Virtualization Client" yum groupinstall "Virtualization Platform" yum groupinstall "Virtualization Tools"</pre>
SUSE Linux Enterprise Server	Starten Sie YaSt und wählen Sie Virtualisierung > Hypervisor und Werkzeuge installieren aus. Mit YaSt können Sie die Netzwerk-Bridge automatisch aktivieren und konfigurieren.

- 5 Überprüfen Sie die Virtualisierungsfähigkeit der Hardware.

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

Die Ausgabe muss vmx enthalten.

- 6 Stellen Sie sicher, dass das KVM-Modul installiert ist.

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

- 7 Bereiten Sie für die Verwendung von KVM als Host für NSX Manager das Bridge-Netzwerk, die Verwaltungsschnittstelle und die NIC-Schnittstellen vor.

Im folgenden Beispiel wird die erste Ethernet-Schnittstelle (eth0 oder ens32) für Konnektivität mit der Linux-Maschine selbst verwendet. Je nach Bereitstellungsumgebung kann diese Schnittstelle DHCP

oder statische IP-Einstellungen verwenden. Bevor Sie den NSX-T Data Center-Hosts Uplink-Schnittstellen zuweisen, stellen Sie sicher, dass die von diesen Uplinks verwendeten Schnittstellenskripts bereits konfiguriert sind. Ohne diese Schnittstellendateien auf dem System können Sie keinen Hosttransportknoten erstellen.

Hinweis Schnittstellennamen können in verschiedenen Umgebungen variieren.

Linux-**Bereitstellung****Netzwerkconfiguration**

Ubuntu

Bearbeiten Sie `/etc/network/interfaces`:

```

auto lo
iface lo inet loopback

auto eth0
iface eth0 inet manual

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

```

Erstellen Sie eine XML-Netzwerkdefinitionsdatei für die Bridge. Erstellen Sie z. B. `/tmp/bridge.xml` mit den folgenden Zeilen:

```

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

```

Definieren und starten Sie das Bridge-Netzwerk mit den folgenden Befehlen:

```

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

```

Überprüfen Sie den Status des Bridge-Netzwerks mit folgendem Befehl:

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

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

RHEL oder CentOS

Bearbeiten Sie `/etc/sysconfig/network-scripts/ifcfg-management_interface`:

Linux

```

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

```

Linux-**Bereitstellung****Netzwerkconfiguration**

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

Bearbeiten Sie `/etc/sysconfig/network-scripts/ifcfg-eth1`:

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

Bearbeiten Sie `/etc/sysconfig/network-scripts/ifcfg-eth2`:

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

Bearbeiten Sie `/etc/sysconfig/network-scripts/ifcfg-br0`:

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

SUSE Linux

Enterprise Server

- 8** Um KVM als Transportknoten zu verwenden, bereiten Sie die Netzwerk-Bridge vor.

Im folgenden Beispiel wird die erste Ethernet-Schnittstelle (eth0 oder ens32) für Konnektivität mit der Linux-Maschine selbst verwendet. Je nach Bereitstellungsumgebung kann diese Schnittstelle DHCP oder statische IP-Einstellungen verwenden.

Hinweis Schnittstellennamen können in verschiedenen Umgebungen variieren.

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

Wichtig Bei Ubuntu müssen alle Netzwerkkonfigurationen in `/etc/network/interfaces` angegeben werden. Erstellen Sie keine individuellen Netzwerkkonfigurationsdateien, wie z. B. `/etc/network/ifcfg-eth1`, die dazu führen können, dass die Transportknotenerstellung fehlschlägt.

Nachdem der KVM-Host als Transportknoten konfiguriert wurde, wird die Bridge-Schnittstelle „`nsx-vtep0.0`“ erstellt. In Ubuntu enthält `/etc/network/interfaces` Einträge wie die folgenden:

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

IN RHEL erstellt der NSX-Hostagent (`nsxa`) eine Konfigurationsdatei namens `ifcfg-nsx-vtep0.0`, die in etwa folgende Einträge enthält:

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

In SUSE,

- 9 Starten Sie den Netzwerkdienst `systemctl restart network` oder den Linux-Server neu, damit die Netzwerkänderungen wirksam werden.

Verwalten der Gast-VMs in der KVM-CLI

NSX Manager können als KVM-VMs installiert werden. Darüber hinaus können Sie KVM als Hypervisor für NSX-T Data Center-Transportknoten verwenden.

Die Verwaltung von KVM-Gast-VMs wird in diesem Handbuch nicht behandelt. Hier finden Sie aber einige einfache KVM-CLI-Befehle für den Einstieg.

Sie können Ihre Gast-VMs in der KVM-CLI mit `virsh`-Befehlen verwalten. Im Folgenden finden Sie einige häufig verwendete `virsh`-Befehle. Weitere Informationen dazu finden Sie in der KVM-Dokumentation.

```
# List running
virsh list

# List all
virsh list --all

# Control instances
virsh start <instance>
```

```
virsh shutdown <instance>
virsh destroy <instance>
virsh undefine <instance>
virsh suspend <instance>
virsh resume <instance>
```

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

In der Linux-CLI zeigen Sie mit dem Befehl `ifconfig` die `vnetX`-Schnittstelle an (die für die Gast-VM erstellte Schnittstelle). Wenn Sie weitere Gast-VMs hinzufügen, werden auch zusätzliche `vnetX`-Schnittstellen hinzugefügt.

```
ifconfig
...

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

Installieren von NSX Manager auf KVM

NSX Manager kann als virtuelle Appliance auf einem KVM-Host installiert werden.

Bei der QCOW2-Installation wird `guestfish` verwendet, ein Linux-Befehlszeilentool zum Schreiben von Einstellungen von virtuellen Maschinen in die QCOW2-Datei.

Voraussetzungen

- KVM-Einrichtung Siehe [Einrichten von KVM](#).
- Rechte zum Bereitstellen eines QCOW2-Images auf dem KVM-Host
- Vergewissern Sie sich, dass das Kennwort in der `guestinfo`-Datei die Anforderungen bezüglich der Kennwortkomplexität erfüllt, sodass Sie sich nach der Installation anmelden können. Siehe [NSX Manager-Installation](#).
- Machen Sie sich mit den NSX Manager-Ressourcenanforderungen vertraut. Siehe [Systemanforderungen für NSX Manager-VM](#).
- Wenn Sie Ubuntu OS installieren möchten, wird empfohlen, vor der Installation von NSX Manager Ubuntu-Version 18.04 auf dem KVM-Host zu installieren.

Verfahren

- 1 Laden Sie das NSX Manager-QCOW2-Image aus dem Ordner **nsx-unified-appliance > exports > kvm** herunter.

- 2 Kopieren Sie das Image auf die KVM-Maschine, die den NSX Manager mithilfe von SCP oder Synchronisierung ausführt.
- 3 (Nur Ubuntu) Fügen Sie den derzeit angemeldeten Benutzer als libvirtd-Benutzer hinzu:

```
adduser $USER libvirtd
```

- 4 Erstellen Sie in dem Verzeichnis, in dem Sie das QCOW2-Image gespeichert haben, eine Datei mit dem Namen „guestinfo.xml“ und füllen Sie diese mit den Eigenschaften der NSX Manager-VM auf.

Eigenschaft	Beschreibung
<ul style="list-style-type: none"> ■ nsx_cli_passwd_0 ■ nsx_cli_audit_passwd_0 ■ nsx_passwd_0 	<p>Ihre Kennwörter müssen den Einschränkungen zur Kennwortkomplexität entsprechen.</p> <ul style="list-style-type: none"> ■ mindestens 12 Zeichen ■ mindestens ein Kleinbuchstabe ■ mindestens ein Großbuchstabe ■ mindestens eine Zahl ■ mindestens ein Sonderzeichen ■ mindestens fünf unterschiedliche Zeichen ■ keine Wörterbuchwörter ■ keine Palindrome ■ mehr als vier monotone Zeichenfolgen ist nicht zulässig
nsx_hostname	Geben Sie den Hostnamen für den NSX Manager ein. Der Hostname muss ein gültiger Domänenname sein. Stellen Sie sicher, dass jeder Teil des Hostnamens (Domäne/Unterdomäne), der per Punkt getrennt ist, mit einem alphabetischen Zeichen beginnen muss.
nsx_role	<ul style="list-style-type: none"> ■ <i>nsx-manager</i>: Erforderlich. Mit diesem Rollennamen wird die NSX Manager-Appliance installiert. ■ <i>nsx-cloud-service-manager</i>: Optional. Verwenden Sie nach Installation von NSX Manager diesen Rollennamen, um die Cloud Service Manager-Appliance für NSX Cloud zu installieren.
nsx_isSSHEnabled	Sie können die Eigenschaft aktivieren oder deaktivieren. Wenn diese Option aktiviert ist, können Sie sich mithilfe von SSH beim NSX Manager anmelden.
nsx_allowSSHRootLogin	Sie können die Eigenschaft aktivieren oder deaktivieren. Wenn diese Option aktiviert ist, können Sie sich mithilfe von SSH als root-Benutzer beim NSX Manager anmelden. Um diese Eigenschaft verwenden zu können, muss nsx_isSSHEnabled aktiviert sein.
<ul style="list-style-type: none"> ■ nsx_dns1_0 ■ nsx_ntp_0 ■ nsx_domain_0 ■ nsx_gateway_0 ■ nsx_netmask_0 ■ nsx_ip_0 	Geben Sie die IP-Adresse des Standard-Gateways, die IPv4-Adresse und Netzmaske des Verwaltungsvernetzwerks, die DNS- und NTP-IP-Adresse ein.

Beispiel:

```
<?xml version="1.0" encoding="UTF-8"?>
<Environment
  xmlns="http://schemas.dmtf.org/ovf/environment/1"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:oe="http://schemas.dmtf.org/ovf/environment/1">
  <PropertySection>
    <Property oe:key="nsx_cli_passwd_0" oe:value="<password>" />
    <Property oe:key="nsx_cli_audit_passwd_0" oe:value="<password>" />
    <Property oe:key="nsx_passwd_0" oe:value="<password>" />
    <Property oe:key="nsx_hostname" oe:value="nsx-manager1" />
    <Property oe:key="nsx_role" oe:value="nsx-manager" />
    <Property oe:key="nsx_isSSHEnabled" oe:value="True" />
    <Property oe:key="nsx_allowSSHRootLogin" oe:value="True" />
    <Property oe:key="nsx_dns1_0" oe:value="10.168.110.10" />
    <Property oe:key="nsx_ntp_0" oe:value="10.168.110.10" />
    <Property oe:key="nsx_domain_0" oe:value="corp.local" />
    <Property oe:key="nsx_gateway_0" oe:value="10.168.110.83" />
    <Property oe:key="nsx_netmask_0" oe:value="255.255.252.0" />
    <Property oe:key="nsx_ip_0" oe:value="10.168.110.19" />
  </PropertySection>
</Environment>
```

Hinweis In diesem Beispiel sind `nsx_isSSHEnabled` und `nsx_allowSSHRootLogin` aktiviert. Wenn diese Optionen deaktiviert sind, können Sie SSH nicht verwenden oder sich nicht bei der NSX Manager-Befehlszeile anmelden. Wenn Sie `nsx_isSSHEnabled` aktivieren, nicht jedoch `nsx_allowSSHRootLogin`, können Sie eine SSH-Verbindung mit NSX Manager herstellen, sich aber nicht als Root anmelden.

- 5 Schreiben Sie mittels `guestfish` die Datei `guestinfo.xml` in das QCOW2-Image.

Hinweis Nachdem die Informationen aus `guestinfo` in ein QCOW2-Image geschrieben wurden, können Sie nicht mehr überschrieben werden.

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

- 6 Stellen Sie das QCOW2-Image mit dem Befehl `virt-install` bereit.

Die vCPU- und RAM-Werte sind für eine große VM geeignet. Der Netzwerk- und Portgruppenname sind spezifisch für Ihre Umgebung. Das Modell muss `virtio` lauten.

```
sudo virt-install \
--import \
--ram 48000 \
--vcpus 12 \
--name <manager-name> \
```

```
--disk path=<manager-qcow2-file-path>,bus=virtio,cache=none \
--network network=<network-name>,portgroup=<portgroup-name>,model=virtio \
--noautoconsole \
--cpu mode=host-passthrough,cache.mode=passthrough

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

- 7 Stellen Sie sicher, dass der NSX Manager bereitgestellt wird.

```
virsh list --all
```

Id	Name	State
18	nsx-manager1	running

- 8 Öffnen Sie die NSX Manager-Konsole und melden Sie sich an.

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

nsx-manager1 login: admin
Password:
```

- 9 Melden Sie sich nach dem Start von NSX Manager als Administrator bei der CLI an und führen Sie den Befehl `get interface eth0` aus, um zu überprüfen, ob die IP-Adresse erwartungsgemäß angewendet wurde.
- 10 Führen Sie `get services` aus, um sicherzustellen, dass die Dienste ausgeführt werden.
- 11 Stellen Sie sicher, dass Ihr NSX Manager über die erforderliche Konnektivität verfügt.

Stellen Sie sicher, dass Sie die folgenden Aufgaben ausführen können.

- Führen Sie für Ihren NSX Manager von einer anderen Maschine aus einen Ping-Vorgang aus.
- Der NSX Manager kann einen Ping-Vorgang für das zugehörige Standard-Gateway ausführen.
- Der NSX Manager kann mithilfe der Verwaltungsschnittstelle einen Ping-Vorgang für die Hypervisor-Hosts ausführen, die sich im selben Netzwerk wie der NSX Manager befinden.
- Der NSX Manager kann einen Ping-Vorgang für den zugehörigen DNS-Server und NTP-Server ausführen.
- Wenn Sie SSH aktiviert haben, stellen Sie sicher, dass Sie eine SSH-Verbindung zu NSX Manager herstellen können.

Wenn keine Konnektivität hergestellt werden kann, stellen Sie sicher, dass sich der Netzwerkadapter der virtuellen Appliance im richtigen Netzwerk oder VLAN befindet.

- 12 Verlassen Sie die KVM-Konsole.

```
control-]
```

- 13 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.

Anmeldung beim neu erstellten NSX Manager

Nach der Installation von NSX Manager können Sie weitere Installationsaufgaben mithilfe der Benutzeroberfläche ausführen.

Nach der Installation von NSX Manager können Sie dem Programm zur Verbesserung der Benutzerfreundlichkeit für NSX-T Data Center beitreten. Unter „Programm zur Verbesserung der Benutzerfreundlichkeit“ im *Administratorhandbuch für NSX-T Data Center* finden Sie weitere Informationen dazu, wie Sie am Programm teilnehmen und sich später wieder abmelden können.

Voraussetzungen

Stellen Sie sicher, dass NSX Manager installiert ist. Siehe [Installieren Sie NSX Manager und die verfügbaren Appliances](#).

Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
Die Nutzungsbedingungen werden angezeigt.
- 2 Lesen und akzeptieren Sie die Bedingungen der Endbenutzer-Lizenzvereinbarung.
- 3 Geben Sie an, ob Sie dem Programm zur Verbesserung der Benutzerfreundlichkeit beitreten möchten.
- 4 Klicken Sie auf **Speichern**

Installieren von Drittanbieterpaketen auf einem KVM-Host

Um einen KVM-Host als Fabric-Knoten vorzubereiten, müssen Sie einige Drittanbieterpakete installieren.

Voraussetzungen

- (RHEL und CentOS Linux) Führen Sie vor der Installation der Drittanbieterpakete die folgenden Befehle aus, um die Virtualisierungspakete zu installieren.

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

Ist eine Installation der Pakete nicht möglich, können Sie sie mit dem Befehl `yum install glibc.i686 nspr` manuell in einer neuen Installation bereitstellen.

- (Ubuntu) Führen Sie vor der Installation der Drittanbieterpakete die folgenden Befehle aus, um die Virtualisierungspakete zu installieren.

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

- (SUSE Linux Enterprise Server) Führen Sie vor der Installation der Drittanbieterpakete die folgenden Befehle aus, um die Virtualisierungspakete zu installieren.

```
libcap-progs
```

Verfahren

- ◆ Führen Sie `apt-get install <package_name>` unter Ubuntu aus, um die Drittanbieterpakete manuell zu installieren.

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

- ◆ Führen Sie `yum install <package_name>` unter RHEL und CentOS Linux aus, um die Drittanbieterpakete manuell zu installieren.

Wenn Sie den bereits bei RHEL und CentOS registrierten Host manuell vorbereiten, müssen Sie keine Drittanbieterpakete auf dem Host installieren.

RHEL 7.6, 7.5 und 7.4 CentOS Linux 7.5 und 7.4

```
wget
PyYAML
libunwind
python-gevent
python-mako
python-netaddr
redhat-lsb-core
tcpdump
```

```
wget
PyYAML
libunwind
python-gevent
python-mako
python-netaddr
redhat-lsb-core
tcpdump
```

- ◆ Führen Sie unter SUSE zypper install <package_name> aus, um die Drittanbieterpakete manuell zu installieren.

SUSE Linux Enterprise Server 12.0

```
python-simplejson
python-PyYAML
python-netaddr
lsb-release
```

Überprüfung der Open vSwitch-Version auf RHEL KVM-Hosts

Wenn OVS-Pakete auf dem RHEL-Host vorhanden sind, müssen Sie die bestehenden Pakete entfernen und die unterstützten Pakete installieren.

Die unterstützte Open vSwitch-Version lautet 2.9.1.8614397-1.

Verfahren

- 1 Stellen Sie sicher, dass die aktuelle Version des Open vSwitch auf dem Host installiert ist.

```
ovs-vswitchd --version
```

Wenn Sie über eine neuere oder ältere Version von Open vSwitch verfügen, müssen Sie diese Open vSwitch-Version durch die unterstützte Version ersetzen.

- 2 Öffnen Sie den Open vSwitch-Ordner.
- 3 Löschen Sie die folgenden Open vSwitch-Pakete.
 - kmod-openvswitch
 - openvswitch
 - openvswitch-selinux-policy
- 4 Fügen Sie alternativ die von NSX-T Data Center benötigten Open vSwitch-Pakete hinzu.
 - a Melden Sie sich als Administrator beim Host an.
 - b Laden Sie die Datei nsx-lcp herunter und kopieren Sie sie in das Verzeichnis /tmp.

- c Dekomprimieren Sie das Paket.

```
tar -zxvf nsx-lcp-<release>-rhel75_x86_64.tar.gz
```

- d Gehen Sie zum Paketverzeichnis.

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

- e Ersetzen Sie die vorhandene Open vSwitch-Version durch die unterstützte Version.

- Verwenden Sie für die neuere Open vSwitch-Version den Befehl `--nodeps`.

Beispiel: `rpm -Uvh kmod-openvswitch-<new version>.e17.x86_64.rpm --nodeps`

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

- Verwenden Sie für die ältere Open vSwitch-Version den Befehl `--force`.

Beispiel: `rpm -Uvh kmod-openvswitch-<new version>.e17.x86_64.rpm --nodeps --force`

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

Bereitstellen von NSX Manager-Knoten zur Bildung eines Cluster mithilfe der CLI

Durch Verknüpfen des NSX Manager zur Bildung eines Clusters über die CLI wird sichergestellt, dass alle NSX Manager-Knoten im Cluster miteinander kommunizieren können.

Voraussetzungen

Die Installation von NSX-T Data Center-Komponenten muss abgeschlossen sein.

Verfahren

- 1 Öffnen Sie eine SSH-Sitzung für den ersten bereitgestellten NSX Manager-Knoten.
- 2 Melden Sie sich mit den Anmeldedaten des Administrators an.
- 3 Führen Sie auf dem NSX Manager-Knoten den Befehl `get certificate api thumbprint` aus.
Die Befehlsausgabe besteht aus einer Reihe von Zahlen, die für diesen NSX Manager eindeutig sind.
- 4 Führen Sie den Befehl `get cluster config` aus, um die Kennung des ersten bereitgestellten NSX Manager-Clusters zu erhalten.
- 5 Fügen Sie den NSX Manager-Knoten zum Cluster hinzu.

Hinweis Sie müssen den Verknüpfungsbefehl für den neu bereitgestellte NSX Manager-Knoten ausführen.

Geben Sie die folgenden NSX Manager-Informationen an:

- Hostname oder IP-Adressen des Knoten, dem Sie beitreten möchten
- Cluster-ID
- Benutzername

- Kennwort
- Zertifikatfingerabdruck

Sie können den CLI-Befehl oder den API-Aufruf verwenden.

- CLI-Befehl

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

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

Der Vorgang zur Verknüpfung und Cluster-Stabilisierung dauert möglicherweise 10 bis 15 Minuten.

6 Fügen Sie den dritten NSX Manager-Knoten zum Cluster hinzu.

Wiederholen Sie Schritt 5.

7 Überprüfen Sie den Cluster-Status, indem Sie den Befehl `get cluster status` auf Ihren Hosts ausführen.

8 Wählen Sie **System > Appliances > Übersicht** und überprüfen Sie die Cluster-Konnektivität.

Nächste Schritte

Erstellen Sie eine Transportzone. Siehe [Erstellen eines eigenständigen Hosts oder Bare-Metal-Server-Transportknotens](#).

Installieren von NSX Edge mithilfe einer ISO-Datei oder einer PXE

Sie können NSX Edge-Geräte automatisiert auf einer Bare-Metal-Bereitstellung oder als VM mit PXE installieren.

Hinweis Beachten Sie, dass die Installation per PXE-Startvorgang für NSX Manager nicht unterstützt wird. Außerdem können Sie keine Netzwerkeinstellungen wie IP-Adresse, Gateway, Netzwerkmaske, NTP oder DNS konfigurieren.

Installieren von NSX Edge per ISO-Datei als virtuelle Appliance

Sie können virtuelle NSX Edge-Maschinen manuell über eine ISO-Datei installieren.

Wichtig Die Installationen der virtuellen Maschinen mit NSX-T Data Center-Komponenten umfassen VMware Tools. Das Entfernen oder Upgrade von VMware Tools wird bei NSX-T Data Center-Appliances nicht unterstützt.

Voraussetzungen

- Siehe NSX Edge-Netzwerkanforderungen im Handbuch [NSX Edge-Installation](#).

Verfahren

- 1 Wechseln Sie zu Ihrem MyVMware-Konto (myvmware.com) und navigieren Sie zu **VMware NSX-T Data Center > Downloads**.
- 2 Suchen Sie die ISO-Datei für NSX Edge und laden Sie sie herunter.
- 3 Wählen Sie im vSphere Client den Host-Datenspeicher aus.
- 4 Wählen Sie **Dateien > Dateien hochladen > Datei in einen Datenspeicher hochladen**, navigieren Sie zu der ISO-Datei und laden Sie sie hoch.

Wenn Sie ein selbstsigniertes Zertifikat verwenden, öffnen Sie die IP-Adresse in einem Browser, akzeptieren Sie das Zertifikat und laden Sie die ISO-Datei erneut hoch.

- 5 Wählen Sie in der Bestandsliste von vSphere Client den Host aus, auf den Sie die ISO-Datei hochgeladen haben. Stattdessen können Sie auch im vSphere Client
- 6 einen Rechtsklick ausführen und **Neue virtuelle Maschine** auswählen.
- 7 Wählen Sie eine Computing-Ressource für die NSX Edge-Appliance aus.
- 8 Wählen Sie einen Datenspeicher für die Dateien der NSX Edge-Appliance aus.
- 9 Akzeptieren Sie die Standardkompatibilität für Ihre NSX Edge-VM.
- 10 Wählen Sie die unterstützten ESXi-Betriebssysteme für Ihre NSX Edge-VM aus.
- 11 Konfigurieren Sie die virtuelle Hardware.

- Neue Festplatte – **200 GB**
- Neues Netzwerk – **VM-Netzwerk**
- Neues CD/DVD-Laufwerk – **ISO-Datei für Datenspeicher**

Sie müssen auf **Verbinden** klicken, um die NSX Edge-ISO-Datei an die VM zu binden.

- 12 Schalten Sie die neue NSX Edge-VM ein.
- 13 Öffnen Sie während des ISO-Starts die VM-Konsole und wählen Sie **Automatisierte Installation**.

Nach dem Drücken der Eingabetaste kann es zu einer Verzögerung von 10 Sekunden kommen.

Während der Installation werden Sie vom Installationsprogramm aufgefordert, eine VLAN-ID für die Verwaltungsschnittstelle einzugeben. Wählen Sie **Ja** aus und geben Sie eine VLAN-ID ein, um eine VLAN-Unterschnittstelle für die Netzwerkschnittstelle zu erstellen. Wählen Sie **Nein** aus, wenn Sie kein VLAN-Tagging für das Paket konfigurieren möchten.

Während des Einschaltens fordert die VM eine Netzwerkkonfiguration über DHCP an. Wenn DHCP in Ihrer Umgebung nicht verfügbar ist, werden Sie aufgefordert, IP-Einstellungen anzugeben.

Standardmäßig lautet das Root-Anmeldekennwort **vmware** und das Admin-Anmeldekennwort **default**.

Wenn Sie sich zum ersten Mal anmelden, werden Sie aufgefordert, das Kennwort zu ändern. Bei dieser Kennwortänderung gelten strenge Komplexitätsregeln, wie die folgenden:

- mindestens 12 Zeichen
- mindestens ein Kleinbuchstabe
- mindestens ein Großbuchstabe
- mindestens eine Zahl
- mindestens ein Sonderzeichen
- mindestens fünf unterschiedliche Zeichen
- keine Wörterbuchwörter
- keine Palindrome
- mehr als vier monotone Zeichenfolgen ist nicht zulässig

Wichtig Die Kerndienste der Appliance werden erst gestartet, wenn ein Kennwort mit ausreichender Komplexität festgelegt wurde.

- 14** Reservieren Sie Arbeitsspeicher für die NSX Edge-Appliance, um eine optimale Leistung zu erreichen.

Legen Sie die Reservierung so fest, dass NSX Edge über ausreichend Arbeitsspeicher verfügt, um eine effiziente Ausführung sicherzustellen. Siehe [Systemanforderungen für NSX Edge-VM](#).

- 15** Nachdem der NSX Edge gestartet ist, melden Sie sich bei der CLI mit Admin-Anmeldedaten an.

Hinweis Wenn Sie sich nach dem Starten des NSX Edge nicht zum ersten Mal als Administrator anmelden, wird der Datenebenendienst nicht automatisch auf dem NSX Edge gestartet.

- 16** Es gibt drei Möglichkeiten, eine Verwaltungsschnittstelle zu konfigurieren.

- Schnittstelle ohne Tagging. Mit diesem Schnittstellentyp wird eine Out-of-Band-Verwaltungsschnittstelle erstellt.

(DHCP) `set interface eth0 dhcp plane mgmt`

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

- Schnittstelle mit Tagging.

`set interface eth0 vlan <vlan_ID> plane mgmt`

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

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

- In-Band-Schnittstelle.

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

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

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

17 (Optional) Starten Sie den SSH-Dienst. Führen Sie `start service ssh` aus.

18 Führen Sie den Befehl `get interface eth0.<vlan_ID>` aus, um zu überprüfen, ob die IP-Adresse wie erwartet angewendet wurde.

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

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

Hinweis Wenn Sie NSX Edge-VMs auf einem nicht von NSX verwalteten Host erstellen, stellen Sie sicher, dass die MTU-Einstellung auf dem physischen Host-Switch für die Datennetzwerkkarte auf 1600 (statt 1500) festgelegt ist.

19 (Schnittstelle mit Tagging und In-Band-Schnittstelle) Jede vorhandene VLAN-Verwaltungsschnittstelle muss gelöscht werden, bevor eine neue erstellt wird.

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

Informationen zum Festlegen einer neuen Schnittstelle finden Sie in Schritt 15.

20 Stellen Sie sicher, dass die NSX Edge-Appliance über die erforderliche Konnektivität verfügt.

Wenn Sie SSH aktiviert haben, stellen Sie sicher, dass Sie eine SSH-Verbindung zu NSX Edge herstellen können.

- Sie können einen Ping-Vorgang für das NSX Edge ausführen.
- NSX Edge kann einen Ping-Vorgang für das zugehörige Standard-Gateway ausführen.
- Das NSX Edge kann einen Ping-Vorgang für die Hypervisor-Hosts ausführen, die im selben Netzwerk wie NSX Edge sind.
- NSX Edge kann einen Ping-Vorgang für den zugehörigen DNS-Server und NTP-Server ausführen.

21 Beheben Sie Konnektivitätsprobleme.

Hinweis Wenn keine Konnektivität hergestellt werden kann, stellen Sie sicher, dass sich der VM-Netzwerkadapter im richtigen Netzwerk oder VLAN befindet.

Standardmäßig beansprucht der NSX Edge-Datenpfad alle Netzwerkkarten (NICs) von virtuellen Maschinen mit Ausnahme der Management-NIC (derjenigen, die eine IP-Adresse und eine Standardroute aufweist). Wenn Sie eine Netzwerkkarte als Verwaltungsschnittstelle falsch zugewiesen haben, führen Sie die folgenden Schritte aus, um mit DHCP die Verwaltungs-IP-Adresse der korrekten Netzwerkkarte zuzuweisen.

- a Melden Sie sich bei der Befehlszeilenschnittstelle (CLI) an, und geben Sie den Befehl **stop service dataplane** ein.
- b Geben Sie den Befehl **set interface *Schnittstelle* dhcp plane mgmt** ein.
- c Platzieren Sie die *Schnittstelle* im DHCP-Netzwerk und warten Sie, bis dieser *Schnittstelle* eine IP-Adresse zugewiesen wurde.
- d Geben Sie den Befehl **start service dataplane** ein.

Die fp-ethX-Ports des Datenpfads, die für VLAN-Uplink und Tunnel-Overlay verwendet werden, werden mit den Befehlen **get interfaces** und **get physical-port** von NSX Edge angezeigt.

Nächste Schritte

Wenn Sie NSX Edge nicht mit der Management Plane verknüpft haben, finden Sie unter [Verbinden von NSX Edge mit der Managementebene](#) weitere Informationen.

Installieren von NSX Edge per ISO-Datei auf einer Bare-Metal-Bereitstellung

Sie können NSX Edge-Geräte manuell über eine ISO-Datei auf einer Bare-Metal-Bereitstellung installieren. Dies umfasst das Konfigurieren von Netzwerkeinstellungen wie IP-Adresse, Gateway, Netzwerkmaste, NTP und DNS.

Voraussetzungen

- Stellen Sie sicher, dass der System-BIOS-Modus auf Legacy-BIOS festgelegt ist.
- Siehe NSX Edge-Netzwerkanforderungen im Handbuch [NSX Edge-Installation](#).

Verfahren

- 1 Suchen Sie nach der ISO-Datei der NSX Edge-Appliance im Ordner **nsx-edgenode > publish > xenial_amd64**.

Laden Sie die ISO-Datei auf Ihren Computer herunter.

- 2 Melden Sie sich beim ILO der Bare-Metal-Bereitstellung an.
- 3 Klicken Sie in der Vorschau der virtuellen Konsole auf **Starten**.
- 4 Wählen Sie **Virtuelle Medien > Virtuelle Medien verbinden** aus.

Warten Sie einige Sekunden, bis die virtuellen Medien eine Verbindung hergestellt haben.

- 5 Wählen Sie **Virtuelle Medien > CD/DVD zuordnen** aus und navigieren Sie zur ISO-Datei.
- 6 Wählen Sie **Nächster Start > Virtuelle CD/DVD/ISO** aus.

- 7 Wählen Sie **Einschalten > System zurücksetzen (Warmstart)** aus.

Die Installationsdauer richtet sich nach der Bare-Metal-Umgebung.

- 8 Wählen Sie **Automatisierte Installation**.

Nach dem Drücken der Eingabetaste kann es zu einer Verzögerung von 10 Sekunden kommen.

- 9 Wählen Sie die anwendbare primäre Netzwerkschnittstelle aus.

Während des Einschaltens fordert das Installationsprogramm eine Netzwerkkonfiguration über DHCP an. Wenn DHCP in Ihrer Umgebung nicht verfügbar ist, werden Sie aufgefordert, IP-Einstellungen anzugeben.

Standardmäßig lautet das Root-Anmeldekennwort **vmware** und das Admin-Anmeldekennwort **default**.

- 10 Öffnen Sie die Konsole von NSX Edge, um den Startvorgang zu verfolgen.

Wenn das Konsolenfenster nicht geöffnet wird, stellen Sie sicher, dass Popups zulässig sind.

- 11 Nachdem der NSX Edge gestartet ist, melden Sie sich bei der CLI mit Admin-Anmeldedaten an.

Hinweis Wenn Sie sich nach dem Starten des NSX Edge nicht zum ersten Mal als Administrator anmelden, wird der Datenebenendienst nicht automatisch auf dem NSX Edge gestartet.

- 12 Nach dem Neustart können Sie sich entweder als Administrator oder als Root anmelden. Das Standardkennwort für die Root-Anmeldung lautet **vmware**.

- 13 Es gibt drei Möglichkeiten, eine Verwaltungsschnittstelle zu konfigurieren.

- Schnittstelle ohne Tagging. Mit diesem Schnittstellentyp wird eine Out-of-Band-Verwaltungsschnittstelle erstellt.

(DHCP) `set interface eth0 dhcp plane mgmt`

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

- Schnittstelle mit Tagging.

`set interface eth0 vlan <vlan_ID> plane mgmt`

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

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

- In-Band-Schnittstelle.

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

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

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

- 14 Führen Sie den Befehl `get interface eth0.<vlan_ID>` aus, um zu überprüfen, ob die IP-Adresse wie erwartet angewendet wurde.

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

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

Hinweis Wenn Sie NSX Edge-VMs auf einem nicht von NSX verwalteten Host erstellen, stellen Sie sicher, dass die MTU-Einstellung auf dem physischen Host-Switch für die Datennetzkarte auf 1600 (statt 1500) festgelegt ist.

- 15 (Schnittstelle mit Tagging und In-Band-Schnittstelle) Jede vorhandene VLAN-Verwaltungsschnittstelle muss gelöscht werden, bevor eine neue erstellt wird.

```
clear interface eth0.<vlan_ID>
```

Informationen zum Festlegen einer neuen Schnittstelle finden Sie in Schritt 13.

- 16 Stellen Sie sicher, dass die NSX Edge-Appliance über die erforderliche Konnektivität verfügt.

Wenn Sie SSH aktiviert haben, stellen Sie sicher, dass Sie eine SSH-Verbindung zu NSX Edge herstellen können.

- Sie können einen Ping-Vorgang für das NSX Edge ausführen.
- NSX Edge kann einen Ping-Vorgang für das zugehörige Standard-Gateway ausführen.
- Das NSX Edge kann einen Ping-Vorgang für die Hypervisor-Hosts ausführen, die im selben Netzwerk wie NSX Edge sind.
- NSX Edge kann einen Ping-Vorgang für den zugehörigen DNS-Server und NTP-Server ausführen.

- 17 Beheben Sie Konnektivitätsprobleme.

Hinweis Wenn keine Konnektivität hergestellt werden kann, stellen Sie sicher, dass sich der VM-Netzwerkadapter im richtigen Netzwerk oder VLAN befindet.

Standardmäßig beansprucht der NSX Edge-Datenpfad alle Netzwerkkarten (NICs) von virtuellen Maschinen mit Ausnahme der Management-NIC (derjenigen, die eine IP-Adresse und eine Standardroute aufweist). Wenn Sie eine Netzwerkkarte als Verwaltungsschnittstelle falsch zugewiesen haben, führen Sie die folgenden Schritte aus, um mit DHCP die Verwaltungs-IP-Adresse der korrekten Netzwerkkarte zuzuweisen.

- a Melden Sie sich bei der Befehlszeilenschnittstelle (CLI) an, und geben Sie den Befehl **stop service dataplane** ein.
- b Geben Sie den Befehl **set interface *Schnittstelle* dhcp plane mgmt** ein.
- c Platzieren Sie die *Schnittstelle* im DHCP-Netzwerk und warten Sie, bis dieser *Schnittstelle* eine IP-Adresse zugewiesen wurde.
- d Geben Sie den Befehl **start service dataplane** ein.

Die fp-ethX-Ports des Datenpfads, die für VLAN-Uplink und Tunnel-Overlay verwendet werden, werden mit den Befehlen **get interfaces** und **get physical-port** von NSX Edge angezeigt.

Nächste Schritte

Verbinden Sie NSX Edge mit der Managementebene. Siehe [Verbinden von NSX Edge mit der Managementebene](#).

Installieren von NSX Edge auf PXE-Server

PXE besteht aus mehreren Komponenten: DHCP, HTTP und TFTP. Hier wird gezeigt, wie Sie einen PXE-Server unter Ubuntu einrichten.

DHCP verteilt IP-Einstellungen dynamisch an NSX-T Data Center-Komponenten wie NSX Edge. In einer PXE-Umgebung ermöglicht es der DHCP-Server NSX Edge, automatisch eine IP-Adresse anzufordern und zu erhalten.

TFTP ist ein Dateiübertragungsprotokoll. Der TFTP-Server überwacht stets PXE-Clients im Netzwerk. Wenn er erkennt, dass ein Netzwerk-PXE-Client PXE-Dienste anfragt, stellt er die NSX-T Data Center-Komponenten-ISO-Datei und die in einer vordefinierten Datei enthaltenen Installationseinstellungen bereit.

Voraussetzungen

- Ein PXE-Server muss in Ihrer Bereitstellungsumgebung verfügbar sein. Der PXE-Server kann auf jeder beliebigen Linux-Distribution eingerichtet sein. Der PXE-Server muss über zwei Schnittstellen verfügen: eine für die externe Kommunikation und eine andere für DHCP-IP- und TFTP-Dienste.

Wenn Sie über mehrere Verwaltungsnetzwerke verfügen, können Sie statische Routen von der NSX-T Data Center-Appliance zu den anderen Netzwerken hinzufügen.

- Stellen Sie sicher, dass in der vordefinierten Konfigurationsdatei die Parameter `net.ifnames=0` und `biosdevname=0` nach `--` festgelegt sind, damit sie nach einem Neustart beibehalten werden.
- Siehe NSX Edge-Netzwerkanforderungen im Handbuch [NSX Edge-Installation](#).

Verfahren

- 1 (Optional) Verwenden Sie eine Kickstart-Datei, um neue TFTP oder DHCP-Dienste auf einem Ubuntu-Server einzurichten.

Eine Kickstart-Datei ist eine Textdatei mit CLI-Befehlen, die Sie nach dem ersten Start auf der Appliance ausführen.

Der Name der Kickstart-Datei basiert auf dem PXE-Server, auf den sie verweist. Beispiel:

```
nsxcli.install
```

Die Datei muss in Ihren Webserver kopiert werden (z. B. unter `/var/www/html/nsx-edge/nsxcli.install`).

In der Kickstart-Datei können Sie CLI-Befehle hinzufügen. Zum Beispiel, um die IP-Adresse der Verwaltungsschnittstelle zu konfigurieren:

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

Um das Kennwort des Admin-Benutzers zu ändern:

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

Wenn Sie in der Datei `preseed.cfg` ein Kennwort angeben, sollten Sie dasselbe Kennwort in der Kickstart-Datei verwenden. Verwenden Sie andernfalls das Standardkennwort „default“.

So verbinden Sie NSX Edge mit der Managementebene:

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

- 2 Erstellen Sie zwei Schnittstellen: eine für das Management und eine andere für DHCP- und TFTP-Dienste.

Stellen Sie sicher, dass sich die DHCP/TFTP-Schnittstelle im selben Subnetz befindet wie NSX Edge.

Beispiel: Wenn sich die NSX Edge-Managementschnittstellen im Subnetz 192.168.210.0/24 befinden, müssen Sie eth1 ebenfalls in diesem Subnetz platzieren.

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

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

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

3 Installieren Sie DHCP-Serversoftware.

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

4 Bearbeiten Sie die Datei `/etc/default/isc-dhcp-server` und fügen Sie die Schnittstelle hinzu, die den DHCP-Dienst bereitstellt.

```
INTERFACES="eth1"
```

5 (Optional) Wenn dieser DHCP-Server der offizielle DHCP-Server für das lokale Netzwerk sein soll, entfernen Sie den Kommentar für die Zeile **authoritative**; in der Datei `/etc/dhcp/dhcpd.conf`.

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

6 Definieren Sie in der Datei `/etc/dhcp/dhcpd.conf` die DHCP-Einstellungen für das PXE-Netzwerk.

Beispiel:

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

7 Starten Sie den DHCP-Dienst.

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

8 Stellen Sie sicher, dass der DHCP-Dienst ausgeführt wird.

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

9 Installieren Sie Apache, TFTP und weitere Komponenten, die für PXE Boot erforderlich sind.

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


- 10** Stellen Sie sicher, dass TFTP und Apache ausgeführt werden.

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

- 11** Fügen Sie die folgenden Zeilen zur Datei `/etc/default/tftpd-hpa` hinzu.

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

- 12** Fügen Sie die folgende Zeile zur Datei `/etc/inetd.conf` hinzu.

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

- 13** Starten Sie den TFTP-Dienst neu.

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

- 14** Kopieren Sie die ISO-Datei des NSX Edge-Installationsprogramms in einen temporären Ordner oder laden Sie sie dorthin herunter.

- 15** Stellen Sie die ISO-Datei bereit und kopieren Sie die Installationskomponenten in den TFTP-Server und den Apache-Server.

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

- 16** (Optional) Bearbeiten Sie die Datei `/var/www/html/nsx-edge/preseed.cfg`, um die verschlüsselten Kennwörter zu ändern.

Sie können ein Linux-Tool wie `mkpasswd` verwenden, um ein Kennwort-Hash zu erstellen.

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

```
Password:
$6$SUFGqs[...]FcoHLij0uFD
```

- a Ändern Sie das Root-Kennwort, bearbeiten Sie `/var/www/html/nsx-edge/preseed.cfg` und suchen Sie nach der folgenden Zeile:

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

- b Ersetzen Sie die Hash-Zeichenfolge.
Sonderzeichen wie `$`, `'`, `"`, oder `\` müssen nicht maskiert werden.
- c Fügen Sie den Befehl `usermod` zu `preseed.cfg` hinzu, um das Kennwort für Root, Admin oder beides festzulegen.

Suche Sie z. B. nach der Zeile `echo 'VMware NSX Edge'`, und fügen Sie den folgenden Befehl hinzu.

```
usermod --password '\$6\$VS3exId0aKmw\$U3g0V7BF0DXlmRI.LR0v/VgloxVotEDp00b02hUF8u/' root; \
usermod --password '\$6\$VS3exId0aKmw\$U3g0V7BF0DXlmRI.LR0v/VgloxVotEDp00b02hUF8u/' admin; \
```

Die Hash-Zeichenfolge stellt ein Beispiel dar. Sie müssen alle Sonderzeichen maskieren. Das Root-Kennwort im ersten `usermod`-Befehl ersetzt das in `d-i passwd/root-password-crypted password 6tgml...` festgelegte Kennwort.

Wenn Sie das Kennwort mit dem Befehl `usermod` festlegen, wird der Benutzer nicht aufgefordert, das Kennwort bei der ersten Anmeldung zu ändern. Andernfalls muss der Benutzer das Kennwort bei der ersten Anmeldung ändern.

- 17** Fügen Sie die folgenden Zeilen zur Datei `/var/lib/tftpboot/pxelinux.cfg/default` hinzu.

Ersetzen Sie `192.168.210.82` durch die IP-Adresse Ihres TFTP-Servers.

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

18 Fügen Sie die folgenden Zeilen zur Datei `/etc/dhcp/dhcpd.conf` hinzu.

Ersetzen Sie 192.168.210.82 durch die IP-Adresse Ihres DHCP-Servers.

```
allow booting;
allow bootp;

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

19 Starten Sie den DHCP-Dienst neu.

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

Hinweis Wenn ein Fehler zurückgegeben wird, beispielsweise „stop: Unknown instance: start: Job failed to start“, führen Sie `sudo /etc/init.d/isc-dhcp-server stop` und dann `sudo /etc/init.d/isc-dhcp-server start` aus. Mit dem Befehl `sudo /etc/init.d/isc-dhcp-server start` können Sie Informationen zur Fehlerursache abrufen.

Nächste Schritte

Installieren Sie NSX Edge mithilfe einer ISO-Datei auf einer Bare-Metal-Bereitstellung. Siehe [Installieren von NSX Edge per ISO-Datei auf einer Bare-Metal-Bereitstellung](#) oder [Installieren von NSX Edge per ISO-Datei als virtuelle Appliance](#).

Konfigurieren des Bare-Metal-Servers zur Verwendung von NSX-T Data Center

6

Zur Verwendung von NSX-T Data Center auf einem Bare-Metal-Server müssen Sie unterstützte Drittanbieterpakete installieren.

NSX-T Data Center unterstützt den Bare-Metal-Server auf zwei Arten: als Hosttransportknoten und als Host für NSX Manager.

Stellen Sie sicher, dass Sie über die unterstützten Versionen des Bare-Metal-Servers verfügen. Siehe [Bare Metal Server-Systemanforderungen](#).

Hinweis Wenn sich Ihre NSX Edges im VM-Formfaktor befinden und Sie beabsichtigen, den NSX-DHCP-Dienst (auf VLAN-basiertem logischen Switch bereitgestellt) zu verwenden, müssen Sie die Option für gefälschte Übertragungen auf den Bare-Metal-Hosts, auf denen die NSX Edges bereitgestellt werden, akzeptieren. Weitere Informationen finden Sie im Abschnitt zu gefälschten Übertragungen in der vSphere-Produktdokumentation.

Dieses Kapitel enthält die folgenden Themen:

- [Installieren von Drittanbieterpaketen auf einem Bare-Metal-Server](#)
- [Erstellen der Anwendungsschnittstelle für Bare-Metal Server-Arbeitslasten](#)

Installieren von Drittanbieterpaketen auf einem Bare-Metal-Server

Um einen Bare-Metal-Server als Fabric-Knoten vorzubereiten, müssen Sie einige Drittanbieterpakete installieren.

Voraussetzungen

- Stellen Sie sicher, dass der Benutzer, der die Installation durchführt, über Administratorberechtigungen für die folgenden Aktionen verfügt, von denen einige möglicherweise sudo-Berechtigungen erfordern:
 - Laden Sie das Paket herunter und dekomprimieren Sie es.
 - Führen Sie den Befehl `dpkg` oder `rpm` aus, um NSX-Komponenten zu installieren bzw. zu deinstallieren.

- Führen Sie den Befehl `nsxcli` zum Ausführen von Befehlen für das Verbinden mit der Managementebene aus.
- Stellen Sie sicher, dass die Virtualisierungspakete installiert sind.
 - RedHat oder CentOS – `yum install libvirt-libs`
 - Ubuntu – `apt-get install libvirt0`
 - SUSE – `zypper install libvirt-libs`

Verfahren

- ◆ Führen Sie unter Ubuntu `apt-get install <package_name>` aus, um die Drittanbieterpakete zu installieren.

Ubuntu 18.04	Ubuntu 16.04
traceroute python-mako python-netaddr python-simplejson python-unittest2 python-yaml python-openssl dkms libvirt0	libunwind8 libgflags2v5 libgoogle-perftools4 traceroute python-mako python-simplejson python-unittest2 python-yaml python-netaddr libboost-filesystem1.58.0 libboost-chrono1.58.0 libgoogle-glog0v5 dkms libboost-date-time1.58.0 python-protobuf python-gevent libsnappy1v5 libleveldb1v5 libboost-program-options1.58.0 libboost-thread1.58.0 libboost-iostreams1.58.0 libvirt0

- ◆ Führen Sie unter RHEL oder CentOS `yum install` aus, um die Drittanbieterpakete zu installieren.

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

- ◆ Führen Sie unter SUSE `zypper install <package_name>` aus, um die Drittanbieterpakete manuell zu installieren.

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

Erstellen der Anwendungsschnittstelle für Bare-Metal Server-Arbeitslasten

Sie müssen NSX-T Data Center konfigurieren und Linux-Drittanbieterpakete installieren, bevor Sie eine Anwendungsschnittstelle für Bare-Metal-Server-Arbeitslasten erstellen oder migrieren können.

NSX-T Data Center unterstützt keine Bindung von Linux-Betriebssystemschnittstellen. Sie müssen Open vSwitch (OVS)-Bindung für Bare Metal Server-Transportknoten verwenden. Weitere Informationen finden Sie im Knowledgebase-Artikel 67835 [Bare Metal Server unterstützt die OVS-Bindung für die Transportknotenkonfiguration in NSX-T](#).

Verfahren

- 1 Installieren Sie die erforderlichen Drittanbieterpakete.
Siehe [Installieren von Drittanbieterpaketen auf einem Bare-Metal-Server](#).
- 2 Konfigurieren Sie die TCP- und UDP-Ports.
Siehe [Von ESXi, KVM-Hosts und Bare-Metal-Server verwendete TCP- und UDP-Ports](#).
- 3 Fügen Sie einen Bare-Metal-Server zum NSX-T Data Center-Fabric hinzu und erstellen Sie einen Transportknoten.
Siehe [Erstellen eines eigenständigen Hosts oder Bare-Metal-Server-Transportknotens](#).
- 4 Erstellen Sie eine Anwendungsschnittstelle mit dem Ansible-Playbook.
Siehe <https://github.com/vmware/bare-metal-server-integration-with-nsxt>.

Konfigurieren des NSX Manager-Clusters

7

In den folgenden Abschnitten wird beschrieben, wie Sie den NSX Manager-Cluster konfigurieren, welche Anforderungen für den Cluster und welche Empfehlungen für bestimmte Site-Bereitstellungen gelten. Außerdem wird beschrieben, wie Sie vSphere HA mit NSX-T Data Center verwenden können, um die schnelle Wiederherstellung zu ermöglichen, falls der Host, auf dem der NSX Manager-Knoten ausgeführt wird, ausfällt.

Dieses Kapitel enthält die folgenden Themen:

- [Anforderungen des NSX Manager-Clusters](#)
- [NSX Manager-Clusteranforderungen für eine, zwei und mehrere Sites](#)

Anforderungen des NSX Manager-Clusters

Für die Konfiguration eines NSX Manager-Clusters gelten folgende Anforderungen:

- In einer Produktionsumgebung muss der NSX Manager-Cluster über drei Mitglieder verfügen, um einen Ausfall der Management- und Steuerungsebene zu vermeiden.

Jedes Clustermitglied muss auf einem eindeutigen Hypervisor-Host mit insgesamt drei physischen Hypervisor-Hosts platziert werden. Dies ist erforderlich, um zu verhindern, dass der Ausfall eines einzelnen physischen Hypervisor-Hosts die NSX-Steuerungsebene beeinträchtigt. Es wird empfohlen, Anti-Affinitätsregeln anzuwenden, um sicherzustellen, dass alle drei Clustermitglieder auf unterschiedlichen Hosts ausgeführt werden.

Der normale Produktionsbetriebszustand ist ein NSX Manager-Cluster mit drei Knoten. Sie können jedoch zusätzliche, temporäre NSX Manager-Knoten hinzufügen, um IP-Adressänderungen zuzulassen.

Wichtig Ab NSX-T Data Center 2.4 enthält der NSX Manager den Prozess der zentralen NSX-Steuerungsebene. Dieser Dienst ist für den Betrieb von NSX entscheidend. Wenn NSX Manager vollständig ausfallen oder der Cluster von drei NSX Managern auf einen NSX Manager reduziert wird, können Sie keine Topologieänderungen an Ihrer Umgebung vornehmen, und VMotion von Maschinen, die von NSX abhängig sind, schlägt fehl.

- In Bereitstellungen für Labor- und Testumgebungen ohne Produktionsarbeitslasten ist die Ausführung eines einzelnen NSX Manager zur Einsparung von Ressourcen möglich. NSX Manager-Knoten können entweder auf ESXi oder auf KVM bereitgestellt werden. Gemischte Bereitstellungen von Managern auf ESXi und KVM werden jedoch nicht unterstützt.

Wichtig Die Anzahl der Sites in einer NSX-T Data Center-Bereitstellung kann sich auf die Anforderungen auswirken. Siehe [NSX Manager-Clusteranforderungen für eine, zwei und mehrere Sites](#).

NSX Manager-Clusteranforderungen für eine, zwei und mehrere Sites

Ihre NSX Manager-Clusterkonfiguration variiert abhängig davon, ob Ihre Bereitstellung für eine, zwei oder mehrere Sites erfolgt.

Sie können vSphere HA mit NSX-T Data Center verwenden, um die schnelle Wiederherstellung zu ermöglichen, falls der Host, auf dem der NSX Manager-Knoten ausgeführt wird, ausfällt.

Hinweis Weitere Informationen finden Sie unter *Erstellen und Verwenden von vSphere HA-Cluster* in der vSphere-Produktdokumentation.

Anforderungen und Empfehlungen für einzelne Sites

Die folgenden Empfehlungen gelten für NSX-T Data Center-Bereitstellungen auf einer einzelnen Site.

- Es empfiehlt sich, dass Sie Ihre NSX Manager auf unterschiedlichen Hosts platzieren, um zu verhindern, dass sich ein einzelner Host-Fehler auf mehrere Manager auswirkt.
- Die maximale Latenz zwischen NSX Managern beträgt 10 ms.
- Sie können NSX Manager in unterschiedlichen vSphere-Clustern oder in einem gemeinsamen vSphere-Cluster platzieren.
- Es wird empfohlen, dass Sie NSX Manager in unterschiedlichen Management-Subnetzen oder in einem gemeinsam genutzten Management-Subnetz platzieren. Bei Verwendung von vSphere HA wird empfohlen, ein gemeinsam genutztes Management-Subnetz zu verwenden, damit NSX Manager, die von vSphere wiederhergestellt werden, Ihre IP-Adresse beibehalten können.
- Es wird empfohlen, dass Sie NSX Manager außerdem in freigegebenem Speicher platzieren. Prüfen Sie für vSphere HA die Anforderungen für diese Lösung.

Sie können auch vSphere HA mit NSX-T verwenden, um die Wiederherstellung eines verlorenen NSX Managers sicherzustellen, sofern der Host ausfällt, auf dem der NSX Manager ausgeführt wird.

Beispielszenario:

- Ein vSphere-Cluster, in dem alle drei NSX Manager bereitgestellt sind.
- Der vSphere-Cluster besteht aus vier oder mehr Hosts.
 - Host-01 mit bereitgestelltem nsxmgr-01
 - Host-02 mit bereitgestelltem nsxmgr-02

- Host-03 mit bereitgestelltem nsxmgr-03
- Host-04 ohne Bereitstellung von NSX Manager
- vSphere HA ist so konfiguriert, dass alle verlorenen NSX Manager (z. B. nsxmgr-01) eines beliebigen Hosts (z. B. Host-01) auf Host-04 wiederhergestellt werden.

Folglich stellt vSphere nach dem Verlust eines Hosts, auf dem ein NSX Manager ausgeführt wird, den verlorenen NSX Manager auf Host-04 wieder her.

Anforderungen und Empfehlungen für zwei Sites

Die folgenden Empfehlungen gelten für NSX-T Data Center-Bereitstellungen auf zwei Sites (Site A/Site B).

- Es wird davon abgeraten, NSX Manager ohne vSphere HA in einem Szenario mit zwei Sites bereitzustellen. In diesem Szenario erfordert eine Site die Bereitstellung von zwei NSX Managern. Der Verlust dieser Site wirkt sich auf den Betrieb von NSX-T Data Center aus.
- Für eine Bereitstellung von NSX Managern in einem Szenario mit zwei Sites mit vSphere HA gelten folgende Überlegungen:
 - Ein einzelner Stretched vSphere-Cluster enthält alle Hosts für NSX Manager.
 - Alle drei NSX Manager werden in einem gemeinsamen Management-Subnetz/VLAN bereitgestellt, damit bei der Wiederherstellung eines verlorenen NSX Managers dessen IP-Adresse beibehalten werden kann.
 - Informationen zur Latenz zwischen Sites finden Sie in den Anforderungen des Speicherprodukts.

Beispielszenario:

- Ein vSphere-Cluster, in dem alle drei NSX Manager bereitgestellt sind.
- Der vSphere-Cluster besteht aus sechs oder mehr Hosts, von denen sich drei Hosts in Site A und drei Hosts in Site B befinden.
- Die drei NSX Manager werden auf unterschiedlichen Hosts mit zusätzlichen Hosts für die Platzierung von wiederhergestellten NSX Managern bereitgestellt.

Site A:

- Host-01 mit bereitgestelltem nsxmgr-01
- Host-02 mit bereitgestelltem nsxmgr-02
- Host-03 mit bereitgestelltem nsxmgr-03

Site B:

- Host-04 ohne Bereitstellung von NSX Manager
- Host-05 ohne Bereitstellung von NSX Manager
- Host-06 ohne Bereitstellung von NSX Manager

- vSphere HA ist so konfiguriert, dass alle verlorenen NSX Manager (z. B. nsxmgr-01) von allen Hosts (z. B. Host-01) in Site A auf einen der Hosts in Site B wiederhergestellt werden.

Auf diese Weise stellt vSphere HA bei einem Ausfall von Site A alle NSX Manager auf Hosts in Site B wieder her.

Wichtig Sie müssen die Anti-Affinitätsregeln ordnungsgemäß konfigurieren, um zu verhindern, dass NSX Manager auf demselben gemeinsamen Host wiederhergestellt werden.

Anforderungen und Empfehlungen für mehrere (drei oder mehr) Sites

Die folgenden Empfehlungen gelten für NSX-T Data Center-Bereitstellungen auf mehreren Sites (Site A/ Site B/Site C).

In einem Szenario mit drei oder mehr Sites können Sie NSX Manager mit oder ohne vSphere HA bereitstellen.

Wenn Sie ohne vSphere HA bereitstellen:

- Es wird empfohlen, separate Management-Subnetze oder VLANs pro Site zu verwenden.
- Die maximale Latenz zwischen NSX Managern beträgt 10 ms.

Beispielsszenario (drei Sites):

- Drei separate vSphere-Cluster, einer pro Site.
- Mindestens ein Host pro Site, auf dem NSX Manager ausgeführt wird:
 - Host-01 mit bereitgestelltem nsxmgr-01
 - Host-02 mit bereitgestelltem nsxmgr-02
 - Host-03 mit bereitgestelltem nsxmgr-03

Fehlerszenarien:

- Ausfall einer einzelnen Site: Zwei verbleibende NSX Manager in anderen Sites werden weiterhin ausgeführt. NSX-T Data Center befindet sich in einem herabgestuften Zustand, ist aber weiterhin betriebsbereit. Es wird empfohlen, manuell einen dritten NSX Manager bereitzustellen, um das verlorene Clustermittglied zu ersetzen.
- Ausfall von zwei Sites: Verlust des Quorums und daher Auswirkungen auf NSX-T Data Center-Vorgänge.

Je nach Umgebungsbedingungen, wie CPU-Geschwindigkeit, Festplattenleistung und andere Bereitstellungsfaktoren, kann die Wiederherstellung von NSX Managern bis zu 20 Minuten dauern.

Transportzonen und Transportknoten

8

Transportzonen und Transportknoten sind wichtige Konzepte in NSX-T Data Center.

Dieses Kapitel enthält die folgenden Themen:

- Erstellen von Transportzonen
- Erstellen eines IP-Pools für Tunnel-Endpoint-IP-Adressen
- Erweiterter Datenpfad
- Konfigurieren von Profilen
- Erstellen eines eigenständigen Hosts oder Bare-Metal-Server-Transportknotens
- Manuelle Installation von NSX-T Data Center-Kernel-Modulen
- NSX Edge-Netzwerkeinrichtung
- Erstellen eines NSX Edge-Transportknotens
- Erstellen eines NSX Edge-Clusters

Erstellen von Transportzonen

Transportzonen bestimmen, welche Hosts und damit auch welche VMs an der Verwendung eines bestimmten Netzwerks teilnehmen können. Dies wird erreicht, indem die Hosts, die einen logischen Switch „sehen“ können, von der Transportzone eingeschränkt werden. Damit wird außerdem begrenzt, welche VMs mit dem logischen Switch verknüpft werden können. Eine Transportzone kann einen oder mehrere Hostcluster umspannen.

Eine NSX-T Data Center-Umgebung kann je nach Ihren Anforderungen eine oder mehrere Transportzonen enthalten. Ein Host kann zu mehreren Transportzonen gehören. Ein logischer Switch kann jeweils nur zu einer Transportzone gehören.

NSX-T Data Center lässt keine Verbindung von VMs zu, die sich in unterschiedlichen Transportzonen im Netzwerk der Ebene 2 befinden. Die Spannweite eines logischen Switches ist auf eine Transportzone begrenzt, sodass sich virtuelle Maschinen in unterschiedlichen Transportzonen nicht im selben Layer 2-Netzwerk befinden können.

Die Overlay-Transportzone wird sowohl von Hosttransportknoten als auch von NSX Edges verwendet. Wenn ein Host- oder NSX Edge-Transportknoten einer Overlay-Transportzone hinzugefügt wird, wird ein N-VDS auf dem Host oder NSX Edge installiert.

Die VLAN-Transportzone wird vom NSX Edge und Host-Transportknoten für die jeweiligen VLAN-Uplinks verwendet. Wenn ein NSX Edge einer VLAN-Transportzone hinzugefügt wird, wird ein VLAN-N-VDS auf dem NSX Edge installiert.

Der N-VDS ermöglicht Paket-Flow von virtuell zu physisch, indem Uplinks und Downlinks eines logischen Routers an physische NICs gebunden werden.

Beim Erstellen einer Transportzone müssen Sie einen Namen für den N-VDS angeben, der auf den Transportknoten installiert wird, wenn diese später der Transportzone hinzugefügt werden. Sie können einen beliebigen Namen für den N-VDS auswählen.

Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **System > Fabric > Transportzonen > Hinzufügen** aus.
- 3 Geben Sie einen Namen für die Transportzone und optional eine Beschreibung ein.
- 4 Geben Sie einen Namen für den N-VDS ein.
- 5 Wählen Sie einen N-VDS-Modus aus.

- **Standard**-Modus, der für alle unterstützten Hosts gilt
- **Erweiterter Datenpfad** ist ein Netzwerk-Stack-Modus, der nur für Transportknoten des ESXi-Hosts in der Version 6.7 und höher gilt und zu einer Transportzone gehören kann.

- 6 Wenn der N-VDS-Modus „Standard“ gewählt wurde, wählen Sie einen Datenverkehrstyp.

Die Optionen hierfür lauten **Overlay** und **VLAN**.

- 7 Wenn der N-VDS-Modus „Erweiterter Datenpfad“ gewählt wurde, wählen Sie einen Datenverkehrstyp.

Die Optionen hierfür lauten **Overlay** und **VLAN**.

Hinweis Im Modus „Erweiterter Datenpfad“ werden nur bestimmte NIC-Konfigurationen unterstützt. Stellen Sie sicher, dass Sie die unterstützten NICs konfigurieren.

- 8 Geben Sie mindestens einen Namen für eine Uplink-Gruppierungsrichtlinie ein. Diese benannten Gruppierungsrichtlinien können von logischen Switches verwendet werden, die mit der Transportzone verbunden sind. Wenn die logischen Switches keine passende Gruppierungsrichtlinie finden, wird die standardmäßige Uplink-Gruppierungsrichtlinie verwendet.
- 9 Die neue Transportzone können Sie auf der Seite **Transportzonen** anzeigen.

- 10** (Optional) Stattdessen können Sie zum Anzeigen der neuen Transportzone auch den API-Aufruf GET <https://<nsx-mgr>/api/v1/transport-zones> verwenden.

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

Nächste Schritte

Optional können Sie ein benutzerdefiniertes Transportzonenprofil erstellen und an die Transportzone binden. Sie können benutzerdefinierte Transportzonenprofile mit der API `POST /api/v1/transportzone-profiles` erstellen. Es gibt keinen Workflow auf der Benutzeroberfläche zum Erstellen eines Transportzonenprofils. Nach der Erstellung des Transportzonenprofils können Sie dieses mit der API `PUT /api/v1/transport-zones/<transport-zone-id>` an die Transportzone binden.

Erstellen Sie einen Transportknoten. Siehe [Erstellen eines eigenständigen Hosts oder Bare-Metal-Server-Transportknotens](#).

Erstellen eines IP-Pools für Tunnel-Endpoint-IP-Adressen

Sie können einen IP-Pool für die Tunnel-Endpoints verwenden. Tunnel-Endpoints sind die Quell- und Ziel-IP-Adressen, die in der externen IP-Kopfzeile verwendet werden, um die Hypervisor-Hosts zu identifizieren, bei denen die NSX-T Data Center-Kapselung von Overlay-Frames beginnt und endet. Sie können auch entweder DHCP oder manuell konfigurierte IP-Pools für Tunnel-Endpoint-IP-Adressen verwenden.

Wenn Sie sowohl ESXi- als auch KVM-Hosts verwenden, könnten Sie in einer möglichen Designoption zwei verschiedene Subnetze für den IP-Pool des ESXi-Tunnel-Endpoints (sub_a) und den IP-Pool des KVM-Tunnel-Endpoints (sub_b) verwenden. In diesem Fall muss auf den KVM-Hosts eine statische Route zu sub_a mit einem dedizierten Standard-Gateway hinzugefügt werden.

Hier sehen Sie ein Beispiel für die resultierende Routing-Tabelle auf einem Ubuntu-Host, wobei sub_a = 192.168.140.0 und sub_b = 192.168.150.0. (Das Management-Subnetz könnte beispielsweise 192.168.130.0 sein.)

Kernel-IP-Routing-Tabelle:

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

Die Route kann auf mindestens zwei verschiedene Arten hinzugefügt werden. Die Route dieser beiden Methoden bleibt nach dem Neustart des Hosts nur bestehen, wenn Sie die Route durch Bearbeitung der Schnittstelle hinzufügen. Wenn Sie eine Route mit dem Befehl zum Hinzufügen einer Route hinzufügen, bleibt diese nach einem Neustart des Hosts nicht erhalten.

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

Fügen Sie die folgende statische Route in `/etc/network/interfaces` vor „up ifconfig nsx-vtep0.0 up“ hinzu:

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

Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Bestandsliste > Gruppen > IP-Pools > Hinzufügen** aus.
- 3 Geben Sie die IP-Pool-Details ein.

Option	Parameterbeispiel
Name und Beschreibung	Geben Sie den IP-Pool und eine optionale Beschreibung ein.
IP-Bereiche	IP-Zuteilungsbereiche 192.168.200.100 – 192.168.200.115
Gateway	192.168.200.1
CIDR	Netzwerkadresse in einer CIDR-Notation 192.168.200.0/24
DNS-Server	Durch Komma getrennte Liste mit DNS-Servern 192.168.66.10
DNS-Suffix	corp.local

Ergebnisse

Der IPv4- oder IPv6-Adressenpool wird auf der Seite „IP-Pool“ aufgeführt.

Sie können auch den API-Aufruf `GET https://<nsx-mgr>/api/v1/pools/ip-pools` verwenden, um die IP-Pool-Liste anzuzeigen.

Nächste Schritte

Erstellen Sie ein Uplink-Profil. Siehe [Erstellen eines Uplink-Profils](#).

Erweiterter Datenpfad

Der erweiterte Datenpfad ist ein Netzwerk-Stack-Modus, der, wenn er konfiguriert ist, eine ausgezeichnete Netzwerkleistung bietet. Er ist in erster Linie für NFV-Arbeitslasten gedacht, für welche die in diesem Modus bereitgestellten Leistungsvorteile erforderlich sind.

Der N-VDS-Switch kann im Modus „Erweiterter Datenpfad“ nur auf einem ESXi-Host konfiguriert werden. ENS unterstützt zudem den Datenverkehr, der durch Edge-VMs fließt.

Im Modus „Erweiterter Datenpfad“ können Sie Folgendes konfigurieren:

- Overlay-Datenverkehr
- VLAN-Datenverkehr

Unterstützte VMkernel-Netzwerkkarten

Aufgrund der Tatsache, dass NSX-T Data Center mehrere ENS-Host-Switches unterstützt, beträgt die maximale Anzahl an VMkernel-Netzwerkkarten pro Host 32.

Allgemeines Verfahren zum Konfigurieren des erweiterten Datenpfads

Als Netzwerkadministrator müssen Sie vor dem Erstellen von Transportzonen, die N-VDS im Modus „Erweiterter Datenpfad“ unterstützen, das Netzwerk mit den unterstützten NIC-Karten und -Treibern vorbereiten. Um die Netzwerkleistung zu verbessern, können Sie die Teaming-Richtlinie „Load Balanced Source“ aktivieren, um NUMA-Knoten zu erkennen.

Die allgemeinen Schritte sind wie folgt:

- 1 Verwenden Sie NIC-Karten, welche den erweiterten Datenpfad unterstützen.

Finden Sie im [VMware-Kompatibilitäts-Handbuch](#) Netzwerkkarten, die den erweiterten Datenpfad unterstützen.

Wählen Sie auf der Seite „VMware-Kompatibilitäts-Handbuch“ unter der Kategorie **E/A-Geräte ESXi 6.7**, E/A-Gerätetyp als **Netzwerk** und Funktion als **Erweiterter N-VDS-Datenpfad**.

- 2 Laden Sie die aktuellen NIC-Treiber von der [Seite „My VMware“](#) herunter und installieren Sie sie.

- a Wechseln Sie zu **Treiber und Tools > Treiber-CDs**.

- b Laden Sie Netzwerkkartentreiber herunter:

VMware ESXi 6.7 ixgbe-ens 1.1.3 NIC Driver for Intel Ethernet Controllers
82599, x520, x540, x550, and x552 family

VMware ESXi 6.7 i40en-ens 1.1.3 NIC Driver for Intel Ethernet Controllers
X710, XL710, XXV710, and X722 family

- 3 Erstellen Sie eine Uplink-Richtlinie.

Siehe [Erstellen eines Uplink-Profiles](#).

- 4 Erstellen Sie eine Transportzone mit N-VDS im Modus „Erweiterter Datenpfad“.

Siehe [Erstellen von Transportzonen](#).

Hinweis Für Overlay-Datenverkehr konfigurierte ENS-Transportzonen: Vergewissern Sie sich bei einer virtuellen Microsoft Windows-Maschine mit dem vNIC-Typ VMXNET3, auf der eine VMware Tools-Version vor 11.0.0 ausgeführt wird, dass die MTU auf 1500 eingestellt ist. Vergewissern Sie sich bei einer virtuellen Microsoft Windows-Maschine, auf der vSphere 6.7 U1 und VMware Tools Version 11.0.0 und höher ausgeführt werden, dass die MTU auf einen Wert kleiner als 8900 festgelegt ist. Vergewissern Sie sich bei virtuellen Maschinen, auf denen andere unterstützte Betriebssysteme ausgeführt werden, dass die MTU der virtuellen Maschine auf einen Wert kleiner als 8900 festgelegt ist.

- 5 Legen Sie einen Host-Transportknoten an. Konfigurieren Sie den N-VDS mit erweitertem Datenpfad mit logischen Kernen und NUMA-Knoten.

Siehe [Erstellen eines eigenständigen Hosts oder Bare-Metal-Server-Transportknotens](#).

„Load Balanced Source“-Teaming-Richtlinienmodus erkennt NUMA

Der für einen N-VDS mit erweitertem Datenpfad definierte „Load Balanced Source“-Teaming-Richtlinienmodus erkennt NUMA, wenn die folgenden Bedingungen erfüllt sind:

- Die **Latenzempfindlichkeit** von VMs ist **Hoch**.
- Der verwendete Netzwerkadapertyp ist VMXNET3.

Wenn die NUMA-Knotenposition entweder der VM oder der physischen NIC nicht verfügbar ist, berücksichtigt die „Load Balanced Source“-Teaming-Richtlinie keine NUMA-Awareness, um VMs und NICs aufeinander abzustimmen.

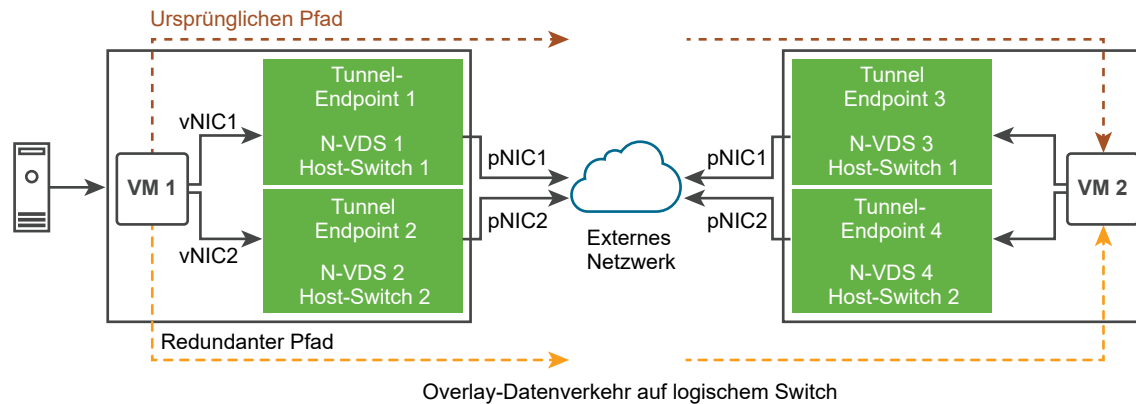
Die Teaming-Richtlinie funktioniert ohne NUMA-Awareness unter den folgenden Bedingungen:

- Der LAG-Uplink wird mit physischen Verbindungen von unterschiedlichen NUMA-Knoten konfiguriert.
- Die virtuelle Maschine (VM) verfügt über Affinität zu mehreren NUMA-Knoten.
- Der ESXi-Host konnte keine NUMA-Informationen für VM- oder physische Verbindungen definieren.

ENS-Unterstützung für SCTP-Anwendungen

In SCTP-Umgebungen verwenden NFV-Arbeitslasten Multihoming- und Redundanzfunktionen, um Stabilität und Zuverlässigkeit für den Datenverkehr, der auf Anwendungen ausgeführt wird, zu erhöhen. Multihoming ist die Fähigkeit, redundante Pfade von einer Quell-VM zu einem Ziel-VM zu unterstützen.

Je nach Anzahl der verfügbaren physischen Netzwerkkarten, die als Uplink für ein Overlay oder VLAN-Netzwerk verwendet werden sollen, sind viele redundante Netzwerkpfade für eine VM zum Senden von Datenverkehr über die Ziel-VM verfügbar. Die redundanten Pfade werden verwendet, wenn die angeheftete pNIC mit einem logischen Switch fehlschlägt. Daher werden dem Datenverkehr, der über das SCTP-Protokoll weitergeleitet wird, redundante Netzwerkpfade durch den N-VDS mit erweitertem Datenpfad bereitgestellt.

Abbildung 8-1. ENS-Datenverkehr, der auf SCTP-Anwendungen ausgeführt wird

Die allgemeinen Aufgaben sehen wie folgt aus:

- 1 Host als NSX-T Data Center-Transportknoten vorbereiten.
- 2 VLAN oder Overlay-Transportzone mit zwei N-VDS-Switches im erweiterten Datenpfad-Modus vorbereiten.
- 3 Heften Sie auf N-VDS-1 die erste physische Netzwerkkarte an den Switch.
- 4 Heften Sie auf N-VDS-2 die zweite physische Netzwerkkarte an den Switch.

Der N-VDS im erweiterten Datenpfad-Modus gewährleistet, dass bei einem Ausfall von pNIC1 Datenverkehr von VM 1 über den redundanten Pfad (vNIC 1 → Tunnel-Endpoint 2 → pNIC 2 → VM 2) geleitet wird. Beachten Sie, dass sich vNIC1 von VM 1 und VM 2 auf einem Subnetz befinden. Analog dazu befinden sich vNIC2 von VM 1 und VM 2 auf einem anderen Subnetz.

Konfigurieren von Profilen

Mit Profilen können Sie identische Funktionen für Netzwerkkarten über mehrere Hosts oder Knoten hinweg konsistent konfigurieren.

Profile sind Container für die Eigenschaften oder Funktionen, die Ihre Netzwerkkarten aufweisen sollen. Anstatt einzelne Eigenschaften oder Funktionen für jeden Netzwerkkarten zu konfigurieren, können Sie die Funktionen in Profilen angeben. Diese können Sie dann über mehrere Hosts oder Knoten hinweg anwenden.

Erstellen eines Uplink-Profiles

Ein Uplink ist ein Link von den NSX Edge-Knoten zu den Top-of-Rack-Switches oder logischen NSX-T Data Center-Switches. Ein Link führt von einer physischen Netzwerkschnittstelle auf einem NSX Edge-Knoten zu einem Switch.

Ein Uplink-Profil definiert Richtlinien für die Uplinks. Die von Uplink-Profilen definierten Einstellungen können Gruppierungsrichtlinien, Aktiv- und Standby-Links, die Transport-VLAN-ID sowie die MTU-Einstellung umfassen.

Konfigurieren von Uplinks für VM-Appliance-basierte NSX Edge-Knoten und Hosttransportknoten:

- Wenn die Failover-Gruppierungsrichtlinie für ein Uplink-Profil konfiguriert ist, können Sie nur einen einzelnen aktiven Uplink in der Gruppierungsrichtlinie konfigurieren. Standby-Uplinks werden nicht unterstützt und dürfen in der Failover-Gruppierungsrichtlinie nicht konfiguriert werden. Wenn Sie NSX Edge als eine virtuelle-Appliance oder einen Hosttransportknoten installieren, verwenden Sie das Standard-Uplink-Profil.
- Wenn die Gruppierungsrichtlinie für die Load Balancer-Quelle für ein Uplink-Profil konfiguriert ist, können Sie mehrere aktive Uplinks auf demselben N-VDS konfigurieren. Jeder Uplink ist einer physischen NIC mit einem eindeutigen Namen und einer IP-Adresse zugeordnet. Die einem Uplink-Endpoint zugewiesene IP-Adresse kann mithilfe der IP-Zuweisung für den N-VDS konfiguriert werden.

Sie müssen die Teaming-Richtlinie **Load Balanced Source** für den Lastausgleich des Datenverkehrs verwenden.

Voraussetzungen

- Siehe NSX Edge-Netzwerkanforderungen im Handbuch [NSX Edge-Installation](#).
- Jeder Uplink im Uplink-Profil muss einem aktiven und verfügbaren physischen Link auf Ihrem Hypervisor-Host oder auf dem NSX Edge-Knoten entsprechen.

Beispiel: Der Hypervisor-Host weist zwei aktive physische Links auf: vmnic0 und vmnic1. Dabei wird vmnic0 für Verwaltungs- und Speichernetzwerke eingesetzt, während vmnic1 nicht verwendet wird. Das würde bedeuten, dass vmnic1 als NSX-T Data Center-Uplink verwendet werden kann, vmnic0 aber nicht. Für das Link-Teaming müssen zwei nicht verwendete physische Links verfügbar sein, wie vmnic1 und vmnic2.

Bei NSX Edge können Tunnel-Endpoint- und VLAN-Uplinks denselben physischen Link verwenden. vmnic0/eth0/em0 könnte beispielsweise für Ihr Verwaltungsnetzwerk eingesetzt werden und vmnic1/eth1/em1 für Ihre fp-ethX-Links.

Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **System > Fabric > Profile > Uplink-Profile > Hinzufügen** aus.

3 Vervollständigen Sie die Details des Uplink-Profiles.

Option	Beschreibung
Name und Beschreibung	Geben Sie einen Uplink-Profilnamen ein. Fügen Sie eine optionale Beschreibung des Uplink-Profiles hinzu.
LAGs	<p>(Optional) Klicken Sie im LAG-Abschnitt auf Hinzufügen für Linkzusammenfassungen (LAGs), die das LACP (Link Aggregation Control Protocol) für das Transportnetzwerk verwenden.</p> <p>Hinweis Für LACP werden mehrere LAGs auf KVM-Hosts nicht unterstützt.</p> <p>Bei den erstellten Namen der aktiven und Standby-Uplinks kann es sich um jeden beliebigen Text zur Darstellung physischer Links handeln. Diese Uplink-Namen werden später referenziert, wenn Sie Transportknoten erstellen. Mit der Transportknoten-Benutzeroberfläche/-API können Sie angeben, welche physischen Links den einzelnen benannten Uplinks entsprechen.</p> <p>Mögliche Optionen für den LAG-Hashing-Mechanismus:</p> <ul style="list-style-type: none"> ■ Quell-MAC-Adresse ■ Ziel-MAC-Adresse ■ Quell- und Ziel-MAC-Adresse ■ Quell- und Ziel-IP-Adresse und VLAN ■ Quell- und Ziel-MAC-Adresse, IP-Adresse und TCP/UDP-Port
Teamings	<p>Im Abschnitt „Teaming“ können Sie entweder eine Standard-Teaming-Richtlinie oder eine benannte Teaming-Richtlinie eingeben. Klicken Sie auf Hinzufügen, um eine benannte Teaming-Richtlinie hinzuzufügen. Eine Teaming-Richtlinie definiert, wie der N-VDS seinen Uplink für Redundanz und Lastausgleich des Datenverkehrs verwendet. Sie können eine Teaming-Richtlinie in den folgenden Modi konfigurieren:</p> <ul style="list-style-type: none"> ■ Failover-Reihenfolge: Ein aktiver Uplink wird zusammen mit einer optionalen Liste mit Standby-Uplinks angegeben. Fällt der aktive Uplink aus, ersetzt der nächste Uplink in der Standby-Liste den aktiven Uplink. Bei dieser Option wird kein Lastausgleich im eigentlichen Sinne durchgeführt. ■ Load Balance-Quelle: Eine Liste aktiver Uplinks wird angegeben, und jede Schnittstelle auf dem Transportknoten wird mit einem aktiven Uplink verbunden. Bei dieser Konfiguration lassen sich mehrere aktive Uplinks gleichzeitig verwenden. <p>Hinweis</p> <ul style="list-style-type: none"> ■ Auf KVM-Hosts: Nur die Teaming-Richtlinie für die Failover-Reihenfolge wird unterstützt, während die Teaming-Richtlinien für die Load Balance-Quelle und die MAC der Load Balance-Quelle nicht unterstützt werden. ■ Auf NSX Edge: Für die Standard-Teaming-Richtlinie werden die Teaming-Richtlinien für die Load Balance-Quelle und die Failover-Reihenfolge unterstützt. Für die benannte Teaming-Richtlinie wird nur die Richtlinie für die Failover-Reihenfolge unterstützt. ■ Auf ESXi-Hosts: Die Teaming-Richtlinien für die MAC der Load Balance-Quelle, die Load Balance-Quelle und die Failover-Reihenfolge werden unterstützt.

Option	Beschreibung
	<p>(ESXi-Hosts und NSX Edge) Sie können die folgenden Richtlinien für eine Transportzone definieren:</p> <ul style="list-style-type: none"> ■ Eine benannte Gruppierungsrichtlinie für jeden VLAN-basierten, logischen Switch oder das Segment. ■ Eine Standard-Gruppierungsrichtlinie für den gesamten N-VDS. <p>Benannte Gruppierungsrichtlinie: Eine benannte Gruppierungsrichtlinie bedeutet, dass Sie für jeden VLAN-basierten, logischen Switch bzw. für jedes VLAN-basierte, logische Segment einen bestimmten Gruppierungsrichtlinienmodus und Uplink-Namen definieren können. Dieser Richtlinientyp bietet Ihnen die Möglichkeit, bestimmte Uplinks je nach Richtlinie zur Datenverkehrslenkung auszuwählen, z. B. basierend auf der Bandbreitenanforderung.</p> <ul style="list-style-type: none"> ■ Wenn Sie eine benannte Gruppierungsrichtlinie definieren, verwendet N-VDS diese benannte Gruppierungsrichtlinie, wenn sie an die VLAN-basierte Transportzone angehängt und schließlich für den spezifischen VLAN-basierten, logischen Switch bzw. das VLAN-basierte, logische Segment im Host ausgewählt wird. ■ Wenn Sie keine benannten Gruppierungsrichtlinien definieren, verwendet N-VDS die Standard-Gruppierungsrichtlinie.

- 4 Geben Sie einen Transport-VLAN-Wert ein. Das Transport-VLAN, das in den Uplink-Profil-Tags festgelegt ist, überlagert nur den Datenverkehr und die VLAN-ID wird vom TEP-Endpunkt verwendet.

- 5 Geben Sie den MTU-Wert ein.

Der MTU-Standardwert für ein Uplink-Profil lautet 1600.

Mit der globalen physischen Uplink-MTU wird der MTU-Wert für alle N-VDS-Instanzen in der NSX-T Data Center-Domäne konfiguriert. Wenn die globale physische Uplink-MTU nicht angegeben ist, wird der MTU-Wert aus der Uplink-Profil-MTU abgeleitet, falls diese konfiguriert ist, oder der Standardwert 1600 wird verwendet. Der MTU-Wert des Uplink-Profiles kann den globalen physischen Uplink-MTU-Wert auf einem bestimmten Host überschreiben.

Mit dem globalen MTU-Wert der logischen Schnittstelle wird der MTU-Wert für alle logischen Routerschnittstellen konfiguriert. Wenn der globale MTU-Wert der logischen Schnittstelle nicht angegeben ist, wird der MTU-Wert vom logischen Tier-0-Router abgeleitet. Der Uplink-MTU-Wert des logischen Routers kann auf einem bestimmten Port den globalen MTU-Wert der logischen Schnittstelle außer Kraft setzen.

Ergebnisse

Zusätzlich zur Benutzeroberfläche können Sie zum Anzeigen der Uplink-Profile auch den API-Aufruf `GET /api/v1/host-switch-profiles` verwenden.

Nächste Schritte

Erstellen Sie eine Transportzone. Siehe [Erstellen von Transportzonen](#).

Konfigurieren von Network I/O Control-Profilen

Mithilfe des Network I/O Control-Profiles (NIOC-Profil) können Sie geschäftskritischen Anwendungen Netzwerkbandbreite zuteilen und Situationen beheben, in denen verschiedene Datenverkehrstypen die gleichen Ressourcen beanspruchen.

Mit dem NIOC-Profil wird ein Mechanismus eingeführt, mit dem Bandbreite für den Systemdatenverkehr basierend auf der Kapazität der physischen Adapter eines Hosts reserviert werden kann. Version 3 der Funktion Network I/O Control ermöglicht eine verbesserte Netzwerkressourcenreservierung und -zuteilung auf dem gesamten Switch.

Network I/O Control Version 3 für NSX-T Data Center unterstützt die Ressourcenverwaltung des Systemdatenverkehrs in Bezug auf virtuelle Maschinen und Infrastrukturdienste, zum Beispiel vSphere Fault Tolerance. Systemdatenverkehr ist strikt einem ESXi-Host zugeordnet.

Bandbreitengarantie für Systemdatenverkehr

Network I/O Control Version 3 stellt Bandbreite für die Netzwerkadapter von virtuellen Maschinen bereit. Zu diesem Zweck werden Konstrukte aus Anteilen, Reservierung und Grenzwerten verwendet. Diese Konstrukte können über die NSX-T Data Center Manager-Benutzeroberfläche definiert werden. Die Bandbreitenreservierung für Datenverkehr über virtuelle Maschinen wird auch bei der Zugangssteuerung verwendet. Wenn Sie eine virtuelle Maschine einschalten, überprüft das Dienstprogramm für die Zugangssteuerung, ob genügend Bandbreite verfügbar ist, bevor eine VM auf einem Host platziert wird, der die Ressourcenkapazität zur Verfügung stellen kann.

Bandbreitenzuteilung für Systemdatenverkehr

Sie können Network I/O Control so konfigurieren, dass eine bestimmte Bandbreitenkapazität für Datenverkehr zugeteilt wird, der von vSphere Fault Tolerance, vSphere vMotion, virtuellen Maschinen usw. generiert wird.

- Verwaltungsdatenverkehr: Datenverkehr für die Hostverwaltung
- Fault Tolerance (FT)-Datenverkehr: Datenverkehr für Failover und Wiederherstellung.
- NFS-Datenverkehr: Datenverkehr im Zusammenhang mit einer Dateiübertragung im Netzwerkdateisystem.
- vSAN-Datenverkehr: Datenverkehr, der vom virtuellen Storage Area Network generiert wird.
- vMotion-Datenverkehr: Datenverkehr für die Migration von Computing-Ressourcen.
- vSphere Replication-Datenverkehr: Datenverkehr für die Replikation.
- vSphere Data Protection-Sicherungsdatenverkehr: Datenverkehr, der durch die Sicherung von Daten generiert wird.
- VM-Datenverkehr: Datenverkehr, der durch virtuelle Maschinen generiert wird.
- iSCSI-Datenverkehr: Datenverkehr, für Internet Small Computer System Interface (iSCSI).

vCenter Server gibt die Zuteilung vom Distributed Switch an jeden physischen Adapter auf den mit dem Switch verbundenen Hosts weiter.

Bandbreitenzuteilungsparameter für Systemdatenverkehr

Anhand von mehreren Konfigurationsparametern teilt der Network I/O Control-Dienst dem Datenverkehr von grundlegenden vSphere-Systemfunktionen Bandbreite zu. Zuteilungsparameter für Systemdatenverkehr.

Zuteilungsparameter für Systemdatenverkehr

- **Anteile:** Anteile von 1 bis 100 geben die relative Priorität eines Systemdatenverkehrstyps im Vergleich zu anderen Systemdatenverkehrstypen an, die auf dem gleichen physischen Adapter aktiv sind. Die relativen Anteile, die einem Systemdatenverkehrstyp zugewiesen werden, und die von anderen Systemfunktionen übermittelte Datenmenge bestimmen die verfügbare Bandbreite für den betreffenden Systemdatenverkehrstyp.
- **Reservierung:** Die Mindestbandbreite in MBit/s, die auf einem einzelnen physischen Adapter garantiert sein muss. Die Gesamtbandbreite, die für alle Systemdatenverkehrstypen reserviert wird, darf 75 Prozent der Bandbreite des physischen Netzwerkadapters mit der geringsten Kapazität nicht überschreiten. Reservierte Bandbreite, die nicht verwendet wird, wird für andere Systemdatenverkehrstypen verfügbar. Network I/O Control verteilt jedoch die Kapazität, die nicht von Systemdatenverkehr verwendet wird, nicht an die Platzierung virtueller Maschinen weiter.
- **Grenzwert:** Die maximale Bandbreite in MBit/s oder GBit/s, die ein Systemdatenverkehrstyp für einen einzelnen physischen Adapter nutzen kann.

Hinweis Sie können höchstens 75 Prozent der Bandbreite eines physischen Netzwerkadapters reservieren.

Beispiel: Bei mit einem ESXi-Host verbundenen 10 GbE-Netzwerkadapters können Sie den diversen Verkehrstypen maximal 7,5 GBit/s zuteilen. Sie können aber auch mehr Kapazität unreserviert lassen. Der Host kann die unreservierte Bandbreite dynamisch je nach den Anteilen, Grenzwerten und dem Gebrauch zuteilen. Der Host reserviert nur so viel Bandbreite, wie für den Betrieb einer Systemfunktion notwendig ist.

Konfigurieren von Network I/O Control (NIOC) und der Bandbreitenzuteilung für Systemdatenverkehr auf einem N-VDS

Um die Mindestbandbreite für den Systemdatenverkehr zu garantieren, der auf NSX-T Data Center-Hosts ausgeführt wird, müssen Sie die Netzwerkressourcenverwaltung auf einem NSX-VDS aktivieren und konfigurieren.

Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **System > Fabric > Profile > NIOC-Profile > Hinzufügen** aus.

3 Geben Sie die Details für das NIOC-Profil ein.

Option	Beschreibung
Name und Beschreibung	Geben Sie einen Namen für das NIOC-Profil ein. Sie können optional die Profildetails eingeben, z. B. welche Arten von Datenverkehr aktiviert werden.
Status	Klicken Sie auf die entsprechenden Schalter, um die in den Datenverkehrsressourcen aufgeführten Bandbreitenzuteilungen zu aktivieren.
Host Infra Traffic-Ressource	Sie können die standardmäßig aufgelisteten Datenverkehrsressourcen akzeptieren. Klicken Sie auf Hinzufügen und geben Sie Ihre Datenverkehrsressource ein, um das NIOC-Profil anzupassen. (Optional) Wählen Sie einen vorhandenen Datenverkehrstyp aus und klicken Sie auf Löschen , um die Ressource aus dem NIOC-Profil zu entfernen.

Das neue NIOC-Profil wird der Liste der NIOC-Profile hinzugefügt.

Konfigurieren von Network I/O Control (NIOC) und der Bandbreitenzuteilung für Systemdatenverkehr auf einem N-VDS mit APIs

Mithilfe von NSX-T Data Center-APIs können Sie Netzwerk und Bandbreite für Anwendungen konfigurieren, die auf dem Host ausgeführt werden.

Verfahren

- 1 Stellen Sie eine Anfrage an den Host, um sowohl system- als auch benutzerdefinierte Host-Switch-Profilen anzuzeigen.
- 2 GET `https://<nsx-mgr>/api/v1/host-switch-profiles?include_system_owned=true`.

Die Beispielantwort zeigt das auf den Host angewendete NIOC-Profil.

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

```

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

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

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

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

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

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

```

```

    "_self": {
      "$ref": "SelfResourceLink"+,
      "readonly": true,
      "title": "Link to this resource"
    },

    "_system_owned": {
      "description": "Indicates system owned resource",
      "readonly": true,
      "type": "boolean"
    },

    "description": {
      "can_sort": true,
      "maxLength": 1024,
      "title": "Description of this resource",
      "type": "string"
    },

    "display_name": {
      "can_sort": true,
      "description": "Defaults to ID if not set",
      "maxLength": 255,
      "title": "Identifier to use when displaying entity in logs or GUI",
      "type": "string"
    },

    "enabled": {
      "default": true,
      "description": "The enabled property specifies the status of NIOC feature.

```

When enabled is set to true, NIOC feature is turned on and the bandwidth allocations specified for the traffic resources are enforced.

When enabled is set to false, NIOC feature is turned off and no bandwidth allocation is guaranteed.

By default, enabled will be set to true."

```

    "nsx_feature": "Nioc",
    "required": false,
    "title": "Enabled status of NIOC feature",
    "type": "boolean"
  },

  "host_infra_traffic_res": {
    "description": "host_infra_traffic_res specifies bandwidth allocation for various traffic resources.",
    "items": {
      "$ref": "ResourceAllocation"+
    },
    "nsx_feature": "Nioc",
    "required": false,
    "title": "Resource allocation associated with NiocProfile",
    "type": "array"
  }
}

```

```

    },

    "id": {
      "can_sort": true,
      "readonly": true,
      "title": "Unique identifier of this resource",
      "type": "string"
    },

    "required_capabilities": {
      "help_summary":
        "List of capabilities required on the fabric node if this profile is
        used.
        The required capabilities is determined by whether specific features are enabled in the
        profile.",
      "items": {
        "type": "string"
      },
      "readonly": true,
      "required": false,
      "type": "array"
    },

    "resource_type": {
      "$ref": "HostSwitchProfileType",
      "required": true
    },

    "tags": {
      "items": {
        "$ref": "Tag"
      },
    },

    "maxItems": 30,
    "title": "Opaque identifiers meaningful to the API user",
    "type": "array"
  },
  "title": "Profile for NIOC",
  "type": "object"
}

```

3 Erstellen Sie ein NIOC-Profil, wenn kein NIOC-Profil vorhanden ist.

POST <https://<nsx-mgr>/api/v1/host-switch-profiles>

```

{
  "description": "Specify limit, shares and reservation for all kinds of traffic.
  Values for limit and reservation are expressed in percentage. And for shares,
  the value is expressed as a number between 1-100.\n\nThe overall reservation among all traffic
  types should not exceed 75%.
  Otherwise, the API request will be rejected.",
  "id": "ResourceAllocation",
  "module_id": "NiocProfile",

```

```

"nsx_feature": "Nioc",
"properties": {
  "limit": {
    "default": -1.0,
    "description": "The limit property specifies the maximum bandwidth allocation for a given
traffic type and is expressed in percentage. The default value for this
field is set to -1 which means the traffic is unbounded for the traffic
type. All other negative values for this property is not supported\nand will be rejected by
the API.",
    "maximum": 100,
    "minimum": -1,
    "required": true,
    "title": "Maximum bandwidth percentage",
    "type": "number"
  },
  "reservation": {
    "default": 0.0,
    "maximum": 75,
    "minimum": 0,
    "required": true,
    "title": "Minimum guaranteed bandwidth percentage",
    "type": "number"
  },
  "shares": {
    "default": 50,
    "maximum": 100,
    "minimum": 1,
    "required": true,
    "title": "Shares",
    "type": "int"
  },
  "traffic_type": {
    "$ref": "HostInfraTrafficType+",
    "required": true,
    "title": "Resource allocation traffic type"
  }
},
"title": "Resource allocation information for a host infrastructure traffic type",
"type": "object"

```

- 4 Aktualisieren Sie die Transportknotenkonfiguration mit der NIOC-Profil-ID des neu erstellten NIOC-Profiles.

PUT <https://<nsx-mgr>/api/v1/transport-nodes/<TN-id>>

```

{
  "resource_type": "TransportNode",
  "description": "Updated NSX configured Test Transport Node",
  "id": "77816de2-39c3-436c-b891-54d31f580961",
  "display_name": "NSX Configured TN",

```

```

"host_switch_spec": {
  "resource_type": "StandardHostSwitchSpec",
  "host_switches": [
    {
      "host_switch_profile_ids": [
        {
          "value": "e331116d-f59e-4004-8cfd-c577ae563a",
          "key": "UplinkHostSwitchProfile"
        },
        {
          "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
          "key": "LldpHostSwitchProfile"
        }
      ]
    },
    {
      "value": "b0185099-8003-4678-b86f-edd47ca2c9ad",
      "key": "NiocProfile"
    }
  ],
  "host_switch_name": "nsxvswitch",
  "pnics": [
    {
      "device_name": "vmnic1",
      "uplink_name": "uplink1"
    }
  ],
  "ip_assignment_spec": {
    "resource_type": "StaticIpPoolSpec",
    "ip_pool_id": "ecddcdde-4dc5-4026-ad4f-8857995d4c92"
  }
},
"transport_zone_endpoints": [
  {
    "transport_zone_id": "e14c6b8a-9edd-489f-b624-f9ef12afbd8f",
    "transport_zone_profile_ids": [
      {
        "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
        "resource_type": "BfdHealthMonitoringProfile"
      }
    ]
  }
],
"host_switches": [
  {
    "host_switch_profile_ids": [
      {
        "value": "e331116d-f59e-4004-8cfd-c577ae563a",
        "key": "UplinkHostSwitchProfile"
      },
      {
        "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
        "key": "LldpHostSwitchProfile"
      }
    ]
  }
]

```

```

],
    "host_switch_name": "nsxvswitch",
    "pnics": [
    {
        "device_name": "vmnic1",
        "uplink_name": "uplink1"
    }
    ],
    "static_ip_pool_id": "ecddcdde-4dc5-4026-ad4f-8857995d4c92"
}
],
"node_id": "41a4eebd-d6b9-11e6-b722-875041b9955d",
"_revision": 0
}

```

- 5 Stellen Sie sicher, dass die NIOC-Profilparameter in der Datei `com.vmware.common.respools.cfg` aktualisiert wurden.

```
# [root@ host:] net-dvs -l
```

```

switch 1d 73 f5 58 99 7a 46 6a-9c cc d0 93 17 bb 2a 48 (vswitch)
max ports: 2560
global properties:

com.vmware.common.opaqueDvs = true ,      propType = CONFIG
com.vmware.nsx.kcp.enable = true ,        propType = CONFIG
com.vmware.common.alias = nsxvswitch ,    propType = CONFIG
com.vmware.common.uplinkPorts: uplink1    propType = CONFIG
com.vmware.common.portset.mtu = 1600, propType = CONFIG
com.vmware.etherswitch.cdp = LLDP, listen propType = CONFIG
com.vmware.common.respools.version = version3, propType = CONFIG
com.vmware.common.respools.cfg:
netsched.pools.persist.ft:0:50:-1:255
netsched.pools.persist.hbr:0:50:-1:255
netsched.pools.persist.vmotion:0:50:-1:255
netsched.pools.persist.vm:0:100:-1:255
netsched.pools.persist.iscsi:0:50:-1:255
netsched.pools.persist.nfs:0:50:-1:255
netsched.pools.persist.mgmt:0:50:-1:255
netsched.pools.persist.vdp:0:50:-1:255
netsched.pools.persist.vsan:0:50:-1:255
propType = CONFIG

```

- 6 Überprüfen Sie die NIOC-Profile im Host-Kernel.

```
# [root@ host:] /get /net/portsets/DvsPortset-1/ports/50335755/nicVnicInfo
```

```

Vnic NIOC Info
{
    Uplink reserved on:vmnic4
    Reservation in Mbps:200
    Shares:50
    Limit in Mbps:4294967295
}

```

```

World ID:1001400726
vNIC Index:0
Respool Tag:0
NIOC Version:3
Active Uplink Bit Map:15
Parent Respool ID:netsched.pools.persist.vm
}

```

7 Überprüfen Sie die NIOC-Profilinformationen.

```
# [root@ host:] /get /net/portsets/DvsPortset-1/uplinks/vmnic4/nioInfo
```

```

Uplink NIOC Info
{
  Uplink device:vmnic4
  Link Capacity in Mbps:750
  vm respool reservation:275
  link status:1
  NetSched Ready:1
  Infrastructure reservation:0
  Total VM reservation:200
  Total vnics on this uplink:1
  NIOC Version:3
  Uplink index in BitMap:0
}

```

Ergebnisse

Das NIOC-Profil wird mit einer vordefinierten Bandbreitenzuteilung für Anwendungen konfiguriert, die auf NSX-T Data Center-Hosts ausgeführt werden.

Hinzufügen eines NSX Edge-Cluster-Profils

Das NSX Edge-Cluster-Profil definiert die Richtlinien für den NSX Edge-Transportknoten.

Voraussetzungen

Stellen Sie sicher, dass der NSX Edge-Cluster verfügbar ist.

Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **System > Fabric > Profile > Edge-Clusterprofile > Hinzufügen** aus.

3 Geben Sie die NSX Edge-Cluster-Profildetails ein.

Option	Beschreibung
Name und Beschreibung	Geben Sie einen Profilnamen für den NSX Edge-Cluster ein. Sie können optional die Profildetails wie z. B. die Einstellung für die bidirektionale Weiterleitungserkennung (BFD) eingeben.
BFD-Prüfintervall	Akzeptieren Sie die Standardeinstellung. BFD ist das Erkennungsprotokoll, das zur Identifizierung der Weiterleitungspfadfehler verwendet wird. Sie können das Intervall für BFD so festlegen, dass ein Weiterleitungspfadfehler erkannt wird.
Für BFD zulässige Hops	Akzeptieren Sie die Standardeinstellung. Sie können die Anzahl der Multihop-BFD-Sitzungen festlegen, die für das Profil zulässig sind.
Dead Multiple für BFD deklarieren	Akzeptieren Sie die Standardeinstellung. Sie können die Anzahl der Vorkommnisse festlegen, bei denen das BFD-Paket nicht eingegangen ist, bevor die Sitzung als ausgefallen markiert wird.
Schwellenwert für Standby-Verlagerung	Akzeptieren Sie die Standardeinstellung.

Hinzufügen eines NSX Edge-Bridge-Profils

Das NSX Edge-Bridge-Profil definiert die Richtlinien für den ESXi-Bridge-Cluster.

Ein Bridge-Cluster ist eine Sammlung von ESXi-Host-Transportknoten.

Voraussetzungen

- Stellen Sie sicher, dass der NSX Edge-Cluster verfügbar ist.
- Stellen Sie sicher, dass der ESXi-Bridge-Cluster verfügbar ist.

Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **System > Fabric > Profile > Edge-Bridge-Profile > Hinzufügen** aus.
- 3 Geben Sie die NSX Edge-Cluster-Profildetails ein.

Option	Beschreibung
Name und Beschreibung	Geben Sie einen Profilnamen für den NSX Edge-Bridge-Cluster ein. Sie können optional die Profildetails wie z. B. die primären und die Backup-Knotendetails eingeben.
Edge-Cluster	Wählen Sie den NSX Edge-Cluster aus, den Sie verwenden möchten.
Primärer Knoten	Weisen Sie den bevorzugten NSX Edge-Knoten aus dem Cluster zu.

Option	Beschreibung
Sicherungsknoten	Weisen Sie den Backup-NSX Edge-Knoten zu, wenn der primäre Knoten fehlschlägt.
Failover-Modus	Wählen Sie entweder den Modus Vorbeugend oder Nicht vorbeugend aus. Die Standard-HA-Modus ist vorbeugend, wodurch der Datenverkehr verlangsamt werden kann, wenn der bevorzugte NSX Edge-Knoten wieder online geht. Der nicht vorbeugende Modus bewirkt keine Verlangsamung des Datenverkehrs.

Hinzufügen eines Transportknotenprofils

Ein Transportknotenprofil erfasst die Konfiguration, die zum Erstellen eines Transportknotens erforderlich ist. Das Transportknotenprofil kann auf einen vorhandenen vCenter Server-Cluster zum Erstellen von Transportknoten für die Mitglieder-Hosts angewendet werden. Transportknotenprofile definieren Transportzonen, Mitglieder-Hosts, N-VDS-Switch-Konfiguration einschließlich Uplink-Profil, IP-Zuweisung, Zuordnung von physischen Netzwerkkarten zu virtuellen Uplink-Schnittstellen usw.

Die Transportknotenerstellung beginnt, wenn ein Transportknotenprofil auf ein vCenter Server-Cluster angewendet wird. NSX Manager bereitet die Hosts im Cluster vor und installiert die NSX-T Data Center-Komponenten auf allen Hosts. Transportknoten für die Hosts werden basierend auf der Konfiguration erstellt, die im Transportknotenprofil angegeben ist.

Um ein Transportknotenprofil zu löschen, müssen Sie zuerst das Profil vom zugehörigen Cluster trennen. Die bestehenden Transportknoten sind nicht betroffen. Neue Hosts, die zum Cluster hinzugefügt werden, werden nicht mehr automatisch in Transportknoten konvertiert.

Überlegung für die Erstellung von Transportknotenprofilen:

- Sie können maximal vier N-VDS-Switches für jede Konfiguration hinzufügen: erweitertes N-VDS, das für VLAN-Transportzonen erstellt wurde, Standard-N-VDS, das für Overlay-Transportzonen erstellt wurde, erweitertes N-VDS, das für Overlay-Transportzonen erstellt wurde.
- Es gibt keinen Grenzwert für die Anzahl der standardmäßigen N-VDS-Switches, die für die VLAN-Transportzone erstellt werden.
- In einer einzelnen Host-Cluster-Topologie, in der mehrere Standard-Overlay-N-VDS-Switches und Edge-VM auf demselben Host ausgeführt werden, bietet NSX-T Data Center Datenverkehrsisolierung, sodass Datenverkehr, der über den ersten N-VDS läuft, vom Datenverkehr, der über den zweiten N-VDS läuft, isoliert wird, usw. Die physischen Netzwerkkarten auf jedem N-VDS müssen der Edge-VM auf dem Host zugeordnet werden, sodass die Nord-Süd-Datenverkehrs-Konnektivität mit der Außenwelt ermöglicht wird. Pakete, die aus einer VM auf der ersten Transportzone verschoben werden, müssen über einen externen Router oder eine externe VM zur VM auf der zweiten Transportzone weitergeleitet werden.
- Jeder N-VDS-Switch-Name muss eindeutig sein. NSX-T Data Center lässt nicht die Verwendung von doppelten Switch-Namen zu.
- Jede Transportzonen-ID muss eindeutig sein. NSX-T Data Center lässt nicht die Verwendung von doppelten IDs zu.
- Sie können maximal 1000 Transportzonen zum Transportknotenprofil hinzufügen.

- Um eine Transportzone hinzuzufügen, muss sie von einem beliebigen N-VDS realisiert werden, das im Transportknotenprofil vorhanden ist.

Voraussetzungen

- Stellen Sie sicher, dass die Hosts Teil eines vCenter Server-Clusters sind.
vCenter Server muss mindestens einen Cluster aufweisen.
- Stellen Sie sicher, dass eine Transportzone konfiguriert ist. Siehe [Erstellen von Transportzonen](#).
- Stellen Sie sicher, dass ein Cluster verfügbar ist. Siehe [Bereitstellen von NSX Manager-Knoten zur Bildung eines Clusters über die Benutzeroberfläche](#).
- Stellen Sie sicher, dass ein IP-Pool konfiguriert ist. Andernfalls muss DHCP in der Netzwerkbereitstellung verfügbar sein. Siehe [Erstellen eines IP-Pools für Tunnel-Endpoint-IP-Adressen](#).
- Stellen Sie sicher, dass ein Compute Manager konfiguriert ist. Siehe [Hinzufügen eines Compute Managers](#).

Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **System > Fabric > Profile > Transportknotenprofile > Hinzufügen** aus.
- 3 Geben Sie einen Namen für das Transportknotenprofil ein.
Sie können optional die Beschreibung über das Transportknotenprofil hinzufügen.
- 4 Wählen Sie die verfügbaren Transportzonen aus und klicken Sie auf die Schaltfläche **>**, um die Transportzonen in das Transportknotenprofil aufzunehmen.

Hinweis Sie können mehrere Transportzonen hinzufügen.

- 5 Klicken Sie auf die Registerkarte **N-VDS** und geben Sie die Switch-Informationen ein.

Option	Beschreibung
N-VDS-Name	Wenn der Transportknoten an eine Transportzone angehängt ist, dann stellen Sie sicher, dass der eingegebene Name für den N-VDS identisch mit dem N-VDS-Namen ist, der in der Transportzone angegeben ist. Ein Transportknoten kann erstellt werden, ohne ihn zu einer Transportzone anzuhängen.
Zugeordnete Transportzonen	Zeigt die Transportzonen, die durch den zugeordneten Host-Switches realisiert werden. Sie können keine Transportzone hinzufügen, wenn sie nicht von einem beliebigen N-VDS im Transportknotenprofil realisiert wurde.
NIOC-Profil	Wählen Sie das NIOC-Profil im Dropdown-Menü aus. Die Bandbreitenzuteilungen aus dem Profil für die Datenverkehrsressourcen werden erzwungen.

Option	Beschreibung
Uplink-Profil	<p>Wählen Sie im Dropdown-Menü ein vorhandenes Profil aus, oder erstellen Sie ein benutzerdefiniertes Uplink-Profil.</p> <p>Hinweis Die Hosts in einem Cluster müssen dasselbe Uplink-Profil haben.</p> <p>Sie können auch das standardmäßige Uplink-Profil verwenden.</p>
LLDP-Profil	<p>Standardmäßig empfängt NSX-T nur LLDP-Pakete von einem LLDP-Nachbarn. NSX-T kann jedoch so konfiguriert werden, dass LLDP-Pakete an einen LLDP-Nachbarn gesendet und LLDP-Pakete von einem LLDP-Nachbarn empfangen werden.</p>
IP-Zuweisung	<p>Wählen Sie DHCP verwenden, IP-Pool verwenden oder Statische IP-Liste verwenden, um eine IP-Adresse zu virtuellen Tunnelendpoints (VTEPs) des Transportknotens zuzuweisen.</p> <p>Wenn Sie Liste statischer IPs verwenden auswählen, müssen Sie eine Liste mit durch Komma getrennten IP-Adressen, ein Gateway und eine Subnetzmaske angeben. Alle VTEPs des Transportknotens müssen sich im selben Subnetz befinden. Andernfalls wird eine Sitzung mit bidirektionalem Flow (BFD) nicht aufgebaut.</p>
IP-Pool	<p>Wenn Sie IP-Pool verwenden für eine IP-Zuweisung ausgewählt haben, geben Sie den Namen des IP-Pools an.</p>
Physische Netzwerkkarten	<p>Fügen Sie physische Netzwerkkarten zum Transportknoten hinzu. Sie können den standardmäßigen Uplink verwenden oder einen vorhandenen Uplink aus dem Dropdown-Menü zuweisen.</p> <p>Klicken Sie auf PNIC hinzufügen, um zusätzliche physische Netzwerkkarten zum Transportknoten zu konfigurieren.</p> <p>Hinweis Die Migration der physischen Netzwerkkarten, die Sie in diesem Feld hinzufügen, hängt davon ab, wie Sie Migration nur von PNIC, Netzwerkzuordnungen für die Installation und Netzwerkzuordnungen für die Deinstallation konfigurieren.</p> <ul style="list-style-type: none"> ■ Um eine verwendete physische Netzwerkkarte (z. B. nach einem standardmäßigen vSwitch oder vSphere-Distributed Switch) ohne eine verbundene VMkernel-Zuordnung zu migrieren, stellen Sie sicher, dass Migration nur von PNIC aktiviert ist. Andernfalls bleibt der Transportknotenstatus Teilweise erfolgreich, und die Fabric-Knoten-LCP-Konnektivität kann nicht hergestellt werden. ■ Um eine verwendete physische Netzwerkkarte mit einer verbundenen VMkernel-Netzwerkzuordnung zu migrieren, deaktivieren Sie Migration nur von PNIC und konfigurieren Sie die VMkernel-Netzwerkzuordnung. ■ Um eine freie physische Netzwerkkarte zu migrieren, aktivieren Sie Migration nur von PNIC.

Option	Beschreibung
Migration nur von PNIC	<p>Vor dem Festlegen dieses Felds berücksichtigen Sie die folgenden Punkte:</p> <ul style="list-style-type: none"> ■ Bringen Sie in Erfahrung, ob die definierte physische Netzwerkkarte eine verwendete oder eine freie Netzwerkkarte ist. ■ Bestimmen Sie, ob VMkernel-Schnittstellen eines Hosts zusammen mit physischen Netzwerkkarten migriert werden müssen. <p>Legen Sie das Feld fest:</p> <ul style="list-style-type: none"> ■ Aktivieren Sie Migration nur von PNIC, wenn Sie nur physische Netzwerkkarten von einem VSS- oder DVS-Switch zu einem N-VDS-Switch migrieren möchten. ■ Deaktivieren Sie Migration nur von PNIC, wenn Sie eine verwendete physische Netzwerkkarte und dessen zugeordnete VMkernel-Schnittstellenzuordnung migrieren möchten. Eine freie oder physische Netzwerkkarte ist an den N-VDS-Switch angehängt, wenn eine Migrationszuordnung für die VMkernel-Schnittstelle angegeben ist. <p>Auf einem Host mit mehreren Host-Switches:</p> <ul style="list-style-type: none"> ■ Wenn alle Host-Switches nur PNICs migrieren sollen, können Sie PNICs in einem einzigen Vorgang migrieren. ■ Wenn einige Hosts-Switches VMkernel-Schnittstellen migrieren sollen und die verbleibenden Host-Switches nur PNICs migrieren sollen: <ol style="list-style-type: none"> 1 Migrieren Sie im ersten-Vorgang nur PNICs. 2 Migrieren Sie im zweiten Vorgang VMkernel-Schnittstellen. Stellen Sie sicher, dass Migration nur von PNIC deaktiviert ist. <p>Sowohl die Migration nur von PNIC als auch die VMkernel-Schnittstellenmigration werden nicht gleichzeitig über mehrere Hosts hinweg unterstützt.</p> <hr/> <p>Hinweis Um die Netzwerkkarte eines Verwaltungsnetzwerks zu migrieren, konfigurieren Sie dessen zugeordnete VMkernel-Netzwerk-Zuordnung und lassen Sie Migration nur von PNIC deaktiviert. Wenn Sie nur die Management-Netzwerkkarte migrieren, verliert der Host die Verbindung.</p> <hr/> <p>Weitere Informationen finden Sie unter VMkernel-Migration auf einen N-VDS-Switch.</p>

Option	Beschreibung
Netzwerkzuordnungen für die Installation	<p>Um VMkernels während der Installation zum N-VDS-Switch zu migrieren, ordnen Sie VMkernels einem vorhandenen logischen Switch zu. Der NSX Manager migriert den VMkernel zum zugeordneten logischen Switch auf N-VDS.</p> <p>Vorsicht Stellen Sie sicher, dass die Management-Netzwerkkarte und die Verwaltungs-VMkernel-Schnittstelle auf einen logischen Switch migriert werden, der mit demselben VLAN verbunden ist, mit dem die Management-Netzwerkkarte vor der Migration verbunden war. Wenn vmnic <n> und VMkernel <n> auf ein anderes VLAN migriert werden, dann wird die Verbindung zum Host unterbrochen.</p> <p>Vorsicht Stellen Sie bei angehefteten physischen Netzwerkkarten sicher, dass die Host-Switch-Zuordnung einer physischen Netzwerkkarte zu einer VMkernel-Schnittstelle mit der Konfiguration aus dem Transportknotenprofil übereinstimmt. Im Rahmen des Validierungsverfahrens überprüft NSX-T Data Center die Zuordnung, und wenn die Validierung bestanden wird, ist die Migration von VMkernel-Schnittstellen zu einem N-VDS-Switch erfolgreich. Es ist auch erforderlich, die Netzwerkzuordnung für Deinstallation zu konfigurieren, da NSX-T Data Center die Zuordnungskonfiguration des Host-Switch nicht speichert, nachdem die VMkernel-Schnittstellen zum N-VDS-Switch migriert wurden. Wenn die Zuordnung nicht konfiguriert ist, kann die Verbindung zu Diensten wie vSAN verloren gehen, nachdem die Migration wieder zurück zum VSS- oder VDS-Switch durchgeführt wurde.</p> <p>Weitere Informationen finden Sie unter VMkernel-Migration auf einen N-VDS-Switch.</p>
Netzwerkzuordnungen für die Deinstallation	<p>Um die Migration des VMkernels während der Deinstallation wiederherzustellen, ordnen Sie VMkernels zu Portgruppen auf VSS oder DVS zu, sodass NSX Manager weiß, zu welcher Portgruppe der VMkernel auf dem VSS oder DVS wieder zurückmigriert werden muss. Stellen Sie bei einem DVS-Switch sicher, dass die Portgruppe den Typ Flüchtig aufweist.</p> <p>Vorsicht Stellen Sie bei angehefteten physischen Netzwerkkarten sicher, dass die Transportknotenprofil-Zuordnung einer physischen Netzwerkkarte zu einer VMkernel-Schnittstelle mit der Konfiguration aus dem Host-Switch übereinstimmt. Es ist erforderlich, die Netzwerkzuordnung für Deinstallation zu konfigurieren, da NSX-T Data Center die Zuordnungskonfiguration des Host-Switch nicht speichert, nachdem die VMkernel-Schnittstellen zum N-VDS-Switch migriert wurden. Wenn die Zuordnung nicht konfiguriert ist, kann die Verbindung zu Diensten wie vSAN verloren gehen, nachdem die Migration wieder zurück zum VSS- oder VDS-Switch durchgeführt wurde.</p> <p>Weitere Informationen finden Sie unter VMkernel-Migration auf einen N-VDS-Switch.</p>

6 Um einen anderen N-VDS-Switch hinzuzufügen, klicken Sie auf **+ N-VDS hinzufügen**.

7 Klicken Sie auf **Speichern**, um die Konfiguration abzuschließen.

Nächste Schritte

Wenden Sie das Transportknotenprofil auf einen vorhandenen vSphere-Cluster an. Siehe [Konfigurieren eines verwalteten Host-Transportknotens](#).

VMkernel-Migration auf einen N-VDS-Switch

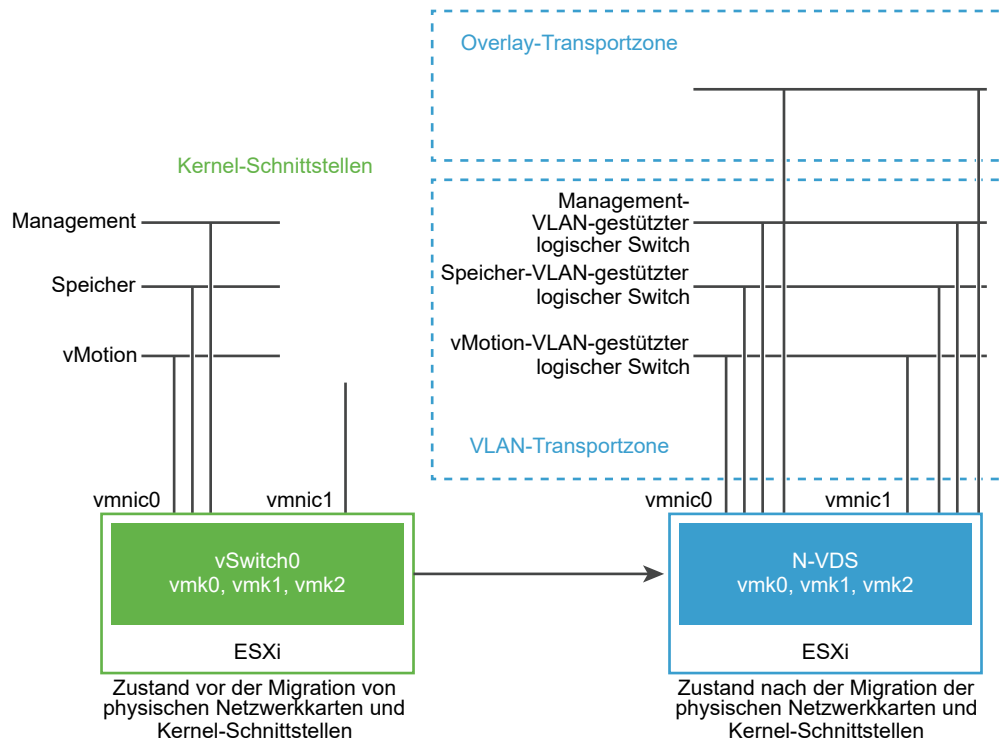
Um VMkernel-Schnittstellen von einem VSS- oder DVS-Switch zu einem N-VDS-Switch auf Clusterebene zu migrieren, konfigurieren Sie das Transportknotenprofil mit für die Migration erforderlichen Netzwerkzuordnungsdetails (ordnen Sie VMkernel-Schnittstellen logischen Switches zu). Konfigurieren Sie analog die Transportknotenkonfiguration, um VMkernel-Schnittstellen auf einem Hostknoten zu migrieren. Um VMkernel-Schnittstellen wieder zurück zu einem VSS- oder DVS-Switch zu migrieren, konfigurieren Sie die Netzwerkzuordnung für die Deinstallation (Zuordnung von logischen Ports zur VMkernel-Schnittstelle) im Transportknotenprofil, das während der Deinstallation realisiert werden soll.

Während der Migration werden derzeit verwendete physische Netzwerkkarten auf einen N-VDS-Switch migriert, während verfügbare oder freie physische Netzwerkkarten nach der Migration an den N-VDS-Switch angehängt werden.

Hinweis Transportknotenprofile werden auf alle Hosts angewendet, die Mitglieder im betreffenden Cluster sind. Wenn Sie jedoch die Migration von VMkernel-Schnittstellen auf bestimmten Hosts einschränken möchten, können Sie den Host direkt konfigurieren. Nach der Migration verarbeitet N-VDS Datenverkehr im VLAN und Overlay-Netzwerk für die Schnittstellen, die mit dem N-VDS-Switch verbunden sind.

Wichtig Konfigurationen, die an einzelnen Hosts vorgenommen werden, werden mit dem Flag überschrieben markiert. Weitere Aktualisierungen des Transportknotenprofils werden nicht auf diese überschriebenen Hosts angewendet. Diese Hosts bleiben im überschriebenen Zustand, bis NSX-T Data Center deinstalliert wird.

Wenn ein Host nur über zwei physische Netzwerkkarten verfügt, können Sie der Redundanz halber beide Netzwerkkarten dem N-VDS zuweisen, einschließlich der zugehörigen VMkernel-Schnittstellen, damit die Schnittstellen die Verbindung zum Host nicht verlieren. Dies ist in der folgenden Abbildung dargestellt.

Abbildung 8-2. Vor und nach der Migration der Netzwerkschnittstellen zu einem N-VDS

Vor der Migration verfügt der ESXi-Host über zwei Uplinks, die von zwei physischen Ports abgeleitet sind, vmnic0 und vmnic1. Hierbei ist vmnic0 für einen aktiven Zustand konfiguriert und an einen VSS angehängt, während vmnic1 nicht verwendet wird. Darüber hinaus sind drei VMkernel-Schnittstellen vorhanden: vmk0, vmk1 und vmk2.

VMkernel-Schnittstellen können Sie mithilfe der NSX-T Data Center Manager-Benutzeroberfläche oder der NSX-T Data Center-APIs migrieren. Siehe *Handbuch für die NSX-T Data Center-API*.

Nach der Migration werden die vmnic0, vmnic1 und deren VMkernel-Schnittstellen zum N-VDS-Switch migriert. Sowohl vmnic0 als auch vmnic1 sind über VLAN und Overlay-Transportzonen verbunden.

Überlegungen für die VMkernel-Migration

- **PNIC- und VMkernel-Migration:** Bevor Sie angeheftete physische Netzwerkkarten und zugehörige VMkernel-Schnittstellen zu einem N-VDS-Switch migrieren, notieren Sie sich die Netzwerkzuordnung (Zuordnung physischer Netzwerkkarten zu Portgruppen) auf dem Host-Switch.
- **Migration nur von PNIC:** Wenn Sie nur PNICs migrieren möchten, stellen Sie sicher, dass die mit der VMkernel-Verwaltungsschnittstelle verbundene physische Verwaltungsnetzwerkkarte nicht migriert wird. Andernfalls wäre ein Verlust der Konnektivität mit dem Host die Folge. Weitere Informationen finden Sie im Feld **Migration nur von PNIC** unter [Hinzufügen eines Transportknotenprofils](#).
- **Migration wiederherstellen:** Bevor Sie die Migration von VMkernel-Schnittstellen zum VSS- oder DVS-Host-Switch für angeheftete physische Netzwerkkarten wiederherstellen möchten, stellen Sie sicher, dass Sie sich die Netzwerkzuordnung (Zuordnung der physischen Netzwerkkarte zur Portgruppe) auf dem Host-Switch notieren. Es ist zwingend erforderlich, das Transportknotenprofil mit der Host-

Switch-Zuordnung im Feld **Netzwerkzuordnung für Deinstallation** zu konfigurieren. Ohne diese Zuordnung weiß NSX-T Data Center nicht, zu welchen Portgruppen die VMkernel-Schnittstellen zurückmigriert werden müssen. Diese Situation kann zu einem Verlust der Konnektivität mit dem vSAN-Netzwerk führen.

- vCenter Server-Registrierung vor der Migration: Wenn Sie vorhaben, einen VMkernel oder eine PNIC zu migrieren, die mit einem DVS-Switch verbunden sind, stellen Sie sicher, dass ein vCenter Server beim NSX Manager registriert ist.
- VLAN-ID-Übereinstimmung: Nach der Migration müssen sich die Verwaltungsnetzwerkkarte und die VMkernel-Verwaltungsschnittstelle auf demselben VLAN befinden, mit dem die Verwaltungsnetzwerkkarte vor der Migration verbunden war. Wenn vmnic0 und vmk0 mit dem Verwaltungsnetzwerk verbunden sind und zu einem anderen VLAN migriert werden, geht die Konnektivität mit dem Host verloren.
- Migration zu VSS-Switch: Zwei VMkernel-Schnittstellen können nicht zur gleichen Portgruppe eines VSS-Switch zurückmigriert werden.
- vMotion: Führen Sie vMotion aus, um VM-Arbeitslasten vor einer VMkernel- und/oder PNIC-Migration auf einen anderen Host zu verschieben. Wenn die Migration fehlschlägt, werden die Arbeitslast-VMs nicht beeinträchtigt.
- vSAN: Wenn der vSAN-Datenverkehr auf dem Host ausgeführt wird, versetzen Sie den Host über vCenter Server in den Wartungsmodus und verschieben Sie die VMs vor der VMkernel- und/oder PNIC-Migration mithilfe der vMotion-Funktion vom Host.
- Migration: Wenn ein VMkernel bereits mit einem Ziel-Switch verbunden ist, kann er weiterhin für die Migration zum selben Switch ausgewählt werden. Mit dieser Eigenschaft wird der VMK- und/oder PNIC-Migrationsvorgang idempotent. Dies ist hilfreich, wenn Sie nur PNICs zu einem Ziel-Switch migrieren möchten. Da für die Migration immer mindestens ein VMkernel und eine PNIC erforderlich sind, wählen Sie einen VMkernel aus, der bereits zu einem Ziel-Switch migriert wurde, wenn Sie nur PNICs zu einem Ziel-Switch migrieren. Wenn kein VMkernel migriert werden muss, erstellen Sie entweder auf dem Quell-Switch oder Ziel-Switch über vCenter Server einen temporären VMkernel. Migrieren Sie den temporären VMkernel zusammen mit den PNICs und löschen Sie ihn über vCenter Server, sobald die Migration abgeschlossen ist.
- Gemeinsame MAC-Nutzung: Wenn eine VMkernel-Schnittstelle und eine PNIC dieselbe MAC nutzen und sich auf demselben Switch befinden, müssen sie zusammen zum selben Ziel-Switch migriert werden, wenn sie beide nach der Migration verwendet werden. Behalten Sie vmk0 und vmnic0 immer auf demselben Switch bei.

Überprüfen Sie die MACs, die von allen VMKs und PNICs auf dem Host verwendet werden, indem Sie die folgenden Befehle ausführen:

```
esxcfg-vmknics -l
```

```
esxcfg-nics -l
```

- Nach der Migration erstellte logische VIF-Ports: Nachdem Sie VMkernel von einem VSS- oder DVS-Switch zu einem N-VDS-Switch migriert haben, wird ein logischer Switch Port des Typs VIF auf dem NSX Manager erstellt. Sie dürfen keine Regeln für verteilte Firewalls auf diesen logischen VIF-Switch-Ports erstellen.

Migrieren von VMkernel-Schnittstellen zu einem N-VDS-Switch

Allgemeiner Workflow zum Migrieren von VMkernel-Schnittstellen zu einem N-VDS-Switch:

- 1 Erstellen Sie bei Bedarf einen logischen Switch.
- 2 Schalten Sie VMs auf dem Host aus, von dem VMkernel-Schnittstellen und PNICs auf einen N-VDS-Switch migriert werden.
- 3 Konfigurieren Sie ein Transportknotenprofil mit einer Netzwerkzuordnung, mit der die VMkernel-Schnittstellen während der Erstellung von Transportknoten migriert werden. Netzwerkzuordnung bedeutet die Zuordnung einer VMkernel-Schnittstelle zu einem logischen Switch.

Weitere Informationen finden Sie unter [Hinzufügen eines Transportknotenprofils](#).

- 4 Stellen Sie sicher, dass die Netzwerkadapterzuordnungen in vCenter Server eine neue Zuordnung des VMkernel-Switches zu einem N-VDS-Switch widerspiegeln. Überprüfen Sie bei angehefteten physischen Netzwerkkarten, ob die Zuordnung in NSX-T Data Center alle VMKernels widerspiegelt, die an eine physische Netzwerkkarte im vCenter Server angeheftet sind.
- 5 Gehen Sie in NSX Manager zu **Netzwerk und Sicherheit – Erweitert > Netzwerke > Switching**. Überprüfen Sie auf der Seite **Switches**, ob die VMkernel-Schnittstelle über einen neu erstellten logischen Port mit dem logischen Switch verbunden ist.
- 6 Wechseln Sie zu **System > Knoten > Host-Transportknoten**. Überprüfen Sie für jeden Transportknoten, ob als Status in der Spalte **Knotenstatus** „Erfolgreich“ angezeigt wird, um zu bestätigen, dass die Transportknotenkonfiguration erfolgreich validiert wurde.
- 7 Überprüfen Sie auf der Seite **Host-Transportknoten** ober als **Konfigurationszustand** „Erfolgreich“ angezeigt wird, um sicher zu sein, dass der Host mit der angegebenen Konfiguration erfolgreich realisiert wurde.

Nach der Migration von VMkernel-Schnittstellen und PNICs von einem VDS- zu einem N-VDS-Switch mithilfe der NSX-T-Benutzeroberfläche oder der Transportknoten-API zeigt vCenter Server Warnungen für den VDS an. Wenn der Host mit dem VDS verbunden werden muss, entfernen Sie den Host vom VDS. vCenter Server zeigt keine Warnung mehr für VDS an.

Weitere Informationen zu Fehlern, die während der Migration auftreten können, finden Sie unter [Fehler bei der VMkernel-Migration](#).

Wiederherstellen der Migration von VMkernel-Schnittstellen zu einem VSS- oder DVS-Switch

Allgemeiner Workflow zum Wiederherstellen der Migration von VMkernel-Schnittstellen von einem N-VDS-Switch zu einem VSS- oder DVS-Switch während der Deinstallation von NSX-T Data Center:

- 1 Schalten Sie auf dem ESXi-Host VMs aus, die mit den logischen Ports verbunden sind, auf denen die VMkernel-Schnittstelle nach der Migration gehostet wird.
- 2 Konfigurieren Sie das Transportknotenprofil mit einer Netzwerkzuordnung, mit der die VMkernel-Schnittstellen während des Deinstallationsvorgangs migriert werden. Die Netzwerkzuordnung während der Deinstallation ordnet die VMkernel-Schnittstellen einer Portgruppe auf dem VSS- oder DVS-Switch auf dem ESXi-Host zu.

Hinweis Wenn Sie die Migration eines VMkernel zu einer Portgruppe auf einem DVS-Switch wiederherstellen, müssen Sie darauf achten, dass als Portgruppentyp **Flüchtig** festgelegt ist.

Weitere Informationen finden Sie unter [Hinzufügen eines Transportknotenprofils](#).

- 3 Stellen Sie sicher, dass die Netzwerkadapterzuordnungen in vCenter Server eine neue Zuordnung des VMkernel-Switches zu einer Portgruppe des VSS- oder DVS-Switches widerspiegeln.
- 4 Gehen Sie in NSX Manager zu **Netzwerk und Sicherheit – Erweitert > Netzwerke > Switching**. Überprüfen Sie auf der Seite **Switches**, ob der logische Switch, der VMkernel-Schnittstellen enthält, gelöscht wird.

Weitere Informationen zu Fehlern, die während der Migration auftreten können, finden Sie unter [Fehler bei der VMkernel-Migration](#).

Aktualisieren der Host-Switch-Zuordnung

Wichtig

- Statusbehaftete-Hosts: Hinzufügen und Aktualisieren werden unterstützt. Um eine vorhandene Zuordnung zu aktualisieren, können Sie der Netzwerkzuordnungsconfiguration einen neuen VMkernel-Schnittstelleneintrag hinzufügen. Wenn Sie die Netzwerkzuordnungsconfiguration einer VMkernel-Schnittstelle aktualisieren, die bereits zum N-VDS-Switch migriert wurde, wird die aktualisierte Netzwerkzuordnung auf dem Host nicht realisiert.
- Statusfreie Hosts: Hinzufügen, Aktualisieren und Entfernen werden unterstützt. Alle Änderungen, die Sie an der Netzwerkzuordnungsconfiguration vornehmen, werden nach dem Neustart des Hosts wirksam.

Um die VMkernel-Schnittstellen auf einen neuen logischen Switch zu aktualisieren, können Sie das Transportknotenprofil so bearbeiten, dass die Netzwerkzuordnungen auf Clusterebene angewendet werden. Wenn die Updates nur auf einen einzelnen Host angewendet werden sollen, konfigurieren Sie den Transportknoten mithilfe von APIs auf Hostebene.

Hinweis Nachdem Sie die Transportknotenconfiguration für einen einzelnen Host aktualisiert haben, werden alle neuen Updates, die über das Transportknotenprofil angewendet werden, nicht auf diesen Host angewendet. Der Status dieses Hosts wechselt zu **Überschrieben**.

- 1 Um alle Hosts in einem Cluster zu aktualisieren, bearbeiten Sie das Feld **Netzwerkzuordnung während der Installation**, um die VMkernel-Zuordnung zu logischen Switches zu aktualisieren.

Weitere Informationen finden Sie unter [Hinzufügen eines Transportknotenprofils](#).

- 2 Speichern Sie die Änderungen. Änderungen an einem Transportknotenprofil werden automatisch auf alle Mitgliedshosts des Clusters angewendet, außer auf Hosts, die mit dem Status Überschrieben gekennzeichnet sind.
- 3 Um einen einzelnen Host zu aktualisieren, bearbeiten Sie die VMkernel-Zuordnung in der Transportknotenkonfiguration.

Hinweis Wenn Sie das Feld **Netzwerkzuordnung während der Installation** mit einer neuen VMkernel-Zuordnung aktualisieren, muss dieselbe VMkernel-Schnittstelle dem Feld **Netzwerkzuordnung während der Deinstallation** hinzugefügt werden.

Weitere Informationen zu Fehlern, die während der Migration auftreten können, finden Sie unter [Fehler bei der VMkernel-Migration](#).

Migrieren von VMkernel-Schnittstellen in einem statusfreien Cluster

- 1 Bereiten Sie einen Host vor und konfigurieren Sie ihn mithilfe von Transportknoten-APIs als Referenzhost.
- 2 Extrahieren Sie ein Hostprofil aus dem Referenzhost.
- 3 Wenden Sie das Hostprofil im vCenter Server auf den statusfreien Cluster an.
- 4 Wenden Sie in das Transportknotenprofil in NSX-T Data Center auf den statusfreien Cluster an.
- 5 Starten Sie jeden Host des Clusters neu.

Es kann einige Minuten dauern, bis die aktualisierten Zustände der Clusterhosts wirksam werden.

Migrationsfehlerszenarien

- Wenn die Migration aus irgendeinem Grund fehlschlägt, versucht der Host drei Mal, die physischen Netzwerkkarten und VMkernel-Schnittstellen zu migrieren.
- Schlägt die Migration weiterhin fehl, stellt der Host die frühere Konfiguration wieder her, indem die VMkernel-Konnektivität mit der physischen Verwaltungsnetzwerkkarte (vnic0) beibehalten wird.
- Falls die Wiederherstellung ebenfalls fehlschlägt, sodass der für die physische Verwaltungsnetzwerkkarte konfigurierte VMkernel verloren gegangen ist, müssen Sie den Host zurücksetzen.

Nicht unterstützte Migrationsszenarien

Die folgenden Szenarien werden nicht unterstützt:

- VMkernel-Schnittstellen von zwei verschiedenen VSS- oder DVS-Switches werden gleichzeitig migriert.
- Auf statusbehafteten Hosts wird die Netzwerkzuordnung aktualisiert, um die VMkernel-Schnittstelle einem anderen logischen Switch zuzuordnen. Beispielsweise wird der VMkernel vor der Migration dem logischen Switch 1 zugeordnet und die VMkernel-Schnittstelle dem logischen Switch 2.

Fehler bei der VMkernel-Migration

Beim Migrieren von VMkernel-Schnittstellen und physischen Netzwerkkarten von einem VSS- oder DVS-Switch auf einen N-VDS-Switch oder beim Rückmigrieren von Schnittstellen zu einem VSS- oder DVS-Host-Switch können Fehler auftreten.

Tabelle 8-1. Fehler bei der VMkernel-Migration

Fehlercode	Problem	Ursache	Lösung
8224	Der in der Konfiguration des Transportknotens angegebene Host-Switch kann nicht gefunden werden.	Die Host-Switch-ID kann nicht gefunden werden.	<ul style="list-style-type: none"> ■ Stellen Sie sicher, dass die Transportzone mit dem Host-Switch-Namen erstellt wurde, und erstellen Sie dann den Transportknoten. ■ Stellen Sie sicher, dass ein gültiger Host-Switch in der Konfiguration des Transportknotens verwendet wird.
8225	VMkernel-Migration wird durchgeführt.	Migration wird durchgeführt.	Warten Sie, bis die Migration abgeschlossen ist, bevor Sie eine andere Aktion durchführen.
8226	VMkernel-Migration wird nur auf einem ESXi-Host unterstützt.	Migration ist nur für ESXi-Hosts gültig.	Stellen Sie vor dem Starten der Migration sicher, dass es sich bei dem Host um einen ESXi-Host handelt.
8227	Der Host-Switch-Name wurde nicht an die VMkernel-Schnittstelle angehängt.	Auf einem Host mit mehreren Host-Switches kann NSX-T Data Center die Verknüpfung zwischen den VMkernel-Schnittstellen und den zugehörigen Host-Switches nicht erkennen.	<p>Wenn der Host mehrere N-VDS-Host-Switches aufweist, stellen Sie sicher, dass der Host-Switch-Name des N-VDS, mit dem der Host verbunden ist, an die VMkernel-Schnittstelle angehängt wird.</p> <p>Beispiel: Die Netzwerkzuordnung für die Deinstallation eines Hosts mit dem N-VDS-Host-Switch-Namen „nsxvswitch1“ und „VMkernel1“ und einem anderen N-VDS-Host-Switch-Namen „nsxvswitch2“ und „VMkernel2“ muss folgendermaßen definiert werden: device_name: VMkernel1@nsxvswitch1, destination_network: DPortGroup.</p>
8228	Im Feld device_name verwendeter Host-Switch wurde auf dem Host nicht gefunden.	Falscher Host-Switch-Name	Geben Sie den korrekten Host-Switch-Namen an.
8229	Die Transportzone des logischen Switches wurde im Transportknoten nicht angegeben.	Transportzone wurde nicht hinzugefügt.	Fügen Sie der Konfiguration des Transportknotens die Transportzone hinzu.

Tabelle 8-1. Fehler bei der VMkernel-Migration (Fortsetzung)

Fehlercode	Problem	Ursache	Lösung
8230	Keine physische Netzwerkkarte auf dem Host-Switch.	Mindestens eine physische Netzwerkkarte muss auf dem Host-Switch vorhanden sein.	Geben Sie mindestens eine physische Netzwerkkarte ein, um ein Uplink-Profil und die Konfiguration der VMkernel-Zuordnung mit einem logischen Switch zu verbinden.
8231	Host-Switch-Name stimmt nicht überein.	Der in vmk1@host_switch verwendete Host-Switch-Name stimmt nicht mit dem vom logischen Ziel-Switch der Schnittstelle verwendeten Host-Switch-Namen überein.	Stellen Sie sicher, dass der in der Konfiguration der Netzwerkzuordnung angegebene Host-Switch-Name mit dem vom logischen Switch der Schnittstelle verwendeten Namen übereinstimmt.
8232	Logischer Switch auf dem Host konnte nicht dargestellt werden.	Die Darstellung des logischen Switches auf dem Host war nicht erfolgreich.	Synchronisieren Sie den Host mit dem NSX Manager.
8233	Unerwarteter logischer Switch in der Netzwerkzuordnung der Schnittstelle.	In der Netzwerkzuordnung der Schnittstelle werden für die Installation und Deinstallation sowohl logische Switches als auch Portgruppen aufgelistet.	Die Netzwerkzuordnung für die Installation darf nur logische Switches als Ziele enthalten. Ebenso darf die Netzwerkzuordnung für die Deinstallation nur Portgruppen als Ziele enthalten.
8294	Logischer Switch ist in der Netzwerkzuordnung der Schnittstelle nicht vorhanden.	Es wurden keine logischen Switches angegeben.	Stellen Sie sicher, dass die logischen Switches in der Konfiguration für die Netzwerkzuordnung der Schnittstelle angegeben werden.
8296	Host-Switch stimmt nicht überein.	Die Netzwerkzuordnung der Schnittstelle für die Deinstallation ist mit dem falschen Host-Switch-Namen konfiguriert.	Stellen Sie sicher, dass der in der Zuordnungskonfiguration verwendete Host-Switch-Name dem Namen entspricht, der auf dem Host-Switch, auf dem sich die VMkernel-Schnittstellen befinden, eingegeben wurde.
8297	Doppelter VMkernel.	Doppelte VMkernel sind für die Migration angegeben.	Stellen Sie sicher, dass keine doppelten VMkernel-Schnittstellen in der Zuordnungskonfiguration der Installation oder Deinstallation angegeben wurden.
8298	Nichtübereinstimmung bei der Anzahl der VMkernel-Schnittstellen und -Ziele.	Falsche Konfiguration.	Stellen Sie sicher, dass für jede VMkernel-Schnittstelle ein entsprechendes Ziel in der Konfiguration angegeben wurde.
8299	Transportknoten kann nicht gelöscht werden, da die VMkernel-Schnittstelle Ports auf dem N-VDS verwendet.	VMkernel-Schnittstellen verwenden Ports aus dem N-VDS-Switch.	Führen Sie eine Rückmigration aller VMkernel-Schnittstellen vom N-VDS-Switch zu einem VSS-/DVS-Switch durch. Versuchen Sie dann, den Transportknoten zu löschen.

Tabelle 8-1. Fehler bei der VMkernel-Migration (Fortsetzung)

Fehlercode	Problem	Ursache	Lösung
9412	VMkernel kann nicht von einem N-VDS auf einen anderen N-VDS migriert werden.	Nicht unterstützte Aktion.	Führen Sie eine Rückmigration der VMkernel-Schnittstelle auf einen VSS- oder DVS-Switch durch. Anschließend können Sie die VMkernel-Schnittstelle auf einen anderen N-VDS-Switch migrieren.
9413	VMkernel-Schnittstellen können nicht auf einen anderen logischen Switch migriert werden.	Auf statusbehafteten Hosts kann ein mit einem logischen Switch verbundener VMkernel nicht auf einen anderen logischen Switch migriert werden.	Führen Sie eine Rückmigration des VMkernels vom logischen Switch zu einem VSS-/DVS-Switch durch. Migrieren Sie den VMkernel anschließend auf einen anderen logischen Switch auf dem N-VDS.
9414	Duplizieren der VMkernel-Schnittstellen.	Duplizieren Sie VMkernel-Schnittstellen, die in der Zuordnungskonfiguration der Installation und Deinstallation zugeordnet sind.	Stellen Sie sicher, dass jede VMkernel-Schnittstelle in den Installations- und Deinstallationszuordnungen eindeutig ist.
9415	Eingeschaltete VMs auf dem Host.	Bei eingeschalteten VMs wird die Migration nicht fortgesetzt.	Schalten Sie die VMs auf dem Host aus, bevor Sie mit der Migration von VMkernel-Schnittstellen beginnen.
9416	VMkernel kann auf dem Host nicht gefunden werden.	In der Konfiguration der Netzwerkzuordnung wurde kein VMkernel angegeben, der auf dem Host vorhanden ist.	Geben Sie einen vorhandenen VMkernel in der Konfiguration der Netzwerkzuordnung an.
9417	Portgruppe nicht gefunden.	Es wurde keine Portgruppe angegeben, die in der Konfiguration der Netzwerkzuordnung auf dem Host vorhanden ist.	Geben Sie eine vorhandene Portgruppe in der Konfiguration der Netzwerkzuordnung an.
9419	Logischer Switch während der Migration nicht gefunden.	Der in der Konfiguration der Netzwerkschnittstellenzuordnung definierte logische Switch wurde nicht gefunden.	Geben Sie einen vorhandenen logischen Switch in der Konfiguration der Netzwerkschnittstellenzuordnung an.
9420	Logischer Port während der Migration nicht gefunden.	Während der Migration findet NSX-T Data Center die auf dem logischen Switch erstellten Ports nicht.	Stellen Sie für eine erfolgreiche Migration sicher, dass keine logischen Ports vom logischen Switch gelöscht werden.
9421	Zum Validieren der Migration fehlen Hostinformationen.	Informationen konnten nicht aus der Bestandsliste abgerufen werden.	Wiederholen Sie den Migrationsvorgang.
9423	An eine VMkernel-Schnittstelle angeheftete physische Netzwerkkarten werden nicht mit dem richtigen Host-Switch migriert.	Eine angeheftete physische Netzwerkkarte wurde in der Umgebung gefunden, aber der VMkernel und die physische Netzwerkkarte werden nicht auf denselben Host-Switch migriert.	Eine einer VMkernel-Schnittstelle zugewiesene physische Netzwerkkarte muss eine Transportknotenkonfiguration aufweisen, die dem VMkernel die physische Netzwerkkarte auf demselben Host-Switch zuordnet.

Tabelle 8-1. Fehler bei der VMkernel-Migration (Fortsetzung)

Fehlercode	Problem	Ursache	Lösung
600	Objekt nicht gefunden.	Die vom logischen Switch verwendete angegebene Transportzone ist nicht vorhanden. Der im VMK-Zuordnungsziel enthaltene logische Switch kann nicht gefunden werden.	<ul style="list-style-type: none"> ■ Geben Sie eine Transportzone an, die in der Umgebung vorhanden ist. ■ Erstellen Sie den gewünschten logischen Switch oder verwenden Sie einen vorhandenen logischen VLAN-Switch.
8310	Der Typ des logischen Switches ist falsch.	Der Typ des logischen Switch lautet „Overlay“.	Erstellen Sie einen logischen VLAN-Switch.
9424	Kann nicht migriert werden, wenn die Einstellung „Nur PNIC-Migration“ und die Einstellung „Netzwerkzuordnung für Installation und Deinstallation“ gleichzeitig konfiguriert sind.	Migration wird nur fortgesetzt, wenn eine dieser Einstellungen konfiguriert wurde.	Stellen Sie sicher, dass entweder die Einstellung „Nur PNIC-Migration“ oder die Einstellung „Netzwerkzuordnung für Installation und Deinstallation“ konfiguriert ist.

Erstellen eines eigenständigen Hosts oder Bare-Metal-Server-Transportknotens

Sie müssen zuerst Ihren ESXi-Host, KVM-Host oder Bare-Metal-Server zur NSX-T Data Center-Fabric hinzufügen und dann den Transportknoten konfigurieren.

Ein Fabric-Knoten ist ein Knoten, der bei der NSX-T Data Center-Management Plane registriert wurde und auf dem NSX-T Data Center-Module installiert sind. Damit ein Host oder Bare-Metal-Server Teil des NSX-T Data Center-Overlays werden kann, muss er zunächst zur NSX-T Data Center-Fabric hinzugefügt werden.

Ein Transportknoten ist ein Knoten, der an einem NSX-T Data Center-Overlay oder NSX-T Data Center-VLAN-Networking teilnimmt.

Bei einem KVM-Host oder Bare-Metal-Server können Sie den N-VDS im Voraus konfigurieren oder die Konfiguration von NSX Manager durchführen lassen. Bei einem ESXi-Host wird der N-VDS immer von NSX Manager konfiguriert.

Hinweis Wenn Sie Transportknoten aus einer Vorlagen-VM erstellen möchten, achten Sie darauf, dass keine Zertifikate für den Host in `/etc/vmware/nsx/` vorhanden sind. Der netcpa-Agent erstellt kein Zertifikat, wenn ein Zertifikat vorhanden ist.

Der Bare-Metal-Server unterstützt ein Overlay- und VLAN-Transportzone. Sie können die Management-Schnittstelle verwenden, um den Bare-Metal-Server zu verwalten. Mit der Anwendungsschnittstelle können Sie auf die Anwendungen auf dem Bare-Metal-Server zugreifen.

Einzelne physische Netzwerkkarten bieten eine IP-Adresse für die Verwaltungs- und Anwendungs-IP-Schnittstellen.

Zwei physische Netzwerkkarten bieten eine physische Netzwerkkarte und eine eindeutige IP-Adresse für die Verwaltungsschnittstelle. Zwei physische Netzwerkkarten bieten auch eine physische Netzwerkkarte und eine eindeutige IP-Adresse für die Anwendungsschnittstelle.

Mehrere physische Netzwerkkarten in einer verbundenen Konfiguration bieten zwei physische Netzwerkkarten und eine eindeutige IP-Adresse für die Verwaltungsschnittstelle. Mehrere physische Netzwerkkarten in einer verbundenen Konfiguration bieten auch zwei physische Netzwerkkarten und eine eindeutige IP-Adresse für die Anwendungsschnittstelle.

Sie können maximal vier N-VDS-Switches für jede Konfiguration hinzufügen: Standard-N-VDS, das für VLAN-Transportzonen erstellt wurde, erweitertes N-VDS, das für VLAN-Transportzonen erstellt wurde, Standard-N-VDS, das für Overlay-Transportzonen erstellt wurde, erweitertes N-VDS, das für Overlay-Transportzonen erstellt wurde.

In einer einzelnen Host-Cluster-Topologie, in der mehrere Standard-Overlay-N-VDS-Switches und Edge-VM auf demselben Host ausgeführt werden, bietet NSX-T Data Center Datenverkehrsisolierung, sodass Datenverkehr, der über den ersten N-VDS läuft, vom Datenverkehr, der über den zweiten N-VDS läuft, isoliert wird, usw. Die physischen Netzwerkkarten auf jedem N-VDS müssen der Edge-VM auf dem Host zugeordnet werden, sodass die Nord-Süd-Datenverkehrs-Konnektivität mit der Außenwelt ermöglicht wird. Pakete, die aus einer VM auf der ersten Transportzone verschoben werden, müssen über einen externen Router oder eine externe VM zur VM auf der zweiten Transportzone weitergeleitet werden.

Voraussetzungen

- Der Host muss mit der Management Plane verbunden sein, und die Konnektivität muss auf Aktiv stehen.
- Eine Transportzone muss konfiguriert sein.
- Es muss entweder ein Uplink-Profil konfiguriert werden, oder Sie können das standardmäßige Uplink-Profil verwenden.
- Ein IP-Pool muss konfiguriert sein, oder DHCP muss in der Netzwerkbereitstellung verfügbar sein.
- Mindestens eine nicht verwendete physische Netzwerkkarte (NIC) muss auf dem Hostknoten verfügbar sein.
- Hostname
- Verwaltungs-IP-Adresse
- Benutzername
- Kennwort
- Optional: (KVM) SHA-256-SSL-Fingerabdruck
- Optional: (ESXi) SHA-256-SSL-Fingerabdruck
- Stellen Sie sicher, dass die erforderlichen Drittanbieterpakete installiert sind. Siehe [Installieren von Drittanbieterpaketen auf einem KVM-Host](#).

Verfahren

- 1 (Optional) Rufen Sie den Hypervisor-Fingerabdruck ab, damit Sie diesen beim Hinzufügen des Hosts zur Fabric angeben können.

- a Sammeln Sie die Informationen zum Hypervisor-Fingerabdruck.

Verwenden Sie eine Linux-Shell.

```
# echo -n | openssl s_client -connect <esxi-ip-address>:443 2>/dev/null | openssl x509 -noout -fingerprint -sha256
```

Verwenden Sie die ESXi-CLI auf dem Host.

```
[root@host:~] openssl x509 -in /etc/vmware/ssl/rui.crt -fingerprint -sha256 -noout
SHA256
Fingerprint=49:73:F9:A6:0B:EA:51:2A:15:57:90:DE:C0:89:CA:7F:46:8E:30:15:CA:4D:5C:95:28:0A:9E:A
2:4E:3C:C4:F4
```

- b Um den SHA-256-Fingerabdruck von einem KVM-Hypervisor abzurufen, führen Sie den Befehl auf dem KVM-Host aus.

```
# awk '{print $2}' /etc/ssh/ssh_host_rsa_key.pub | base64 -d | sha256sum -b | sed 's/ .*$//' | xxd -r -p | base64
```

- 2 Wählen Sie **System > Fabric > Knoten > Host-Transportknoten** aus.
- 3 Wählen über das Feld „Verwaltet von“ **Eigenständige Hosts** aus und klicken Sie auf **+ Hinzufügen**.
- 4 Geben Sie Details für den eigenständigen Host oder den Bare-Metal-Server ein, die zur Fabric hinzugefügt werden sollen.

Option	Beschreibung
Name und Beschreibung	Geben Sie den Namen ein, um den eigenständigen Host oder Bare-Metal-Server zu identifizieren. Sie können optional die Beschreibung des Betriebssystems hinzufügen, die für den Host oder den Bare-Metal-Server verwendet werden.
IP-Adressen	Geben Sie die IP-Adresse des Hosts oder Bare-Metal-Servers ein.
Betriebssystem	Wählen Sie im Dropdown-Menü das Betriebssystem aus. In Abhängigkeit von Ihrem Host oder Bare-Metal-Server können Sie ein beliebiges unterstütztes Betriebssystem auswählen. Siehe Systemvoraussetzungen .
Benutzername und Kennwort	Geben Sie den Benutzernamen und das Kennwort für den Hostbenutzer ein.
SHA-256-Fingerabdruck	Geben Sie den Host-Fingerabdruck-Wert für die Authentifizierung ein. Wenn Sie den Fingerabdruckwert leer lassen, werden Sie aufgefordert, den vom Server bereitgestellten Wert zu akzeptieren. Es dauert einige Sekunden, bis NSX-T Data Center den Host erkennt und authentifiziert.

- 5 (Erforderlich) Wählen Sie für einen KVM-Host oder Bare-Metal-Server den N-VDS-Typ aus.

Option	Beschreibung
NSX erstellt	NSX Manager erstellt den N-VDS. Diese Option ist standardmäßig ausgewählt.
Vorkonfiguriert	Der N-VDS ist bereits konfiguriert.

Bei einem ESXi-Host ist der N-VDS-Typ immer auf **NSX erstellt** festgelegt.

- 6 Geben Sie die Standard-N-VDS-Details ein. Mehrere N-VDS-Switches können auf einem einzelnen Host konfiguriert werden.

Option	Beschreibung
Transportzone	Wählen Sie aus dem Dropdown-Menü die Transportzone aus, zu der dieser Transportknoten gehört.
N-VDS-Name	Muss mit dem N-VDS-Namen der Transportzone identisch sein, zu der dieser Knoten gehört.
NIOC-Profil	Wählen Sie für einen ESXi-Host das NIOC-Profil im Dropdown-Menü aus.
Uplink-Profil	Wählen Sie im Dropdown-Menü ein vorhandenes Profil aus, oder erstellen Sie ein benutzerdefiniertes Uplink-Profil. Sie können auch das standardmäßige Uplink-Profil verwenden.
LLDP-Profil	Standardmäßig empfängt NSX-T nur LLDP-Pakete von einem LLDP-Nachbarn. NSX-T kann jedoch so eingestellt werden, dass LLDP-Pakete an einen LLDP-Nachbarn gesendet und LLDP-Pakete von einem LLDP-Nachbarn empfangen werden.
IP-Zuweisung	Wählen Sie DHCP verwenden , IP-Pool verwenden oder Liste statischer IPs verwenden . Wenn Sie Liste statischer IPs verwenden auswählen, müssen Sie eine Liste mit durch Komma getrennten IP-Adressen, ein Gateway und eine Subnetzmaske angeben.
IP-Pool	Wenn Sie IP-Pool verwenden für die IP-Zuweisung ausgewählt haben, geben Sie den Namen des IP-Pools an.

Option	Beschreibung
Physische Netzwerkkarten	<p>Fügen Sie physische Netzwerkkarten zum Transportknoten hinzu. Sie können den standardmäßigen Uplink verwenden oder einen vorhandenen Uplink aus dem Dropdown-Menü zuweisen.</p> <p>Klicken Sie auf PNIC hinzufügen, um zusätzliche physische Netzwerkkarten zum Transportknoten zu konfigurieren.</p> <hr/> <p>Hinweis Die Migration der physischen Netzwerkkarten, die Sie in diesem Feld hinzufügen, hängt davon ab, wie Sie Migration nur von PNIC, Netzwerkzuordnungen für die Installation und Netzwerkzuordnungen für die Deinstallation konfigurieren.</p> <hr/> <ul style="list-style-type: none"> ■ Um eine verwendete physische Netzwerkkarte (z. B. nach einem standardmäßigen vSwitch oder vSphere-Distributed Switch) ohne eine verbundene VMkernel-Zuordnung zu migrieren, stellen Sie sicher, dass Migration nur von PNIC aktiviert ist. Andernfalls bleibt der Transportknotenstatus Teilweise erfolgreich, und die Fabric-Knoten-LCP-Konnektivität kann nicht hergestellt werden. ■ Um eine verwendete physische Netzwerkkarte mit einer verbundenen VMkernel-Netzwerkzuordnung zu migrieren, deaktivieren Sie Migration nur von PNIC und konfigurieren Sie die VMkernel-Netzwerkzuordnung. ■ Um eine freie physische Netzwerkkarte zu migrieren, aktivieren Sie Migration nur von PNIC. <hr/>

Option	Beschreibung
Migration nur von PNIC	<p>Vor dem Festlegen dieses Felds berücksichtigen Sie die folgenden Punkte:</p> <ul style="list-style-type: none"> ■ Bringen Sie in Erfahrung, ob die definierte physische Netzwerkkarte eine verwendete oder eine freie Netzwerkkarte ist. ■ Bestimmen Sie, ob VMkernel-Schnittstellen eines Hosts zusammen mit physischen Netzwerkkarten migriert werden müssen. <p>Legen Sie das Feld fest:</p> <ul style="list-style-type: none"> ■ Aktivieren Sie Migration nur von PNIC, wenn Sie nur physische Netzwerkkarten von einem VSS- oder DVS-Switch zu einem N-VDS-Switch migrieren möchten. ■ Deaktivieren Sie Migration nur von PNIC, wenn Sie eine verwendete physische Netzwerkkarte und dessen zugeordnete VMkernel-Schnittstellenzuordnung migrieren möchten. Eine freie oder physische Netzwerkkarte ist an den N-VDS-Switch angehängt, wenn eine Migrationszuordnung für die VMkernel-Schnittstelle angegeben ist. <p>Auf einem Host mit mehreren Host-Switches:</p> <ul style="list-style-type: none"> ■ Wenn alle Host-Switches nur PNICs migrieren sollen, können Sie PNICs in einem einzigen Vorgang migrieren. ■ Wenn einige Hosts-Switches VMkernel-Schnittstellen migrieren sollen und die verbleibenden Host-Switches nur PNICs migrieren sollen: <ol style="list-style-type: none"> 1 Migrieren Sie im ersten-Vorgang nur PNICs. 2 Migrieren Sie im zweiten Vorgang VMkernel-Schnittstellen. Stellen Sie sicher, dass Migration nur von PNIC deaktiviert ist. <p>Sowohl die Migration nur von PNIC als auch die VMkernel-Schnittstellenmigration werden nicht gleichzeitig über mehrere Hosts hinweg unterstützt.</p> <hr/> <p>Hinweis Um die Netzwerkkarte eines Verwaltungsnetzwerks zu migrieren, konfigurieren Sie dessen zugeordnete VMkernel-Netzwerk-Zuordnung und lassen Sie Migration nur von PNIC deaktiviert. Wenn Sie nur die Management-Netzwerkkarte migrieren, verliert der Host die Verbindung.</p> <hr/> <p>Weitere Informationen finden Sie unter VMkernel-Migration auf einen N-VDS-Switch.</p>

Option	Beschreibung
Netzwerkzuordnungen für die Installation	<p>Um VMkernels während der Installation zum N-VDS-Switch zu migrieren, ordnen Sie VMkernels einem vorhandenen logischen Switch zu. Der NSX Manager migriert den VMkernel zum zugeordneten logischen Switch auf N-VDS.</p> <p>Vorsicht Stellen Sie sicher, dass die Management-Netzwerkkarte und die Verwaltungs-VMkernel-Schnittstelle auf einen logischen Switch migriert werden, der mit demselben VLAN verbunden ist, mit dem die Management-Netzwerkkarte vor der Migration verbunden war. Wenn vmnic <n> und VMkernel <n> auf ein anderes VLAN migriert werden, dann wird die Verbindung zum Host unterbrochen.</p> <p>Vorsicht Stellen Sie bei angehefteten physischen Netzwerkkarten sicher, dass die Host-Switch-Zuordnung einer physischen Netzwerkkarte zu einer VMkernel-Schnittstelle mit der Konfiguration aus dem Transportknotenprofil übereinstimmt. Im Rahmen des Validierungsverfahrens überprüft NSX-T Data Center die Zuordnung, und wenn die Validierung bestanden wird, ist die Migration von VMkernel-Schnittstellen zu einem N-VDS-Switch erfolgreich. Gleichzeitig ist es erforderlich, die Netzwerkzuordnung für Deinstallation zu konfigurieren, da NSX-T Data Center die Zuordnungskonfiguration des Host-Switch nicht speichert, nachdem die VMkernel-Schnittstellen zum N-VDS-Switch migriert wurden. Wenn die Zuordnung nicht konfiguriert ist, kann die Verbindung zu Diensten wie vSAN verloren gehen, nachdem die Migration wieder zurück zum VSS- oder VDS-Switch durchgeführt wurde.</p> <p>Weitere Informationen finden Sie unter VMkernel-Migration auf einen N-VDS-Switch.</p>
Netzwerkzuordnungen für die Deinstallation	<p>Um die Migration des VMkernels während der Deinstallation wiederherzustellen, ordnen Sie VMkernels zu Portgruppen auf VSS oder DVS zu, sodass NSX Manager weiß, zu welcher Portgruppe der VMkernel auf dem VSS oder DVS wieder zurückmigriert werden muss. Stellen Sie bei einem DVS-Switch sicher, dass die Portgruppe den Typ <code>Flüchtig</code> aufweist.</p> <p>Vorsicht Stellen Sie bei angehefteten physischen Netzwerkkarten sicher, dass die Transportknotenprofil-Zuordnung einer physischen Netzwerkkarte zu einer VMkernel-Schnittstelle mit der Konfiguration aus dem Host-Switch übereinstimmt. Es ist erforderlich, die Netzwerkzuordnung für Deinstallation zu konfigurieren, da NSX-T Data Center die Zuordnungskonfiguration des Host-Switch nicht speichert, nachdem die VMkernel-Schnittstellen zum N-VDS-Switch migriert wurden. Wenn die Zuordnung nicht konfiguriert ist, kann die Verbindung zu Diensten wie vSAN verloren gehen, nachdem die Migration wieder zurück zum VSS- oder VDS-Switch durchgeführt wurde.</p> <p>Weitere Informationen finden Sie unter VMkernel-Migration auf einen N-VDS-Switch.</p>

- 7 Geben Sie die N-VDS-Details für den erweiterten Datenpfad ein. Mehrere N-VDS-Switches können auf einem einzelnen Host konfiguriert werden.

Option	Beschreibung
N-VDS-Name	Muss mit dem N-VDS-Namen der Transportzone identisch sein, zu der dieser Knoten gehört.
IP-Zuweisung	<p>Wählen Sie DHCP verwenden, IP-Pool verwenden oder Liste statischer IPs verwenden.</p> <p>Wenn Sie Liste statischer IPs verwenden auswählen, müssen Sie eine Liste mit durch Komma getrennten IP-Adressen, ein Gateway und eine Subnetzmaske angeben.</p>
IP-Pool	Wenn Sie IP-Pool verwenden für eine IP-Zuweisung ausgewählt haben, geben Sie den Namen des IP-Pools an.
Physische Netzwerkkarten	<p>Fügen Sie physische Netzwerkkarten zum Transportknoten hinzu. Sie können den standardmäßigen Uplink verwenden oder einen vorhandenen Uplink aus dem Dropdown-Menü zuweisen.</p> <p>Klicken Sie auf PNIC hinzufügen, um zusätzliche physische Netzwerkkarten zum Transportknoten zu konfigurieren.</p> <p>Hinweis Die Migration der physischen Netzwerkkarten, die Sie in diesem Feld hinzufügen, hängt davon ab, wie Sie Migration nur von PNIC, Netzwerkzuordnungen für die Installation und Netzwerkzuordnungen für die Deinstallation konfigurieren.</p> <ul style="list-style-type: none"> ■ Um eine verwendete physische Netzwerkkarte (z. B. nach einem standardmäßigen vSwitch oder vSphere-Distributed Switch) ohne eine verbundene VMkernel-Zuordnung zu migrieren, stellen Sie sicher, dass Migration nur von PNIC aktiviert ist. Andernfalls bleibt der Transportknotenstatus Teilweise erfolgreich, und die Fabric-Knoten-LCP-Konnektivität kann nicht hergestellt werden. ■ Um eine verwendete physische Netzwerkkarte mit einer verbundenen VMkernel-Netzwerkzuordnung zu migrieren, deaktivieren Sie Migration nur von PNIC und konfigurieren Sie die VMkernel-Netzwerkzuordnung. ■ Um eine freie physische Netzwerkkarte zu migrieren, aktivieren Sie Migration nur von PNIC.
Uplink	Wählen Sie ein Uplink-Profil im Dropdown-Menü aus.

Option	Beschreibung
CPU-Konfiguration	<p>Wählen Sie im Dropdown-Menü „NUMA-Knotenindex“ denjenigen NUMA-Knoten, den Sie einem N-VDS-Switch zuweisen möchten. Der erste auf dem Knoten vorhandene NUMA-Knoten wird mit dem Wert 0 dargestellt.</p> <p>Sie können die Anzahl der NUMA-Knoten auf Ihrem Host herausfinden, indem Sie den Befehl <code>esxcli hardware memory get</code> ausführen.</p> <p>Hinweis Wenn Sie die Anzahl der NUMA-Knoten ändern möchten, die eine Affinität zu einem N-VDS-Switch haben, können Sie den NUMA-Knotenindexwert aktualisieren.</p>
	<p>Wählen Sie im Dropdown-Menü „Lcore pro NUMA-Knoten“ die Anzahl der logischen Kerne aus, die vom erweiterten Datenpfad verwendet werden müssen. Die maximale Anzahl der logischen Kerne, die auf dem NUMA-Knoten angelegt werden können, können Sie durch Ausführen des Befehls <code>esxcli network ens maxLcores get</code> ermitteln.</p> <p>Hinweis Wenn Sie die vorhandenen NUMA-Knoten und logischen Kerne vollständig ausschöpfen, kann ein neuer Switch, der dem Transportknoten hinzugefügt wurde, nicht für den ENS-Verkehr aktiviert werden.</p>

8 Geben Sie bei einem vorkonfigurierten N-VDS die folgenden Details an:

Option	Beschreibung
Externe N-VDS-ID	Muss mit dem N-VDS-Namen der Transportzone identisch sein, zu der dieser Knoten gehört.
VTEP	Name des virtuellen Tunnel-Endpoints.

9 Überprüfen Sie den Verbindungsstatus auf der Seite **Host-Transportknoten**.

Nach dem Hinzufügen des Hosts oder Bare-Metal-Servers als Transportknoten ändert sich die Verbindung zu NSX Manager nach 3-4 Minuten „Aktiv“.

10 Alternativ können Sie den Verbindungsstatus mit CLI-Befehlen anzeigen.

- ◆ Geben Sie für ESXi den Befehl `esxcli network ip connection list | grep 1234` ein.

```
# esxcli network ip connection list | grep 1234
tcp    0    0 192.168.210.53:20514 192.168.110.34:1234 ESTABLISHED 1000144459 newreno
netcpa
```

- ◆ Geben Sie für KVM den Befehl `netstat -anp --tcp | grep 1234` ein.

```
user@host:~$ netstat -anp --tcp | grep 1234
tcp    0    0 192.168.210.54:57794 192.168.110.34:1234 ESTABLISHED -
```


- 11 Stellen Sie sicher, dass die NSX-T Data Center-Module auf Ihrem Host oder dem Bare-Metal-Server installiert sind.

Nachdem ein Host oder Bare-Metal-Server zur NSX-T Data Center-Fabric hinzugefügt wurde, wird eine Sammlung von NSX-T Data Center-Modulen auf dem Host oder Bare-Metal-Server installiert.

Die Module auf unterschiedlichen Hosts werden wie folgt zu Paketen zusammengestellt:

- KVM unter RHEL oder CentOS – RPM-Dateien
- KVM unter Ubuntu – DEB-Dateien
- Geben Sie unter ESXi den Befehl `esxcli software vib list | grep nsx` ein.

Das Datum ist der Tag, an dem die Installation durchgeführt wurde.

- Geben Sie unter RHEL oder CentOS den Befehl `yum list installed` oder `rpm -qa` ein.
- Geben Sie unter Ubuntu den Befehl `dpkg --get-selections` ein.

- 12 (Optional) Ändern Sie die Abrufintervalle bestimmter Prozesse, wenn Sie über mindestens 500 Hypervisoren verfügen.

Im NSX Manager treten möglicherweise eine hohe CPU-Nutzung und Performance-Probleme auf, wenn mehr als 500 Hypervisoren vorhanden sind.

- a Kopieren Sie mit dem NSX-T Data Center-CLI-Befehl `copy file` oder der API `POST /api/v1/node/file-store/<file-name>?action=copy_to_remote_file` das Skript `aggsvc_change_intervals.py` auf einen Host.
- b Führen Sie das Skript aus, das sich im Dateispeicher von NSX-T Data Center befindet.

```
python aggsvc_change_intervals.py -m '<NSX ManagerIPAddress>' -u 'admin' -p '<password>' -i 900
```

- c (Optional) Setzen Sie die Abrufintervalle auf ihre Standardwerte zurück.

```
python aggsvc_change_intervals.py -m '<NSX ManagerIPAddress>' -u 'admin' -p '<password>' -r
```

Ergebnisse

Hinweis Wenn Sie für einen durch NSX-T Data Center erstellten N-VDS nach dem Erstellen des Transportknotens die Konfiguration (z. B. die IP-Zuweisung zum Tunnel-Endpoint) ändern möchten, müssen Sie diese Änderung über die NSX Manager-GUI vornehmen, und nicht über die Befehlszeilenschnittstelle (CLI) auf dem Host.

Nächste Schritte

Migrieren Sie Netzwerkschnittstellen von einem vSphere-Standard-Switch zu einem N-VDS. Siehe [VMkernel-Migration auf einen N-VDS-Switch](#).

Konfigurieren eines verwalteten Host-Transportknotens

Wenn Sie einen vCenter Server haben, können Sie die Installation und die Erstellung von Transportknoten auf allen NSX-T Data Center-Hosts automatisieren, anstatt eine manuelle Konfiguration vorzunehmen.

Wenn der Transportknoten bereits konfiguriert ist, ist die automatisierte Transportknotenerstellung für diesen Knoten nicht anwendbar.

Voraussetzungen

- Stellen Sie sicher, dass alle Hosts auf dem vCenter Server eingeschaltet sind.
- Stellen Sie sicher, dass die Systemanforderungen erfüllt sind. Siehe [Systemvoraussetzungen](#).
- Stellen Sie sicher, dass eine Transportzone verfügbar ist. Siehe [Erstellen von Transportzonen](#).
- Stellen Sie sicher, dass ein Transportknotenprofil konfiguriert ist. Siehe [Hinzufügen eines Transportknotenprofils](#).

Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.

- 2 Wählen Sie **System > Fabric > Knoten > Host-Transportknoten** aus.

- 3 Wählen Sie im Dropdown-Menü „Verwaltet von“ einen vorhandenen vCenter Server aus.

Auf der Seite sind die verfügbaren vSphere-Cluster bzw. ESXi-Hosts aus dem ausgewählten vCenter Server aufgeführt. Möglicherweise müssen Sie einen Cluster erweitern, um die ESXi-Hosts anzuzeigen.

- 4 Wählen Sie einen einzelnen Host in der Liste aus und klicken Sie auf **NSX konfigurieren**.

Das Dialogfeld „NSX konfigurieren“ wird geöffnet.

- a Überprüfen Sie den Hostnamen im Bereich „Hostdetails“. Optional können Sie eine Beschreibung hinzufügen.
- b Klicken Sie auf **Weiter**, um zum Bereich **NSX konfigurieren** zu wechseln.
- c Wählen Sie die verfügbaren Transportzonen aus und klicken Sie auf die Schaltfläche **>**, um die Transportzonen in das Transportknotenprofil aufzunehmen.

- 5 Überprüfen Sie den Hostnamen im Bereich „Hostdetails“ und klicken Sie auf **Weiter**.

Optional können Sie eine Beschreibung hinzufügen.

- 6 Wählen Sie im Bereich **NSX konfigurieren** die gewünschten Transportzonen aus.

Sie können mehr als eine Transportzone auswählen.

- 7 (Optional) Zeigen Sie den ESXi-Verbindungsstatus an.

```
# esxcli network ip connection list | grep 1235
tcp    0    0  192.168.210.53:20514  192.168.110.34:1234  ESTABLISHED  1000144459  newreno  netcpa
```

- 8 Stellen Sie auf der Seite mit Host-Transportknoten sicher, dass der NSX Manager-Konnektivitätsstatus von Hosts im Cluster „Aktiv“ ist und der Konfigurationszustand von NSX-T Data Center „Erfolgreich“ ist.

Sie können auch sehen, dass die Transportzone auf die Hosts im Cluster angewendet wird.

- 9 (Optional) Entfernen Sie eine NSX-T Data Center-Installation und einen Transportknoten von einem Host in der Transportzone.

- a Wählen Sie einen oder mehrere Hosts aus und klicken Sie auf **Aktionen > NSX entfernen**.

Die Deinstallation dauert bis zu drei Minuten. Durch die Deinstallation von NSX-T Data Center wird die Transportknotenkonfiguration für Hosts getrennt und der Host wird von der/den Transportzone(n) und vom N-VDS-Switch getrennt. Jeder neue Host, der dem vCenter Server-Cluster hinzugefügt wird, wird erst dann automatisch konfiguriert, wenn das Transportknotenprofil erneut auf den Cluster angewendet wird.

- 10 (Optional) Entfernen Sie einen Transportknoten aus der Transportzone.

- a Wählen Sie einen einzelnen Transportknoten aus und klicken Sie auf **Aktionen > Aus Transportzone entfernen**.

Nächste Schritte

Erstellen Sie einen logischen Switch und weisen Sie ihm logische Ports zu. Informationen finden Sie im Abschnitt „Erweiterte Switching“ in *Administratorhandbuch für NSX-T Data Center*.

Konfigurieren von ESXi-Hosttransportknoten mit Linkaggregation (LAG)

Dieses Verfahren beschreibt, wie Sie ein Uplink-Profil mit Konfiguration einer Linkaggregationsgruppe erstellen, und wie Sie einen ESXi-Hosttransportknoten für die Verwendung dieses Uplink-Profiles konfigurieren.

Voraussetzungen

- Machen Sie sich mit den Schritten zum Erstellen eines Uplink-Profiles vertraut. Siehe [Erstellen eines Uplink-Profiles](#).
- Machen Sie sich mit den Schritten zum Erstellen eines Hosttransportknotens vertraut. Siehe [Erstellen eines eigenständigen Hosts oder Bare-Metal-Server-Transportknotens](#).

Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **System > Fabric > Profile > Uplink-Profile > Hinzufügen** aus.
- 3 Geben Sie einen Namen und optional eine Beschreibung ein.
Geben Sie z. B. den Namen **Uplink-Profil1** ein.

- 4 Klicken Sie unter **LAG** auf **Hinzufügen**, um eine Linkaggregationsgruppe hinzufügen.
Beispielsweise fügen Sie eine **lag1** genannte LAG mit 2 Uplinks hinzu.
- 5 Wählen Sie unter **Teamings** die Option **Standard-Teaming** aus.
- 6 Geben Sie im Feld **Aktive Uplinks** den Namen der in Schritt 4 hinzugefügten LAG ein. In diesem Beispiel ist der Name **lag1**.
- 7 Geben Sie einen Wert für den **Transport-VLAN** und die **MTU** ein.
- 8 Klicken Sie unten im Dialogfeld auf **Hinzufügen**.
- 9 Klicken Sie unter **Teamings** auf **Hinzufügen**, um einen Eintrag für die Linkaggregation hinzuzufügen.
- 10 Wählen Sie **Fabric > Knoten > Host-Transportknoten > Hinzufügen** aus.
- 11 Geben Sie auf der Registerkarte **Hostdetails** die IP-Adresse, den Betriebssystemnamen, die Administratoranmeldedaten und den SHA-256-Fingerabdruck des Hosts ein.
- 12 Wählen Sie auf der Registerkarte **N-VDS** das in Schritt 3 erstellte Uplink-Profil **uplink-profile1** aus.
- 13 Im Feld **Physische Netzwerkkarten** spiegelt die Dropdown-Liste der physischen Netzwerkkarten und Uplinks die neuen Netzwerkkarten und das Uplink-Profil wider. Insbesondere werden die Uplinks **lag1-0** und **lag1-1** in Übereinstimmung mit der in Schritt 4 erstellten LAG **lag1** angezeigt. Wählen Sie eine physische Netzwerkkarte für **lag1-0** und eine physische Netzwerkkarte für **lag1-1** aus.
- 14 Geben Sie die Daten in die übrigen Felder ein.

Vollständig reduzierte NSX-T-Bereitstellung mit vSphere-Cluster

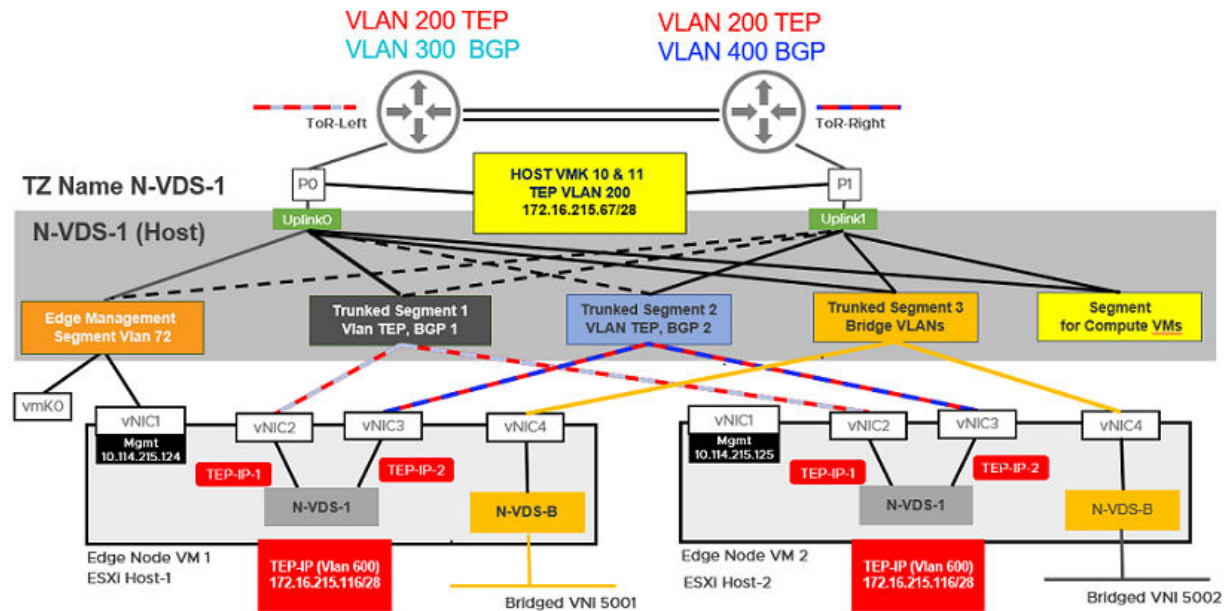
Konfigurieren Sie NSX Manager, Host-Transportknoten zum Ausführen von Arbeitslast-VMs und NSX Edge-VMs auf einem einzelnen Cluster. Jeder Host im Cluster stellt zwei physische NICs bereit, die für NSX-T konfiguriert sind.

Wichtig Stellen Sie ab NSX-T-Version 2.4.2 oder 2.5 die vollständig reduzierte vSphere-Einzel-Cluster-Topologie bereit.

Die bei dieser Vorgehensweise referenzierte Topologie verwendet Folgendes:

- Mit den Hosts im Cluster konfiguriertes vSAN.
- Mindestens zwei physische Netzwerkkarten pro Host.
- vMotion- und Management-VMkernel-Schnittstellen.

Abbildung 8-3. Topologie: einzelner N-VDS-Switch, der die Host-Kommunikation mit NSX Edge und Gast-VMs verwaltet



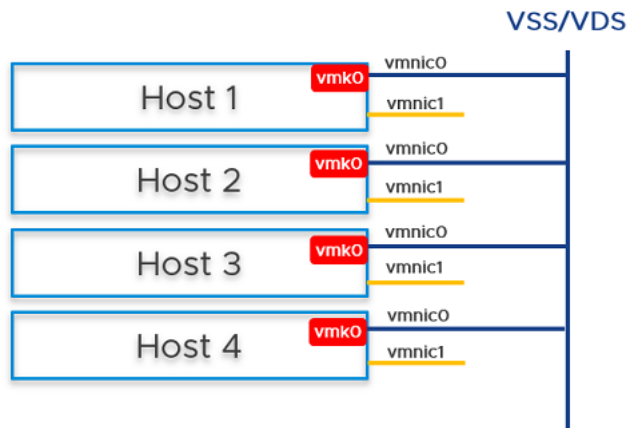
Hinweis Selbst wenn der Host über vier physische NICs verfügt, können nur zwei davon für die Bereitstellung der vollständig reduzierten Topologie verwendet werden. Diese Vorgehensweise verweist auf physische NICs auf dem Host als vmnic0 und vmnic1.

Voraussetzungen

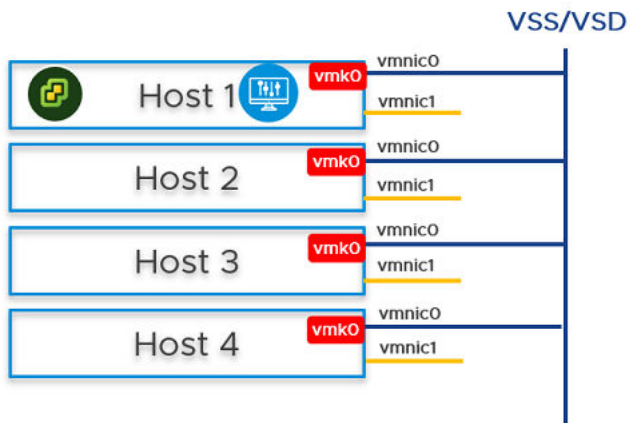
- Alle Hosts müssen Teil eines vSphere-Clusters sein.
- Auf jedem Host sind zwei physische Netzwerkkarten aktiviert.
- Registrieren Sie alle Hosts bei einem vCenter Server.
- Überprüfen Sie auf dem vCenter Server, ob freigegebener Speicher für die Verwendung durch die Hosts verfügbar ist.
- Stellen Sie sicher, dass die VLAN-ID, die für den TEP und den Host-TEP verwendet wird, sich von der des NSX Edge unterscheidet.

Verfahren

- 1 Bereiten Sie vier ESXi-Hosts mit vmnic0 auf vSS oder vDS vor, vmnic1 ist frei.



- 2 Installieren Sie vCenter Server auf Host 1, konfigurieren Sie eine vSS/vDS-Portgruppe und installieren Sie NSX Manager auf der Portgruppe, die auf dem Host erstellt wurde.

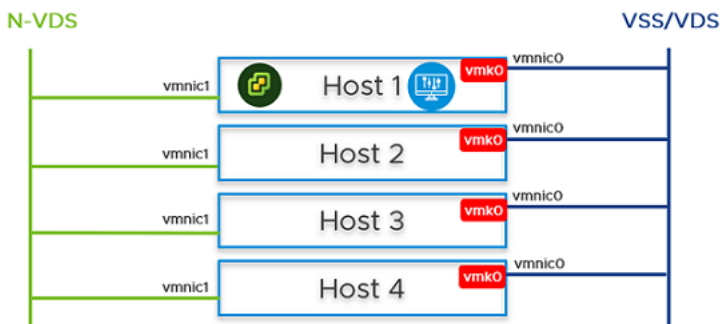


- 3 Bereiten Sie ESXi-Hosts 1, 2, 3 und 4 als Transportknoten vor.
 - a Erstellen Sie VLAN-Transportzonen mit einer benannten Teaming-Richtlinie. Siehe [Erstellen von Transportzonen](#).
 - b Erstellen Sie einen IP-Pool oder DHCP für Tunnel-Endpoint-IP-Adressen für die Hosts. Siehe [Erstellen eines IP-Pools für Tunnel-Endpoint-IP-Adressen](#).
 - c Erstellen Sie einen IP-Pool oder DHCP für Tunnel-Endpoint-IP-Adressen für den Edge-Knoten. Siehe [Erstellen eines IP-Pools für Tunnel-Endpoint-IP-Adressen](#).
 - d Erstellen Sie ein Uplink-Profil mit einer benannten Teaming-Richtlinie. Siehe [Erstellen eines Uplink-Profiles](#).

- e Konfigurieren Sie Hosts als Transportknoten, indem Sie das Transportknotenprofil anwenden. In diesem Schritt migriert das Transportknotenprofil nur vmnic1, die nicht verwendete physische NIC, zum N-VDS-Switch. Nachdem das Transportknotenprofil auf die Cluster-Hosts angewendet wurde, wird der N-VDS-Switch erstellt und vmnic1 ist mit dem N-VDS-Switch verbunden. Siehe [Hinzufügen eines Transportknotenprofils](#).

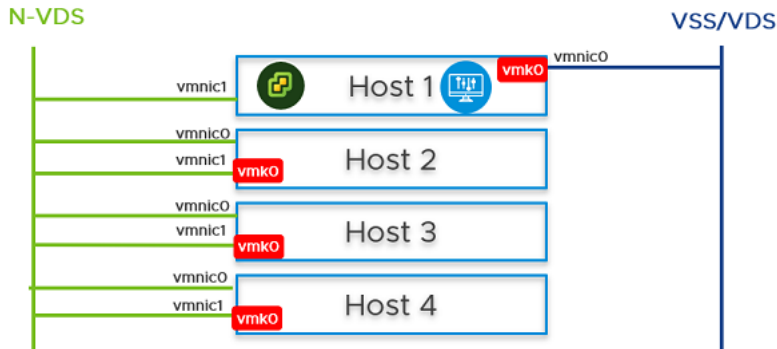
Transportknotenprofil bearbeiten – TNP-host ?

N-VDS-Name *	vds-1	▼
Zugeordnete Transportzonen	tz	
NIOC-Profil *	nsx-default-nioc-hostswitch-profile	▼
	ODER Neues NIOC-Profil erstellen	
Uplink-Profil *	hostnodeprofile	▼
	ODER Neues Uplink-Profil erstellen	
LLDP-Profil *	LLDP [Send Packet Enabled]	▼
IP-Zuweisung *	IP-Pool verwenden	▼
IP-Pool *	ippoolhostnode	▼
	ODER Neuen IP-Pool erstellen und verwenden	
Physische Netzwerkkarten	vmnic1	activeuplinkhost ▼
		PNIC hinzufügen
Migration nur von PNIC	<input checked="" type="checkbox"/> Ja	
Aktivieren Sie diese Option, wenn auf dem für die Migration ausgewählten PNIC keine VMKs existieren		
Netzwerkzuordnungen für die Installation	Zuordnung hinzufügen	
Netzwerkzuordnungen für die Deinstallation	Zuordnung hinzufügen	



vmnic1 auf allen Hosts werden dem N-VDS-Switch hinzugefügt. Von den beiden physischen Netzwerkkarten wird also eine auf den N-VDS-Switch migriert. Die vmnic0-Schnittstelle ist weiterhin mit dem vSS- oder vDS-Switch verbunden, wodurch sichergestellt wird, dass die Konnektivität mit dem Host verfügbar ist.

- 4 Erstellen Sie auf der NSX Manager-Benutzeroberfläche VLAN-gestützte Segmente für NSX Manager, vCenter Server, NSX Edge. Stellen Sie sicher, dass für jedes der VLAN-gestützten Segmente die richtige Teaming-Richtlinie ausgewählt ist.
- 5 Auf Host 2, Host 3 und Host 4 müssen Sie den vmk0-Adapter und vmnic0 zusammen von VSS/VDS auf den N-VDS-Switch migrieren. Aktualisieren Sie die NSX-T-Konfiguration auf jedem Host. Stellen Sie bei der Migration sicher, dass vmnic0 einem aktiven Uplink zugeordnet ist.



Netzwerkzuordnungen für die Installation

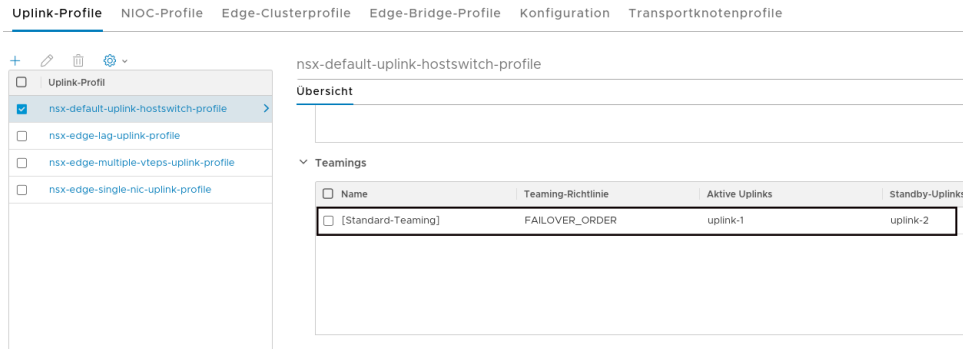
Die Host-Konnektivität geht möglicherweise verloren, wenn vmnic0 und vmk0 migriert werden. Das Ändern des logischen Switches für den statusbehafteten Host (eigenständig oder geclustert) wirkt sich nicht aus und der Vorgang schlägt fehl.

+ HINZUFÜGEN LÖSCHEN

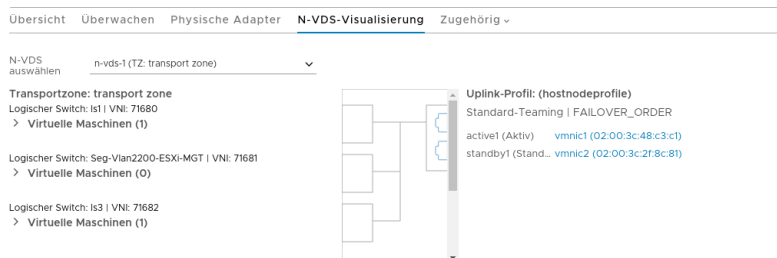
<input type="checkbox"/> VMkernel-Adapter *	VLAN-Segment/logischer Switch *
<input type="checkbox"/> vmk0	Seg-Vlan2200-ESXi-MGT

ABBRECHEN

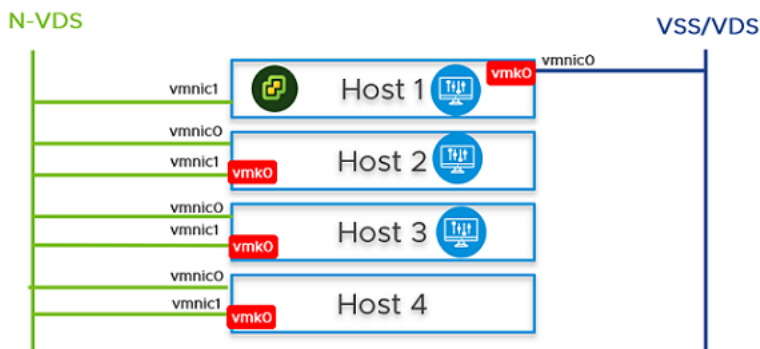
HINZUFÜGEN



- 6 Wechseln Sie in vCenter Server zu Host 2, Host 3 und Host 4. Stellen Sie sicher, dass der vmk0-Adapter mit der physischen vmnic0-NIC auf dem N-VDS verbunden und erreichbar ist.
- 7 Wechseln Sie in der NSX Manager-Benutzeroberfläche zu Host 2, Host 3 und Host 4. Überprüfen Sie, ob sich beide pNICs auf dem N-VDS-Switch befinden.



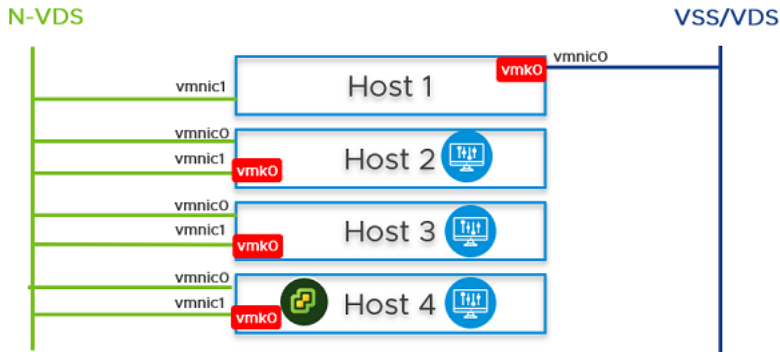
- 8 Erstellen Sie ein logisches Segment und fügen Sie NSX Manager an das logische Segment an. Warten Sie etwa 10 Minuten, bis sich der Cluster formiert hat, und stellen Sie sicher, dass dies richtig durchgeführt wurde.
- 9 Installieren Sie NSX Manager auf Host 2 und Host 3 über die NSX Manager-Benutzeroberfläche.



- 10 Schalten Sie den ersten NSX Manager-Knoten aus. Warten Sie etwa 10 Minuten.

- 11 Verbinden Sie NSX Manager und vCenter Server erneut mit dem zuvor erstellten logischen Switch. Schalten Sie NSX Manager auf Host 4 ein. Warten Sie etwa 10 Minuten, um sicherzustellen, dass sich der Cluster in einem stabilen Zustand befindet. Wenn der erste NSX Manager ausgeschaltet ist, führen Sie eine kalte vMotion aus, um NSX Manager und vCenter Server von Host 1 auf Host 4 zu migrieren.

Informationen zu vMotion-Einschränkungen finden Sie unter <https://kb.vmware.com/s/article/56991>.



- 12 Wechseln Sie auf der NSX Manager-Benutzeroberfläche zu Host 1, migrieren Sie vmk0 und vmnic0 zusammen von VSS zum N-VDS-Switch.
- 13 Stellen Sie im Feld **Netzwerkuordnung für Installation** sicher, dass der vmk0-Adapter dem logischen Management-Segment auf dem N-VDS-Switch zugeordnet ist.

NSX konfigurieren

1 Hostdetails
2 NSX konfigurieren

IP-Zuweisung
Liste statischer IPs verwenden

Liste statischer IPs
172.16.228.36

Gateway
172.16.228.33

Subnetzmaske
255.255.255.240

Physische Netzwerkkarten

vmnic1
uplink-1

vmnic2
uplink-2

Migration nur von PNIC
Nein

Aktivieren Sie diese Option, wenn auf dem für die Migration ausgewählten PNIC keine VMs existieren

Netzwerkuordnungen für die Installation
Zuordnung hinzufügen

Netzwerkuordnungen für die Deinstallation
Zuordnung hinzufügen

ABBRECHEN
ZURÜCK
FERTIGSTELLEN

Netzwerkzuordnungen für die Installation



Die Host-Konnektivität geht möglicherweise verloren, wenn vmnic0 und vmk0 migriert werden.
Das Ändern des logischen Switches für den statusbehafteten Host (eigenständig oder geclustert) wirkt sich nicht aus und der Vorgang schlägt fehl.

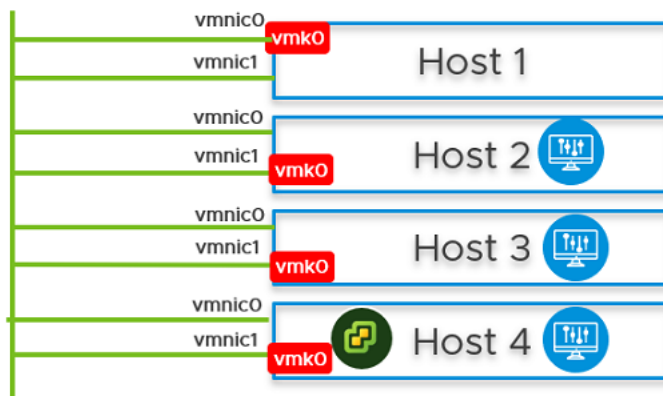
+ HINZUFÜGEN LÖSCHEN

<input type="checkbox"/> VMkernel-Adapter *	VLAN-Segment/logischer Switch *
<input type="checkbox"/> vmk0	Seg-Vlan2200-ESXi-MGT

ABBRECHEN

HINZUFÜGEN

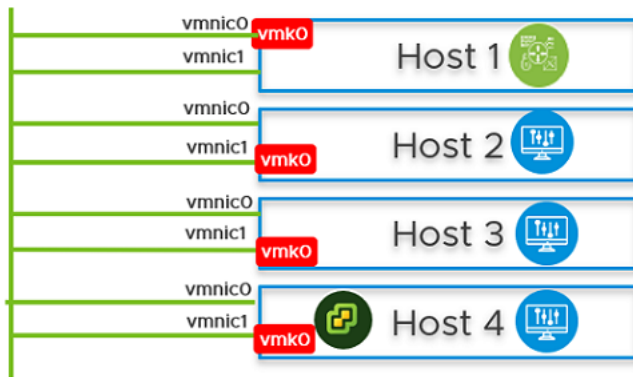
N-VDS



- 14 Installieren Sie auf Host 1 die NSX Edge-VM über die Benutzeroberfläche von NSX Manager.

Siehe [Erstellen eines NSX Edge-Transportknotens](#).

N-VDS



- 15 Verbinden Sie die NSX Edge-VM mit der Management Plane.
Siehe [Verbinden von NSX Edge mit der Managementebene](#).
- 16 Um die Konnektivität für den Nord-Süd-Datenverkehr einzurichten, konfigurieren Sie die NSX Edge-VM mit einem externen Router.
- 17 Stellen Sie sicher, dass die Nord-Süd-Datenverkehrskonnektivität zwischen der NSX Edge-VM und dem externen Router besteht.
- 18 Richten Sie die BFD-Konnektivität zwischen NSX Manager und der NSX Edge-VM ein und überprüfen Sie sie.
- 19 Im Falle eines Stromausfalls, bei dem der gesamte Cluster neu gestartet wird, kann die NSX-T-Verwaltungskomponente möglicherweise nicht mehr mit dem N-VDS kommunizieren. Um dieses Szenario zu vermeiden, führen Sie die folgenden Schritte aus:

Vorsicht Jeder API-Befehl, der falsch ausgeführt wird, führt zu einem Verlust der Konnektivität mit NSX Manager.

Hinweis In einer einzelnen Clusterkonfiguration werden Verwaltungskomponenten auf einem N-VDS-Switch als VMs gehostet. Der N-VDS-Port, mit dem die Verwaltungskomponente standardmäßig eine Verbindung herstellt, wird aus Sicherheitsgründen als blockierter Port initialisiert. Im Falle eines Stromausfalls, bei dem alle vier Hosts (empfohlene Mindestanzahl) neu gestartet werden müssen, ist der Standardzustand für den Neustart des Verwaltungs-VM-Ports „blockiert“. Um zirkuläre Abhängigkeiten zu vermeiden, wird empfohlen, einen Port auf dem N-VDS im Zustand „nicht blockiert“ zu erstellen. Ein nicht blockierter Port stellt sicher, dass die NSX-T-Verwaltungskomponente bei einem Neustart des Clusters mit dem N-VDS kommunizieren kann, um wieder eine normale Funktion zu gewährleisten.

Am Ende der Teilaufgabe übernimmt der Migrationsbefehl Folgendes:

- UUID des Host-Knotens, auf dem sich der NSX Manager befindet.
- UUID der NSX Manager-VM und migriert sie auf den statischen logischen Port, der sich in einem nicht blockierten Zustand befindet.

Wenn alle Hosts aus- oder eingeschaltet sind oder eine NSX Manager-VM auf einen anderen Host verschoben wird, wird sie, nachdem NSX Manager wiederhergestellt wurde, an einen nicht blockierten Port angehängt. Dadurch wird der Verlust der Konnektivität mit der Verwaltungskomponente von NSX-T verhindert.

- a Wechseln Sie zu **Netzwerk und Sicherheit – Erweitert** → **Switching** und wählen Sie das MGMT-VLAN-Segment aus. Suchen und kopieren Sie die UUID auf der Registerkarte **Übersicht**. Die in diesem Beispiel verwendete UUID ist `c3fd8e1b-5b89-478e-abb5-d55603f04452`.
- b Um logische Ports zu erstellen, die im Status **UNBLOCKED_VLAN** initialisiert werden, erstellen Sie vier JSON-Dateien, drei für NSX Manager und eine für vCenter Server Appliance (VCSA). Ersetzen Sie den Wert für `logical_switch_id` durch die UUID des zuvor erstellten Segments MGMT-VLAN-Segment.

```
mgrhost.json
{
  "admin_state": "UP",
  "attachment": {
    "attachment_type": "VIF",
    "id": "nsxmgr-port-147"
  },
  "display_name": "NSX Manager Node 147 Port",
  "init_state": "UNBLOCKED_VLAN",
  "logical_switch_id": "c3fd8e1b-5b89-478e-abb5-d55603f04452"
}
```

- c Erstellen Sie den logischen Port für den Manager mit einem API-Client oder mithilfe des curl-Befehls.

```
root@nsx-mgr-147:/var/CollapsedCluster# curl -X POST -k -u
'<username>:<password>' -H 'Content-Type:application/json' -d @mgr.json https://
localhost/api/v1/logical-ports
{
  "logical_switch_id" : "c3fd8e1b-5b89-478e-abb5-d55603f04452",
  "attachment" : {
    "attachment_type" : "VIF",
    "id" : "nsxmgr-port-147"
  },
  "admin_state" : "UP",
  "address_bindings" : [ ],
  "switching_profile_ids" : [ {
    "key" : "SwitchSecuritySwitchingProfile",
    "value" : "fbc4fb17-83d9-4b53-a286-ccdf04301888"
  }, {
    "key" : "SpoofGuardSwitchingProfile",
    "value" : "fad98876-d7ff-11e4-b9d6-1681e6b88ec1"
  }, {
    "key" : "IpDiscoverySwitchingProfile",
    "value" : "0c403bc9-7773-4680-a5cc-847ed0f9f52e"
  }, {
    "key" : "MacManagementSwitchingProfile",
    "value" : "1e7101c8-cfef-415a-9c8c-ce3d8dd078fb"
  }, {
    "key" : "PortMirroringSwitchingProfile",
    "value" : "93b4b7e8-f116-415d-a50c-3364611b5d09"
  }, {
    "key" : "QosSwitchingProfile",
    "value" : "f313290b-eba8-4262-bd93-fab5026e9495"
  } ],
  "init_state" : "UNBLOCKED_VLAN",
  "ignore_address_bindings" : [ ],
  "resource_type" : "LogicalPort",
  "id" : "02e0d76f-83fa-4839-a525-855b47ecb647",
  "display_name" : "NSX Manager Node 147 Port",
  "_create_user" : "admin",
  "_create_time" : 1574716624192,
  "_last_modified_user" : "admin",
  "_last_modified_time" : 1574716624192,
  "_system_owned" : false,
  "_protection" : "NOT_PROTECTED",
  "_revision" : 0
}
```

Switches **Ports** Switching-Profile

+ HINZUFÜGEN BEARBEITEN LÖSCHEN AKTIONEN >						
Suchen						
<input type="checkbox"/>	Logischer Port	ID	Administrativer	Betriebsstatus	Switching-Profile	Logischer Switch
<input type="checkbox"/>	1356a49d-dc33-42be-9e83-4c6...	1356...d0ee	Aktiv	Aktiv	nsx-default-switch-security-non...	LR:80fb...2662
<input type="checkbox"/>	61d5708b-a4ff-4954-b217-8338...	61d5...b43a	Aktiv	Aktiv	nsx-default-switch-security-non...	LR:42ac...ad24
<input type="checkbox"/>	NSX Manager Node 147 Port	58ad...a1cb	Aktiv	Inaktiv	nsx-default-switch-security-vif...	VM:nsx-mgr-147
<input type="checkbox"/>	ubuntu12.04.1-2G-LAMP/ubuntu1...	3fb2...f698	Aktiv	Aktiv	nsx-default-switch-security-vif...	VM:vm1
<input type="checkbox"/>	vmnic@n-vds-1@94b323e6-1ee...	2021...4d76	Aktiv	Aktiv	nsx-default-switch-security-vif...	VIF:abf2...0495
<input type="checkbox"/>	worker/worker.vmx@94b323e6...	50b7...9b4c	Aktiv	Aktiv	nsx-default-switch-security-vif...	VM:vm3

- d Verschieben Sie NSX Manager in den statisch erstellten logischen Port.
- e Um die NSX Manager-VM-Instanz-ID zu kopieren, wechseln Sie zu „Netzwerk und Sicherheit – Erweitert“ → „Bestand“ → „Virtuelle Maschinen“. Wählen Sie die NSX Manager-VM aus. Suchen und kopieren Sie die ID auf der Registerkarte **Übersicht**. Die in diesem Beispiel verwendete ID ist `5028d756-d36f-719e-3db5-7ae24aa1d6f3`.
- f Um die Host-ID zu finden, auf der NSX Manager installiert ist, wechseln Sie zu **System -> Fabric -> Knoten -> Host-Transportknoten**. Wählen Sie den Host aus und klicken Sie auf die Registerkarte **Übersicht**. Suchen und kopieren Sie die Host-ID. Die in diesem Beispiel verwendete ID ist `11161331-11f8-45c7-8747-34e7218b687f`.
- g Migrieren Sie NSX Manager vom VM-Netzwerk zum zuvor erstellten logischen Port im MGMT-VLAN-Segment. Der Wert `vnuc_migration_dest` ist die Anhang-ID der Ports, die zuvor für NSX Manager erstellt wurden.

```
root@nsx-mgr-147:/var/CollapsedCluster# curl -k -X PUT -u 'username:<password>' -H
'Content-Type:application/json' -d @mgrhost.json
'https://localhost/api/v1/transport-nodes/11161331-11f8-45c7-8747-34e7218b687f?
vnuc_migration_dest=nsxmgr-port-147'
```

- h Stellen Sie in der NSX Manager-Benutzeroberfläche sicher, dass die statisch erstellte logische Portgruppe aktiv ist.

Switches Ports Switching-Profile							
+ HINZUFÜGEN		BEARBEITEN	LÖSCHEN	AKTIONEN		Suchen	
<input type="checkbox"/>	Logischer Port	ID	Administrativer	Betriebsstatus	Switching-Profil	Anhang	Logischer Switch
<input type="checkbox"/>	1356a49d-dc33-42be-9e83-4c6...	1356...d0ee	Aktiv	Aktiv	nsx-default-switch-security-non...	LR:80fb...2662	Is3
<input type="checkbox"/>	61d5708b-a4ff-4954-b217-8338...	61d5...b43a	Aktiv	Aktiv	nsx-default-switch-security-non...	LR:42ac...ad24	Is1
<input type="checkbox"/>	NSX Manager Node 147 Port	58ad...a1cb	Aktiv	Aktiv	nsx-default-switch-security-vif...	VM.nsx-mgr-147	Is1
<input type="checkbox"/>	ubuntu12.04.1-2G-LAMP/ubuntu1...	3fb2...f698	Aktiv	Aktiv	nsx-default-switch-security-vif...	VM.vml	Is1
<input type="checkbox"/>	vmnic@n-vds-1@94b323e6-1ee...	2021...4d76	Aktiv	Aktiv	nsx-default-switch-security-vif...	VIF.abf2...0495	Seg-Vlan2200-ESXi-MGT
<input type="checkbox"/>	worker/worker.vmx@94b323e6...	50b7...9b4c	Aktiv	Aktiv	nsx-default-switch-security-vif...	VM.vml3	Is3

- i Wiederholen Sie die vorherigen Schritte für jeden NSX Manager im Cluster.

Überprüfen des Transportknotenstatus

Stellen Sie sicher, dass die Transportknotenerstellung ordnungsgemäß funktioniert.

Nach dem Erstellen eines Hosttransportknotens wird der N-VDS auf dem Host installiert.

Verfahren

- 1 Melden Sie sich beim NSX-T Data Center an.
- 2 Navigieren Sie zur Seite „Transportknoten“ und zeigen Sie den N-VDS-Status an.

- 3 Alternativ können Sie zum Anzeigen des N-VDS unter ESXi den Befehl `esxcli network ip interface list` ausführen.

Unter ESXi sollte die Befehlsausgabe eine vmk-Schnittstelle (z. B. vmk10) mit einem VDS-Namen enthalten, der mit dem Namen übereinstimmt, den Sie beim Konfigurieren der Transportzone und des Transportknotens verwendet haben.

```
# esxcli network ip interface list
...

vmk10
  Name: vmk10
  MAC Address: 00:50:56:64:63:4c
  Enabled: true
  Portset: DvsPortset-1
  Portgroup: N/A
  Netstack Instance: vxlan
  VDS Name: overlay-hostswitch
  VDS UUID: 18 ae 54 04 2c 6f 46 21-b8 ae ef ff 01 0c aa c2
  VDS Port: 10
  VDS Connection: 10
  Opaque Network ID: N/A
  Opaque Network Type: N/A
  External ID: N/A
  MTU: 1600
  TSO MSS: 65535
  Port ID: 67108895
...
```

Wenn Sie den vSphere Client verwenden, können Sie den installierten N-VDS auf der Benutzeroberfläche anzeigen, indem Sie **Konfiguration > Netzwerkadapter** für den Host auswählen.

Der KVM-Befehl zum Prüfen der N-VDS-Installation lautet `ovs-vsctl show`. Beachten Sie, dass bei KVM der N-VDS-Name `nsx-switch.0` lautet. Dieser stimmt nicht mit dem Namen in der Transportknotenkonfiguration überein. Dies ist so vorgesehen.

```
# ovs-vsctl show
...
  Bridge "nsx-switch.0"
    Port "nsx-uplink.0"
      Interface "em2"
    Port "nsx-vtep0.0"
      tag: 0
      Interface "nsx-vtep0.0"
        type: internal
    Port "nsx-switch.0"
```



```
Interface "nsx-switch.0"
  type: internal
  ovs_version: "2.4.1.3340774"
```

4 Prüfen Sie die zugewiesene Tunnel-Endpoint-Adresse des Transportknotens.

Die Schnittstelle vmk10 erhält eine IP-Adresse vom NSX-T Data Center-IP-Pool oder von DHCP (wie hier gezeigt):

```
# esxcli network ip interface ipv4 get
Name      IPv4 Address      IPv4 Netmask      IPv4 Broadcast    Address Type      DHCP DNS
-----
vmk0      192.168.210.53    255.255.255.0     192.168.210.255   STATIC            false
vmk1      10.20.20.53       255.255.255.0     10.20.20.255      STATIC            false
vmk10    192.168.250.3     255.255.255.0     192.168.250.255   STATIC            false
```

In KVM können Sie den Tunnel-Endpoint und die IP-Zuteilung mit dem Befehl `ifconfig` prüfen.

```
# ifconfig
...
nsx-vtep0.0 Link encap:Ethernet HWaddr ba:30:ae:aa:26:53
            inet addr:192.168.250.4 Bcast:192.168.250.255 Mask:255.255.255.0
            ...
```

5 Überprüfen Sie die API auf die Statusinformationen des Transportknotens.

Verwenden Sie den API-Aufruf `GET https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/state`. Beispiel:

```
{
  "state": "success",
  "host_switch_states": [
    {
      "endpoints": [
        {
          "default_gateway": "192.168.250.1",
          "device_name": "vmk10",
          "ip": "192.168.250.104",
          "subnet_mask": "255.255.255.0",
          "label": 69633
        }
      ],
      "transport_zone_ids": [
        "efd7f38f-c5da-437d-af03-ac598f82a9ec"
      ],
      "host_switch_name": "overlay-hostswitch",
      "host_switch_id": "18 ae 54 04 2c 6f 46 21-b8 ae ef ff 01 0c aa c2"
    }
  ]
}
```

```

    }
  ],
  "transport_node_id": "2d030569-5769-4a13-8918-0c309c63fdb9"
}

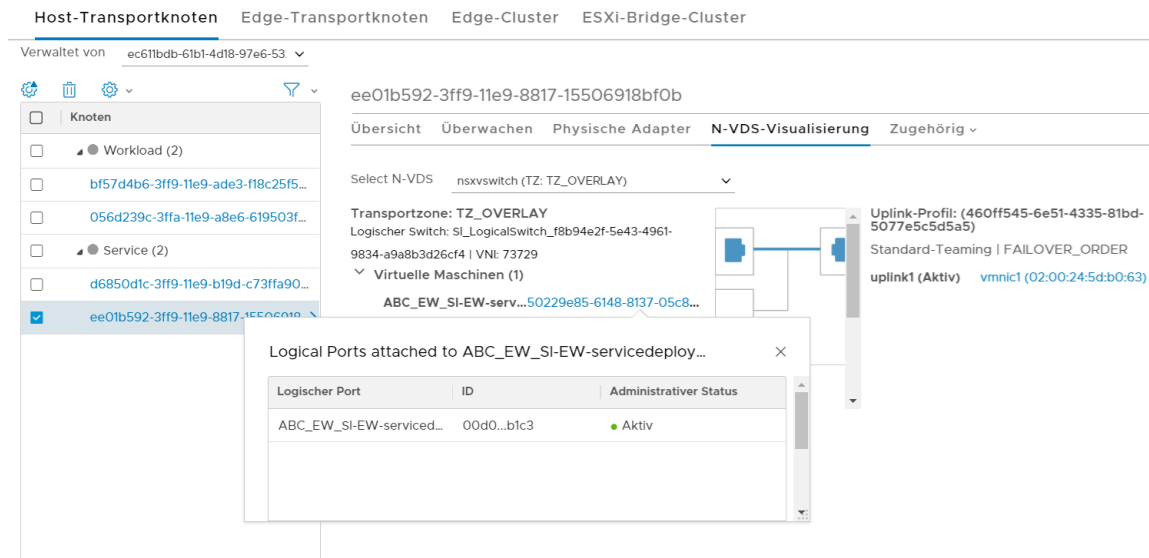
```

Optische Darstellung eines N-VDS

Sie erhalten eine detaillierte Ansicht eines N-VDS auf einer einzelnen Hostebene. NSX-T Data Center stellt eine optische Darstellung des Konnektivitätsstatus zwischen dem Uplink des N-VDS und den VMs bereit, die einer Transportzone zugeordnet sind. Zu den optisch dargestellten Objekten gehören die Teaming-Richtlinie - Uplink und physische Netzwerkkarte, die Konnektivität für VMs bereitstellen. Bei dem anderen optisch dargestellten Satz von Objekten handelt es sich um VMs, zugeordnete logische Ports und Switches und den Status der VMs. Die optische Darstellung erleichtert die Verwaltung des N-VDS.

Hinweis Nur ESXi-Hosts unterstützen die Darstellung von N-VDS-Objekten.

Abbildung 8-4. N-VDS-Visualisierung



Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **System > Fabric > Knoten > Host-Transportknoten** aus.
- 3 Wählen Sie im Feld „Verwaltet von“ die Option **Eigenständiger Host** oder *Compute Manager* aus.
- 4 Wählen Sie den Host aus.
- 5 Klicken Sie auf die Registerkarte **Darstellung des N-VDS**.
- 6 Wählen Sie einen N-VDS aus.

NSX-T stellt mit VMs verbundene Uplink-Profilen, virtuellen Maschinen zugeordnete logische Ports und mit einer Transportzone verknüpfte logische Switches optisch dar.

- 7 Wählen Sie eine VM aus, um die mit einer VM verbundenen Uplink-Profil und den logischen Port anzuzeigen, mit denen eine VM verknüpft ist.

NSX-T stellt die Konnektivität zwischen einer VM und ein Uplink-Profil optisch dar.

- 8 Wählen Sie das Uplink-Profil aus, um die VMs anzuzeigen, die mit einem Uplink-Profil verknüpft sind.
- 9 Zum Anzeigen logischer Ports, die mit einer VM verknüpft sind, erweitern Sie den logischen Switch und klicken auf die VM.

Die Details des logischen Ports werden in einem separaten Dialogfeld angezeigt.

Hinweis Der Administratorstatus eines logischen Ports wird im Dialogfeld angezeigt. Wenn der Betriebsstatus nicht verfügbar ist, wird er im Dialogfeld nicht angezeigt.

Manuelle Installation von NSX-T Data Center-Kernel-Modulen

Anstatt die NSX-T Data Center-Benutzeroberflächenoptionen **Fabric > Knoten > Hosts > Hinzufügen** oder die API POST `/api/v1/fabric/nodes` zu verwenden, können Sie NSX-T Data Center-Kernel-Module auch manuell mit der Hypervisor-Befehlszeile installieren.

Hinweis Sie können auf einem Bare-Metal-Server keine NSX-T Data Center-Kernel-Module installieren.

Manuelles Installieren von NSX-T Data Center-Kernel-Modulen auf ESXi-Hypervisoren

Um Hosts auf die Teilnahme an NSX-T Data Center vorzubereiten, müssen Sie NSX-T Data Center-Kernel-Module auf ESXi-Hosts installieren. So können Sie die NSX-T Data Center-Steuerungskomponenten- und Managementebenen-Fabric erstellen. In VIB-Dateien gepackte NSX-T Data Center-Kernel-Module werden im Hypervisor-Kernel ausgeführt und stellen Dienste wie Distributed Routing, verteilte Firewall und Bridging-Funktionen bereit.

Sie können die NSX-T Data Center-VIBs manuell herunterladen und zum Host-Image hinzufügen. Die Download-Pfade für jede Version von NSX-T Data Center variieren. Rufen Sie die jeweiligen VIBs stets über die NSX-T Data Center-Download-Seite ab.

Verfahren

- 1 Melden Sie sich als Root oder als Benutzer mit Administratorrechten beim Host an.
- 2 Gehen Sie zum Verzeichnis `/tmp`.

```
[root@host:~]: cd /tmp
```

- 3 Laden Sie die Datei `nsx-lcp` herunter und kopieren Sie sie in das Verzeichnis `/tmp`.
- 4 Führen Sie den Installationsbefehl aus.

```
[root@host:/tmp]: esxcli software vib install -d /tmp/nsx-lcp-<release>.zip
```

Installation Result

Message: Operation finished successfully.

Reboot Required: false

VIBs Installed: VMware_bootbank_nsx-aggsservice_<release>, VMware_bootbank_nsx-da_<release>, VMware_bootbank_nsx-esx-datapath_<release>, VMware_bootbank_nsx-exporter_<release>, VMware_bootbank_nsx-host_<release>, VMware_bootbank_nsx-lldp_<release>, VMware_bootbank_nsx-mpa_<release>, VMware_bootbank_nsx-netcpa_<release>, VMware_bootbank_nsx-python-protobuf_<release>, VMware_bootbank_nsx-sfhc_<release>, VMware_bootbank_nsxa_<release>, VMware_bootbank_nsxcli_<release>

VIBs Removed:

VIBs Skipped:

Je nachdem, was bereits auf dem Host installiert wurde, können einige VIBs installiert, andere entfernt und wieder andere übersprungen werden. Ein Neustart ist nur erforderlich, wenn in der Befehlsausgabe `Reboot Required: true` steht.

Ergebnisse

Wenn Sie einen ESXi-Host zur NSX-T Data Center-Fabric hinzufügen, werden die folgenden VIBs auf dem Host installiert.

nsx-adf	(Automatisiertes Diagnose-Framework) Erfasst und analysiert Leistungsdaten, um sowohl lokale (auf dem Host) als auch zentrale (datencenterübergreifende) Diagnosen zu Leistungsproblemen zu erstellen.
nsx-aggsservice	Stellt hostseitige Bibliotheken für den NSX-T Data Center-Zusammenfassungsdienst bereit. Der NSX-T Data Center-Zusammenfassungsdienst wird auf den Managementebenenknoten ausgeführt und ruft Laufzeitstatistiken von NSX-T Data Center-Komponenten ab.
nsx-cli-libs	Stellt die NSX-T Data Center-CLI auf Hypervisor-Hosts bereit.
nsx-common-libs	Stellen einige Hilfsklassen bereit, unter anderem AES, SHA-1, UUID und Bitmap.
nsx-context-mux	Bietet NSX Guest Introspektion-Relaisfunktionalität. Ermöglicht VMware Tools Gast-Agents das Weiterleiten von Gastkontext an interne und registrierte Partner-Appliances von Drittanbietern.
nsx-esx-datapath	Bietet NSX-T Data Center-Paket-Verarbeitungsfunktionalität auf der Data Plane.
nsx-exporter	Stellt Hostagents bereit, die Laufzeitstatistiken an den Zusammenfassungsdienst melden, der auf der Management Plane ausgeführt wird.
nsx-host	Liefert Metadaten für das VIB-Paket, das auf dem Host installiert ist.
nsx-metrics-libs	Stellt Metrik-Hilfsklassen für das Erfassen von Daemon-Metriken bereit.

nsx-mpa	Stellt Kommunikation zwischen NSX Manager und Hypervisor-Hosts bereit.
nsx-nestdb-libs	NestDB ist eine Datenbank, in der NSX-Konfigurationen im Zusammenhang mit dem Host gespeichert werden (gewünschter/ Laufzeitstatus usw.).
nsx-netcpa	Stellt Kommunikation zwischen der zentralen Control Plane und Hypervisors bereit. Erhält den logischen Netzwerkzustand von der zentralen Control Plane und programmiert diesen Zustand auf der Data Plane.
nsx-opsagent	Gibt Operations Agent-Ausführungen (Transportknoten-Realisation, Link-Layer-Discovery-Protokoll-LLDP, Traceflow, Paketerfassung usw.) an die Management Plane weiter.
nsx-platform-client	Stellt einen allgemeinen CLI-Ausführungs-Agent für die zentrale CLI und die Erfassung von Überwachungsprotokollen bereit.
nsx-profiling-libs	Bietet die Funktionalität der Profilerstellung basierend auf gpeftool, welches auch für die Daemon-Prozess-Profilerstellung verwendet wird.
nsx-proxy	Stellt den einzigen Northbound-Kontaktpunkt-Agent bereit, der mit der zentralen Control Plane und der Management Plane kommuniziert.
nsx-python-gevent	Enthält Python Gevent
nsx-python-greenlet	Enthält die Python Greenlet-Bibliothek (Drittanbieterbibliotheken).
nsx-python-logging	Enthält die Python-Protokolle.
nsx-python-protobuf	Bietet Python-Bindungen für Protokollpuffer.
nsx-rpc-libs	Diese Bibliothek bietet NSX-RPC-Funktionalität.
nsx-sfhc	Dienst-Fabric-Hostkomponente (Service Fabric Host Component; SFHC). Liefert einen Hostagenten für die Verwaltung des Lebenszyklus des Hypervisors als Fabric-Host im Bestand der Managementebene. Darüber erhalten Sie einen Kanal für Vorgänge wie NSX-T Data Center-Upgrade sowie Deinstallation und Überwachung von NSX-T Data Center-Modulen auf Hypervisors.
nsx-shared-libs	Enthält die gemeinsam genutzten NSX-Bibliotheken.
nsx-upm-libs	Bietet einheitliche Profil-Verwaltungsfunktionen für eine verminderte clientseitige Konfiguration und das Vermeiden einer doppelten Datenübertragung.
nsx-vdpi	Bietet Deep Packet Inspection-Funktionen für die verteilte Firewall für NSX-T Data Center.
nsxcli	Stellt die NSX-T Data Center-CLI auf Hypervisor-Hosts bereit.
vsipfwlib	Bietet verteilte Firewall-Funktionalität.

Zur Überprüfung können Sie die Befehle `esxcli software vib list | grep nsx` und `esxcli software vib list | grep vsipfwlib` auf dem ESXi-Host ausführen. Alternativ können Sie den Befehl `esxcli software vib list | grep <yyyy-mm-dd>` ausführen, wobei es sich beim Datum um das Installationsdatum handelt.

Nächste Schritte

Fügen Sie den Host der NSX-T Data Center-Management Plane hinzu. Siehe [Bereitstellen von NSX Manager-Knoten zur Bildung eines Cluster mithilfe der CLI](#).

Manuelles Installieren von NSX-T Data Center-Kernel-Modulen auf Ubuntu-KVM-Hypervisors

Um Hosts auf die Teilnahme an NSX-T Data Center vorzubereiten, können Sie NSX-T Data Center-Kernel-Module manuell auf Ubuntu-KVM-Hosts installieren. So können Sie die NSX-T Data Center-Steuerungskomponenten- und Managementebenen-Fabric erstellen. In DEB-Dateien gepackte NSX-T Data Center-Kernel-Module werden im Hypervisor-Kernel ausgeführt und stellen Dienste wie Distributed Routing, verteilte Firewall und Bridging-Funktionen bereit.

Sie können die NSX-T Data Center-DEBs manuell herunterladen und zum Host-Image hinzufügen. Beachten Sie, dass die Download-Pfade von Version zu Version von NSX-T Data Center variieren können. Rufen Sie die jeweiligen DEBs stets über die NSX-T Data Center-Download-Seite ab.

Voraussetzungen

- Stellen Sie sicher, dass die erforderlichen Drittanbieterpakete installiert sind. Siehe [Installieren von Drittanbieterpaketen auf einem KVM-Host](#).

Verfahren

- 1 Melden Sie sich als Benutzer mit Administratorrechten beim Host an.
- 2 (Optional) Gehen Sie zum Verzeichnis /tmp.

```
cd /tmp
```

- 3 Laden Sie die Datei nsx-lcp herunter und kopieren Sie sie in das Verzeichnis /tmp.
- 4 Dekomprimieren Sie das Paket.

```
tar -xvf nsx-lcp-<release>-ubuntu-trusty_amd64.tar.gz
```

- 5 Gehen Sie zum Paketverzeichnis.

```
cd nsx-lcp-trusty_amd64/
```

6 Installieren Sie die Pakete.

```
sudo dpkg -i *.deb
```

7 Laden Sie das OVS-Kernel-Modul erneut.

```
/etc/init.d/openvswitch-switch force-reload-kmod
```

Wenn der Hypervisor DHCP auf OVS-Schnittstellen verwendet, starten Sie die Netzwerkschnittstelle, auf der DHCP konfiguriert ist, neu. Sie können den alten Dhclient-Prozess auf der Netzwerkschnittstelle manuell anhalten und einen neuen Dhclient-Prozess auf dieser Schnittstelle starten.

8 Zur Überprüfung können Sie den Befehl `dpkg -l | grep nsx` ausführen.

```
user@host:~$ dpkg -l | grep nsx
```

ii	nsx-agent	<release>	amd64	NSX Agent
ii	nsx-aggservice	<release>	all	NSX Aggregation Service Lib
ii	nsx-cli	<release>	all	NSX CLI
ii	nsx-da	<release>	amd64	NSX Inventory Discovery Agent
ii	nsx-host	<release>	all	NSX host meta package
ii	nsx-host-node-status-reporter	<release>	amd64	NSX Host Status Reporter for
	Aggregation Service			
ii	nsx-lldp	<release>	amd64	NSX LLDP Daemon
ii	nsx-logical-exporter	<release>	amd64	NSX Logical Exporter
ii	nsx-mpa	<release>	amd64	NSX Management Plane Agent Core
ii	nsx-netcpa	<release>	amd64	NSX Netcpa
ii	nsx-sfhc	<release>	amd64	NSX Service Fabric Host
	Component			
ii	nsx-transport-node-status-reporter	<release>	amd64	NSX Transport Node Status
	Reporter			
ii	nsxa	<release>	amd64	NSX L2 Agent

Eventuelle Fehler entstehen wahrscheinlich aufgrund von unvollständigen Abhängigkeiten. Mit dem Befehl `apt-get install -f` kann versucht werden, Abhängigkeiten aufzulösen und die NSX-T Data Center-Installation zu wiederholen.

Nächste Schritte

Fügen Sie den Host der NSX-T Data Center-Managementebene hinzu. Siehe [Bereitstellen von NSX Manager-Knoten zur Bildung eines Cluster mithilfe der CLI](#).

Manuelles Installieren von NSX-T Data Center-Kernel-Modulen auf RHEL- und CentOS-KVM-Hypervisors

Um Hosts auf die Einbindung in NSX-T Data Center vorzubereiten, können Sie NSX-T Data Center-Kernel-Module manuell auf RHEL- oder CentOS-KVM-Hosts installieren.

So können Sie die NSX-T Data Center-Steuerungskomponenten- und Managementebenen-Fabric erstellen. In RPM-Dateien gepackte NSX-T Data Center-Kernel-Module werden im Hypervisor-Kernel ausgeführt und stellen Dienste wie Distributed Routing, verteilte Firewall und Bridging-Funktionen bereit.

Sie können die NSX-T Data Center-RPMs manuell herunterladen und zum Host-Image hinzufügen. Beachten Sie, dass die Download-Pfade von Version zu Version von NSX-T Data Center variieren können. Rufen Sie die jeweiligen RPMs stets über die NSX-T Data Center-Download-Seite ab.

Voraussetzungen

Erreichbarkeit eines RHEL- oder CentOS-Repositorys.

Verfahren

- 1 Melden Sie sich als Administrator beim Host an.
- 2 Laden Sie die Datei nsx-lcp herunter und kopieren Sie sie in das Verzeichnis /tmp.
- 3 Dekomprimieren Sie das Paket.

```
tar -zxvf nsx-lcp-<release>-rhel7.4_x86_64.tar.gz
```

- 4 Gehen Sie zum Paketverzeichnis.

```
cd nsx-lcp-rhel74_x86_64/
```

- 5 Installieren Sie die Pakete.

```
sudo yum install *.rpm
```

Beim Ausführen des Yum-Installationsbefehls werden sämtliche NSX-T Data Center-Abhängigkeiten aufgelöst, vorausgesetzt, dass die RHEL- oder CentOS-Hosts auf ihre jeweiligen Repositorys zugreifen können.

- 6 Laden Sie das OVS-Kernel-Modul erneut.

```
/etc/init.d/openvswitch force-reload-kmod
```

Wenn der Hypervisor DHCP auf OVS-Schnittstellen verwendet, starten Sie die Netzwerkschnittstelle, auf der DHCP konfiguriert ist, neu. Sie können den alten Dhclient-Prozess auf der Netzwerkschnittstelle manuell anhalten und einen neuen Dhclient-Prozess auf dieser Schnittstelle starten.

- 7 Zur Überprüfung können Sie den Befehl `rpm -qa | egrep 'nsx|openvswitch|nicira'` ausführen.

Die installierten Pakete in der Ausgabe müssen mit den Paketen im Verzeichnis „nsx-rhel74“ oder „nsx-centos74“ übereinstimmen.

Nächste Schritte

Fügen Sie den Host der NSX-T Data Center-Managementebene hinzu. Siehe [Bereitstellen von NSX Manager-Knoten zur Bildung eines Cluster mithilfe der CLI](#).

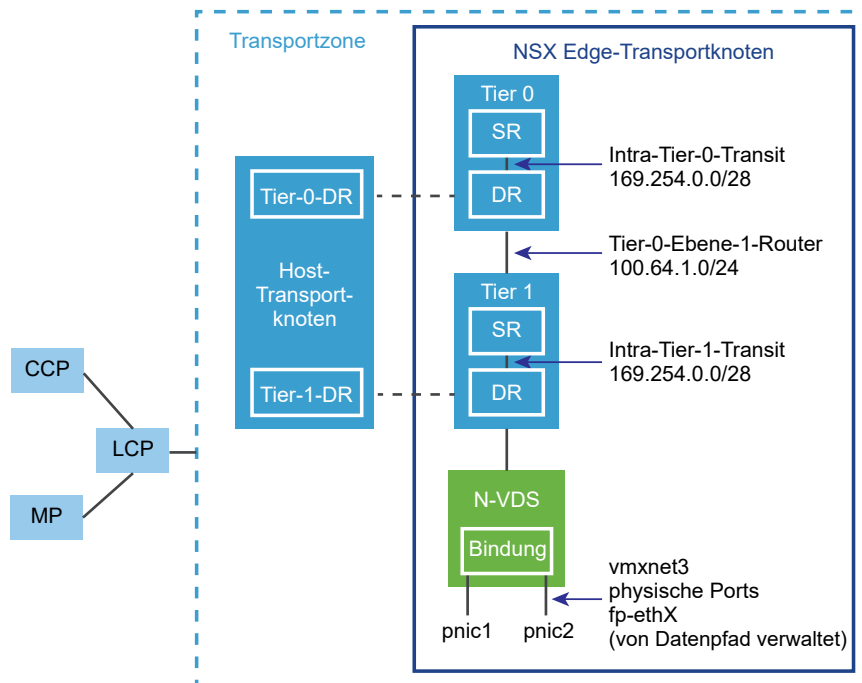
NSX Edge-Netzwerkeinrichtung

NSX Edge kann über ISO, OVA/OVF oder PXE-Start installiert werden. Stellen Sie unabhängig von der Installationsmethode sicher, dass das Hostnetzwerk vor der Installation von NSX Edge vorbereitet ist.

Übersicht über NSX Edge in einer Transportzone

Die Übersicht über NSX-T Data Center zeigt zwei Transportknoten in einer Transportzone. Ein Transportknoten ist ein Host. Der andere ist ein NSX Edge.

Abbildung 8-5. Übersicht über NSX Edge



Beim ersten Bereitstellen eines NSX Edge können Sie ihn sich als leeren Container vorstellen. Der NSX Edge führt erst dann Aktionen aus, wenn Sie logische Router erstellen. NSX Edge liefert die Rechenleistung für logische Ebene-0- und Ebene-1-Router. Jeder logische Router enthält einen Dienstrouter (Service Router; SR) und einen verteilten Router (Distributed Router; DR). Ein Router wird als verteilt bezeichnet, wenn er auf allen Transportknoten in derselben Transportzone repliziert wird. In

dieser Abbildung enthält der Hosttransportknoten dieselben DRs, die auch in den Ebene-0- und Ebene-1-Routern enthalten sind. Ein Dienstrouter ist erforderlich, wenn der logische Router für die Ausführung von Diensten, wie NAT, konfiguriert wird. Alle logischen Ebene-0-Router weisen einen Dienstrouter auf. Ein Ebene-1-Router kann bei Bedarf je nach Ihren Designüberlegungen einen Dienstrouter enthalten.

Standardmäßig verwenden die Links zwischen dem SR und dem DR das Subnetz 169.254.0.0/28. Diese routerübergreifenden Transit-Links werden automatisch erstellt, wenn Sie einen logischen Ebene-0- oder Ebene-1-Router bereitstellen. Sie müssen die Linkkonfiguration nur dann ändern, wenn das Subnetz 169.254.0.0/28 bereits in Ihrer Bereitstellung verwendet wird. Auf einem logischen Ebene-1-Router ist der SR nur vorhanden, wenn Sie beim Erstellen des logischen Ebene-1-Routers einen NSX Edge-Cluster auswählen.

Der Standard-Adressbereich für die Verbindungen von Ebene-0 zu Ebene-1 lautet 100.64.0.0/10. Jede Tier-0-zu-Tier-1-Peer-Verbindung erhält ein /31-Subnetz innerhalb des 100.64.0.0/10-Adressraums. Dieser Link wird automatisch erstellt, wenn Sie einen Ebene-1-Router erstellen und mit einem Ebene-0-Router verbinden. Sie müssen die Schnittstellen auf diesem Link nur dann ändern, wenn das Subnetz 100.64.0.0/10 bereits in Ihrer Bereitstellung verwendet wird.

Jede NSX-T Data Center-Bereitstellung verfügt über einen Managementebenen-Cluster (Management Plane Cluster; MP) und einen Steuerungskomponentencluster (Control Plane Cluster; CCP). Der MP und der CCP geben Konfigurationen an die lokale Steuerungskomponente (LCP) jeder Transportzone weiter. Wenn ein Host oder NSX Edge der Managementebene beitrifft, baut der Managementebenen-Agent (MPA) Konnektivität mit dem Host oder NSX Edge auf und der Host oder NSX Edge wird zu einem NSX-T Data Center-Fabric-Knoten. Wenn der Fabric-Knoten dann als Transportknoten hinzugefügt wird, wird LCP-Konnektivität mit dem Host oder NSX Edge aufgebaut.

Zuletzt zeigt die Abbildung ein Beispiel für zwei physikalische Netzwerkkarten (pNIC1 und pNIC2), die zur Gewährleistung hoher Verfügbarkeit verbunden sind. Der Datenpfad verwaltet die physischen Netzwerkkarten. Sie können entweder als VLAN-Uplinks zu einem externen Netzwerk oder als Tunnel-Endpoint-Links zu internen von NSX-T Data Center verwalteten VM-Netzwerken dienen.

Es wird empfohlen, mindestens zwei physische Links auf jeder NSX Edge zuzuteilen, die als virtuelle Maschine bereitgestellt wird. Optional können Sie die Portgruppen auf demselben pNIC mit unterschiedlichen VLAN-IDs überlappen. Der erste gefundene Netzwerkklink wird für das Management verwendet. Beispiel: Bei einer NSX Edge-VM kann zuerst der Link vnic1 gefunden werden. Bei einer Bare-Metal-Installation kann der erste gefundene Link eth0 oder em0 sein. Die restlichen Links werden für die Uplinks und Tunnel verwendet. Einer davon könnte z. B. für einen Tunnel-Endpoint für von NSX-T Data Center verwaltete VMs dienen. Der andere könnte als TOR-Uplink von NSX Edge zu extern verwendet werden.

Sie können die Informationen zum physischen Link der NSX Edge anzeigen, indem Sie sich bei der CLI als Administrator anmelden und die Befehle `get interfaces` und `get physical-ports` ausführen. In der API können Sie den API-Aufruf `GET fabric/nodes/<edge-node-id>/network/interfaces` verwenden. Im nächsten Abschnitt werden physische Links ausführlicher erläutert.

Unabhängig davon, ob Sie NSX Edge als VM-Appliance oder in einer Bare-Metal-Bereitstellung installieren, stehen Ihnen mehrere Optionen für die Netzwerkkonfiguration zur Verfügung, je nach Ihrer Bereitstellung.

Transportzonen und N-VDS

Um das NSX Edge-Networking zu verstehen, müssen Sie sich etwas mit Transportzonen und N-VDS auskennen. Transportzonen steuern die Reichweite von Layer 2-Netzwerken in NSX-T Data Center. N-VDS ist ein Software-Switch, der auf einem Transportknoten erstellt wird. Ein N-VDS dient dazu, logische Router-Uplinks und -Downlinks an physische Netzwerkkarten (NICs) zu binden. Für jede Transportzone, zu der ein NSX Edge gehört, wird ein einzelner N-VDS auf dem NSX Edge installiert.

Es gibt zwei Arten von Transportzonen:

- Overlay für internes NSX-T Data Center-Tunneling zwischen Transportknoten.
- VLAN für Uplinks außerhalb von NSX-T Data Center.

Ein NSX Edge kann zu gar keinen oder zahlreichen VLAN-Transportzonen gehören. Ohne VLAN-Transportzonen kann der NSX Edge dennoch über Uplinks verfügen, da die NSX Edge-Uplinks denselben N-VDS verwenden können, der für die Overlay-Transportzone installiert wurde. Sie können dies tun, wenn Sie möchten, dass jeder NSX Edge nur einen N-VDS hat. Bei einer weiteren Designoption könnte der NSX Edge zu mehreren VLAN-Transportzonen gehören (einer für jeden Uplink).

Am häufigsten wird ein Design mit drei Transportzonen verwendet: eine Overlay- und zwei VLAN-Transportzonen für redundante Uplinks.

Um dieselbe VLAN-ID für ein Transportnetzwerk für Overlay-Datenverkehr und für anderen VLAN-Datenverkehr, beispielsweise einen VLAN-Uplink, zu verwenden, konfigurieren Sie die ID auf zwei verschiedenen N-VDS, einem für VLAN und dem anderen für Overlay.

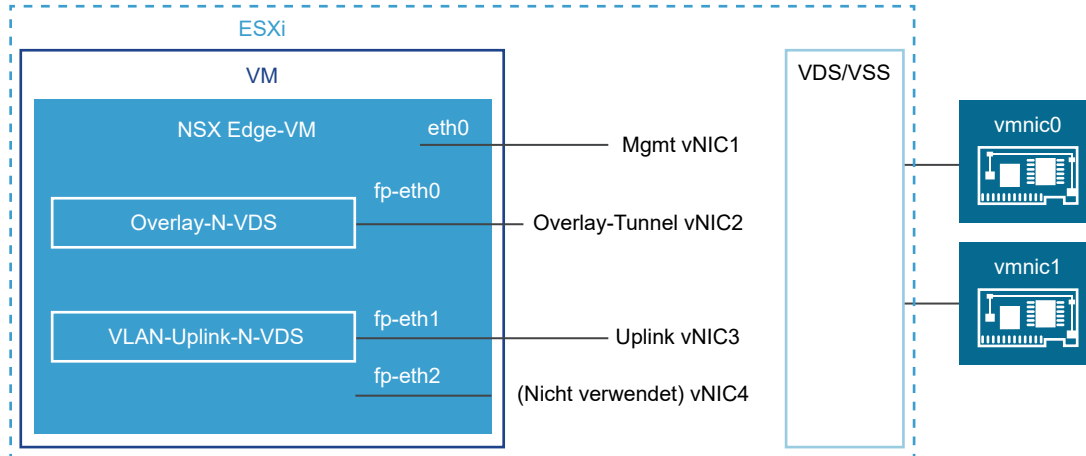
NSX Edge-Networking über virtuelle Appliance/VM

Wenn Sie NSX Edge als virtuelle Appliance oder VM installieren, werden interne Schnittstellen erstellt (mit dem Namen fp-ethX, wobei X für 0, 1, 2 und 3 steht). Diese Schnittstellen werden für Uplinks zu Top-of-Rack-(ToR-)Switches und für NSX-T Data Center-Overlay-Tunneling zugeteilt.

Beim Erstellen des NSX Edge-Transportknotens können Sie fp-ethX-Schnittstellen auswählen, die den Uplinks und dem Overlay-Tunnel zugeordnet werden. Sie können festlegen, wie die fp-ethX-Schnittstellen verwendet werden.

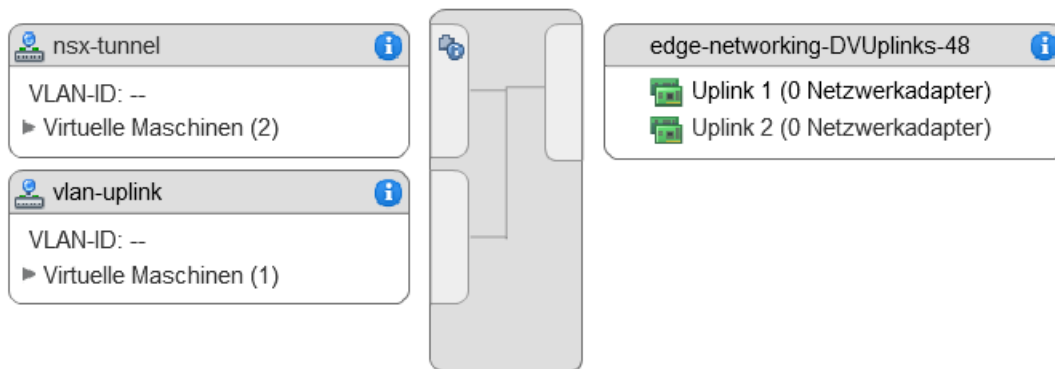
Auf dem vSphere Distributed Switch oder dem vSphere Standard Switch müssen Sie mindestens zwei vNICs zu NSX Edge zuordnen: einen für die NSX Edge-Verwaltung und einen für Uplinks und Tunnel.

In der folgenden physischen Beispieltopologie wird fp-eth0 für den NSX-T Data Center-Overlay-Tunnel verwendet. Fp-eth1 wird für den VLAN-Uplink verwendet. fp-eth2 und fp-eth3 werden nicht verwendet. vNIC1 wird dem Verwaltungsnetzwerk zugewiesen.

Abbildung 8-6. Ein Vorschlag für die Linkeinrichtung zum NSX Edge-VM-Networking

Der in dieser Abbildung gezeigte NSX Edge gehört zu zwei Transportzonen (einer Overlay- und einer VLAN-Zone) und verfügt daher über zwei N-VDS: einen für Tunnel- und einen für Uplink-Datenverkehr.

Dieser Screenshot zeigt die Portgruppen der virtuellen Maschine, den nsx-Tunnel und den VLAN-Uplink.



Bei der Bereitstellung müssen Sie die Netzwerknamen angeben, die mit den in den VM-Portgruppen konfigurierten Namen übereinstimmen. Um beispielsweise die VM-Portgruppen des Beispiels abzugleichen, können Ihre Netzwerk-Ovftool-Einstellungen wie folgt aussehen, wenn Sie das Ovftool zur Bereitstellung von NSX Edge verwenden:

```
--net:"Network 0=Mgmt" --net:"Network 1=nsx-tunnel" --net:"Network 2=vlan-uplink"
```

Das hier gezeigte Beispiel verwendet die VM-Portgruppennamen **Mgmt**, **nsx-tunnel** und **vlan-uplin**. Sie können die VM-Portgruppen beliebig benennen.

Die für NSX Edge konfigurierten Tunnel- und Uplink-VM-Portgruppen müssen nicht den VMkernel-Ports oder bestimmten IP-Adressen zugeordnet sein. Dies liegt daran, dass sie nur auf Layer 2 verwendet werden. Wenn Ihre Bereitstellung DHCP verwendet, um eine Adresse zur Verwaltungsschnittstelle zur Verfügung zu stellen, müssen Sie sicherstellen, dass dem Verwaltungsnetzwerk nur eine Netzwerkkarte zugewiesen ist.

Beachten Sie, dass die VLAN- und Tunnel-Portgruppen als Trunk-Ports konfiguriert sind. Dies ist erforderlich. Bei einem Standard-vSwitch konfigurieren Sie beispielsweise die Trunk-Ports wie folgt: **Host > Konfiguration > Networking > Networking hinzufügen > Virtuelle Maschine > VLAN-ID Alle (4095)**.

Wenn Sie einen Appliance-basierten oder VM-NSX Edge verwenden, können Sie Standard-vSwitches oder vSphere Distributed Switches verwenden.

Die NSX Edge-VM kann auf einem vorbereiteten NSX-T Data Center-Host installiert und als Transportknoten konfiguriert werden. Es gibt zwei Arten der Bereitstellung:

- Die NSX Edge-VM kann über VSS/VDS-Portgruppen bereitgestellt werden, wobei VSS/VDS separate PNIC(s) auf dem Host verbrauchen. Der Hosttransportknoten nutzt separate PNIC(s) für den auf dem Host installierten N-VDS. Der N-VDS des Hosttransportknotens koexistiert mit einem VSS oder VDS, wobei beide separate PNICs nutzen. Der Host-TEP (Tunnelendpunkt) und der NSX Edge-TEP können im selben Subnetz oder in verschiedenen Subnetzen verfügbar sein.
- Die NSX Edge-VM kann über VLAN-unterstützte logische Switches auf dem N-VDS des Host-Transportknotens bereitgestellt werden. Der Host TEP und der NSX Edge-TEP müssen sich in unterschiedlichen Subnetzen befinden.

Optional können Sie mehrere NSX Edge-Appliances/-VMs auf einem einzelnen Host installieren und dieselben Portgruppen für Management, VLAN und Tunnel-Endpoint können von allen installierten NSX Edges verwendet werden.

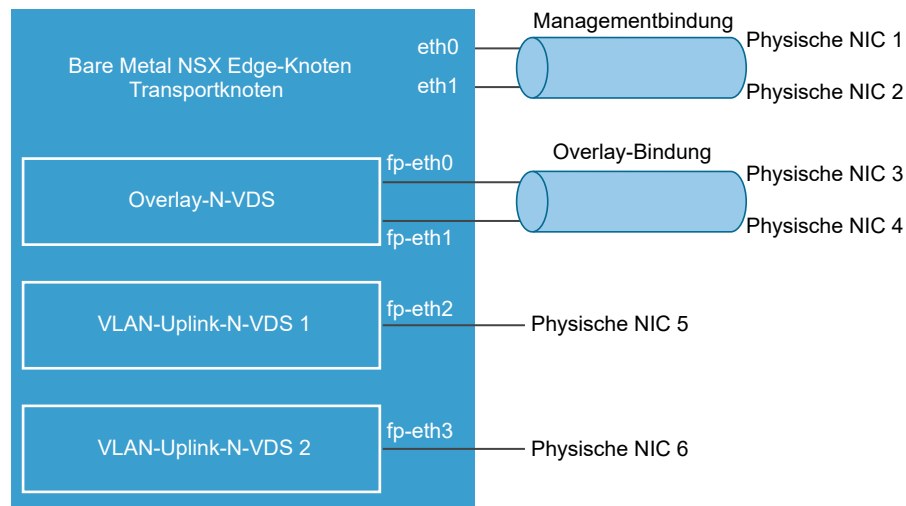
Wenn die zugrunde liegenden physischen Links eingerichtet und die VM-Portgruppen konfiguriert sind, können Sie NSX Edge installieren.

NSX Edge-Networking auf Bare-Metal-Bereitstellung

Ein Bare-Metal-NSX Edge enthält interne Schnittstellen (mit dem Namen fp-ethX, wobei X für 0, 1, 2, 3 oder 4 steht). Wie viele fp-ethX-Schnittstellen erstellt werden, hängt davon ab, wie viele physische NICs im Bare-Metal-NSX Edge vorkommen. Bis zu vier dieser Schnittstellen können für Uplinks zu Top-of-Rack(ToR)-Switches und NSX-T Data Center-Overlay-Tunneling zugeteilt werden.

Beim Erstellen des NSX Edge-Transportknotens können Sie fp-ethX-Schnittstellen auswählen, die den Uplinks und dem Overlay-Tunnel zugeordnet werden.

Sie können festlegen, wie die fp-ethX-Schnittstellen verwendet werden. In der folgenden physischen Beispieltopologie werden fp-eth0 und fp-eth1 für den NSX-T Data Center-Overlay-Tunnel verwendet. fp-eth2 und fp-eth3 werden als redundante VLAN-Uplinks zu TORs eingesetzt.

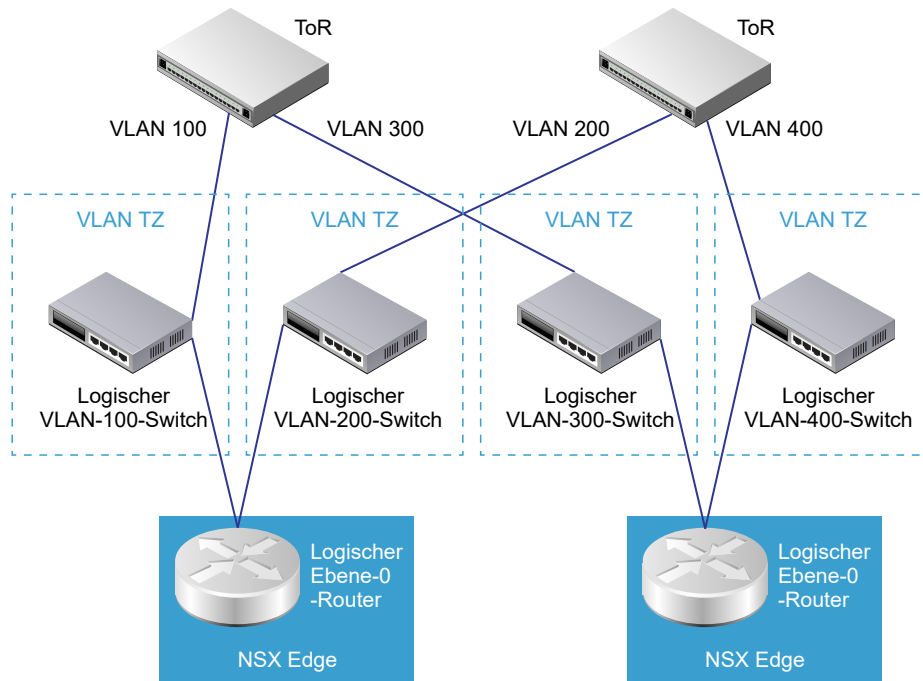
Abbildung 8-7. Ein Vorschlag für die Linkeinrichtung für Bare-Metal-NSX Edge-Networking

NSX Edge-Uplink-Redundanz

Dank NSX Edge-Uplink-Redundanz können zwei VLAN-ECMP-Uplinks (Equal-Cost-MultiPath) in der TOR-Netzwerkverbindung von NSX Edge zu extern verwendet werden.

Wenn Sie über zwei ECMP-VLAN-Uplinks verfügen, müssen für eine hohe Verfügbarkeit und eine vollständig vernetzte Konnektivität auch über zwei TOR-Switches verfügen. Jedem logischen VLAN-Switch ist eine VLAN-ID zugeordnet.

Wenn Sie einen NSX Edge zu einer VLAN-Transportzone hinzufügen, wird ein neuer N-VDS installiert. Wenn Sie beispielsweise, wie in der Abbildung gezeigt, einen NSX Edge-Knoten zu vier VLAN-Transportzonen hinzufügen, werden vier N-VDS auf dem NSX Edge installiert.

Abbildung 8-8. Ein Vorschlag für eine ECMP-VLAN-Einrichtung für NSX Edges zu TORs

Hinweis Für eine auf einem ESXi-Host mit dem vSphere Distributed Switch (vDS) anstelle von N-VDS bereitgestellte virtuelle Edge-Maschine müssen Sie wie folgt vorgehen:

- Aktivieren Sie die gefälschte Übertragung, damit DHCP funktioniert.
- Aktivieren Sie den promiskuitiven Modus für die virtuelle Edge-Maschine, um unbekannte Unicast-Pakete zu empfangen, da MAC-Lernen standardmäßig deaktiviert ist. Für vDS 6.6 oder höhere Versionen ist dies nicht notwendig, da der MAC-Lernvorgang für diese Versionen standardmäßig aktiviert ist.

Erstellen eines NSX Edge-Transportknotens

Sie können einen NSX Edge zur NSX-T Data Center-Fabric hinzufügen und mit der Konfiguration des NSX Edge als Transportknoten fortfahren.

Ein Transportknoten ist ein Knoten, der an einem NSX-T Data Center-Overlay oder NSX-T Data Center-VLAN-Networking teilnehmen kann. Jeder Knoten kann als Transportknoten dienen, wenn er einen N-VDS enthält. Solche Knoten umfassen, sind jedoch nicht beschränkt auf NSX Edges.

Ein NSX Edge kann zu einer Overlay-Transportzone und mehreren VLAN-Transportzonen gehören. Wenn eine VM Zugriff auf die Außenwelt erfordert, muss das NSX Edge zu derselben Transportzone gehören, zu der auch der logische Switch der VM gehört. Im Allgemeinen gehört das NSX Edge zu mindestens einer VLAN-Transportzone, um den Uplink-Zugriff bereitzustellen.

Hinweis Wenn Sie Transportknoten aus einer Vorlagen-VM erstellen möchten, achten Sie darauf, dass keine Zertifikate für den Host in `/etc/vmware/nsx/` vorhanden sind. Der netcpa-Agent erstellt kein Zertifikat, wenn bereits ein Zertifikat vorhanden ist.

Voraussetzungen

- Transportzonen müssen konfiguriert sein.
- Stellen Sie sicher, dass der Compute Manager konfiguriert ist. Siehe [Hinzufügen eines Compute Managers](#).
- Ein Uplink-Profil muss konfiguriert sein. Alternativ können Sie auch das standardmäßige Uplink-Profil für Bare-Metal-NSX Edge-Knoten verwenden.
- Ein IP-Pool muss konfiguriert sein, oder in der Netzwerkbereitstellung verfügbar sein.
- Mindestens eine nicht verwendete physische Netzwerkkarte (NIC) muss auf dem Host- oder NSX Edge-Knoten verfügbar sein.

Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **System > Fabric > Knoten > Edge-Transportknoten > Edge-VM hinzufügen** aus.
- 3 Geben Sie einen Namen für NSX Edge ein.
- 4 Geben Sie den Hostnamen oder FQDN von vCenter Server ein.
- 5 Reservieren Sie Arbeitsspeicher für die NSX Edge-Appliance, um eine optimale Leistung zu erreichen.

Legen Sie die Reservierung so fest, dass NSX Edge über ausreichend Arbeitsspeicher verfügt, um eine effiziente Ausführung sicherzustellen. Siehe [Systemanforderungen für NSX Edge-VM](#).

- 6 Geben Sie die Befehlszeilenschnittstelle (CLI) und die Root-Kennwörter für den NSX Edge an.

Ihre Kennwörter müssen den Einschränkungen zur Kennwortkomplexität entsprechen.

- mindestens 12 Zeichen
- mindestens ein Kleinbuchstabe
- mindestens ein Großbuchstabe
- mindestens eine Zahl
- mindestens ein Sonderzeichen
- mindestens fünf unterschiedliche Zeichen
- keine Wörterbuchwörter
- keine Palindrome
- mehr als vier monotone Zeichenfolgen ist nicht zulässig

7 Geben Sie die Details zum NSX Edge ein.

Option	Beschreibung
Compute Manager	Wählen Sie im Dropdown-Menü den Compute Manager aus. Der Compute Manager entspricht dem in der Management Plane registrierten vCenter Server.
Cluster	Weisen Sie den Cluster zu, den der NSX Edge aus dem Dropdown-Menü verknüpfen wird.
Ressourcenpool oder Host	Weisen Sie entweder einen Ressourcenpool oder einen bestimmten Host für den NSX Edge aus dem Dropdown-Menü zu.
Datenspeicher	Wählen Sie einen Datenspeicher für die NSX Edge-Dateien aus dem Dropdown-Menü.

8 Geben Sie die Details zur NSX Edge-Schnittstelle ein.

Option	Beschreibung
IP-Zuweisung	Wählen Sie für die IP-Adresse DHCP oder Statisch aus. Wenn Sie Statisch auswählen, müssen Sie eine Liste mit durch Komma getrennten IP-Adressen, ein Gateway und eine Subnetzmaske angeben.
Verwaltungsschnittstelle	Wählen Sie im Dropdown-Menü die VM-Netzwerkschnittstelle aus.

9 Wählen Sie die Transportzonen aus, zu denen dieser Transportknoten gehört.

Ein NSX Edge-Transportknoten gehört zu mindestens zwei Transportzonen, einem Overlay für NSX-T Data Center-Konnektivität und einem VLAN für Uplink-Konnektivität.

Hinweis Mehrere VTEPs in einer Transportzone müssen für dasselbe Netzwerksegment konfiguriert sein. Wenn VTEPs in einer Transportzone für unterschiedliche Netzwerksegmente konfiguriert sind, können keine BFD-Sitzungen zwischen den VTEPs eingerichtet werden.

10 Geben Sie die N-VDS-Informationen ein.

Option	Beschreibung
Edge-Switchname	Wählen Sie im Dropdown-Menü den Overlay-Switch aus.
Uplink-Profil	Wählen Sie ein Uplink-Profil im Dropdown-Menü aus. Die verfügbaren Uplinks hängen von der Konfiguration im gewählten Uplink-Profil ab.
IP-Zuweisung	Wählen Sie IP-Pool verwenden oder Liste statischer IPs verwenden für den Overlay-N-VDS aus. Wenn Sie Liste statischer IPs verwenden auswählen, müssen Sie eine Liste mit durch Komma getrennten IP-Adressen, ein Gateway und eine Subnetzmaske angeben.

Option	Beschreibung
IP-Pool	Wenn Sie IP-Pool verwenden für die IP-Zuweisung ausgewählt haben, geben Sie den Namen des IP-Pools an.
Datapath-Schnittstellen	Wählen Sie den Datenpfadnamen für die Uplink-Schnittstelle aus.

Hinweis Das LLDP-Profil wird auf einer NSX Edge-VM-Appliance nicht unterstützt.

11 Überprüfen Sie den Verbindungsstatus auf der Seite **Transportknoten**.

Nach dem Hinzufügen des NSX Edge als Transportknoten ändert sich der Verbindungsstatus in 10-12 Minuten in Aktiv.

12 (Optional) Zeigen Sie den Transportknoten mit dem API-Aufruf GET `https://<nsx-manager>/api/v1/transport-nodes/<transport-node-id>` an.

13 (Optional) Statusinformationen werden über den API-Aufruf GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/status` angezeigt.

Nächste Schritte

Fügen Sie den NSX Edge-Knoten zu einem NSX Edge-Cluster hinzu. Siehe [Erstellen eines NSX Edge-Clusters](#).

Erstellen eines NSX Edge-Clusters

Durch Erstellung eines Clusters aus NSX Edges mit mehreren Knoten können Sie sicherstellen, dass mindestens ein NSX Edge immer verfügbar ist.

Um einen logischen Tier-0-Router oder einen Tier-1-Router mit zustandsbehafteten Diensten wie NAT, Load Balancer usw. zu erstellen, müssen Sie ihn mit einem NSX Edge-Cluster verknüpfen. Selbst wenn also nur ein NSX Edge vorhanden ist, muss dieses dennoch zu einem NSX Edge-Cluster gehören, um nützlich zu sein.

Ein NSX Edge-Transportknoten kann jeweils nur einem NSX Edge-Cluster hinzugefügt werden.

Ein NSX Edge-Cluster kann mehrere logische Router stützen.

Sie können den NSX Edge-Cluster nach seiner Erstellung bearbeiten, um weitere NSX Edges hinzuzufügen.

Voraussetzungen

- Installieren Sie mindestens einen NSX Edge-Knoten.
- Verbinden Sie die NSX Edges mit der Managementebene.
- Fügen Sie die NSX Edges als Transportknoten hinzu.
- Erstellen Sie optional ein NSX Edge-Clusterprofil für Hochverfügbarkeit (HA). Sie können aber auch das standardmäßige NSX Edge-Clusterprofil verwenden.

Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **System > Fabric > Knoten > Edge-Cluster > Hinzufügen** aus.
- 3 Geben Sie einen Namen für den NSX Edge-Cluster ein.
- 4 Wählen Sie ein NSX Edge-Clusterprofil im Dropdown-Menü aus.
- 5 Wählen Sie im Dropdown-Menü „Mitgliedstyp“ einen NSX Edge-Knoten aus.

Wenn die virtuelle Maschine in einer Public Cloud-Umgebung bereitgestellt ist, wählen Sie Public Cloud-Gateway aus. Andernfalls wählen Sie NSX Edge-Knoten aus.
- 6 Wählen Sie in der Spalte **Verfügbar** die NSX Edges aus und klicken Sie auf den Pfeil nach rechts, um diese in die Spalte **Ausgewählt** zu verschieben.

Nächste Schritte

Jetzt können Sie logische Netzwerktopologien erstellen und Dienste konfigurieren. Siehe *Administratorhandbuch für NSX-T Data Center*.

Automatische Bereitstellung statusfreier Cluster

9

Statusfreie Hosts behalten die Konfiguration nicht bei, daher benötigen sie einen Server für die automatische Bereitstellung, um die erforderlichen Startdateien bereitzustellen, wenn die Hosts eingeschaltet werden.

In diesem Abschnitt finden Sie Informationen zum Einrichten eines statusfreien Clusters mithilfe von vSphere Auto Deploy und dem NSX-T-Transportknotenprofil, um einen Host mit einem neuen Image-Profil erneut bereitzustellen, das eine andere Version von ESXi und NSX-T enthält. Hosts, die für die automatische Bereitstellung von vSphere eingerichtet sind, verwenden einen Server mit automatischer Bereitstellung und vSphere-Hostprofile, um Hosts anzupassen. Diese Hosts können auch für das NSX-T-Transportknotenprofil eingerichtet werden, um NSX-T auf den Hosts zu konfigurieren.

Daher kann ein statusfreier Host für die automatische Bereitstellung von vSphere und des NSX-T-Transportknotenprofils eingerichtet werden, um einen Host mit einer benutzerdefinierten ESXi- und NSX-T-Version erneut bereitzustellen.

Dieses Kapitel enthält die folgenden Themen:

- [Allgemeine Aufgaben zum automatischen Bereitstellen statusfreier Cluster](#)
- [Voraussetzungen und unterstützte Versionen](#)
- [Erstellen eines benutzerdefinierten Image-Profiles für statusfreie Hosts](#)
- [Zuordnen des benutzerdefinierten Images zu den Referenz- und Zielhosts](#)
- [Einrichten der Netzwerkkonfiguration auf dem Referenzhost](#)
- [Konfigurieren des Referenzhosts als Transportknoten in NSX-T](#)
- [Extrahieren und Überprüfen des Hostprofils](#)
- [Überprüfen der Hostprofilzuordnung mit dem statusfreien Cluster](#)
- [Aktualisieren der Hostanpassung](#)
- [Auslösen der automatischen Bereitstellung auf Zielhosts](#)
- [Fehlerbehebung für das Host- und Transportknotenprofil](#)

Allgemeine Aufgaben zum automatischen Bereitstellen statusfreier Cluster

Allgemeine Aufgaben zum automatischen Bereitstellen eines statusfreien Clusters.

Die allgemeinen Aufgaben zum Einrichten eines statusfreien Clusters mit automatischer Bereitstellung lauten wie folgt:

- 1 Voraussetzungen und unterstützte Versionen. Siehe [Voraussetzungen und unterstützte Versionen](#).
- 2 (Referenzhost) Erstellen Sie ein benutzerdefiniertes Image-Profil. Siehe [Erstellen eines benutzerdefinierten Image-Profiles für statusfreie Hosts](#).
- 3 (Referenz- und Zielhosts) Ordnen Sie das benutzerdefinierte Image-Profil zu. Siehe [Zuordnen des benutzerdefinierten Images zu den Referenz- und Zielhosts](#).
- 4 (Referenzhost) Richten Sie die Netzwerkkonfiguration in ESXi ein. Siehe [Einrichten der Netzwerkkonfiguration auf dem Referenzhost](#).
- 5 (Referenzhost) Konfigurieren Sie diesen als Transportknoten in NSX. Siehe [Konfigurieren des Referenzhosts als Transportknoten in NSX-T](#).
- 6 (Referenzhost) Extrahieren und überprüfen Sie das Hostprofil. Siehe [Extrahieren und Überprüfen des Hostprofils](#).
- 7 (Referenz- und Zielhosts) Überprüfen Sie die Hostprofilzuordnung mit dem statusfreien Cluster. Siehe [Überprüfen der Hostprofilzuordnung mit dem statusfreien Cluster](#).
- 8 (Referenzhost) Aktualisieren Sie die Hostanpassung. Siehe [Aktualisieren der Hostanpassung](#).
- 9 (Zielhosts) Lösen Sie die automatische Bereitstellung aus. Siehe [Auslösen der automatischen Bereitstellung auf Zielhosts](#).
 - a Vor dem Anwenden des Transportknotenprofils. Siehe [Neustarten von Hosts vor der TNP-Anwendung](#).
 - b Wenden Sie das Transportknotenprofil an. Siehe [Anwenden von TNP auf einem statusfreien Cluster](#).
 - c Nach dem Anwenden des Transportknotenprofils. Siehe [Neustarten von Hosts nach der TNP-Anwendung](#).
- 10 Beheben Sie Probleme mit dem Hostprofil und Transportknotenprofil. Siehe [Fehlerbehebung für das Host- und Transportknotenprofil](#).

Voraussetzungen und unterstützte Versionen

Voraussetzungen und unterstützte Versionen von ESXi und NSX-T.

Unterstützte Workflows

- Mit Image-Profil und Hostprofil

Voraussetzungen

- Nur homogene Cluster (alle Hosts innerhalb eines Clusters müssen entweder statusfrei oder statusbehaftet sein) werden unterstützt.
- Der Image Builder-Dienst muss aktiviert sein.
- Der automatische Bereitstellungsdienst muss aktiviert sein.

Unterstützte NSX-und ESXi-Versionen

Unterstützte EXSi-Version	ESXi 67ep6	ESXi 67u2	ESXi 67u3	ESXi 67ep7
NSX-T Data Center 2.4	Ja	Ja	Nein	Nein
NSX-T Data Center 2.4.1	Ja	Ja	Nein	Nein
NSX-T Data Center 2.4.2	Ja	Ja	Nein	Nein
NSX-T Data Center 2.4.3	Ja	Ja	Nein	Nein
NSX-T Data Center 2.5	Ja	Ja	Ja	Ja

Erstellen eines benutzerdefinierten Image-Profiles für statusfreie Hosts

Identifizieren Sie in Ihrem Datacenter einen Host, der als Referenzhost vorbereitet werden soll.

Wenn der Referenz Host zum ersten Mal gestartet wird, ordnet ESXi die Standardregel dem Referenzhost zu. In diesem Verfahren fügen wir ein benutzerdefiniertes Image-Profil (ESXi und NSX VIBs) hinzu und verknüpfen den Referenzhost mit dem neuen benutzerdefinierten Image. Ein Image-Profil mit dem NSX-T-Image reduziert die Installationszeit erheblich. Dasselbe benutzerdefinierte Image ist mit den Zielhosts im statusfreien Cluster verknüpft.

Hinweis Alternativ können Sie dem Referenzcluster und statusfreien Zielcluster nur ein ESXi-Image-Profil hinzufügen. Die NSX-T-VIBs werden heruntergeladen, wenn Sie das Transportknotenprofil auf dem statusfreien Cluster anwenden. Siehe [Hinzufügen eines Softwaredepots](#).

Voraussetzungen

Stellen Sie sicher, dass der automatische Bereitstellungsdienst und der Image-Erstellungsdienst aktiviert sind. Siehe [Verwenden von vSphere Auto Deploy zum erneuten Bereitstellen von Hosts](#).

Verfahren

- 1 Erstellen Sie zum Importieren von NSX-T-Paketen ein Softwaredepot.
- 2 Laden Sie die nsx-lcp-Pakete herunter.
 - a Melden Sie sich bei <https://my.vmware.com> an.
 - b Wählen Sie auf der Seite „VMware NSX-T Data Center herunterladen“ die NSX-T-Version aus.

- c Suchen Sie auf der Seite „Produkt-Downloads“ die NSX-T-Kernel-Module für eine bestimmte VMware ESXi-Version.
- d Klicken Sie auf **Jetzt herunterladen**, um mit dem Herunterladen des nsx-lcp-Pakets zu beginnen.
- e Importieren Sie nsx-lcp-Pakete in das Softwaredepot.

NSX Kernel Module for VMware ESXi 6.7
Dateigröße: 37,64 MB
Dateityp: zip

[Jetzt herunterladen](#)

Name: nsx-lcp-2.5.0.0.0.14663975-esx67.zip
Release-Datum: 2019-09-19
Build-Nummer: 14663974

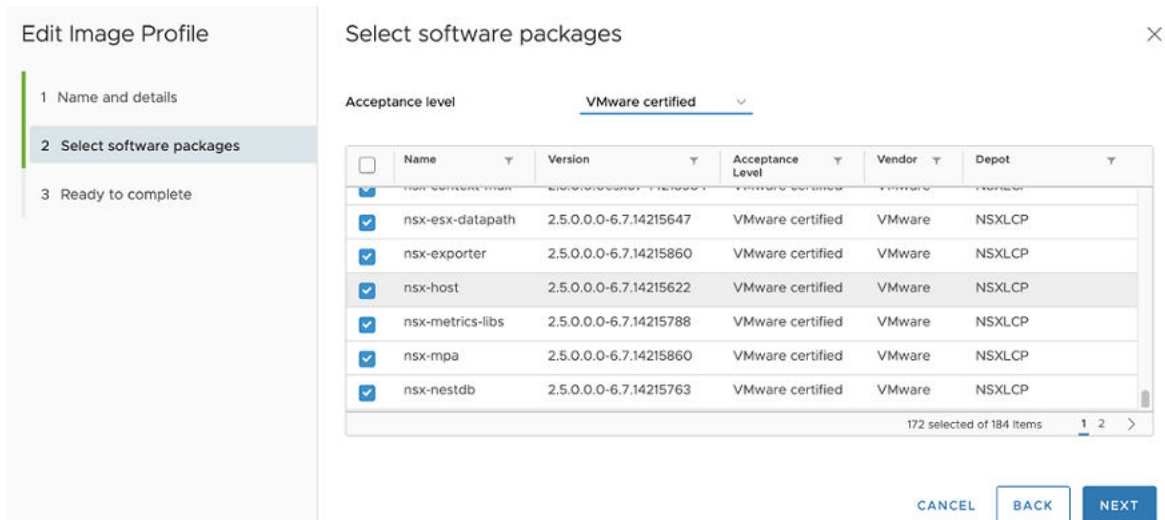
NSX Kernel Module for VMware ESXi 6.7
This package includes the required kernel modules to enable NSX on ESXi 6.7 if needed for a manual installation. Use esxccli to install manually or include as part of an automated deployment system of the ESXi hosts.

MD5SUM: f224a0e12fc1722ae5b5259d279bfa1
SHA1SUM: a97d3125a26a47b94ec8408acd369d42681d3027
SHA256SUM:
1ed76de6a7f22d227eb4be30a2e0aa91492a876b7b164814198de3
1eec77bc44

- 3 Erstellen Sie ein weiteres Softwaredepot zum Importieren von ESXi-Paketen.

Der vSphere Web Client zeigt zwei Depots an, die auf dem Referenzhost erstellt wurden.

- 4 Erstellen Sie ein benutzerdefiniertes Softwaredepot, um zuvor importierte ESXi-Images und nsx-lcp-Pakete zu klonen.
 - a Wählen Sie das ESXi-Image-Profil aus dem ESXi-Softwaredepot aus, das im vorherigen Schritt erstellt wurde.
 - b Klicken Sie auf **Klonen**.
 - c Geben Sie im Assistenten zum Klonen von Image-Profilen einen Namen für das benutzerdefinierte Image ein, das erstellt werden soll.
 - d Wählen Sie das benutzerdefinierte Softwaredepot aus, in dem das geklonte Image (ESXi) verfügbar sein muss.
 - e Wählen Sie im Fenster „Softwarepakete auswählen“ die Akzeptanzstufe für **VMware Certified** aus. Die ESXi-VIBs sind vorausgewählt.
 - f Identifizieren und wählen Sie die NSX-T-Pakete manuell in der Liste der Pakete aus und klicken Sie auf **Weiter**.
 - g Überprüfen Sie im Bildschirm „Bereit zum Abschließen“ die Details und klicken Sie auf **Fertigstellen**, um das geklonte Image mit den ESXi- und NSX-T-Paketen in dem benutzerdefinierten Softwaredepot zu erstellen.



Nächste Schritte

Verknüpfen Sie das benutzerdefinierte Image mit den Referenz- und Zielhosts. Siehe [Zuordnen des benutzerdefinierten Images zu den Referenz- und Zielhosts](#).

Zuordnen des benutzerdefinierten Images zu den Referenz- und Zielhosts

Wenn Sie den Referenzhost und die Zielhosts mit dem neuen benutzerdefinierten Image starten, das ESXi und NSX-Pakete enthält, ordnen Sie das benutzerdefinierte Image-Profil zu.

Zu diesem Zeitpunkt wird das benutzerdefinierte Image nur den Referenz- und Zielhosts zugeordnet, aber die NSX-Installation erfolgt nicht.

Wichtig Führen Sie dieses Verfahren für die benutzerdefinierte Image-Zuordnung auf Referenz- und Zielhosts durch.

Voraussetzungen

Verfahren

- 1 Navigieren Sie auf dem ESXi-Host zu **Menü > Automatische Bereitstellung > Bereitgestellte Hosts**.
- 2 Wenn Sie das benutzerdefinierte Image-Profil einem Host zuordnen möchten, wählen Sie das benutzerdefinierte Image aus.
- 3 Klicken Sie auf **Image-Profilzuordnung bearbeiten**.
- 4 Klicken Sie im Assistenten „Image-Profilzuordnung bearbeiten“ auf **Durchsuchen** und wählen Sie das benutzerdefinierte Depot sowie das benutzerdefinierte Image-Profil aus.
- 5 Aktivieren Sie die Option **Signaturprüfung für Image-Profile überspringen**.

6 Klicken Sie auf **OK**.

Software-Depots	Regeln bereitstellen	Bereitgestellte Hosts	Erkannte Hosts	Skriptpakete	Konfigurieren
<p>① Das mit der Auto Deploy-Funktion mit den Hosts verknüpfte Image-Profil, Hostprofil und der Speicherort werden unten aufgelistet. Die Verknüpfungen können sich vom tatsächlichen Hostzustand unterscheiden.</p> <p>ÜBEREINSTIMMUNG DER HOSTZUORDNUNGEN ÜBERPRÜFEN... HOSTZUORDNUNGEN STANDARDISIEREN IMAGE-PROFILZUORDNUNG BEARBEITEN</p>					
<input type="checkbox"/>	Host	Verknüpftes Image-Profil	Verknüpftes Hostprofil	Verknüpfter Speicherort	Verknüpftes Skriptpaket
<input type="checkbox"/>	10.144.139.147	CustomDepot(ESXi and NSX)		1-datacenter-1964	
<input type="checkbox"/>	10.144.137.225	CustomDepot(ESXi and NSX)		Statless-Cluster	

Ergebnisse

Nächste Schritte

Richten Sie die Netzwerkkonfiguration auf dem Referenzhost ein. Siehe [Einrichten der Netzwerkkonfiguration auf dem Referenzhost](#).

Einrichten der Netzwerkkonfiguration auf dem Referenzhost

Auf dem Referenzhost wird ein Standard-Switch mit einem VMkernel-Adapter erstellt, um die Netzwerkkonfiguration für ESXi einzurichten.

Diese Netzwerkkonfiguration wird im Hostprofil erfasst, das vom Referenzhost extrahiert wird. Während einer statusfreien Bereitstellung repliziert das Hostprofil diese Netzwerkkonfigurationseinstellung auf jedem Zielhost.

Verfahren

- 1 Konfigurieren Sie auf dem ESXi-Host einen vSphere Standard Switch (VSS) oder einen verteilten virtuellen Switch (DVS), indem Sie einen VMkernel-Adapter hinzufügen.
- 2 Stellen Sie sicher, dass der neu hinzugefügte VSS/DVS-Switch auf der Seite „VMkernel-Adapter“ angezeigt wird.

Übersicht	Überwachen	Konfigurieren	Berechtigungen	VMs	Datenspeicher	Netzwerke
VMkernel-Adapter <p>Netzwerk hinzufügen... Aktualisieren Bearbeiten... Entfernen</p>						
Gerät	Netzwerkbezeichn...	Switch	IP-Adresse	TCP/IP-Stack	vH	
vmk0	Management N...	vSwitch0	10.192.193.193	Standard	D	
vmk1	VMkernel	vSwitch2	192.163.242.185	Standard	D	

Nächste Schritte

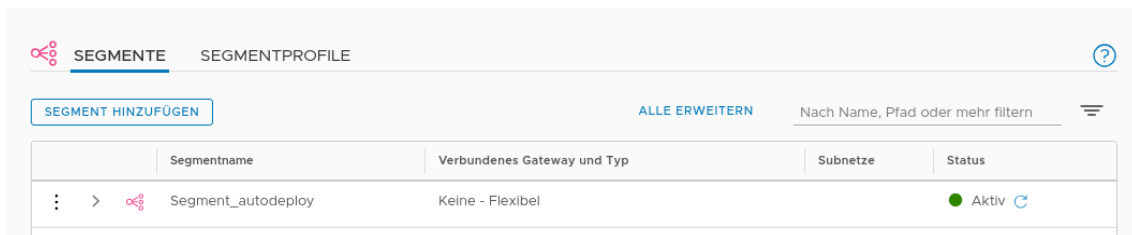
Konfigurieren Sie den Referenzhost als Transportknoten in NSX-T. Siehe [Konfigurieren des Referenzhosts als Transportknoten in NSX-T](#).

Konfigurieren des Referenzhosts als Transportknoten in NSX-T

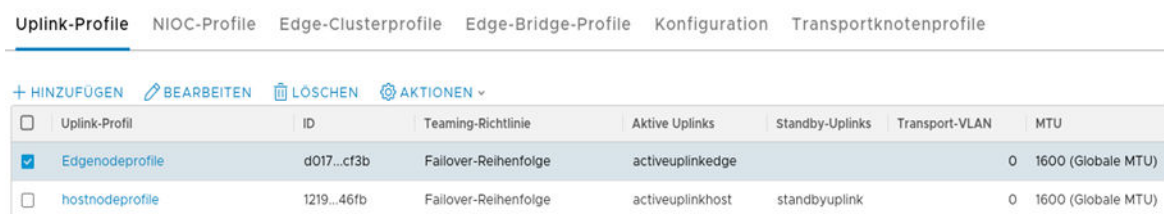
Nachdem der Referenzhost mit dem benutzerdefinierten Image-Profil verknüpft und mit einem VSS-Switch konfiguriert wurde, richten Sie den Referenzhost als Transportknoten in NSX-T ein.

Verfahren

- 1 Melden Sie sich in einem Browser bei NSX-T unter „https://<NSXManager_IPAddress>“ an.
- 2 Den Referenzhost finden Sie unter **System -> Knoten -> Host-Transportknoten**.
- 3 Erstellen Sie eine VLAN-Transportzone, um die Spanne des virtuellen Netzwerks zu definieren. Die Spanne wird durch Anhängen von N-VDS-Switches an die Transportzone definiert. Basierend auf diesem Anhang kann N-VDS auf Segmente zugreifen, die innerhalb der Transportzone definiert sind. Siehe [Erstellen einer Transportzone](#).
- 4 Erstellen Sie ein VLAN-Segment in der Transportzone. Das erstellte Segment wird als logischer Switch angezeigt.
 - a Navigieren Sie zu **Netzwerk -> Segmente**.
 - b Wählen Sie die Transportzone aus, an die das Segment angehängt werden soll.
 - c Geben Sie die VLAN-ID ein.
 - d Klicken Sie auf **Speichern**.



- 5 Erstellen Sie ein Uplink-Profil für den Referenzhost, der definiert, wie ein N-VDS eine Verbindung mit dem physischen Netzwerk herstellt. Siehe [Erstellen eines Uplink-Profiles](#).



- 6 Konfigurieren Sie den Referenzhost als Transportknoten. Siehe [Konfigurieren eines verwalteten Hosttransportknotens](#).
 - a Wählen Sie auf der Seite „Host-Transportknoten“ den Referenzhost aus.
 - b Klicken Sie auf „NSX konfigurieren“ und wählen Sie die zuvor erstellte Transportzone, N-VDS und das Uplink-Profil aus.

- 7 Klicken Sie im Abschnitt „Zu installierende Netzwerkzuordnungen“ auf **Zuordnung hinzufügen**, um die Zuordnung der VMkernel zum Segment/logischen Switch hinzuzufügen.

Netzwerkzuordnungen für die Installation



Die Host-Konnektivität geht möglicherweise verloren, wenn vmnic0 und vmk0 migriert werden.

Das Ändern des logischen Switches für den statusbehafteten Host (eigenständig oder geclustert) wirkt sich nicht aus und der Vorgang schlägt fehl.

[+ HINZUFÜGEN](#) [LÖSCHEN](#)

<input checked="" type="checkbox"/> VMkernel-Adapter *	VLAN-Segment/logischer Switch *
<input checked="" type="checkbox"/> vmk0	segment-autodeploy

- 8 Klicken Sie auf **Fertigstellen**, um die Installation von NSX-T auf dem Referenzhost zu starten.

Während der Installation werden VMkernel-Adapter und physische Netzwerkkarten (NICs) von einem VSS- oder DVS-Switch zu einem N-VDS-Switch migriert. Nach der Installation wird für den Konfigurationszustand des Referenzhosts Erfolg angezeigt.

Hinweis Der Referenzhost wird unter „Weitere Hosts“ aufgeführt.

Host-Transportknoten

Edge-Transportknoten

Edge-Cluster

ESXi-Bridge-Cluster

Verwaltet von

vc

NSX KONFIGURIEREN

NSX ENTFERNEN

AKTIONEN

Anzeiger Alle

<input type="checkbox"/>	Knoten	ID	IP-Adressen	Betriebssystem	NSX-Konfigurati	Konfigurationszi	Knotenstatus	Tunnel	Transportzonen	NSX-Version	N-VDS
<input type="checkbox"/>	Other Hosts (2)	MoRef-I...					1 Host herabg...				
<input checked="" type="checkbox"/>	hostnode	6d4c...f...	10.160.169.8...	ESXi 6.7.0	Konfiguriert	Erfolgreich	Aktiv	↑1	tz	2.5.0.0.0.14...	1
<input type="checkbox"/>	10.192.193.193	42ea...8...	10.192.193.1...	ESXi 6.7.0	Konfiguriert	Erfolgreich	Herabgestuft	Nicht v...	tz	2.5.0.0.0.14...	1

- 9 Stellen Sie in vCenter Server sicher, dass die PNICs- und VMkernel-Adapter auf dem VSS-Switch migriert und mit dem N-VDS-Switch verbunden sind.

VMkernel-Adapter				
Netzwerk hinzufügen... Aktualisieren Bearbeiten... Entfernen				
Gerät	Netzwerkbezeichnung	Switch	IP-Adresse	TCP/IP-Stack
vmk0	Management Network	vSwitch0	10.160.169.87	Standard
vmk1	Segment_autodeploy	vds-1	169.254.171.95	Standard

Nächste Schritte

Extrahieren und überprüfen Sie das Hostprofil. Siehe [Extrahieren und Überprüfen des Hostprofils](#).

Extrahieren und Überprüfen des Hostprofils

Nachdem Sie das Hostprofil vom Referenzhost extrahiert haben, überprüfen Sie die NSX-T-Konfiguration, die im Hostprofil extrahiert wurde. Sie besteht aus einer ESXi- und NSX-T-Konfiguration, die auf die Zielhosts angewendet wird.

Verfahren

- 1 Informationen zum Extrahieren des Hostprofils finden Sie unter [Extrahieren und Konfigurieren des Hostprofils vom Referenzhost](#).

2 Überprüfen Sie die NSX-Konfiguration im extrahierten Hostprofil.

FAVORITEN

ALLE

Q Filter

> Allgemeine Systemeinstellungen

> Andere

> Erweiterte Konfigurationseinstellungen

> Netzwerkkonfiguration

> Standard-Switch

> VM-Portgruppe

> Hostportgruppe

> Konfiguration der physischen Netzwerkkarte

vSphere Distributed Switch

Virtuelle Netzwerkkarte des Hosts

> vNIC des NSX-Hosts:

> vNIC des NSX-Hosts : Segment_autodeploy

> Netstack-Instanz

Netzwerk-Core-Dump-Einstellungen

> Sicherheit und Dienste

> Speicherkonfiguration

vNIC des NSX-Hosts : Segment_autodeploy

LogicSwitch ermitteln, mit dem diese virtuelle Netzwerkkarte verbunden werden soll

LogicSwitch zum Anschließen auswählen

*LogicSwitch-Name

Segment_autodeploy

Festlegen, wann die virtuelle Netzwerkkarte im LogicSwitch erstellt werden soll

Objekt immer erstellen

Eigenschaften für den statusfreien Start von virtuellen Netzwerkkarten im LogicSwitch

Konfigurationsparameter für den statusfreien Start (sehen Sie vor dem Ändern in der Dokumentation nach)

*VLAN (sehen Sie vor dem Ändern in der Dokumentation nach)

0

*Gruppierungsrichtlinien (sehen Sie vor dem Ändern in der Dokumentation nach)

first uplink

Verwendete aktive Uplinks (sehen Sie vor dem Ändern in der Dokumentation nach)

vmnic1

Verwendete Standby-Uplinks (sehen Sie vor dem Ändern in der Dokumentation nach)

--

*Verwendeter OpaqueSwitch-Name (sehen Sie vor dem Ändern in der Dokumentation nach)

vds-1

> Netzwerkkonfiguration

> Standard-Switch

> VM-Portgruppe

> Hostportgruppe

> Konfiguration der physischen Netzwerkkarte

vSphere Distributed Switch

Virtuelle Netzwerkkarte des Hosts

> vNIC des NSX-Hosts:

> vNIC des NSX-Hosts : Segment_autodeploy

> Netstack-Instanz

Netzwerk-Core-Dump-Einstellungen

> Sicherheit und Dienste

> Speicherkonfiguration

Festlegen, wie die MAC-Adresse für vmknic entschieden werden soll

Benutzer zur Eingabe der MAC-Adresse auffordern, falls keine Standardadresse verfügbar ist

Namensrichtlinie für VMkernel-Netzwerkadapter

Zugewiesener Schnittstellenname

VMkernel-Netzwerkadapter

vmk1

MTU-Richtlinie

Angegebene MTU zuweisen

*MTU

1500

TCP/IP-Stack:

Netstack-Instanz, mit der vmknic verbunden ist

*Name

defaultTcpipStack

Ergebnisse

Das Hostprofil enthält eine Konfiguration, die sich auf ESXi und NSX bezieht, da der Host für beide Umgebungen vorbereitet wurde.

Nächste Schritte

Überprüfen Sie die Hostprofilzuordnung mit dem statusfreien Cluster. Siehe [Überprüfen der Hostprofilzuordnung mit dem statusfreien Cluster](#).

Überprüfen der Hostprofilzuordnung mit dem statusfreien Cluster

Um den statusfreien Ziel-Cluster mit der ESXi- und NSX-Konfiguration vorzubereiten, ordnen Sie das vom Referenzhost extrahierte Hostprofil dem statusfreien Ziel-Cluster zu.

Wenn Sie dem statusfreien Cluster kein Hostprofil zuordnen, können neue Knoten, die dem Cluster hinzugefügt werden, nicht automatisch mit ESXi- und NSX-VIBs bereitgestellt werden.

Verfahren

- 1 Hängen Sie das Hostprofil an den statusfreien Cluster an oder trennen Sie es. Siehe [Anhängen von Einheiten an oder Trennen von Einheiten von einem Hostprofil](#).
- 2 Vergewissern Sie sich auf der Registerkarte „Bereitgestellte Hosts“, dass der vorhandene statusfreie Host dem korrekten Image und dem Hostprofil zugeordnet ist.
- 3 Wenn die Hostprofilzuordnung fehlt, wählen Sie den Zielhost aus und klicken Sie auf „Hostzuordnungen standardisieren“, um das Aktualisieren des Images und des Hostprofils auf dem Zielhost zu erzwingen.

Software-Depots	Regeln bereitstellen	Bereitgestellte Hosts	Erkannte Hosts	Skriptpakete	Konfigurieren
<p>Das mit der Auto Deploy-Funktion mit den Hosts verknüpfte Image-Profil, Hostprofil und der Speicherort werden unten aufgelistet. Die Verknüpfungen können sich vom tatsächlichen Hostzustand unterscheiden.</p> <p>ÜBEREINSTIMMUNG DER HOSTZUORDNUNGEN ÜBERPRÜFEN... HOSTZUORDNUNGEN STANDARDISIEREN IMAGE-PROFILZUORDNUNG BEARBEITEN</p>					
<input type="checkbox"/>	Host	Verknüpftes Image-Profil	Verknüpftes Hostprofil	Verknüpfter Speicherort	Verknüpftes Skriptpaket
<input type="checkbox"/>	10.144.139.147	CustomDepot(ESXi and NSX)		1-datacenter-1964	
<input type="checkbox"/>	10.144.137.225	CustomDepot(ESXi and NSX)	Host Profile_ReferenceHost	Statless-Cluster	

Nächste Schritte

Aktualisieren Sie die Hostanpassung. Siehe [Aktualisieren der Hostanpassung](#).

Aktualisieren der Hostanpassung

Nach dem Anhängen des Hostprofils an den Zielcluster sind möglicherweise zusätzliche benutzerdefinierte Einträge auf dem Host erforderlich, um die ESXi- und NSX-T-Pakete erfolgreich darauf bereitzustellen.

Verfahren

- 1 Wenn die Hosts nach dem Anhängen des Hostprofils an den Zielcluster nicht mit benutzerdefinierten Werten aktualisiert werden, wird vom System die folgende Meldung angezeigt.

Host Profile


AKTIONEN

Übersicht

Überwachen

Konfigurieren

Hosts



Name:

Host Profile

Beschreibung:

Erstellt am:

07.11.2019 14:36

Letzte Änderung:

07.11.2019 14:36

Version:

6.7.0

Der Host 10.160.183.211 muss zusätzlich angepasst werden.

Der Host 10.160.170.243 muss zusätzlich angepasst werden.

- 2 Navigieren Sie zum Aktualisieren der Hostanpassungen zum Hostprofil, klicken Sie auf **Aktionen -> Hostanpassungen bearbeiten**.

- 3 Geben Sie für die ESXi-Versionen 67ep6, 67ep7, 67u2 das MUX-Benutzerkennwort ein.

Customize hosts

Enter host customizations.

IMPORT HOST CUSTOMIZATIONS ⓘ

Required	Property Name	Path	Value
No	MAC Address	Networking configu...	02:00:0c:23:e9:9a
Yes	Adapter MA...	Storage configurati...	02:00:0c:23:e9:9a
Yes	Activate	Storage configurati...	false
Yes	Password	Security and...	Security and Services > Security Settings > Security > User Configuration > mux_user > Pass...

- 4 Stellen Sie sicher, dass alle erforderlichen Felder mit den entsprechenden Werten aktualisiert wurden.

Nächste Schritte

Lösen Sie die automatische Bereitstellung auf Zielhosts aus. Siehe [Auslösen der automatischen Bereitstellung auf Zielhosts](#).

Auslösen der automatischen Bereitstellung auf Zielhosts

Wenn dem Cluster ein neuer Knoten zum hinzugefügt wird, muss er manuell neu gestartet werden, damit die ESXi- und NSX-T- VIBs konfiguriert werden können.

Hinweis Gilt nur für statusfreie Hosts.

Es gibt zwei Möglichkeiten, Hosts für die Auslösung der automatischen Bereitstellung von ESXi- und NSX-T-VIBs vorzubereiten, die konfiguriert werden sollen.

- Starten Sie die Hosts neu, bevor Sie TNP auf den statusfreien Cluster anwenden.
- Starten Sie die Hosts neu, nachdem Sie TNP auf den statusfreien Cluster angewendet haben.

Wenn Sie VMkernel-Adapter bei der Installation von NSX-T auf den Hosts migrieren möchten, finden Sie weitere Informationen unter:

- [Szenarien, in denen sich der statusfreie Host im Zielcluster befindet](#)
- [Szenarien, in denen sich der statusfreie Host außerhalb des Zielclusters befindet](#)

Nächste Schritte

Starten Sie die Hosts neu, bevor Sie TNP auf den statusfreien Cluster anwenden. Siehe [Neustarten von Hosts vor der TNP-Anwendung](#).

Neustarten von Hosts vor der TNP-Anwendung

Gilt nur für statusfreie Hosts. In diesem Szenario wird das Transportknotenprofil nicht auf den statusfreien Cluster angewendet, d. h., dass NSX-T nicht auf dem Zielhost installiert und konfiguriert ist.

Verfahren

1 Starten Sie Hosts neu.

Der Zielhost beginnt mit dem ESXi-Image. Nach dem Start verbleibt der Zielhost im Wartungsmodus, bis das TNP-Profil auf den Zielhost angewendet wird und die Installation von NSX-T abgeschlossen ist. Profile werden in der folgenden Reihenfolge auf Hosts angewendet:

Profile werden in der folgenden Reihenfolge auf Hosts angewendet.

- Das Image-Profil wird auf den Host angewendet.
- Die Hostprofilkonfiguration wird auf den Host angewendet.
- Die NSX-T-Konfiguration wird auf den Host angewendet.

2 Auf dem ESXi-Host ist der VMkernel-Adapter an ein temporäres Segment mit dem Namen <N-LogicalSegment> angehängt, da der Host noch kein Transportknoten ist. Nach der Installation von NSX-T wird der temporäre Switch durch den tatsächlichen N-VDS-Switch und das logische Segment ersetzt.

Gerät	Netzwerkbezeichnung	Switch	IP-Adresse	TCP/IP-Stack
vmk0	Management Network	vSwitch0	10.160.169.87	Standard
vmk1	Segment_autodeploy	vds-1	169.254.171.95	Standard

ESXi-VIBs werden auf alle neu gestarteten Hosts angewendet. Ein temporärer NSX-Switch auf einem ESXi-Host. Wenn TNP auf die Hosts angewendet wird, wird der temporäre Switch durch den tatsächlichen NSX-T-Switch ersetzt.

Nächste Schritte

Wenden Sie TNP auf den statusfreien Cluster an. Siehe [Anwenden von TNP auf einem statusfreien Cluster](#).

Anwenden von TNP auf einem statusfreien Cluster

Die Konfiguration und Installation von NSX-T erfolgt nur dann auf den Ziel-Hosts, wenn TNP auf den Cluster angewendet wird.

Verfahren

- 1 Notieren Sie die Einstellungen, die im Hostprofil vom Referenzhost extrahiert wurden. Die entsprechenden Entitäten im TNP-Profil müssen denselben Wert haben. Beispielsweise muss der im Hostprofil und TNP verwendete N-VDS-Name identisch sein.

Weitere Informationen zu extrahierten Hostprofil-Einstellungen finden Sie unter [Extrahieren und Überprüfen des Hostprofils](#).

- 2 Fügen Sie ein TNP hinzu. Siehe [Hinzufügen eines Transportknotenprofils](#).
- 3 Stellen Sie sicher, dass die Werte der folgenden Parameter sowohl im neuen TNP-Profil als auch im vorhandenen Hostprofil identisch sind.
 - N-VDS-Name: Stellen Sie sicher, dass der im Hostprofil und TNP referenzierte N-VDS-Name identisch ist.
 - Uplink-Profil: Stellen Sie sicher, dass das im Hostprofil und TNP referenzierte Uplink-Profil identisch ist.
 - PNIC: Wenn Sie eine physische Netzwerkkarte (NIC) einem Uplink-Profil zuordnen, überprüfen Sie zuerst die im Hostprofil verwendete Netzwerkkarte (NIC) und ordnen Sie diese physische Netzwerkkarte (NIC) dem Uplink-Profil zu.
 - Netzwerkzuordnung für Installation: Überprüfen Sie beim Zuordnen des Netzwerks während der Installation zuerst für das Hostprofil die Zuordnung zwischen VMkernel und Segment und fügen Sie dieselbe Zuordnung in TNP hinzu.
 - Netzwerkzuordnung für Deinstallation: Überprüfen Sie beim Zuordnen des Netzwerks während der Deinstallation zuerst für das Hostprofil die Zuordnung zwischen VMkernel und VSS/DVS und fügen Sie dieselbe Zuordnung in TNP hinzu.

- 4 Fügen Sie ein TNP hinzu, indem Sie in allen erforderlichen Feldern Eingaben vornehmen. Siehe [Hinzufügen eines Transportknotenprofils](#).

Stellen Sie sicher, dass die Werte der folgenden Parameter sowohl im neuen TNP-Profil als auch im vorhandenen Hostprofil identisch sind.

- Transportzone: Stellen Sie sicher, dass die im Hostprofil und TNP referenzierte Transportzone identisch ist.
- N-VDS-Name: Stellen Sie sicher, dass der im Hostprofil und TNP referenzierte N-VDS-Name identisch ist.
- Uplink-Profil: Stellen Sie sicher, dass das im Hostprofil und TNP referenzierte Uplink-Profil identisch ist.
- PNIC: Wenn Sie eine physische Netzwerkkarte (NIC) einem Uplink-Profil zuordnen, überprüfen Sie zuerst die im Hostprofil verwendete Netzwerkkarte (NIC) und ordnen Sie diese physische Netzwerkkarte (NIC) dem Uplink-Profil zu.

- Netzwerkzuordnung für Installation: Überprüfen Sie beim Zuordnen des Netzwerks während der Installation zuerst für das Hostprofil die Zuordnung zwischen VMkernel und logischem Switch und fügen Sie dieselbe Zuordnung in TNP hinzu.
- Netzwerkzuordnung für Deinstallation: Überprüfen Sie beim Zuordnen des Netzwerks während der Deinstallation zuerst für das Hostprofil die Zuordnung zwischen VMkernel und VSS/DVS und fügen Sie dieselbe Zuordnung in TNP hinzu.

N-VDS-Name *	vds-tzvian	
Zugeordnete Transportzonen	tz-33	
NIOC-Profil *	nsx-default-nioc-hostswitch-profile	
	ODER Neues NIOC-Profil erstellen	
Uplink-Profil *	nsx-default-uplink-hostswitch-profile	
	ODER Neues Uplink-Profil erstellen	
LLDP-Profil *	LLDP [Send Packet Enabled]	
IP-Zuweisung *		
Physische Netzwerkkarten	vmnic1	uplink-1
		PNIC hinzufügen
Migration nur von PNIC	<input type="checkbox"/> Nein	
Aktivieren Sie diese Option, wenn auf dem für die Migration ausgewählten PNIC keine VMKs existieren		
Netzwerkzuordnungen für die Installation	1 Zuordnung	
Netzwerkzuordnungen für die Deinstallation	Zuordnung hinzufügen	





Wenn die TNP-Konfiguration nach der TNP-Anwendung auf Zielknoten nicht mit der Hostprofil-Konfiguration übereinstimmt, wird der Knoten aufgrund von Konformitätsfehlern möglicherweise nicht angezeigt.

- 5 Stellen Sie sicher, dass das TNP-Profil erfolgreich erstellt wurde.

- 6 Wenden Sie das TNP-Profil auf den Zielcluster an und klicken Sie auf **Speichern**.



- 7 Stellen Sie sicher, dass das TNP-Profil erfolgreich auf den Zielcluster angewendet wird. Das bedeutet, dass NSX erfolgreich auf allen Knoten des Clusters konfiguriert wurde.
- 8 Stellen Sie in vSphere sicher, dass die physischen Netzwerkkarten (NICs) oder VMkernel-Adapter an den N-VDS-Switch angehängt sind.

   				
Gerät	Netzwerkbezeichnung	Switch	IP-Adresse	TCP/IP-Stack
vmk0	Management Network	vSwitch0	10.160.169.87	Standard
vmk1	Segment_autodeploy	vds-1	169.254.171.95	Standard

- 9 Stellen Sie in NSX sicher, dass der ESXi-Host erfolgreich als Transportknoten konfiguriert ist.

Nächste Schritte

Alternativ können Sie einen Zielhost nach dem Anwenden von TNP auf den Cluster neu starten. Siehe [Neustarten von Hosts nach der TNP-Anwendung](#).

Neustarten von Hosts nach der TNP-Anwendung

Gilt nur für statusfreie Hosts. Wenn dem Cluster ein neuer Knoten hinzugefügt wird, starten Sie den Knoten manuell neu, damit die ESXi- und NSX-T-Pakete darauf konfiguriert werden.

Verfahren

- 1 Wenden Sie TNP auf den statusfreien Cluster an, der bereits mit dem Hostprofil vorbereitet wurde. Siehe [Erstellen und Anwenden von TNP auf statusfreie Cluster](#).
- 2 Starten Sie Hosts neu.

Wenn Sie nach dem Anwenden des TNP-Profiles auf den statusfreien Cluster einen neuen Knoten neu starten, der dem Cluster hinzugefügt wird, wird dieser Knoten automatisch mit NSX-T auf dem Host konfiguriert.

Nächste Schritte

Stellen Sie sicher, dass Sie jeden neuen Knoten neu starten, der dem Cluster hinzugefügt wird, um ESXi und NSX-T automatisch auf dem neu gestarteten Knoten bereitzustellen und zu konfigurieren.

Informationen zur Fehlerbehebung bei Problemen im Zusammenhang mit dem Hostprofil und dem Transportknotenprofil beim Konfigurieren der automatischen Bereitstellung finden Sie unter [Fehlerbehebung für das Host- und Transportknotenprofil](#).

Szenarien, in denen sich der statusfreie Host im Zielcluster befindet

In diesem Abschnitt werden Anwendungsfälle beschrieben, in denen ein statusfreier Host im Zielcluster vorhanden ist.

Wichtig Auf einem statusfreien Zielhost:

- Die Migration des vmk0-Adapters von VSS/DVS auf N-VDS wird in NSX-T 2.4 und NSX-T 2.4.1 nicht unterstützt.
 - Die Migration des vmk0-Adapters von VSS/DVS auf N-VDS wird in NSX-T 2.5 unterstützt.
-

Zielhost	Referenzhostkonfiguration	Schritte zum automatischen Bereitstellen von Zielhosts
Auf dem Zielhost ist der vmk0-Adapter konfiguriert.	Für das vom Referenzhost extrahierte Hostprofil ist vmk0 auf einem N-VDS-Switch konfiguriert. In NSX-T ist für TNP nur die vmk0-Migrationszuordnung konfiguriert.	<ol style="list-style-type: none"> 1 Hängen Sie das Hostprofil an den Zielhost an. Der vmk0-Adapter ist an einen vSwitch angehängt. 2 Aktualisieren Sie bei Bedarf die Hostanpassungen. 3 Starten Sie den Host neu. Das Hostprofil wird auf den Host angewendet. vmk0 ist an einen temporären Switch angehängt. 4 Wenden Sie TNP an. Der vmk0-Adapter wird zu N-VDS migriert. Der Zielhost wird erfolgreich mit ESXi- und NSX-T-VIBs bereitgestellt.
Auf dem Zielhost ist der vmk0-Adapter konfiguriert.	Für das vom Referenzhost extrahierte Hostprofil ist vmk0 auf einem vSwitch und vmk1 auf einem N-VDS-Switch konfiguriert. In NSX-T ist für TNP nur die vmk1-Migrationszuordnung konfiguriert.	<ol style="list-style-type: none"> 1 Hängen Sie das Hostprofil an den Zielhost an. Der vmk0-Adapter ist an einen vSwitch angehängt, aber vmk1 wird auf keinem Switch erkannt. 2 Aktualisieren Sie bei Bedarf die Hostanpassungen. 3 Starten Sie den Host neu. vmk0 ist an einen vSwitch angehängt und vmk1 ist an einen temporären NSX-Switch angehängt. 4 Wenden Sie TNP an. Der vmk1-Adapter wird zu N-VDS migriert. 5 (optional) Wenn der Host nicht mit dem Hostprofil konform bleibt, starten Sie den Host neu, damit der Host übereinstimmt. Der Zielhost wird erfolgreich mit ESXi- und NSX-T-VIBs bereitgestellt.
Auf dem Zielhost ist der vmk0-Adapter konfiguriert.	Für das vom Referenzhost extrahierte Hostprofil ist vmk0 auf einem vSwitch und vmk1 auf einem N-VDS-Switch konfiguriert. In NSX-T sind für TNP die vmk0- und vmk1-Migrationszuordnungen konfiguriert.	<ol style="list-style-type: none"> 1 Hängen Sie das Hostprofil an den Zielhost an. Der vmk0-Adapter ist an einen vSwitch angehängt, aber vmk1 wird auf keinem Switch erkannt. 2 Aktualisieren Sie bei Bedarf die Hostanpassungen. 3 Starten Sie den Host neu. Der vmk0-Adapter ist an einen vSwitch angehängt und vmk1 ist an einen temporären NSX-Switch angehängt. 4 Wenden Sie TNP an. 5 (optional) Wenn der Host nicht mit dem Hostprofil konform bleibt, starten Sie den Host neu, damit der Host übereinstimmt. Der Zielhost wird erfolgreich mit ESXi- und NSX-T-VIBs bereitgestellt.

Zielhost	Referenzhostkonfiguration	Schritte zum automatischen Bereitstellen von Zielhosts
Auf dem Zielhost sind vmk0- und vmk1-Adapter konfiguriert.	Für das vom Referenzhost extrahierte Hostprofil ist vmk0 auf einem vSwitch und vmk1 auf einem N-VDS-Switch konfiguriert. In NSX-T ist für TNP eine vmk1-Migrationszuordnung konfiguriert.	<ol style="list-style-type: none"> 1 Hängen Sie das Hostprofil an den Zielhost an. Die vmk0- und vmk1-Adapter sind an einen vSwitch angehängt. 2 Aktualisieren Sie bei Bedarf die Hostanpassungen. 3 Den Host neu starten. 4 Wenden Sie TNP an. Der vmk0-Adapter ist an einen vSwitch angehängt und vmk1 ist an einen N-VDS-Switch angehängt. 5 (optional) Wenn der Host nicht mit dem Hostprofil konform bleibt, starten Sie den Host neu, damit der Host übereinstimmt. <p>Der Zielhost wird erfolgreich mit ESXi- und NSX-T-VIBs bereitgestellt.</p>
Auf dem Zielhost sind vmk0- und vmk1-Adapter konfiguriert.	Für das vom Referenzhost extrahierte Hostprofil sind vmk0 und vmk1 auf einem N-VDS-Switch konfiguriert. In NSX-T sind für TNP die vmk0- und vmk1-Migrationszuordnungen konfiguriert.	<ol style="list-style-type: none"> 1 Hängen Sie das Hostprofil an den Zielhost an. Die vmk0- und vmk1-Adapter sind an einen vSwitch angehängt. 2 Aktualisieren Sie bei Bedarf die Hostanpassungen. 3 Starten Sie den Host neu. 4 Wenden Sie TNP an. vmk0 und vmk1 werden zu einem N-VDS-Switch migriert. <p>Der Zielhost wird erfolgreich mit ESXi- und NSX-T-VIBs bereitgestellt.</p>

Szenarien, in denen sich der statusfreie Host außerhalb des Zielclusters befindet

In diesem Abschnitt werden Anwendungsfälle beschrieben, in denen ein statusfreier Host außerhalb des Zielclusters vorhanden ist.

Wichtig Auf statusfreien Hosts:

- Die Migration des vmk0-Adapters von VSS/DVS auf N-VDS wird in NSX-T 2.4 und NSX-T 2.4.1 nicht unterstützt.
- Die Migration des vmk0-Adapters von VSS/DVS auf N-VDS wird in NSX-T 2.5 unterstützt.

Zielhostzustand	Referenzhostkonfiguration	Schritte zum automatischen Bereitstellen von Zielhosts
<p>Der Host befindet sich im ausgeschalteten Zustand (erster Start). Er wird später dem Cluster hinzugefügt.</p> <p>Die Standardregel für die automatische Bereitstellung wird für den Zielcluster konfiguriert und dem Hostprofil zugeordnet.</p> <p>Das Transportknotenprofil wird auf dem Cluster angewendet.</p>	<p>Für das vom Referenzhost extrahierte Hostprofil sind der VMkernel-Adapter 0 (vmk0) auf einem vSwitch und der VMkernel-Adapter 1 (vmk1) auf einem N-VDS-Switch konfiguriert.</p> <p>In NSX-T ist für TNP nur die vmk1-Migrationszuordnung konfiguriert.</p>	<p>1 Schalten Sie den Host ein.</p> <p>Nach dem Einschalten des Hosts.</p> <ul style="list-style-type: none"> ■ Der Host wird dem Cluster hinzugefügt. ■ Das Hostprofil wird auf den Zielhost angewendet. ■ Der vmk0-Adapter befindet sich auf dem vSwitch und der vmk1-Adapter befindet sich auf einem temporären Switch. ■ TNP wird ausgelöst. ■ Nachdem TNP auf den Cluster angewendet wurde, befindet sich der vmk0-Adapter auf dem vSwitch und vmk1 wird auf den N-VDS-Switch migriert. <p>2 (Optional) Wenn der Host nicht mit dem Hostprofil konform bleibt, starten Sie den Host neu, damit der Host übereinstimmt.</p> <p>Der Host wird erfolgreich mit ESXi- und NSX-T-VIBs bereitgestellt.</p>
<p>Der Host befindet sich im ausgeschalteten Zustand (erster Start). Er wird später dem Cluster hinzugefügt.</p> <p>Die Standardregel für die automatische Bereitstellung wird für den Zielcluster konfiguriert und dem Hostprofil zugeordnet.</p> <p>Das Transportknotenprofil wird auf dem Cluster angewendet.</p>	<p>Für das vom Referenzhost extrahierte Hostprofil sind der VMkernel-Adapter 0 (vmk0) und der VMkernel-Adapter 1 (vmk1) auf einem N-VDS-Switch konfiguriert.</p> <p>In NSX-T sind für TNP die vmk0- und vmk1-Migration konfiguriert.</p>	<p>1 Schalten Sie den Host ein.</p> <p>Nach dem Einschalten des Hosts.</p> <ul style="list-style-type: none"> ■ Der Host wird dem Cluster hinzugefügt. ■ Das Hostprofil wird auf den Zielhost angewendet. ■ Die vmk0- und vmk1-Adapter befinden sich auf einem temporären Switch. ■ TNP wird ausgelöst. ■ Nachdem TNP auf den Cluster angewendet wurde, werden vmk0 und vmk1 auf den N-VDS-Switch migriert. <p>Der Host wird erfolgreich mit ESXi- und NSX-T-VIBs bereitgestellt.</p>

Zielhostzustand	Referenzhostkonfiguration	Schritte zum automatischen Bereitstellen von Zielhosts
<p>Der Host befindet sich im eingeschalteten Zustand. Er wird später dem Cluster hinzugefügt.</p> <p>Die Standardregel für die automatische Bereitstellung wird für den Zielcluster konfiguriert und dem Hostprofil zugeordnet.</p> <p>Auf dem Zielhost ist nur der vmk0-Adapter konfiguriert.</p>	<p>Für das vom Referenzhost extrahierte Hostprofil sind der VMkernel-Adapter 0 (vmk0) auf einem vSwitch und der VMkernel-Adapter 1 (vmk1) auf einem N-VDS-Switch konfiguriert.</p> <p>In NSX-T ist für TNP eine vmk1-Migrationszuordnung konfiguriert.</p>	<ol style="list-style-type: none"> 1 Verschieben Sie den Host, sodass er Teil des Clusters ist. 2 Starten Sie den Host neu. <p>Nachdem der Host neu gestartet wurde, wird das Hostprofil auf den Zielhost angewendet.</p> <ul style="list-style-type: none"> ■ Der vmk0-Adapter ist an einen vSwitch angehängt, während der vmk1-Adapter an einen temporären NSX-Switch angehängt ist. ■ TNP wird ausgelöst. ■ vmk1 wird zum N-VDS-Switch migriert. <ol style="list-style-type: none"> 3 (Optional) Wenn der Host nicht mit dem Hostprofil konform bleibt, starten Sie den Host neu, damit der Host übereinstimmt. <p>Der Host wird erfolgreich mit ESXi- und NSX-T-VIBs bereitgestellt.</p>
<p>Der Host befindet sich im eingeschalteten Zustand. Er wird später dem Cluster hinzugefügt.</p> <p>Die Standardregel für die automatische Bereitstellung wird für den Zielcluster konfiguriert und dem Hostprofil zugeordnet.</p> <p>Auf dem Zielhost ist nur der vmk0-Adapter konfiguriert.</p>	<p>Für das vom Referenzhost extrahierte Hostprofil sind der VMkernel-Adapter 0 (vmk0) und der VMkernel-Adapter 1 (vmk1) auf N-VDS konfiguriert.</p> <p>In NSX-T sind für TNP die vmk0- und vmk1-Migration konfiguriert.</p>	<ol style="list-style-type: none"> 1 Verschieben Sie den Host, sodass er Teil des Clusters ist. 2 Starten Sie den Host neu. <p>Nachdem der Host neu gestartet wurde, wird das Hostprofil auf den Zielhost angewendet.</p> <ul style="list-style-type: none"> ■ Die vmk0- und vmk1-Adapter sind an einen temporären NSX-Switch angehängt. ■ TNP wird ausgelöst. ■ vmk0 und vmk1 sind an einen N-VDS-Switch angehängt. <p>Der Host wird erfolgreich mit ESXi- und NSX-T-VIBs bereitgestellt.</p>

Zielhostzustand	Referenzhostkonfiguration	Schritte zum automatischen Bereitstellen von Zielhosts
Der Host befindet sich im eingeschalteten Zustand. Er wird später dem Cluster hinzugefügt. Die Standardregel für die automatische Bereitstellung wird für den Zielcluster konfiguriert und dem Hostprofil zugeordnet. Auf dem Zielhost sind die vmk0- und vmk1-Netzwerkzuordnungen konfiguriert.	Für das vom Referenzhost extrahierte Hostprofil sind der VMkernel-Adapter 0 (vmk0) auf einem vSwitch und der VMkernel-Adapter 1 (vmk1) auf einem N-VDS-Switch konfiguriert. In NSX-T ist für TNP eine vmk1-Migration konfiguriert.	<ol style="list-style-type: none"> 1 Verschieben Sie den Host, sodass er Teil des Clusters ist. 2 Starten Sie den Host neu. Nachdem der Host neu gestartet wurde, wird das Hostprofil auf den Zielhost angewendet. <ul style="list-style-type: none"> ■ Der vmk0-Adapter ist an einen vSwitch angehängt, während der vmk1-Adapter an einen temporären NSX-Switch angehängt ist. ■ TNP wird ausgelöst. ■ vmk1 wird zum N-VDS-Switch migriert. 3 (Optional) Wenn der Host nicht mit dem Hostprofil konform bleibt, starten Sie den Host neu, damit der Host übereinstimmt. <p>Der Host wird erfolgreich mit ESXi- und NSX-T-VIBs bereitgestellt.</p>
Der Host befindet sich im eingeschalteten Zustand. Er wird später dem Cluster hinzugefügt. Die Standardregel für die automatische Bereitstellung wird für den Zielcluster konfiguriert und dem Hostprofil zugeordnet. Auf dem Host sind die vmk0- und vmk1-Netzwerkzuordnungen konfiguriert.	Auf dem Referenzhost sind für das Hostprofil der VMkernel-Adapter 0 (vmk0) und der VMkernel-Adapter 1 (vmk1) auf einem N-VDS-Switch konfiguriert. In NSX-T sind für TNP die vmk0- und vmk1-Migration konfiguriert.	<ol style="list-style-type: none"> 1 Verschieben Sie den Host, sodass er Teil des Clusters ist. 2 Starten Sie den Host neu. Nachdem der Host neu gestartet wurde, wird das Hostprofil auf den Zielhost angewendet. <ul style="list-style-type: none"> ■ Die vmk0- und vmk1-Adapter sind an einen temporären NSX-Switch angehängt. ■ TNP wird ausgelöst. ■ Die vmk0- und vmk1-Adapter werden zum N-VDS-Switch migriert. <p>Der Host wird erfolgreich mit ESXi- und NSX-T-VIBs bereitgestellt.</p>

Fehlerbehebung für das Host- und Transportknotenprofil

Beheben Sie Probleme mit Hostprofilen und TNPs, wenn sie für die automatische Bereitstellung von statusfreien Clustern verwendet werden.

Szenario	Beschreibung
Hostprofil ist nicht portabel.	<p>Problem: keiner der vCenter-Server kann das Hostprofil verwenden, das die NSX-T-Konfiguration enthält.</p> <p>Probleumlösung: Keine</p>
Regel-Engine für automatische Bereitstellung	<p>Problem: Das Hostprofil kann nicht in Regeln zum automatischen Bereitstellen verwendet werden, um neue Cluster bereitzustellen. Wenn neue Cluster bereitgestellt werden, werden die Hosts mit Basisnetzwerk bereitgestellt und sie bleiben im Wartungsmodus.</p> <p>Probleumlösung: Bereiten Sie jeden Cluster über die NSX-T-GUI vor. Siehe Anwenden von TNP auf einem statusfreien Cluster.</p>

Szenario	Beschreibung
Prüfung von Konformitätsfehlern.	<p>Problem: Die Hostprofilwartung kann die Konformitätsfehler im Zusammenhang mit der NSX-T-Konfiguration nicht beheben.</p> <ul style="list-style-type: none"> ■ Die auf dem Hostprofil und in TNP konfigurierten physischen Netzwerkkarten unterscheiden sich. ■ Zuordnung zwischen vNIC-zu-LS-Zuordnung. Hostprofil findet eine Nichtübereinstimmung in der Zuordnung zwischen logischem Switch und vNIC mit dem TNP-Profil. ■ Nichtübereinstimmung zwischen VMkernel und verbundenem N-VDS auf Hostprofil und TNP. ■ Nichtübereinstimmung des opaken Switches auf Hostprofil und TNP. <p>Problemumgehung: Stellen Sie sicher, dass die NSX-T-Konfiguration auf dem Hostprofil und TNP übereinstimmt. Starten Sie den Host neu, um die Konfigurationsänderungen umzusetzen. Der Host wird angezeigt.</p>
Wartung	<p>Problem: Wenn NSX-T-spezifische Konformitätsfehler vorliegen, wird die Hostprofilwartung auf diesem Cluster blockiert.</p> <p>Falsche Konfiguration:</p> <ul style="list-style-type: none"> ■ Zuordnung zwischen vNIC-zu-LS-Zuordnung ■ Zuordnung physischer Netzwerkkarten <p>Problemumgehung: Stellen Sie sicher, dass die NSX-T-Konfiguration auf dem Hostprofil und TNP übereinstimmt. Starten Sie den Host neu, um die Konfigurationsänderungen umzusetzen. Der Host wird angezeigt.</p>
Anhängen	<p>Problem: In einem mit NSX-T konfigurierten Cluster kann das Hostprofil nicht auf Hostebene angehängt werden.</p> <p>Problemumgehung: Keine</p>
Trennen	<p>Problem: Beim Trennen und Anhängen eines neuen Hostprofils in einem Cluster, der mit NSX-T konfiguriert ist, wird die NSX-T-Konfiguration nicht entfernt. Auch wenn der Cluster mit dem neu angehängten Hostprofil konform ist, weist er weiterhin die NSX-T-Konfiguration aus einem vorherigen Profil auf.</p> <p>Problemumgehung: Keine</p>
Aktualisieren	<p>Problem: Wenn der Benutzer die NSX-T-Konfiguration im Cluster geändert hat, extrahieren Sie ein neues Hostprofil. Aktualisieren Sie das Hostprofil manuell für alle verloren gegangenen Einstellungen.</p> <p>Problemumgehung: Keine</p>
Transportknotenkonfiguration auf Hostebene	<p>Problem: Nachdem der anportsport-Knoten automatisch bereitgestellt wurde, fungiert er als einzelne Einheit. Eine Aktualisierung dieses Transportknotens stimmt möglicherweise nicht mit TNP überein.</p> <p>Problemumgehung: Aktualisieren Sie den Cluster. Eine Aktualisierung in einem eigenständigen Transportknoten kann die zugehörige Migrationsspezifikation nicht beibehalten. Bei der Migration schlägt das Posten des Neustarts möglicherweise fehl.</p>
Das Hostprofil kann nicht angewendet werden, da die mux_user-Kennwortrichtlinie und das Kennwort nicht zurückgesetzt wurden.	<p>Problem: nur auf Hosts, auf denen Versionen vor vSphere 6.7 U3 ausgeführt werden. Die Hostwartung und Hostprofilanwendung auf Hosts schlagen möglicherweise fehl, es sei denn, das Kennwort mux_user wird zurückgesetzt.</p> <p>Problemumgehung: Bearbeiten Sie unter „Richtlinien & Profile“ das Hostprofil, um die Kennwortrichtlinie „mux_user“ zu ändern und setzen Sie das Kennwort mux_user zurück.</p>

Szenario	Beschreibung
Die PeerDNS-Konfiguration wird auf dem VMkernel-Adapter, der für die Migration zum NVDS-Switch ausgewählt wurde, nicht unterstützt.	<p>Problem: Wenn ein für die Migration auf NVDS ausgewählter VMkernel-Adapter Peer-DNS-fähig ist, schlägt die Hostprofilanwendung fehl.</p> <p>Problemumgehung: Bearbeiten Sie das extrahierte Hostprofil, indem Sie die Peer-DNS-Einstellung auf dem VMkernel-Adapter deaktivieren, der auf einen NVDS-Switch migriert werden muss. Stellen Sie alternativ sicher, dass Sie keine Peer-DNS-fähigen VMkernel-Adapter auf einen NVDS-Switch migrieren.</p>
DHCP-Adresse der VMkernel-NIC-Adresse wird nicht beibehalten	<p>Problem: Wenn der Referenzhost statusbehaftet ist, können statusfreie Hosts, für die ein vom statusbehafteten Referenzhost extrahiertes Profil verwendet wird, die zugehörige MAC-Adresse für die VMkernel-Verwaltung nicht beibehalten, die vom per PXE gestarteten MAC abgeleitet wurde. Dies führt zu DHCP-Adressierungsproblemen.</p> <p>Problemumgehung: Bearbeiten des extrahierten Hostprofil des statusbehafteten Hosts und ändern Sie die Einstellung Bestimmung der MAC-Adresse für vmknic festlegen in MAC-Adresse verwenden, von der das System per PXE gestartet wurde.</p>
Ein Fehler bei der Hostprofilanwendung in vCenter kann zu NSX-Konfigurationsfehlern auf dem Host führen.	<p>Problem: Wenn die Hostprofilanwendung in vCenter fehlschlägt, schlägt die NSX-Konfiguration möglicherweise ebenfalls fehl.</p> <p>Problemumgehung: Stellen Sie in vCenter sicher, dass das Hostprofil erfolgreich angewendet wurde. Korrigieren Sie die Fehler und versuchen Sie es erneut.</p>
LAGs werden auf statusfreien ESXi-Hosts nicht unterstützt.	<p>Problem: Das als LAGs in NSX konfigurierte Uplink-Profil wird auf einem statusfreien ESXi-Host, der von einem vCenter Server oder in NSX verwaltet wird, nicht unterstützt.</p> <p>Problemumgehung: Keine</p>

Deinstallieren von NSX-T Data Center von einem Host-Transportknoten

10

Die Schritte zum Deinstallieren von NSX-T Data Center von einem Host-Transportknoten variieren je nach Host-Typ und dessen Konfiguration.

- **Überprüfen der Host-Netzwerkzuordnungen für die Deinstallation**

Bevor Sie NSX-T Data Center von einem ESXi-Host deinstallieren, stellen Sie sicher, dass Sie die entsprechenden Netzwerkzuordnungen für die Deinstallation konfiguriert haben. Die Zuordnungen sind erforderlich, wenn der ESXi-Host über VMkernel-Schnittstellen verfügt, die mit N-VDS verbunden sind.

- **Deinstallieren von NSX-T Data Center von einem vSphere-Cluster**

Wenn Sie NSX-T Data Center auf einem vSphere-Cluster mithilfe von Transportknotenprofilen installiert haben, können Sie diese Anweisungen befolgen, um NSX-T Data Center von allen Hosts im Cluster zu deinstallieren.

- **Deinstallieren von NSX-T Data Center von einem Host in einem vSphere-Cluster**

Sie können NSX-T Data Center von einem einzelnen Host deinstallieren, der von vCenter Server verwaltet wird. Die anderen Hosts im Cluster sind davon nicht betroffen.

- **Deinstallieren von NSX-T Data Center von einem eigenständigen Host**

Sie können NSX-T Data Center von einem eigenständigen Host deinstallieren. Eigenständige Hosts können ESXi oder KVM sein.

Überprüfen der Host-Netzwerkzuordnungen für die Deinstallation

Bevor Sie NSX-T Data Center von einem ESXi-Host deinstallieren, stellen Sie sicher, dass Sie die entsprechenden Netzwerkzuordnungen für die Deinstallation konfiguriert haben. Die Zuordnungen sind erforderlich, wenn der ESXi-Host über VMkernel-Schnittstellen verfügt, die mit N-VDS verbunden sind.

Die Deinstallationszuordnung legt fest, wo die Schnittstellen nach der Deinstallation verbunden sind. Es sind Deinstallationszuordnungen für physische Schnittstellen (vmnicX) und VMkernel-Schnittstellen (vmkX) vorhanden. Beim Deinstallieren werden VMkernel-Schnittstellen von ihren aktuellen Verbindungen zu den Portgruppen verschoben, die in der Deinstallationszuordnung angegeben sind. Wenn eine physische Schnittstelle in der Deinstallationszuordnung enthalten ist, wird die physische Schnittstelle mit dem entsprechenden vSphere Distributed Switch oder vSphere Standard Switch verbunden, der auf der Zielportgruppe der VMkernel-Schnittstellen basiert.

Vorsicht Die Deinstallation von NSX-T Data Center von einem ESXi-Host ist störend, wenn die physischen Schnittstellen oder VMkernel-Schnittstellen mit N-VDS verbunden sind. Wenn der Host oder Cluster an anderen Anwendungen wie z. B. vSAN teilnimmt, sind diese Anwendungen möglicherweise von der Deinstallation betroffen.






Es gibt zwei Möglichkeiten, die Netzwerkzuordnungen für die Deinstallation zu konfigurieren.

- In der Transportknotenkonfiguration, die für den jeweiligen Host gilt.
- In einer Transportknoten-Profilkonfiguration, die dann auf einen Cluster angewendet werden kann.

Hinweis Sie müssen über einen Compute Manager verfügen, der so konfiguriert ist, dass ein Transportknotenprofil auf einen Cluster angewendet wird.

Wenn ein Compute Manager konfiguriert ist, kann ein Host sowohl über eine Transportknotenkonfiguration als auch über eine Transportknotenprofilkonfiguration verfügen. Wenn beide vorhanden sind, ist die Konfiguration des Transportknotens aktiv. Stellen Sie sicher, dass die Netzwerkzuordnungen für die Deinstallation für die aktive Konfiguration ordnungsgemäß konfiguriert sind.

In diesem Beispiel wird dem Cluster cluster-1 das Transportknotenprofil TNP-1 zugewiesen. Der Host TN-1 zeigt „Konfigurationskonflikt“ an. Diese Konfliktmeldung gibt an, dass eine andere Konfiguration auf TN-1 angewendet wurde. Die Übereinstimmung bleibt bestehen, bis die Konfiguration des Transportknotens mit der Profilkonfiguration des Transportknotens übereinstimmt. Der Transportknoten TN-2 verwendet die Netzwerkzuordnungen aus dem Transportknotenprofil, und der Transportknoten TN-1 verwendet seine eigene Konfiguration.

 NSX KONFIGURIEREN  NSX ENTFERNEN  AKTIONEN ▾					
<input type="checkbox"/>	Knoten	ID	IP-Adresse	Betriebssystem	NSX-Konfiguration
<input type="checkbox"/>	New Cluster (2)	MoR...			 TNP-1
<input type="checkbox"/>	tn-1	926...	10...	ESXi ...	 Nichtübereinstimmung bei Konfiguration
<input type="checkbox"/>	tn-2	901f....	10...	ESXi ...	Konfiguriert

Voraussetzungen

- Stellen Sie sicher, dass die entsprechenden Portgruppen für die Verwendung in der Deinstallationszuordnung konfiguriert sind. Sie müssen flüchtige vSphere Distributed Switch-Portgruppen oder vSphere Standard Switch-Portgruppen verwenden.

- Konfigurieren Sie einen Compute Manager, wenn Sie eine vSphere Distributed-Switch-Portgruppe in den Deinstallationszuordnungen für einen eigenständigen ESXi-Host verwenden möchten. Siehe [Hinzufügen eines Compute Managers](#). Wenn kein Compute Manager konfiguriert ist, müssen Sie eine vSphere Standard Switch-Portgruppe verwenden.

Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **System > Fabric > Knoten > Host-Transportknoten** aus.
- 3 Stellen Sie für jeden Host, den Sie deinstallieren möchten, sicher, dass die Netzwerkzuordnung für die Deinstallation eine Portgruppe für jede VMkernel-Schnittstelle enthält, die sich auf N-VDS befindet. Fügen Sie fehlende Zuordnungen hinzu.

Wichtig Bei der Portgruppe in der Netzwerkzuordnung für die Deinstallation muss es sich um eine flüchtige vSphere Distributed Switch-Portgruppe oder um eine vSphere Standard Switch-Portgruppe handeln.

- a Wenn Sie VMkernel-Schnittstellen anzeigen möchten, melden Sie sich bei vCenter Server an, wählen Sie den Host aus und klicken Sie auf **Konfigurieren > VMkernel-Adapter**.
- b Wenn die Konfiguration des Transportknotens die aktive Konfiguration ist, wählen Sie den Host aus und klicken Sie auf **Bearbeiten** (bei eigenständigen Hosts) oder auf **NSX konfigurieren** (bei verwalteten Hosts). Klicken Sie auf **Weiter** und anschließend auf **Netzwerkzuordnungen für die Deinstallation**. Zeigen Sie die Zuordnungen auf den Registerkarten **VMKNic-Zuordnungen** und **Physische Netzwerkkartenzuordnungen** an.
- c Wenn das Transportknotenprofil die aktive Konfiguration ist, klicken Sie in der Spalte **NSX-Konfiguration** auf den Namen des Transportknotenprofils für den Cluster und klicken Sie dann auf **Bearbeiten**. Klicken Sie auf der Registerkarte **N-VDS** auf **Netzwerkzuordnungen für die Deinstallation**. Zeigen Sie die Zuordnungen auf den Registerkarten **VMKNic-Zuordnungen** und **Physische Netzwerkkartenzuordnungen** an.

Deinstallieren von NSX-T Data Center von einem vSphere-Cluster

Wenn Sie NSX-T Data Center auf einem vSphere-Cluster mithilfe von Transportknotenprofilen installiert haben, können Sie diese Anweisungen befolgen, um NSX-T Data Center von allen Hosts im Cluster zu deinstallieren.

Weitere Informationen zu Transportknotenprofilen finden Sie unter [Hinzufügen eines Transportknotenprofils](#).

Vorsicht Die Deinstallation von NSX-T Data Center von einem ESXi-Host ist störend, wenn die physischen Schnittstellen oder VMkernel-Schnittstellen mit N-VDS verbunden sind. Wenn der Host oder Cluster an anderen Anwendungen wie z. B. vSAN teilnimmt, sind diese Anwendungen möglicherweise von der Deinstallation betroffen.

Wenn Sie kein Transportknotenprofil zum Installieren von NSX-T Data Center verwendet haben oder wenn Sie NSX-T Data Center aus einer Teilmenge der Hosts im Cluster entfernen möchten, finden Sie weitere Informationen unter [Deinstallieren von NSX-T Data Center von einem Host in einem vSphere-Cluster](#).

Hinweis Durch das Entfernen eines Hosts von einem Cluster wird NSX-T Data Center nicht deinstalliert. Befolgen Sie diese Anweisungen, um NSX-T Data Center von einem Host in einem Cluster zu deinstallieren: [Deinstallieren von NSX-T Data Center von einem Host in einem vSphere-Cluster](#).

Voraussetzungen

- Stellen Sie sicher, dass für die Hosts, die Sie deinstallieren möchten, Netzwerk-Deinstallationszuordnungen konfiguriert sind. Siehe [Überprüfen der Host-Netzwerkzuordnungen für die Deinstallation](#).
- Stellen Sie sicher, dass sich die Hosts, die Sie deinstallieren möchten, in vSphere im Wartungsmodus befinden.

Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **System > Fabric > Knoten > Host-Transportknoten** aus.
- 3 Wählen Sie im Dropdown-Menü **Verwaltet von** den vCenter Server aus.
- 4 Wählen Sie den Cluster aus, den Sie deinstallieren möchten, und klicken Sie auf **NSX entfernen**.
- 5 Stellen Sie sicher, dass die NSX-T Data Center-Software vom Host entfernt wurde.
 - a Melden Sie sich als Root bei der Befehlszeilenschnittstelle des Hosts an.
 - b Führen Sie diesen Befehl aus, um nach NSX-T Data Center-VIBs zu suchen

```
esxcli software vib list | grep -E 'nsx|vsipfwlib'
```

Wenn die NSX-T Data Center-Software erfolgreich entfernt wurde, werden keine VIBs aufgeführt. Wenn NSX-VIBs auf dem Host verbleiben, wenden Sie sich an den VMware Support.

Deinstallieren von NSX-T Data Center von einem Host in einem vSphere-Cluster

Sie können NSX-T Data Center von einem einzelnen Host deinstallieren, der von vCenter Server verwaltet wird. Die anderen Hosts im Cluster sind davon nicht betroffen.

Vorsicht Die Deinstallation von NSX-T Data Center von einem ESXi-Host ist störend, wenn die physischen Schnittstellen oder VMkernel-Schnittstellen mit N-VDS verbunden sind. Wenn der Host oder Cluster an anderen Anwendungen wie z. B. vSAN teilnimmt, sind diese Anwendungen möglicherweise von der Deinstallation betroffen.

Voraussetzungen

- Stellen Sie sicher, dass für die Hosts, die Sie deinstallieren möchten, Netzwerk-Deinstallationszuordnungen konfiguriert sind. Siehe [Überprüfen der Host-Netzwerkzuordnungen für die Deinstallation](#).
- Stellen Sie sicher, dass sich die Hosts, die Sie deinstallieren möchten, in vSphere im Wartungsmodus befinden.

Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **System > Fabric > Knoten > Host-Transportknoten** aus.
- 3 Wählen Sie im Dropdown-Menü **Verwaltet von** den vCenter Server aus.
- 4 Wenn auf den Cluster ein Transportknotenprofil angewendet wurde, wählen Sie den Cluster aus und klicken Sie auf **Aktionen > TN-Profil trennen**.

Wenn auf dem Cluster ein Transportknotenprofil angewendet wurde, wird in der Spalte **NSX-Konfiguration** für den Cluster der Profilname angezeigt.

- 5 Wählen Sie den Host aus und klicken Sie auf **NSX entfernen**.
- 6 Stellen Sie sicher, dass die NSX-T Data Center-Software vom Host entfernt wurde.
 - a Melden Sie sich als Root bei der Befehlszeilenschnittstelle des Hosts an.
 - b Führen Sie diesen Befehl aus, um nach NSX-T Data Center-VIBs zu suchen

```
esxcli software vib list | grep -E 'nsx|vsipfwlib'
```

Wenn die NSX-T Data Center-Software erfolgreich entfernt wurde, werden keine VIBs aufgeführt. Wenn NSX-VIBs auf dem Host verbleiben, wenden Sie sich an den VMware Support.

- 7 Wenn auf dem Cluster ein Transportknotenprofil angewendet wurde und Sie es erneut anwenden möchten, wählen Sie den Cluster aus, klicken Sie auf **NSX konfigurieren** und wählen Sie das Profil im Dropdown-Menü **Bereitstellungsprofil auswählen** aus.

Deinstallieren von NSX-T Data Center von einem eigenständigen Host

Sie können NSX-T Data Center von einem eigenständigen Host deinstallieren. Eigenständige Hosts können ESXi oder KVM sein.

Vorsicht Die Deinstallation von NSX-T Data Center von einem ESXi-Host ist störend, wenn die physischen Schnittstellen oder VMkernel-Schnittstellen mit N-VDS verbunden sind. Wenn der Host oder Cluster an anderen Anwendungen wie z. B. vSAN teilnimmt, sind diese Anwendungen möglicherweise von der Deinstallation betroffen.

Voraussetzungen

Wenn Sie NSX-T Data Center von einem eigenständigen ESXi-Host deinstallieren, überprüfen Sie die folgenden Einstellungen:

- Stellen Sie sicher, dass für die Hosts, die Sie deinstallieren möchten, Netzwerk-Deinstallationszuordnungen konfiguriert sind. Siehe [Überprüfen der Host-Netzwerkzuordnungen für die Deinstallation](#).
- Stellen Sie sicher, dass sich die Hosts, die Sie deinstallieren möchten, in vSphere im Wartungsmodus befinden.

Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **System > Fabric > Knoten > Host-Transportknoten** aus.
- 3 Wählen Sie im Dropdown-Menü **Verwaltet von** den Eintrag **Keine: Eigenständige Hosts** aus.
- 4 Wählen Sie den Host aus und klicken Sie auf **Löschen**. Stellen Sie im angezeigten Bestätigungsdialogfeld sicher, dass **NSX-Komponenten deinstallieren** ausgewählt und **Löschen erzwingen** deaktiviert ist. Klicken Sie auf **Löschen**.

Die NSX-T Data Center-Software wurde vom Host entfernt. Es kann bis zu 5 Minuten dauern, bis die gesamte NSX-T Data Center-Software entfernt wurde.

- 5 Wenn die Deinstallation fehlschlägt, wählen Sie den Host aus und klicken Sie erneut auf **Löschen**. Deaktivieren Sie im Bestätigungsdialogfeld **NSX-Komponenten deinstallieren** und wählen Sie **Löschen erzwingen** aus.

Der Host-Transportknoten wird aus der Management Plane gelöscht, aber auf dem Host ist möglicherweise noch NSX-T Data Center-Software installiert.

- 6 Stellen Sie sicher, dass die NSX-T Data Center-Software vom Host entfernt wurde.
 - a Melden Sie sich als Root bei der Befehlszeilenschnittstelle des Hosts an.
 - b Führen Sie den entsprechenden Befehl aus, um nach NSX-T Data Center-Softwarepaketen zu suchen.

Tabelle 10-1. Paketlistenbefehle

Hostbetriebssystem	Befehl
ESXi	<code>esxcli software vib list grep -E 'nsx vsipfwlib'</code>
Red Hat Enterprise Linux und CentOS Linux	<code>rpm -qa grep -E 'nsx vsipfwlib'</code>
Ubuntu	<code>dpkg -l grep -E 'nsx vsipfwlib'</code>
SUSE Linux Enterprise Server	<code>zypper packages --installed-only grep -E 'nsx vsipfwlib'</code>

Wenn die NSX-T Data Center-Software erfolgreich entfernt wurde, werden keine Pakete aufgeführt. Wenn noch NSX-Softwarepakete auf dem Host verbleiben, wenden Sie sich an den VMware Support.

Installieren von NSX Cloud-Komponenten

11

NSX Cloud bietet eine zentrale Oberfläche zur Verwaltung Ihrer Public Cloud-Netzwerke.

NSX Cloud ist unabhängig von anbieterspezifischem Networking, das keinen Hypervisor-Zugriff in einer Public Cloud benötigt.

Dies bietet verschiedene Vorteile:

- Sie können Anwendungen unter Verwendung des gleichen Netzwerks und der gleichen Sicherheitsprofile, die in der Produktionsumgebung verwendet werden, entwickeln und testen.
- Entwickler können ihre Anwendungen verwalten, bis sie bereit für die Bereitstellung sind.
- Mit Notfallwiederherstellung können Sie nach einem ungeplanten Ausfall oder einem Sicherheitsrisiko für Ihre Public Cloud eine Wiederherstellung durchführen.
- Wenn Sie Ihre Arbeitslasten zwischen Public Clouds migrieren, gewährleistet NSX Cloud, dass ähnliche Sicherheitsrichtlinien auf Workload-VMs angewendet werden – unabhängig von deren neuem Standort.

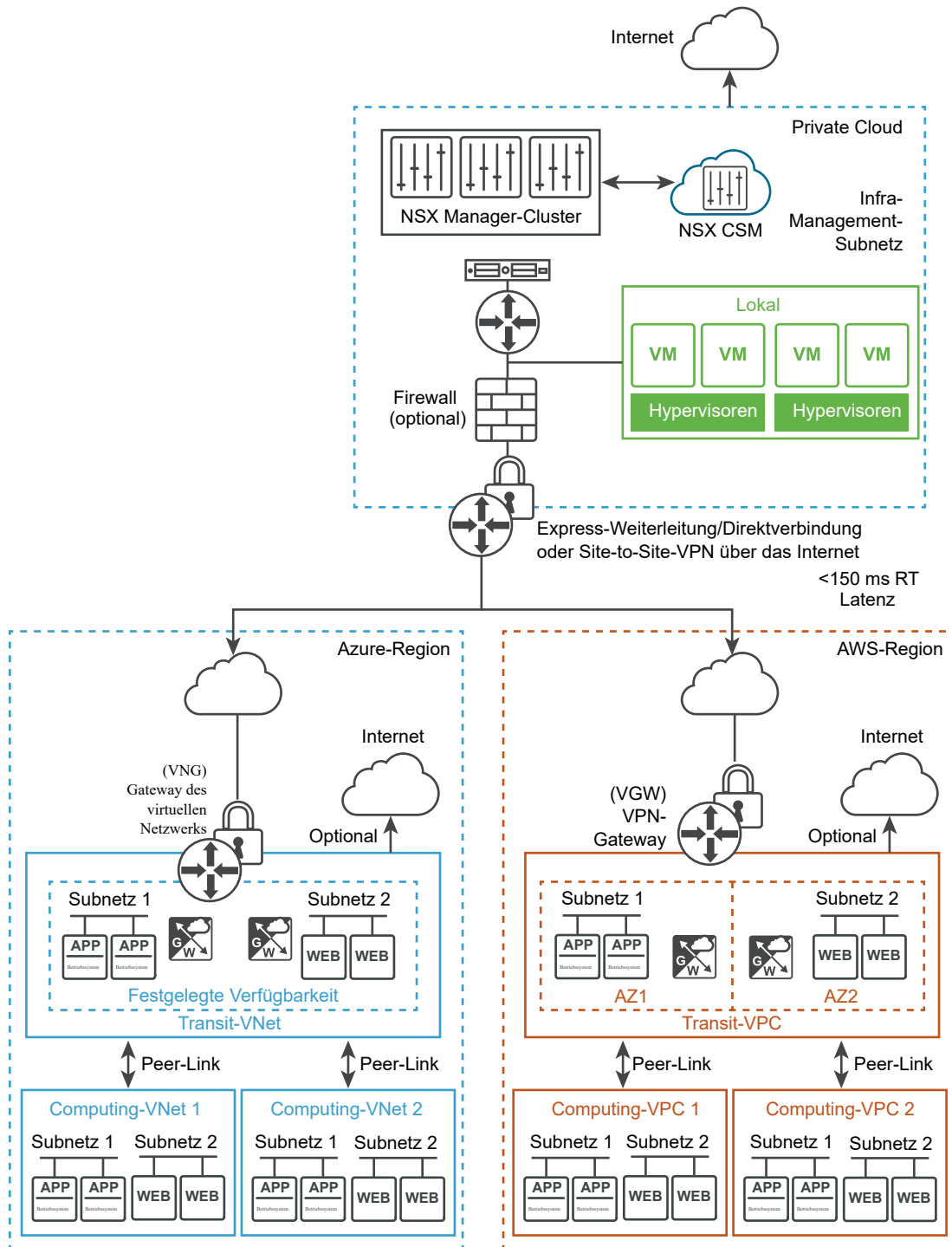
Dieses Kapitel enthält die folgenden Themen:

- [Architektur und Komponenten von NSX Cloud](#)
- [Überblick über das Installieren und Konfigurieren von NSX Cloud-Komponenten für Ihre Public Cloud](#)
- [Installieren von CSM und Herstellen einer Verbindung zu NSX Manager](#)
- [Public Cloud mit lokaler Bereitstellung verbinden](#)
- [Ihr Public Cloud-Konto hinzufügen](#)
- [Bereitstellen oder Verknüpfen von NSX Public Cloud Gateways](#)
- [Bereitstellung von PCG aufheben](#)

Architektur und Komponenten von NSX Cloud

NSX Cloud integriert die NSX-T Data Center-Hauptkomponenten in Ihre Public Cloud, um Netzwerkfunktionalität und Sicherheit in allen Implementierungen bereitzustellen.

Abbildung 11-1. Die Architektur von NSX Cloud



Hauptkomponenten

Die Hauptkomponenten von NSX Cloud sind:

- **NSX Manager** für die Managementebene mit richtlinienbasiertem Routing, rollenbasierter Zugriffssteuerung (RBAC), Steuerungsebene und definiertem Laufzeitstatus.

- *Cloud Service Manager (CSM)* für die Integration in NSX Manager, um der Verwaltungsebene Public Cloud-spezifische Informationen zur Verfügung zu stellen.
- *NSX Public Cloud Gateway (PCG)* für Konnektivität zu den NSX-Verwaltungs- und -Steuerungsebenen sowie den NSX Edge-Gateway-Diensten und für API-basierte Kommunikation mit den Public Cloud-Elementen. Weitere Informationen finden Sie unter [Bereitstellen oder Verknüpfen von NSX Public Cloud Gateways](#).
- *NSX Agent*-Funktionalität, die einen NSX-verwalteten Datenpfad für Workload-VMs bereitstellt.

Bereitstellungsmodi

NSX Public Cloud Gateway kann entweder eine eigenständige Gateway-Appliance sein oder von Ihren Public Cloud-VPCs oder -VNetns gemeinsam genutzt werden, um so eine Hub-and-Spoke-Topologie zu erhalten.

Die selbstverwaltete VPC oder das selbstverwaltete VNet fungiert als Transit-VPC: Wenn Sie PCG in einer VPC oder einem VNet bereitstellen, wird die VPC oder das VNet als selbstverwaltet qualifiziert, d. h. Sie können die in dieser VPC oder diesem VNet gehosteten VMs unter NSX-Verwaltung stellen. Dieser VPC oder VNet qualifiziert sich auch als Transit-VPC oder VNet, da Sie die darauf bereitgestellte PCG für das Onboarding der in anderen VPCs oder VNetns gehosteten VMs nutzen können.

Computing-VPC- oder VNet-Verknüpfungen mit einer Transit-VPC oder einem Transit-VNet: VPCs oder VNetns, auf denen das PCG nicht bereitgestellt ist, sondern die auf eine Transit-VPC oder ein Transit-VNet verweisen, werden als *Computing*-VPCs oder -VNetns bezeichnet.

Überblick über das Installieren und Konfigurieren von NSX Cloud-Komponenten für Ihre Public Cloud

In der Prüfliste erhalten Sie einen Überblick über die Schritte zum Aktivieren von NSX-T Data Center, um Ihre Workload-VMs in der Public Cloud zu verwalten.

Workflow für Tag 0 zum Herstellen einer Verbindung von NSX Cloud zu Ihrer Public Cloud

Dieser Workflow bietet einen Überblick über die erforderlichen Schritte, um mit NSX Cloud für Ihre Public Cloud zu beginnen.

Hinweis Stellen Sie bei der Planung Ihrer Bereitstellung sicher, dass die lokalen NSX-T Data Center-Appliances über eine gute Konnektivität mit dem in der Public Cloud bereitgestellten PCG verfügen. Die Transit-VPCs/-VNetns müssen sich außerdem in derselben Region befinden wie die Computing-VPCs/-VNetns.

Tabelle 11-1. Workflow für Tag 0 zum Herstellen einer Verbindung von NSX Cloud zu Ihrer Public Cloud

Aufgabe	Anweisungen
<input type="checkbox"/> Installieren Sie CSM und stellen Sie eine Verbindung zu NSX Manager her.	Siehe Installieren von CSM und Herstellen einer Verbindung zu NSX Manager .
<input type="checkbox"/> Fügen Sie eines oder mehrere Ihrer Public-Cloud-Konten zu CSM hinzu.	Siehe Ihr Public Cloud-Konto hinzufügen .
<input type="checkbox"/> Stellen Sie PCG in Ihren Transit-VPCs oder VNets bereit und verknüpfen Sie sich mit Ihren Rechen-VPCs oder VNets.	Siehe Bereitstellen oder Verknüpfen von NSX Public Cloud Gateways .
<input type="checkbox"/> Führen Sie das Onboarding von Workload-VMs durch, indem Sie sie in Ihrer Public Cloud taggen und den NSX-Agent darauf installieren.	Befolgen Sie die Anweisungen unter Onboarding von Workload-VMs im <i>Administratorhandbuch für NSX-T Data Center</i> .

Installieren von CSM und Herstellen einer Verbindung zu NSX Manager

Verwenden Sie den Setup-Assistenten, um CSM mit NSX Manager zu verbinden und Proxyserver einzurichten, sofern vorhanden.

Installieren von CSM

Cloud Service Manager (CSM) ist ein wesentlicher Bestandteil von NSX Cloud.

Installieren Sie CSM, nachdem Sie die Kernkomponenten von NSX-T Data Center installiert haben.

Detaillierte Anweisungen finden Sie unter [Installieren Sie NSX Manager und die verfügbaren Appliances](#).

Hinweis Bei der Installation von NSX Cloud müssen Sie die FQDN-Nutzung (DNS) auf NSX Managern aktivieren. Siehe [Veröffentlichen der FQDNs der NSX Manager](#).

Verbinden von CSM mit NSX Manager

Sie müssen die CSM-Appliance mit NSX Manager verbinden, damit diese Komponenten miteinander kommunizieren können.

Voraussetzungen

- NSX Manager muss installiert sein und Sie benötigen den Benutzernamen und das Kennwort für das Administratorkonto, um sich bei NSX Manager anzumelden.
- CSM muss installiert sein, und Ihnen muss in CSM die Rolle „Enterprise-Administrator“ zugewiesen sein.

Verfahren

- 1 Melden Sie sich über einem Webbrowser bei CSM an.

- 2 Wenn Sie im Setup-Assistenten dazu aufgefordert werden, klicken Sie auf **Mit Setup beginnen**.
- 3 Geben Sie im Bildschirm „NSX Manager-Anmeldedaten“ die folgenden Details ein:

Option	Beschreibung
NSX Manager-Hostname	Geben Sie den vollqualifizierten Domännennamen (FQDN) von NSX Manager ein, falls dieser verfügbar ist. Sie können auch die IP-Adresse von NSX Manager eingeben.
Administratoren-Anmeldedaten	Geben Sie den Benutzernamen und das Kennwort eines Enterprise-Administrators für NSX Manager ein.
Manager-Fingerabdruck	Geben Sie optional den Fingerabdruckwert des NSX Manager ein. Wenn Sie dieses Feld leer lassen, wird der Fingerabdruck vom System erkannt und im nächsten Bildschirm angezeigt.

- 4 (Optional) Wenn Sie keinen Fingerabdruckwert für NSX Manager bereitgestellt haben oder der Wert falsch war, wird der Bildschirm **Fingerabdruck überprüfen** angezeigt. Aktivieren Sie das Kontrollkästchen, um den vom System erkannten Fingerabdruck zu akzeptieren.
- 5 Klicken Sie auf **Verbinden**.

Hinweis Wenn Sie diese Einstellung im Setup-Assistenten ausgelassen haben oder den zugehörigen NSX Manager ändern möchten, melden Sie sich bei CSM an und klicken Sie auf **System > Einstellungen** und dann auf **Konfigurieren** im Fenster **Zugeordneter NSX-Knoten**.

CSM überprüft den NSX Manager-Fingerabdruck und stellt eine Verbindung her.

- 6 (Optional) Richten Sie den Proxy-Server ein. Weitere Anweisungen finden Sie unter [\(Optional\) Proxy-Server konfigurieren](#).

(Optional) Proxy-Server konfigurieren

Wenn Sie den gesamten internetgebundenen HTTP/HTTPS-Verkehr über einen zuverlässigen HTTP-Proxy routen und überwachen möchten, können Sie in CSM bis zu fünf Proxyserver konfigurieren.

Die gesamte Public Cloud-Kommunikation von PCG und CSM wird über den ausgewählten Proxyserver geleitet.

Proxysteinstellungen für PCG sind unabhängig von Proxysteinstellungen für CSM. Sie haben die Auswahl zwischen keinem oder einem anderen Proxyserver für PCG.

Sie können die folgenden Authentifizierungsebenen auswählen:

- Auf Anmeldedaten basierende Authentifizierung.
- Zertifikatsbasierte Authentifizierung zum Abfangen von HTTPS.
- Keine Authentifizierung.

Verfahren

- 1 Klicken Sie auf **System > Einstellungen**. Klicken Sie dann im Bereich mit dem Titel **Proxyserver auf Konfigurieren**.

Hinweis Sie können diese Details auch bereitstellen, wenn Sie den CSM-Setup-Assistenten verwenden, der bei der Erstinstallation von CSM verfügbar ist.

- 2 Geben Sie auf dem Bildschirm „Proxy-Server konfigurieren“ die folgenden Details ein:

Option	Beschreibung
Standard	Verwenden Sie dieses Optionsfeld, um den Standard-Proxyserver anzugeben.
Profilname	Geben Sie einen Namen für das Proxyserverprofil an. Dies ist ein Pflichtfeld.
Proxyserver	Geben Sie die IP-Adresse des Proxyservers ein. Dies ist ein Pflichtfeld.
Port	Geben Sie den Port des Proxiservers ein. Dies ist ein Pflichtfeld.
Authentifizierung	Optional Wenn Sie eine zusätzliche Authentifizierung einrichten möchten, aktivieren Sie dieses Kontrollkästchen und geben Sie einen gültigen Benutzernamen und das Kennwort ein.
Benutzername	Dies ist erforderlich, wenn Sie das Kontrollkästchen „Authentifizierung“ aktivieren.
Kennwort	Dies ist erforderlich, wenn Sie das Kontrollkästchen „Authentifizierung“ aktivieren.
Zertifikat	Optional Wenn Sie ein Authentifizierungszertifikat für das Abfangen von HTTPS bereitstellen möchten, aktivieren Sie dieses Kontrollkästchen und fügen Sie das Zertifikat durch Kopieren/Einfügen in das angezeigte Textfeld ein.
Kein Proxy	Wählen Sie diese Option, wenn Sie keinen der konfigurierten Proxyserver verwenden möchten.

(Optional) Einrichten von vIDM für Cloud Service Manager

Wenn Sie VMware Identity Manager verwenden, können Sie diesen so einrichten, dass innerhalb von NSX Manager auf CSM zugegriffen werden kann.

Verfahren

- 1 Konfigurieren Sie vIDM für NSX Manager und CSM. Weitere Informationen finden Sie unter [Konfigurieren der Integration von VMware Identity Manager](#) im *Administratorhandbuch für NSX-T Data Center*.
- 2 Weisen Sie dem vIDM-Benutzer dieselbe Rolle für NSX Manager und CSM zu. Weisen Sie beispielsweise die Rolle **Enterprise-Administrator** dem Benutzer mit dem Namen **vIDM_admin** zu. Sie müssen sich sowohl bei NSX Manager als auch bei CSM anmelden und demselben Benutzernamen dieselbe Rolle zuweisen. Detaillierte Anweisungen finden Sie unter [Hinzufügen einer Rollenzuweisung oder Prinzipalidentität](#) im *Administratorhandbuch für NSX-T Data Center*.
- 3 Melden Sie sich bei NSX Manager an. Sie werden zur vIDM-Anmeldung umgeleitet.

- 4 Geben Sie die Anmeldedaten des vIDM-Benutzers ein. Nachdem Sie sich angemeldet haben, können Sie zwischen NSX Manager und CSM wechseln, indem Sie auf das Anwendungssymbol klicken.



Public Cloud mit lokaler Bereitstellung verbinden

Sie müssen geeignete Konnektivitätsoptionen verwenden, um Ihre lokale Bereitstellung mit Ihren Public Cloud-Konten oder -Abonnements zu verbinden.

Zugriff auf Ports und Protokolle auf CSM für Hybrid-Konnektivität ermöglichen

Öffnen Sie die notwendigen Netzwerkports und genehmigen Sie die erforderlichen Protokolle auf NSX Manager, um Public-Cloud-Konnektivität zu aktivieren.

Erlauben des Zugriffs auf NSX Manager von der Public Cloud

Öffnen Sie die folgenden Netzwerkports und Protokolle, um Konnektivität zu Ihrer lokalen NSX Manager-Bereitstellung zu ermöglichen:

Tabelle 11-2.

Von	Zu	Protokoll/Port	Beschreibung
PCG	NSX Manager	TCP/5671	Eingehender Datenverkehr von der Public Cloud zum lokalen NSX-T Data Center für die Kommunikation auf Managementebene.
PCG	NSX Manager	TCP/8080	Eingehender Datenverkehr von der Public Cloud zum lokalen NSX-T Data Center für den Zugriff auf ein HTTP-Repository zum Upgraden der NSX Cloud-Komponenten.
PCG	NSX Controller	TCP/1234, TCP/1235	Eingehender Datenverkehr von der Public Cloud zum lokalen NSX-T Data Center für die Kommunikation auf Steuerungsebene.
PCG	DNS	UDP/53	Eingehender Datenverkehr von Public Cloud zu lokalem NSX-T Data Center-DNS (wenn Sie den lokalen DNS-Server verwenden)
CSM	PCG	TCP/7442	CSM-Konfigurations-Push

Tabelle 11-2. (Fortsetzung)

Von	Zu	Protokoll/Port	Beschreibung
Beliebig	NSX Manager	TCP/443	NSX Manager-Benutzeroberfläche
Beliebig	CSM	TCP/443	CSM-Benutzeroberfläche

Wichtig Die gesamte Kommunikation der NSX-T Data Center-Infrastruktur nutzt SSL-basierte Verschlüsselung. Stellen Sie sicher, dass Ihre Firewall SSL-Datenverkehr über nicht standardmäßige Ports zulässt.

Ihr Microsoft Azure-Netzwerk mit Ihrer lokalen NSX-T Data Center-Bereitstellung verbinden

Zwischen Ihrem Microsoft Azure-Netzwerk und Ihren lokalen NSX-T Data Center-Appliances muss eine Verbindung eingerichtet sein.

Hinweis Sie müssen bereits NSX Manager installiert und eine Verbindung zu CSM in Ihrer lokalen Bereitstellung hergestellt haben.

Übersicht

- Verbinden Sie Ihr Microsoft Azure-Abonnement mit dem lokalen NSX-T Data Center.
- Konfigurieren Sie Ihre VNets mit den notwendigen CIDR-Blöcken und Subnetzen, die für NSX Cloud erforderlich sind.
- Synchronisieren Sie die Uhrzeit auf der CSM-Apliance mit dem Microsoft Azure Storage-Server oder NTP.

Verbinden Sie Ihr Microsoft Azure-Abonnement mit dem lokalen NSX-T Data Center

Jede Public Cloud bietet Optionen für die Verbindung mit einer lokalen Bereitstellung. Sie können eine der verfügbaren Konnektivitätsoptionen, die Ihren Anforderungen genügt, auswählen. Einzelheiten finden Sie in der [Microsoft Azure-Referenzdokumentation](#).

Hinweis Sie müssen die anwendbaren Sicherheitsüberlegungen und Best Practices von Microsoft Azure überprüfen und implementieren. Zum Beispiel sollte für alle privilegierten Benutzerkonten, die auf das Microsoft Azure-Portal oder die Azure-API zugreifen, Multi-Faktor-Authentifizierung (MFA) aktiviert sein. MFA stellt sicher, dass nur ein autorisierter Benutzer auf das Portal zugreifen kann und reduziert die Wahrscheinlichkeit eines Zugriffs, selbst wenn Anmeldeinformationen gestohlen oder weitergegeben werden. Weitere Informationen und Empfehlungen hierzu finden Sie in der [Azure Security Center-Dokumentation](#).

Ihr VNet konfigurieren

Erstellen Sie in Microsoft Azure routenfähige CIDR-Blöcke und richten Sie die erforderlichen Subnetze ein.

- Ein Management-Subnetz mit einer empfohlenen Spanne von mindestens /28 zur Handhabung von:
 - Datenverkehr zu lokalen Appliances
 - API-Datenverkehr zu Cloud-Anbieter-API-Endpunkten
- Ein Downlink-Subnetz mit einer empfohlenen Spanne von /24 für die Workload-VMs.
- Ein – oder für HA zwei – Uplink-Subnetze mit einer empfohlenen Spanne von /24 für das Routing von Nord-Süd-Datenverkehr, der VNet verlässt oder dort ankommt.

Details zur Verwendung dieser Subnetze finden Sie unter [Bereitstellen oder Verknüpfen von NSX Public Cloud Gateways](#).

Ihr Amazon Web Services-Netzwerk (AWS-Netzwerk) mit Ihrer lokalen NSX-T Data Center-Bereitstellung verbinden

Zwischen Ihrem Amazon Web Services-Netzwerk (AWS-Netzwerk) und Ihren lokalen NSX-T Data Center-Appliances muss eine Verbindung eingerichtet sein.

Hinweis Sie müssen bereits NSX Manager installiert und eine Verbindung zu CSM in Ihrer lokalen Bereitstellung hergestellt haben.

Übersicht

- Verbinden Sie Ihr AWS-Konto mit lokalen NSX Manager-Appliances, indem Sie eine der verfügbaren Optionen verwenden, die Ihre Anforderungen am besten erfüllt.
- Konfigurieren Sie Ihre VPC mit Subnetzen und anderen Anforderungen für NSX Cloud.

Verbinden Sie Ihr AWS-Konto mit Ihrer lokalen NSX-T Data Center-Bereitstellung.

Jede Public Cloud bietet Optionen für die Verbindung mit einer lokalen Bereitstellung. Sie können eine der verfügbaren Konnektivitätsoptionen, die Ihren Anforderungen genügt, auswählen. Einzelheiten finden Sie in der [AWS-Referenzdokumentation](#).

Hinweis Sie müssen die anwendbaren Sicherheitsüberlegungen und Best Practices von AWS überprüfen und implementieren; Informationen hierzu finden Sie in den [Best Practices für die AWS-Sicherheit](#).

Konfigurieren Sie Ihre VPC

Sie benötigen die folgenden Konfigurationen:

- sechs Subnetze zur Unterstützung von PCG mit Hochverfügbarkeit

- ein Internet-Gateway (IGW)
- eine private und eine öffentliche Routingtabelle
- Subnetz-Zuordnung mit Routingtabellen
- aktivierte DNS-Auflösung und DNS-Hostnamen

Folgen Sie diesen Richtlinien, um Ihre VPC zu konfigurieren:

- 1 Wenn Ihre VPC ein /16-Netzwerk verwendet, richten Sie für jedes bereitzustellende Gateway drei Subnetze ein.

Wichtig Wenn Sie Hochverfügbarkeit nutzen, richten Sie in einer anderen Verfügbarkeitszone drei weitere Subnetze ein.

- **Management-Subnetz:** Dieses Subnetz wird für das Management des Datenverkehrs zwischen lokalen NSX-T Data Center und PCG verwendet. Der empfohlene Bereich ist /28.
- **Uplink-Subnetz:** Dieses Subnetz wird für den Nord-Süd-Internetverkehr genutzt. Der empfohlene Bereich ist /24.
- **Downlink-Subnetz:** Dieses Subnetz umfasst den IP-Adressbereich der Workload-VMs und sollte entsprechend dimensioniert werden. Beachten Sie, dass Sie für Debugging-Zwecke eventuell zusätzliche Schnittstellen auf den Arbeitslast-VMs einbinden müssen.

Hinweis Kennzeichnen Sie die Subnetze entsprechend, z. B.

Management-Subnetz, Uplink-Subnetz, Dowlink-Subnetz, da Sie die Subnetze auswählen müssen, wenn Sie PCG in dieser VPC bereitstellen.

Weitere Informationen finden Sie unter [Bereitstellen oder Verknüpfen von NSX Public Cloud Gateways](#).

- 2 Stellen Sie sicher, dass Sie über ein Internetgateway (IGW) verfügen, das mit dieser VPC verknüpft ist.
- 3 Stellen Sie sicher, dass in der Routingtabelle für die VPC das **Ziel** auf **0.0.0.0/0** gesetzt ist und das **Zielgerät** das an die VPC angeschlossene IGW ist.
- 4 Stellen Sie sicher, dass Sie für diese VPC DNS-Auflösung und DNS-Hostnamen aktiviert haben.

Ihr Public Cloud-Konto hinzufügen

Um Ihre Public Cloud-Bestandsliste hinzuzufügen, müssen Sie in Ihrer Public Cloud Rollen erstellen, um den Zugriff auf NSX Cloud zu ermöglichen, und dann die erforderlichen Informationen in CSM hinzufügen.

Einrichten eines sicheren Zugriffs auf Ihre Microsoft Azure-Bestandsliste

Damit NSX Cloud im Rahmen Ihres Abonnements funktioniert, richten Sie einen Service Principal ein, welcher die erforderlichen Berechtigungen gewährt, sowie Rollen für CSM und PCG basierend auf der Microsoft Azure-Funktion für die Verwaltung von Identitäten für Azure-Ressourcen.

Hinweis Wenn Sie bereits ein AWS-Konto zu CSM hinzugefügt haben, aktualisieren Sie den MTU-Wert in **NSX Manager > Fabric > Profil > Uplink-Profile > PCG-Uplink-Host-Switch-Profil** auf 1500, bevor Sie das Microsoft Azure-Konto hinzufügen. Dies kann auch über die NSX Manager-REST-APIs erfolgen.

Übersicht:

- Ihr Microsoft Azure-Abonnement enthält ein oder mehrere VNets, die unter NSX-T Data Center-Verwaltung gestellt werden sollen. Das VNet befindet sich möglicherweise im Übergangsmodus (Transit) oder im Computing-Modus. Im Transit-VNet stellen Sie das PCG bereit. Sie können andere VNets mit dem Transit-VNet verknüpfen und das Onboarding für die darin gehosteten Workload-VMs vornehmen. Die mit dem Transit-VNet verknüpften VNets werden als Computing-VNets bezeichnet.
- NSX Cloud bietet ein PowerShell-Skript, um den Service Principal zu generieren, sowie Rollen, welche die Funktion der verwalteten Identität von Microsoft Azure verwenden, um die Authentifizierung zu verwalten, während Ihre Microsoft Azure-Anmeldedaten gut geschützt sind. Sie können mit diesem Skript auch mehrere Abonnements unter einem Service Principal aufnehmen.
- Sie haben die Möglichkeit, den Service Principal für all Ihre Abonnements wiederzuverwenden oder nach Bedarf neue Service Principals zu erstellen. Es gibt ein zusätzliches Skript für den Fall, dass Sie separate Service Principals für weitere Abonnements erstellen möchten.
- Für mehrere Abonnements müssen Sie, ganz gleich, ob Sie einen einzelnen Service Principal für alle oder mehrere Service Principals verwenden, die JSON-Dateien für die Rollen CSM und PCG aktualisieren, um jeden zusätzlichen Abonnementnamen unter dem Abschnitt *AssignableScopes* hinzuzufügen.
- Wenn Sie bereits über einen NSX Cloud Service Principal in Ihrem VNet verfügen, können Sie ihn aktualisieren, indem die Skripte erneut ausführen und dabei den Service Principal-Namen in den Parametern auslassen.
- Der Service Principal-Name muss für Ihr Microsoft Azure Active Directory eindeutig sein. Sie können den gleichen Service Principal in verschiedenen Abonnements unter der gleichen Active Directory-Domäne oder unterschiedliche Service Principals pro Abonnement verwenden. Sie können jedoch nicht zwei Service Principals mit demselben Namen erstellen.
- Sie müssen der Eigentümer sein oder über Berechtigungen zum Erstellen und Zuweisen von Rollen in allen Microsoft Azure-Abonnements verfügen.
- Die folgenden Szenarien werden unterstützt:
 - **Szenario 1:** Sie verfügen über ein einzelnes Microsoft Azure-Abonnement, das Sie mit NSX Cloud aktivieren möchten.

- **Szenario 2:** Sie verfügen über mehrere Microsoft Azure-Abonnements unter demselben Microsoft Azure-Verzeichnis, die Sie mit NSX Cloud aktivieren möchten, Sie möchten jedoch für all Ihre Abonnements nur einen einzigen NSX Cloud Service Principal verwenden.
- **Szenario 3:** Sie verfügen über mehrere Microsoft Azure-Abonnements unter demselben Microsoft Azure-Verzeichnis, die Sie mit NSX Cloud aktivieren möchten, Sie möchten jedoch unterschiedliche NSX Cloud Service Principal-Namen für unterschiedliche Abonnements verwenden.

Es folgt eine Übersicht des Prozesses:

- 1 Verwenden Sie das NSX Cloud PowerShell-Skript:
 - Erstellen Sie ein Service Principal-Konto für NSX Cloud.
 - Eine Rolle für CSM erstellen.
 - Eine Rolle für PCG erstellen.
- 2 (Optional) Erstellen Sie Service Principals für andere Abonnements, die Sie verknüpfen möchten.
- 3 Fügen Sie das Microsoft Azure-Abonnement zu CSM hinzu.

Hinweis Wenn Sie mehrere Abonnements verwenden, müssen Sie, egal ob Sie denselben oder unterschiedliche Service Principals verwenden, jedes Abonnement separat in CSM hinzufügen.

Generieren des Service Principal und von Rollen

NSX Cloud bietet PowerShell-Skripte, mit denen Sie den erforderlichen Dienstprinzipal und die Rollen für ein oder mehrere Abonnements generieren können.

Voraussetzungen

- Sie müssen PowerShell 5.0+ mit dem AzureRM-Modul installiert haben.
- Sie müssen der Eigentümer sein oder über Berechtigungen zum Erstellen und Zuweisen von Rollen in allen Microsoft Azure-Abonnements verfügen.

Hinweis Die Antwortzeiten von Microsoft Azure können dazu führen, dass das Skript beim ersten Ausführen fehlschlägt. Wenn das Skript fehlschlägt, versuchen Sie es erneut auszuführen.

Verfahren

- 1 Laden Sie auf einem Windows-Desktop oder -Server die ZIP-Datei `CreateNSXCloudCredentials.zip` von der NSX-T Data Center-**Download-Seite > Treiber & Tools > NSX-Cloud-Skripte > Microsoft Azure** herunter.

2 Entpacken Sie den folgenden Inhalt der ZIP-Datei in Ihr Windows-System:

Skript/Datei	Beschreibung
CreateNSXRoles.ps1	<p>Das PowerShell-Skript zum Generieren des NSX Cloud Dienstprinzips und der verwalteten Identitätsrollen für CSM und PCG. Dieses Skript verwendet die folgenden Parameter:</p> <ul style="list-style-type: none"> ■ <code>-subscriptionId <the Transit_VNet's_Azure_subscription_ID></code> ■ (optional) <code>-servicePrincipalName <Service_Principal_Name></code> ■ (optional) <code>-useOneServicePrincipal</code>
AddServicePrincipal.ps1	<p>Ein optionales Skript, das erforderlich ist, wenn Sie jedem Abonnement mehrere Abonnements hinzufügen und verschiedene Dienstprinzipale zuweisen möchten. Weitere Informationen finden Sie unter Szenario 3 in den folgenden Schritten. Dieses Skript verwendet die folgenden Parameter:</p> <ul style="list-style-type: none"> ■ <code>-computeSubscriptionId <the_Compute_VNet's_Azure_subscription_ID></code> ■ <code>-transitSubscriptionId <the Transit_VNet's_Azure_Subscription_ID></code> ■ <code>-csmRoleName <CSM_Role_Name></code> ■ <code>-servicePrincipalName <Service_Principal_Name></code>
nsx_csm_role.JSON	<p>Eine JSON-Vorlage für den Namen und die Berechtigungen der CSM-Rolle. Diese Datei ist als Eingabe in das PowerShell-Skript erforderlich und muss sich im selben Ordner wie das Skript befinden.</p>
nsx_pcg_role.JSON	<p>Eine JSON-Vorlage für den Namen und die Berechtigungen der PCG-Rolle. Diese Datei ist als Eingabe in das PowerShell-Skript erforderlich und muss sich im selben Ordner wie das Skript befinden.</p> <p>Hinweis Der PCG-(Gateway-)Rollenname ist standardmäßig <code>nsx-pcg-role</code>. Sie müssen diesen Wert beim Hinzufügen Ihres Abonnements in CSM angeben.</p>

3 **Szenario 1:** Sie verfügen über ein einzelnes Microsoft Azure-Abonnement, das Sie mit NSX Cloud aktivieren möchten.

- Wechseln Sie aus einer PowerShell-Instanz in das Verzeichnis, in das Sie die Microsoft Azure-Skripte und die JSON-Dateien heruntergeladen haben.
- Führen Sie das Skript mit dem Namen „CreateNSXRoles.ps1“ mit dem Parameter `-SubscriptionId` wie folgt aus:

```
.\CreateNSXRoles.ps1 -subscriptionId <the_single_Azure_subscription_ID>
```

Hinweis Wenn Sie den Service Principal-Standardnamen `nsx-service-admin` überschreiben möchten, können Sie auch den Parameter `-servicePrincipalName` verwenden. Der SPN muss in Ihrem Microsoft Azure Active Directory eindeutig sein.

- 4 Szenario 2:** Sie verfügen über mehrere Microsoft Azure-Abonnements unter demselben Microsoft Azure-Verzeichnis, die Sie mit NSX Cloud aktivieren möchten, Sie möchten jedoch für all Ihre Abonnements nur einen einzigen NSX Cloud Service Principal verwenden.

- a Wechseln Sie aus einer PowerShell-Instanz in das Verzeichnis, in das Sie die Microsoft Azure-Skripte und die JSON-Dateien heruntergeladen haben.
- b Bearbeiten Sie jede der JSON-Dateien, um eine Liste anderer Abonnement-IDs unter dem Abschnitt mit dem Titel „*AssignableScopes*“ hinzuzufügen, beispielsweise:

```
"AssignableScopes": [
  "/subscriptions/aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee",
  "/subscriptions/aaaaaaaa-bbbb-cccc-dddd-ffffffffffff",
  "/subscriptions/aaaaaaaa-bbbb-cccc-dddd-000000000000"
```

Hinweis Sie müssen das im Beispiel gezeigte Format verwenden, um Abonnement-IDs hinzuzufügen: `"/subscriptions/<Subscription_ID>"`

- c Führen Sie das Skript mit dem Namen `CreateNSXRoles.ps1` mit den Parametern `-subscriptionID` und `-useOneServicePrincipal` aus:

```
.\CreateNSXRoles.ps1 -subscriptionId <the_Transit_VNet's_Azure_subscription_ID> -
useOneServicePrincipal
```

Hinweis Lassen Sie den Dienstprinzipalnamen hier weg, wenn Sie den Standardnamen verwenden möchten: `nsx-service-admin`. Wenn dieser Dienstprinzipalname bereits in Ihrem Microsoft Azure Active Directory vorhanden ist, führt die Ausführung dieses Skripts ohne Dienstprinzipalnamen dazu, dass der Dienstprinzipal aktualisiert wird.

- 5 Szenario 3:** Sie verfügen über mehrere Microsoft Azure-Abonnements unter demselben Microsoft Azure-Verzeichnis, die Sie mit NSX Cloud aktivieren möchten, Sie möchten jedoch unterschiedliche NSX Cloud Service Principal-Namen für unterschiedliche Abonnements verwenden.

- a Wechseln Sie aus einer PowerShell-Instanz in das Verzeichnis, in das Sie die Microsoft Azure-Skripte und die JSON-Dateien heruntergeladen haben.
- b Führen Sie die Schritte **b** und **c** aus dem zweiten Szenario aus, um in jeder der JSON-Dateien mehrere Abonnements zum Abschnitt „*AssignableScopes*“ hinzuzufügen.

- c Führen Sie das Skript mit dem Namen `CreateNSXRoles.ps1` mit dem Parameter `-subscriptionID` aus:

```
.\CreateNSXRoles.ps1 -subscriptionId <One of the subscription_IDs>
```

Hinweis Lassen Sie den Dienstprinzipalnamen hier weg, wenn Sie den Standardnamen verwenden möchten: `nsx-service-admin`. Wenn dieser Dienstprinzipalname in Ihrem Microsoft Azure Active Directory vorhanden ist, führt die Ausführung dieses Skripts ohne Dienstprinzipalnamen dazu, dass der Dienstprinzipal aktualisiert wird.

- d Führen Sie das Skript mit dem Namen `AddServicePrincipal.ps1` mit den folgenden Parametern aus:

Parameter	Wert
<code>-computeSubscriptionId</code>	Die Azure-Abonnement-ID von Compute_VNet
<code>-transitSubscriptionId</code>	Die Azure-Abonnement-ID des Transit-VNet
<code>-csmRoleName</code>	Sie können diesen Wert aus der Datei <code>nsx_csm_role.JSON</code> beziehen.
<code>-servicePrincipalName</code>	Neuer Dienstprinzipalname

```
./AddServicePrincipal.ps1 -computeSubscriptionId <the_Compute_VNet's_Azure_subscription_ID>
-transitSubscriptionId <the_Transit_VNet's_Azure_Subscription_ID>
-csmRoleName <CSM_Role_Name>
-servicePrincipalName <new_Service_Principal_Name>
```

- 6 Suchen Sie nach einer Datei im selben Verzeichnis, in dem Sie das PowerShell-Skript ausgeführt haben. Sie heißt in etwa: `NSXCloud_ServicePrincipal_<your_subscription_ID>_<NSX_Cloud_Service_Principal_name>`. Diese Datei enthält Informationen, die Sie benötigen, um Ihr Microsoft Azure-Abonnement in CSM hinzuzufügen.

- Client-ID
- Client-Schlüssel
- Mandanten-ID
- Abonnement-ID

Ergebnisse

Es werden die folgenden Konstrukte erstellt:

- eine Azure-AD-Anwendung für NSX Cloud.
- einen Azure Resource Manager Service Principal für die NSX Cloud-Anwendung.
- eine Rolle für CSM, die dem Service-Principal-Konto zugeordnet ist.
- eine Rolle für PCG, um die Arbeit an Ihrem Public-Cloud-Bestand zu ermöglichen.

- Eine Datei mit einem Namen wie `NSXCloud_ServicePrincipal_<your_subscription_ID>_<NSX_Cloud_Service_Principal_name>` wird in demselben Verzeichnis erstellt, in dem Sie das PowerShell-Skript ausgeführt haben. Diese Datei enthält Informationen, die Sie benötigen, um Ihr Microsoft Azure-Abonnement in CSM hinzuzufügen.

Hinweis In den JSON-Dateien, die zum Erstellen der Rollen CSM und PCG verwendet werden, finden Sie eine Liste der Berechtigungen, die ihnen nach dem Erstellen der Rollen zur Verfügung stehen.

Nächste Schritte

Ihr Microsoft-Azure-Abonnement in CSM hinzufügen

Hinweis Beim Aktivieren von NSX Cloud für mehrere Abonnements müssen Sie jedes separate Abonnement einzeln dem CSM hinzufügen. Wenn Sie beispielsweise insgesamt über fünf Abonnements verfügen, müssen Sie fünf Microsoft Azure-Konten in CSM hinzufügen, wobei alle anderen Werte gleich, die Abonnement-IDs jedoch unterschiedlich sind.

Ihr Microsoft-Azure-Abonnement in CSM hinzufügen

Nachdem Sie über die Details des NSX Cloud Service Principal und der CSM- und PCG-Rollen verfügen, können Sie Ihr Microsoft Azure-Abonnement in CSM hinzufügen.

Voraussetzungen

- Sie müssen in NSX-T Data Center über die Rolle „Enterprise-Administrator“ verfügen.
- Sie müssen über die Ausgabe des PowerShell-Skripts mit Details zum NSX Cloud Service Principal verfügen.
- Sie müssen den Wert der PCG-Rolle kennen, den Sie beim Ausführen des PowerShell-Skripts angegeben haben, um die Rollen und den Service Principal zu erstellen. Der Standardwert ist `nsx-pcg-role`.

Verfahren

- 1 Melden Sie sich unter Verwendung eines Kontos mit der Rolle „Enterprise-Administrator“ bei CSM an.
- 2 Wechseln Sie zu **CSM > Clouds > Azure**.
- 3 Klicken Sie auf **+ Hinzufügen** und geben Sie die folgenden Details an:

Option	Beschreibung
Name	Geben Sie einen geeigneten Namen an, um dieses Konto in CSM zu identifizieren. Sie können über mehrere Microsoft Azure-Abonnements verfügen, denen dieselbe Microsoft Azure-Mandanten-ID zugeordnet ist. Benennen Sie Ihr Konto, Sie können Konten in CSM entsprechend benennen, z. B. Azure-DevOps-Konto, Azure-Finance-Konto usw.
Client-ID	Kopieren Sie diesen Wert und fügen Sie ihn aus der Ausgabe des PowerShell-Skripts ein.

Option	Beschreibung
Schlüssel	Kopieren Sie diesen Wert und fügen Sie ihn aus der Ausgabe des PowerShell-Skripts ein.
Abonnement-ID	Kopieren Sie diesen Wert und fügen Sie ihn aus der Ausgabe des PowerShell-Skripts ein.
Mandanten-ID	Kopieren Sie diesen Wert und fügen Sie ihn aus der Ausgabe des PowerShell-Skripts ein.
Gateway-Rollenname	Der Standardwert ist <code>nsx-pcg-role</code> . Dieser Wert ist aus der Datei <code>nsx_pcg_role.json</code> verfügbar, wenn Sie die Standardeinstellung geändert haben.
Cloud-Tags	Standardmäßig ist diese Option aktiviert und erlaubt es, dass Ihre Microsoft Azure-Tags in NSX Manager angezeigt werden

4 Klicken Sie auf **Speichern**.

CSM fügt das Konto hinzu, und nach drei Minuten können Sie es im Bereich **Konten** sehen.

Nächste Schritte

[Bereitstellen von PCG in einem selbstverwalteten VNet oder einem Transit-VNet](#)

Einrichten eines sicheren Zugriffs auf Ihre Microsoft Azure-Bestandsliste

Möglicherweise verfügen Sie über ein oder mehrere AWS-Konten mit VPCs und Workload-VMs, die Sie unter NSX-T Data Center-Verwaltung möchten.

Übersicht:

- Sie können die Transit-/Computing-VPC-Topologie, bei der Sie das PCG in einer VPC bereitstellen, nutzen, wodurch Sie sie zur Transit-VPC machen und andere VPCs, so genannte Computing-VPCs, damit verknüpfen.
- NSX Cloud liefert ein Shell-Skript, das Sie von der AWS-CLI Ihres AWS-Kontos ausführen können, um das IAM-Profil und die Rolle anzulegen und um eine vertrauenswürdige Beziehung für Transit- und Computing-VPCs erstellen zu können.
- Die folgenden Szenarien werden unterstützt:
 - **Szenario 1:** Sie möchten ein einzelnes AWS-Konto mit NSX Cloud verwenden.
 - **Szenario 2:** Sie möchten mehrere Unterkonten auf dem AWS nutzen, die von einem AWS-Hauptkonto verwaltet werden.
 - **Szenario 3:** Sie möchten mehrere AWS-Konten mit der NSX Cloud verwenden.

Es folgt eine Übersicht des Prozesses:

- 1 Verwenden Sie das NSX Cloud-Shell-Skript, das die AWS-CLI erfordert, für folgende Aufgaben:
 - Ein Uplink-Profil erstellen.
 - Eine Rolle für PCG erstellen.

- (Optional) Eine vertrauenswürdige Beziehung zwischen dem AWS-Konto, das die Transit-VPC hostet, und dem AWS-Konto, das die Computing-VPC hostet, erstellen.

2 Das AWS-Konto in CSM hinzufügen.

Generieren des IAM-Profiles und der PCG-Rolle

NSX Cloud enthält ein SHELL-Skript, um die Einrichtung von einem oder mehreren Ihrer AWS-Konten durch das Anlegen eines IAM-Profiles und einer Rolle für das PCG zu vereinfachen. Letztere ist an das Profil angehängt, welches die erforderlichen Berechtigungen für Ihr AWS-Konto liefert.

Wenn Sie vorhaben, eine Transit-VPC mit mehreren Computing-VPCs in zwei verschiedenen AWS-Konten zu verknüpfen, können Sie das Skript zum Erstellen einer vertrauenswürdigen Beziehung zwischen diesen Konten verwenden.

Hinweis Der PCG-(Gateway-)Rollenname ist standardmäßig `nsx_pcg_service`. Wenn Sie einen anderen Wert für den Gateway-Rollenname möchten, können Sie ihn im Skript ändern, notieren Sie sich diesen Wert jedoch, da er für das Hinzufügen des AWS-Kontos zur CSM erforderlich ist.

Voraussetzungen

Bevor Sie das Skript ausführen, müssen Sie auf Ihrem Linux-System oder einem kompatiblen System Folgendes installiert und konfiguriert haben:

- AWS-CLI
- jq (ein JSON-Parser)
- openssl

Hinweis Wenn Sie mehrere AWS-Konten verwenden, müssen die Konten mit einer geeigneten Methode mittels Peering verbunden werden.

Verfahren

- 1 Laden Sie auf einem Linux- oder kompatiblen Desktop oder Server das SHELL-Skript mit dem Namen `nsx_csm_iam_script.sh` von der NSX-T Data Center-**Download-Seite > Treiber & Tools > NSX Cloud-Skripte > AWS** herunter.
- 2 **Szenario 1:** Sie möchten ein einzelnes AWS-Konto mit NSX Cloud verwenden.
 - a Führen Sie das Skript aus, beispielsweise:

```
bash nsx_csm_iam_script.sh
```

- b Geben Sie bei entsprechender Aufforderung mit der Frage `Do you want to create an IAM user for CSM and an IAM role for PCG? [yes/no]` `yes` ein.

- c Geben Sie bei der Frage `What do you want to name the IAM User?` einen Namen für den IAM-Benutzer ein.

Hinweis Der IAM-Benutzername muss in Ihrem AWS-Konto eindeutig sein.

- d Geben Sie bei der Frage `Do you want to add trust relationship for any Transit VPC account?` `[yes/no]`no ein.

Wenn das Skript erfolgreich ausgeführt wird, werden das IAM-Profil und eine Rolle für PCG in Ihrem AWS-Konto erstellt. Die Werte werden in der Ausgabedatei `aws_details.txt` in demselben Verzeichnis gespeichert, in dem Sie das Skript ausgeführt haben. Im nächsten Schritt führen Sie die Anweisungen unter [Ihr AWS-Konto zu CSM hinzufügen](#) und dann [Bereitstellen von PCG in einer selbstverwalteten VPC oder Transit-VPC](#) aus, um die Einrichtung einer Transit-VPC oder selbstverwalteten VPC abzuschließen.

3 **Szenario 2:** Sie möchten mehrere Unterkonten auf dem AWS nutzen, die von einem AWS-Hauptkonto verwaltet werden.

- a Führen Sie das Skript über Ihr AWS-Hauptkonto aus.

```
bash nsx_csm_iam_script.sh
```

- b Geben Sie bei entsprechender Aufforderung mit der Frage `Do you want to create an IAM user for CSM and an IAM role for PCG?` `[yes/no]` yes ein.
- c Geben Sie bei der Frage `What do you want to name the IAM User?` einen Namen für den IAM-Benutzer ein.

Hinweis Der IAM-Benutzername muss in Ihrem AWS-Konto eindeutig sein.

- d Geben Sie bei der Frage `Do you want to add trust relationship for any Transit VPC account?` `[yes/no]`no ein.

Hinweis Mit einem AWS-Hauptkonto müssen Sie, wenn Ihre Transit-VPC die Berechtigung zum Anzeigen von Computing-VPCs in den Unterkonten hat, keine vertrauenswürdige Beziehung zu Ihren Unterkonten mehr herstellen. Befolgen Sie andernfalls die Schritte für **Szenario 3**, um mehrere Konten einzurichten.

Wenn das Skript erfolgreich ausgeführt wird, werden das IAM-Profil und eine Rolle für das PCG in Ihrem AWS-Hauptkonto erstellt. Die Werte werden in der Ausgabedatei im selben Verzeichnis gespeichert, in dem Sie das Skript ausgeführt haben. Der Dateiname lautet `aws_details.txt`. Im nächsten Schritt führen Sie die Anweisungen unter [Ihr AWS-Konto zu CSM hinzufügen](#) und dann [Bereitstellen von PCG in einer selbstverwalteten VPC oder Transit-VPC](#) aus, um die Einrichtung einer Transit-VPC oder selbstverwalteten VPC abzuschließen.

4 Szenario 3: Sie möchten mehrere AWS-Konten mit der NSX Cloud verwenden.

Hinweis Stellen Sie sicher, dass die AWS-Konten mittels Peering verbunden sind, bevor Sie fortfahren.

- a Notieren Sie sich die 12-stellige AWS-Kontonummer für das Konto, auf dem Sie die Transit-VPC hosten möchten.
- b Richten Sie die Transit-VPC im AWS-Konto ein, indem Sie die Schritte a bis d für *Szenario 1* befolgen. Schließen Sie das Verfahren zum Hinzufügen des Kontos in CSM und Bereitstellen eines PCG darin ab.
- c Laden Sie das Skript NSX Cloud von einem Linux-System oder einem kompatiblen System in Ihrem anderen AWS-Konto, auf dem Sie die Computing-VPCs hosten möchten, herunter und führen Sie es aus.

Hinweis Alternativ können Sie die AWS-Profile mit anderen Konto-Anmeldedaten nutzen, um so das Skript für Ihr anderes AWS-Konto wieder unter Verwendung desselben Systems auszuführen.

- d Geben Sie bei der Frage `Do you want to create an IAM user for CSM and an IAM role for PCG?` [yes/no] `yes` ein.

Hinweis Wenn Sie dieses AWS-Konto bereits im CSM hinzugefügt haben und das Skript für die Verbindung mit einem anderen AWS-Konto wiederverwenden möchten, können Sie `no` eingeben und das Anlegen des IAM-Benutzers überspringen.

- e Geben Sie bei der Frage `What do you want to name the IAM User?` einen Namen für den IAM-Benutzer ein.

Hinweis Der IAM-Benutzername muss in Ihrem AWS-Konto eindeutig sein.

- f Geben Sie bei der Frage `Do you want to add trust relationship for any Transit VPC account?` [yes/no] `yes` ein.
- g Geben Sie die 12-stellige AWS-Kontonummer, die Sie sich bei der Frage `What is the Transit VPC account number?` in Schritt 1 notiert haben, ein bzw. kopieren und fügen Sie sie ein.

Eine vertrauenswürdige IAM-Beziehung wird zwischen den beiden AWS-Konten eingerichtet, und es wird eine externe ID (ExternalID) vom Skript generiert.

Wenn das Skript erfolgreich ausgeführt wird, werden das IAM-Profil und eine Rolle für das PCG in Ihrem AWS-Hauptkonto erstellt. Die Werte werden in der Ausgabedatei im selben Verzeichnis gespeichert, in dem Sie das Skript ausgeführt haben. Der Dateiname lautet `aws_details.txt`. Im nächsten Schritt führen Sie die Anweisungen unter [Ihr AWS-Konto zu CSM hinzufügen](#) und dann unter [Verknüpfung mit einer Transit-VPC oder einem Transit-VNet](#) aus, um die Verknüpfung mit einer Transit-VPC abzuschließen.

Ihr AWS-Konto zu CSM hinzufügen

Fügen Sie Ihr AWS-Konto mithilfe der vom Skript generierten Werte hinzu.

Verfahren

- 1 Melden Sie sich bei CSM mit der Rolle „Enterprise-Administrator“ an.
- 2 Navigieren Sie zu **CSM > Clouds > AWS**.
- 3 Klicken Sie auf **+Hinzufügen** und geben Sie mit Hilfe der Ausgabedatei `aws_details.txt`, die aus dem Skript NSX Cloud generiert wurde, die folgenden Details ein:

Option	Beschreibung
Name	Geben Sie einen aussagekräftigen Namen für dieses AWS-Konto ein
Zugriffsschlüssel	Geben Sie den Zugriffsschlüssel Ihres Kontos ein
Geheimer Schlüssel	Geben Sie den geheimen Schlüssel Ihres Kontos ein
Cloud-Tags	Standardmäßig ist diese Option aktiviert und ermöglicht es, dass Ihre AWS-Tags in NSX Manager angezeigt werden
Gateway-Rollenname	Der Standardwert ist <code>nsx_pcg_service</code> . Sie können diesen Wert in der Ausgabe des Skripts in der Datei <code>aws_details.txt</code> finden.

Ergebnisse

Das AWS-Konto wird in CSM hinzugefügt.

In der Registerkarte „VPCs“ von CSM können Sie alle VPCs in Ihrem AWS-Konto einsehen.

In der Registerkarte „Instanzen“ von CSM können Sie die EC2-Instanzen in dieser VPC einsehen.

Nächste Schritte

[Bereitstellen von PCG in einer selbstverwalteten VPC oder Transit-VPC](#)

Bereitstellen oder Verknüpfen von NSX Public Cloud Gateways

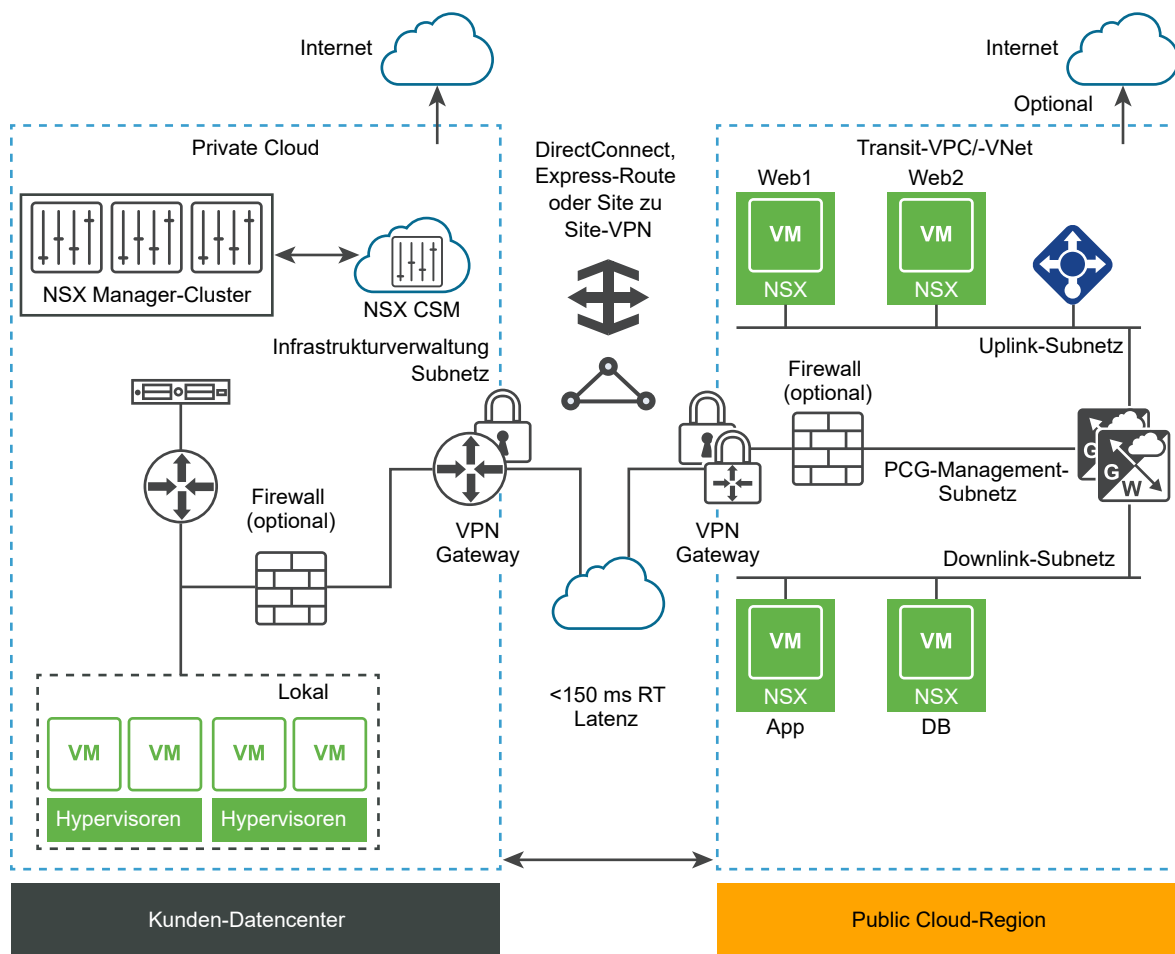
Das NSX Public Cloud Gateway (PCG) ermöglicht Nord-Süd-Konnektivität zwischen der Public Cloud und den lokalen Verwaltungskomponenten von NSX-T Data Center.

Das PCG kann entweder eine eigenständige-Gateway-Appliance sein oder von Ihren Public Cloud-VPCs oder -VNetns gemeinsam genutzt werden, um eine Hub-and-Spoke-Topologie zu erhalten.

Hinweis PCG wird für jede unterstützte Public Cloud in einer einzelnen Standardgröße bereitgestellt:

Public Cloud	PCG-Instanztyp
AWS	C4.xlarge Hinweis Einige Regionen unterstützen den Typ der C4.xlarge-Instanz möglicherweise nicht. Einzelheiten finden Sie in der AWS-Dokumentation.
Microsoft Azure	Standard-DS3 Version 2

Abbildung 11-2. Die Architektur von NSX Public Cloud Gateway



Transit- oder selbstverwaltete(s) VPC oder -VNet: Wenn Sie das PCG in einer VPC oder einem VNet bereitstellen, wird die VPC oder das VNet als *selbstverwaltet* qualifiziert, d. h. Sie können VMs, die in dieser VPC oder diesem VNet gehostet werden, unter NSX-Verwaltung stellen. Diese VPC bzw. dieses VNet wird auch als *Transit-VPC* oder -VNet qualifiziert, da Sie das darauf bereitgestellte PCG für das

Onboarding der in anderen VPCs oder VNets gehosteten VMs nutzen können. Das PCG nutzt die folgenden Subnetze, die Sie in Ihrem VPC/VNet eingerichtet haben. Siehe [Ihr Microsoft Azure-Netzwerk mit Ihrer lokalen NSX-T Data Center-Bereitstellung verbinden](#) oder [Ihr Amazon Web Services-Netzwerk \(AWS-Netzwerk\) mit Ihrer lokalen NSX-T Data Center-Bereitstellung verbinden](#).

- **Management-Subnetz:** Dieses Subnetz wird für das Management des Datenverkehrs zwischen lokalen NSX-T Data Center und PCG verwendet. Der empfohlene Bereich ist /28.
- **Uplink-Subnetz:** Dieses Subnetz wird für den Nord-Süd-Internetverkehr genutzt. Der empfohlene Bereich ist /24.
- **Downlink-Subnetz:** Dieses Subnetz umfasst den IP-Adressbereich der Workload-VMs und sollte entsprechend dimensioniert werden. Beachten Sie, dass Sie für Debugging-Zwecke eventuell zusätzliche Schnittstellen auf den Arbeitslast-VMs einbinden müssen.

Computing-VPC oder -VNet: VPCs oder VNets, auf denen das PCG nicht bereitgestellt ist, jedoch über eine Verknüpfung zu einer Transit-VPC oder einem Transit-VNet verfügen, werden als *Computing-VPCs* oder -VNets bezeichnet.

Die PCG-Bereitstellung orientiert sich an Ihrem Netzwerkadressierungsplan mit FQDNs für die NSX-T Data Center-Komponenten und einem DNS-Server, der diese FQDNs auflösen kann.

Hinweis Es wird nicht empfohlen, IP-Adressen für die Verbindung der Public Cloud mit NSX-T Data Center unter Verwendung eines PCGs zu verwenden. Sollten Sie diese Option jedoch wählen, ändern Sie bitte nicht Ihre IP-Adressen.

Bereitstellen von PCG in einem selbstverwalteten VNet oder einem Transit-VNet

Folgen Sie diesen Anweisungen, um PCG in Ihrem Microsoft Azure-VNet bereitzustellen.

Das VNet, in dem Sie PCG bereitstellen, kann als ein Transit-VNet fungieren, mit dem sich andere VNets (so genannte Computing-VNets) verbinden können. Dieses VNet kann auch VMs verwalten und als ein selbstverwaltetes VNet fungieren.

Folgen Sie diesen Anweisungen, um PCGbereitzustellen. Wenn Sie eine Verknüpfung mit einem vorhandenen Transit-VNet herstellen möchten, finden Sie weitere Informationen dazu unter [Verknüpfung mit einer Transit-VPC oder einem Transit-VNet](#).

Voraussetzungen

- Ihre Public Cloud-Konten müssen bereits in CSM hinzugefügt worden sein.
- In dem VNet, in dem Sie PCG bereitstellen, müssen die erforderlichen Subnetze für die Hochverfügbarkeit angepasst sein: *Uplink*, *Downlink* und *Verwaltung*.

Verfahren

- 1 Melden Sie sich unter Verwendung eines Kontos mit der Rolle „Enterprise-Administrator“ bei CSM an.
- 2 Klicken Sie auf **Clouds > Azure** und navigieren Sie zur Registerkarte **VNets**.

- 3 Klicken Sie auf ein VNet, in dem Sie ein PCG bereitstellen möchten.
- 4 Klicken Sie auf **Gateways bereitstellen**. Der Assistent **Primäres Gateway bereitstellen** wird geöffnet.
- 5 Verwenden Sie für allgemeine Eigenschaften die folgenden Richtlinien:

Option	Beschreibung
Öffentlicher SSH-Schlüssel	Geben Sie einen öffentlichen SSH-Schlüssel an, der während der Bereitstellung des PCGs validiert werden kann. Dies ist für jede PCG-Bereitstellung erforderlich.
Quarantäne-Richtlinie für das zugehörige VNet	Belassen Sie dies im Standardmodus deaktiviert , wenn Sie das PCG erstmalig bereitstellen. Sie können diesen Wert nach Onboarding von VMs ändern. Weitere Informationen finden Sie unter Verwalten der Quarantäne-Richtlinie im <i>Administratorhandbuch für NSX-T Data Center</i> .
Lokales Speicherkonto	<p>Wenn Sie CSM ein Microsoft Azure-Abonnement hinzufügen, steht CSM eine Liste Ihrer Microsoft Azure-Speicherkonten zur Verfügung. Wählen Sie im Dropdown-Menü das Speicherkonto aus. Wenn Sie mit der Bereitstellung des PCGs fortfahren, kopiert CSM die öffentlich verfügbare VHD des PCGs in dieses Speicherkonto der ausgewählten Region.</p> <p>Hinweis Wenn das VHD-Image bereits für eine frühere PCG-Bereitstellung in dieses Speicherkonto in der Region kopiert wurde, wird das Image von diesem Speicherort aus für nachfolgende Bereitstellungen verwendet, um die gesamte Bereitstellungszeit zu verkürzen.</p>
VHD-URL	<p>Wenn Sie ein anderes PCG-Image verwenden möchten, das im öffentlichen VMware-Repository nicht verfügbar ist, können Sie die URL der PCG-VHD hier eingeben. Die VHD-Datei muss im selben Konto und derselben Region, in dem/der dieses VNet erstellt wird, vorhanden sein.</p> <p>Hinweis Die VHD muss das richtige URL-Format aufweisen. Es wird empfohlen, die Option Zum Kopieren klicken in Microsoft Azure zu verwenden.</p>
Proxyserver	<p>Wählen Sie einen Proxy-Server aus, der für den internetgebundenen Datenverkehr von diesem PCG verwendet werden soll. Die Proxy-Server werden in CSM konfiguriert. Sie können denselben Proxy-Server auswählen wie CSM, falls vorhanden, oder wählen Sie einen anderen Proxy-Server aus CSM, oder wählen Sie Kein Proxy-Server.</p> <p>Weitere Informationen zur Konfiguration von Proxy-Servern in CSM finden Sie unter (Optional) Proxy-Server konfigurieren.</p>
Erweitert	Die erweiterten DNS-Einstellungen bieten Flexibilität bei der Auswahl der DNS-Server zum Auflösen von NSX-T Data Center-Verwaltungskomponenten.
Über DHCP des Public-Cloud-Anbieters beziehen	Wählen Sie diese Option, wenn Sie Microsoft Azure-DNS-Einstellungen verwenden möchten. Dies ist die Standardeinstellung für DNS, wenn Sie keine der anderen Optionen auswählen, um dies zu überschreiben.

Option	Beschreibung
DNS-Server des Public-Cloud-Anbieters überschreiben	Wählen Sie diese Option, wenn Sie die IP-Adresse(n) eines oder mehrerer DNS-Server zum Auflösen von NSX-T Data Center-Appliances sowie der Workload-VMs in diesem VNet manuell eingeben möchten.
DNS-Server des Public-Cloud-Anbieters nur für NSX-T Data Center-Appliances verwenden	Wählen Sie diese Option, wenn Sie den Microsoft Azure-DNS-Server für die Auflösung der NSX-T Data Center-Verwaltungskomponenten verwenden möchten. Mit dieser Einstellung können Sie zwei DNS-Server verwenden: einen für das PCG, der NSX-T Data Center-Appliances auflöst, einen anderen für das VNet, der Ihre Workload-VMs in diesem VNet auflöst.

6 Klicken Sie auf **Weiter**.

7 Verwenden Sie für **Subnetze** die folgenden Richtlinien:

Option	Beschreibung
HA für NSX Cloud-Gateway aktivieren	Wählen Sie diese Option, um Hochverfügbarkeit zu ermöglichen.
Subnetze	Wählen Sie diese Option, um Hochverfügbarkeit zu ermöglichen.
Öffentliche IP für Management-Netzwerkkarte (Mgmt NIC)	Wählen Sie Neue IP-Adresse zuteilen , um der Management-Netzwerkkarte eine öffentliche IP-Adresse bereitzustellen. Sie können die öffentliche IP-Adresse manuell bereitstellen, wenn Sie eine freie öffentliche IP-Adresse wiederverwenden möchten.
Öffentliche IP für Uplink-Netzwerkkarte (NIC)	Wählen Sie Neue IP-Adresse zuteilen , um der Uplink-Netzwerkkarte (NIC) eine öffentliche IP-Adresse bereitzustellen. Sie können die öffentliche IP-Adresse manuell bereitstellen, wenn Sie eine freie öffentliche IP-Adresse wiederverwenden möchten.

Nächste Schritte

Integrieren Sie Ihre Workload-VMs. Informationen zum Tag-N-Workflow finden Sie unter **Onboarding und Verwalten von Workload-VMs** im *Administratorhandbuch für NSX-T Data Center*.

Bereitstellen von PCG in einer selbstverwalteten VPC oder Transit-VPC

Befolgen Sie die Anweisungen zur Bereitstellung von PCG in Ihrer AWS-VPC.

Die VPC, in der Sie eine PCG bereitstellen, kann als Transit-VPC fungieren, mit der sich andere VPCs (so genannte Computing-VPCs) verbinden können. Diese VPC kann auch VMs verwalten und als eine selbstverwaltete VPC fungieren.

Folgen Sie diesen Anweisungen, um PCGbereitzustellen. Wenn Sie eine Verknüpfung mit einer vorhandenen Transit-VPC herstellen möchten, finden Sie weitere Informationen dazu unter [Verknüpfung mit einer Transit-VPC oder einem Transit-VNet](#).

Voraussetzungen

- Ihre Public Cloud-Konten müssen bereits in CSM hinzugefügt worden sein.

- Auf der VPC, auf der Sie PCG bereitstellen, müssen die erforderlichen Subnetze für die Hochverfügbarkeit angepasst sein: *Uplink*, *Downlink* und *Verwaltung*.
- Die Konfiguration für die Netzwerkzugriffskontrollliste Ihrer VPC muss eine Regel zum ZULASSEN des eingehenden Datenverkehrs enthalten.

Verfahren

- 1 Melden Sie sich unter Verwendung eines Kontos mit der Rolle „Enterprise-Administrator“ bei CSM an.
- 2 Klicken Sie auf **Clouds > AWS > <AWS_account_name>** und öffnen Sie die Registerkarte **VPCs**.
- 3 Wählen Sie auf der Registerkarte **VPCs** einen AWS-Regionsnamen, z. B. us-west. Die AWS-Region muss identisch sein mit der, in der Sie die Computing-VPC erstellt haben.
- 4 Wählen Sie eine für NSX Cloud konfigurierte Computing-VPC aus.
- 5 Klicken Sie auf Gateways bereitstellen.
- 6 Vervollständigen Sie die allgemeinen Gateway-Details:

Option	Beschreibung
PEM-Datei	Wählen Sie eine der PEM-Dateien aus dem Dropdown-Menü aus. Diese Datei muss sich in der gleichen Region befinden, in der NSX Cloud bereitgestellt wurde und in der Sie Ihre Computing-VPC erstellt haben. Dadurch wird Ihr AWS-Konto eindeutig identifiziert.
Quarantäne-Richtlinie für die zugehörige VPC	Belassen Sie dies im Standardmodus deaktiviert , wenn Sie das PCG erstmalig bereitstellen. Sie können diesen Wert nach Onboarding von VMs ändern. Weitere Informationen finden Sie unter Verwalten der Quarantäne-Richtlinie im <i>Administratorhandbuch für NSX-T Data Center</i> .
Proxyserver	Wählen Sie einen Proxy-Server aus, der für den internetgebundenen Datenverkehr von diesem PCG verwendet werden soll. Die Proxy-Server werden in CSM konfiguriert. Sie können denselben Proxy-Server auswählen wie CSM, falls vorhanden, einen anderen Proxy-Server aus CSM auswählen oder Kein Proxy-Server wählen. Weitere Informationen zur Konfiguration von Proxy-Servern in CSM finden Sie unter (Optional) Proxy-Server konfigurieren .
Erweitert	Die erweiterten Einstellungen bieten zusätzliche Optionen, falls erforderlich.
AMI-ID aufheben	Benutzen Sie diese erweiterte Funktion, um eine andere AMI-ID für das PCG zu vergeben als die, die in Ihrem AWS-Konto verfügbar ist.
Über DHCP des Public-Cloud-Anbieters beziehen	Wählen Sie diese Option, wenn Sie AWS-Einstellungen verwenden möchten. Dies ist die Standardeinstellung für DNS, wenn Sie keine der anderen Optionen auswählen, um dies zu überschreiben.

Option	Beschreibung
DNS-Server des Public-Cloud-Anbieters überschreiben	Wählen Sie diese Option, wenn Sie die IP-Adresse(n) eines oder mehrerer DNS-Server zum Auflösen von NSX-T Data Center-Appliances sowie der Workload-VMs in diesem VPC manuell eingeben möchten.
DNS-Server des Public-Cloud-Anbieters nur für NSX-T Data Center-Appliances verwenden	Wählen Sie diese Option, wenn Sie den AWS-DNS-Server für die Auflösung der NSX-T Data Center-Verwaltungskomponenten verwenden möchten. Mit dieser Einstellung können Sie zwei DNS-Server verwenden: einen für das PCG, der NSX-T Data Center-Appliances auflöst, einen anderen für die VPC, der Ihre Workload-VMs in dieser VPC auflöst.

7 Klicken Sie auf Weiter.

8 Vervollständigen Sie die Subnetz-Details.

Option	Beschreibung
HA für Public Cloud Gateway aktivieren	Die empfohlene Einstellung ist „Aktivieren“, wodurch ein hochverfügbares Aktiv/Standby-Paar eingerichtet wird, um ungeplante Ausfallzeiten zu vermeiden.
Primäre Gateway-Einstellungen	Wählen Sie eine Verfügbarkeitszone, wie z. B. us-west-1a, aus dem Dropdown-Menü als primäres Gateway für HA. Weisen Sie die Uplink-, Downlink- und Management-Subnetze aus dem Dropdown-Menü zu.
Sekundäre Gateway-Einstellungen	Wählen Sie eine andere Verfügbarkeitszone, wie z. B. us-west-1b, aus dem Dropdown-Menü als sekundäres Gateway für HA. Das sekundäre Gateway wird verwendet, wenn das primäre Gateway ausfällt. Weisen Sie die Uplink-, Downlink- und Management-Subnetze aus dem Dropdown-Menü zu.
Öffentliche IP für Management-Netzwerkkarte (Mgmt NIC)	Wählen Sie Neue IP-Adresse zuteilen , um der Management-Netzwerkkarte eine öffentliche IP-Adresse bereitzustellen. Sie können die öffentliche IP-Adresse manuell bereitstellen, wenn Sie eine freie öffentliche IP-Adresse wiederverwenden möchten.
Öffentliche IP für Uplink-Netzwerkkarte (NIC)	Wählen Sie Neue IP-Adresse zuteilen , um der Uplink-Netzwerkkarte (NIC) eine öffentliche IP-Adresse bereitzustellen. Sie können die öffentliche IP-Adresse manuell bereitstellen, wenn Sie eine freie öffentliche IP-Adresse wiederverwenden möchten.

Klicken Sie auf Bereitstellen.

9 Überwachen Sie den Status der primären (und sekundären, falls Sie diese ausgewählt haben) PCG-Bereitstellung. Dieser Vorgang kann 10–12 Minuten dauern.

10 Klicken Sie auf Fertig stellen, wenn PCG erfolgreich bereitgestellt wurde.

Nächste Schritte

Integrieren Sie Ihre Workload-VMs. Informationen zum Tag-N-Workflow finden Sie unter **Onboarding und Verwalten von Workload-VMs** im *Administratorhandbuch für NSX-T Data Center*.

Verknüpfung mit einer Transit-VPC oder einem Transit-VNet

Sie können eine oder mehrere Computing-VPCs oder -VNet mit einer Transit-VPC oder -VNet verknüpfen.

Voraussetzungen

- Stellen Sie sicher, dass Sie über eine Transit-VPC oder ein VNet mit einem PCG im Status **Aktiv** verfügen.
- Stellen Sie sicher, dass die VPC bzw. das VNet, die/das Sie verknüpfen möchten, über VPN oder Peering mit der Transit-VPC oder dem Transit-VNet verbunden ist.
- Stellen Sie sicher, dass sich die Transit-VPC bzw. das Transit-VNet in derselben Region befindet wie die Computing-VPC bzw. das Computing-VNet.

Hinweis In der routenbasierten IPSec-VPN-Konfiguration müssen Sie die IP-Adresse für den VTI-Port (Virtual Tunnel Interface) angeben. Diese IP muss sich in einem anderen Subnetz als die Arbeitslast-VMs befinden. Dadurch wird verhindert, dass der eingehende Datenverkehr der Arbeitslast-VM an den VTI-Port geleitet wird, von dem er gelöscht wird.

Hinweis In der Public Cloud ist die Anzahl der Regeln für den eingehenden/ausgehenden Datenverkehr durch einen Standardgrenzwert pro Sicherheitsgruppe beschränkt und NSX Cloud erstellt Standardsicherheitsgruppen. Dies wirkt sich darauf aus, wie viele Computing-VPCs/-VNet mit einer Transit-VPC oder einem Transit-VNet verknüpft werden können. Wenn ein CIDR-Block pro VPC/VNet angenommen wird, unterstützt NSX Cloud 10 Computing-VPCs/-VNet pro Transit-VPC/-VNet. Wenn Sie über mehr als einen CIDR-Block in einer Computing-VPC bzw. einem Computing-VNet verfügen, wird die Anzahl der unterstützten Computing-VPCs/-VNet pro Transit-VPC/-VNet reduziert. Sie können die Standardgrenzwerte anpassen, indem Sie sich an Ihren Public-Cloud-Anbieter wenden.

Verfahren

- 1 Melden Sie sich unter Verwendung eines Kontos mit der Rolle „Enterprise-Administrator“ bei CSM an.
- 2 Klicken Sie auf **Clouds > AWS/Azure > <public cloud_account_name>** und gehen Sie zur Registerkarte **VPCs/VNets**.
- 3 Wählen Sie auf der Registerkarte **VPCs** oder **VNets** den Namen einer Region aus, in der Sie einen oder mehrere Computing-VPCs oder -VNet hosten.
- 4 Wählen Sie eine für NSX Cloud konfigurierte Computing-VPC bzw. -VNet aus.
- 5 Klicken Sie auf **MIT TRANSIT-VPC VERKNÜPFEN** oder auf **MIT TRANSIT-VNET VERKNÜPFEN**.

6 Füllen Sie die Optionen im Fenster **Mit Transit-VPC oder -VNet verknüpfen** aus:

Option	Beschreibung
Transit-VPC oder -VNet	<p>Wählen Sie aus dem Dropdown-Menü eine Transit-VPC oder ein Transit-VNet aus. Die Transit-VPC oder das Transit-VNet, die bzw. das Sie auswählen, muss bereits per VPN oder Peering mit dieser VPC verknüpft sein.</p> <hr/> <p>Hinweis Beim Herstellen einer Verbindung zum Transit-VNet müssen Sie DNS-Weiterleitung in diesem VNet konfigurieren. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation.</p>
Quarantäne-Standardrichtlinie	<p>Belassen Sie dies im Standardmodus deaktiviert, wenn Sie das PCG erstmalig bereitstellen. Sie können diesen Wert nach Onboarding von VMs ändern. Weitere Informationen finden Sie unter Verwalten der Quarantäne-Richtlinie im <i>Administratorhandbuch für NSX-T Data Center</i>.</p>

Nächste Schritte

Integrieren Sie Ihre Workload-VMs. Informationen zum Tag-N-Workflow finden Sie unter **Onboarding und Verwalten von Workload-VMs** im *Administratorhandbuch für NSX-T Data Center*.

Automatisch erstellte logische Entitäten und Cloud-native Sicherheitsgruppen

Die Bereitstellung von PCG in einem Transit-VPC/-VNet und die Verknüpfung eines Computing-VPC/-VNet damit löst notwendige Konfigurationen in NSX-T Data Center und in der Public Cloud aus.

Automatisch erstellte logische NSX-T-Elemente

In NSX-T Data Center werden eine Reihe von logischen Entitäten erstellt.

Wichtig Löschen Sie keine dieser automatisch erstellten Entitäten.

Systementitäten

Sie können die folgenden Entitäten unter **System** einsehen:

Tabelle 11-3. Automatisch erstellte Systementitäten

Logische Systementität	Wie viele werden erstellt?	Nomenklatur	Geltungsbereich
Transportzonen	Es werden zwei Transportzonen für jede Transit-VPC/jedes Transit-VNet erstellt.	<ul style="list-style-type: none"> ■ TZ-<VPC/VNet-ID>-OVERLAY ■ TZ-<VPC/VNet-ID>-VLAN 	Geltungsbereich: global
Edge-Transportknoten	Für jedes bereitgestellte PCG wird ein Edge-Transportknoten angelegt, zwei, wenn die Bereitstellung im Hochverfügbarkeitsmodus erfolgt.	<ul style="list-style-type: none"> ■ PublicCloudGatewayTN-<VPC/VNET-ID> ■ PublicCloudGatewayTN-<VPC/VNET-ID>-preferred 	Geltungsbereich: global
Edge-Cluster	Für jedes bereitgestellte PCG wird ein Edge-Cluster angelegt, entweder einzeln oder als Bestandteil eines Hochverfügbarkeitspaars.	PCG-cluster-<VPC/VNet-ID>	Geltungsbereich: global

Bestandslisten-Entitäten

Die folgenden Entitäten werden unter **Bestand** erstellt:

Tabelle 11-4. Automatisch erstellte Bestandslisten-Entitäten

Logische Bestandslisten-Entität	Wie viele werden erstellt?	Nomenklatur	Geltungsbereich
Domäne	Eine pro Transit-VPC/-VNet	cloud-<Transit VPC/VNet-ID>	Geltungsbereich: Freigabe über alle PCGs hinweg
Hinweis Das Domänen -Objekt ist eine experimentelle Funktion in NSX-T Data Center 2.4. Die automatisch erstellten Domänen werden in der Benutzeroberfläche angezeigt. Domänen sind jedoch nicht mehr in der Benutzeroberfläche von NSX-T Data Center 2.4.1 sichtbar.			
Gruppen	Zwei Gruppen in der Standard -Domäne	<ul style="list-style-type: none"> ■ cloud-default-route ■ cloud-metadata services 	Geltungsbereich: Freigabe über alle PCGs hinweg
Hinweis In NSX-T Data Center wird die Standarddomäne angezeigt. In NSX-T Data Center 2.4.1 ist das Domänenobjekt jedoch nicht sichtbar.			

Tabelle 11-4. Automatisch erstellte Bestandslisten-Entitäten (Fortsetzung)

Logische Bestandslisten-Entität	Wie viele werden erstellt?	Nomenklatur	Geltungsbereich
Gruppen	Eine Gruppe erstellt auf Transit-VPC/-VNet-Ebene als übergeordnete Gruppe für einzelne Segmente, die auf Computing-VPC/-VNet-Ebene erstellt wurden.	cloud-<Transit VPC/VNet ID>-all-segments	Geltungsbereich: für alle Computing-VPCs/-VNets freigegeben
Gruppen	Zwei Gruppen: <ul style="list-style-type: none"> ■ Netzwerk-CIDR-Gruppe für alle CIDRs der Computing-VPC/des Computing-VNet ■ Lokale Segment-Gruppe für alle verwalteten Segmente innerhalb der Computing-VPC/des Computing-VNet 	<ul style="list-style-type: none"> ■ cloud-<Compute VPC/VNet ID>-cidr ■ cloud-<Compute VPC/VNet ID>-local-segments 	Geltungsbereich: für alle Computing-VPC/-VNets freigegeben

Sicherheitsentitäten

Tabelle 11-5. Automatisch erstellte Sicherheitsentitäten

Logische Sicherheitsentität	Wie viele werden erstellt?	Nomenklatur	Geltungsbereich
Verteilte Firewall (Ost-West)	Zwei pro Transit-VPC/-VNet: <ul style="list-style-type: none"> ■ Statusfrei ■ Statusbehaftet 	<ul style="list-style-type: none"> ■ cloud-stateless-<VPC/VNet ID> ■ cloud-stateful-<VPC/VNet ID> 	<ul style="list-style-type: none"> ■ Statusbehaftete Regel, um Datenverkehr innerhalb lokal verwalteter Segmente zuzulassen ■ Statusbehaftete Regel, um Datenverkehr von nicht verwalteten VMs abzuweisen
Gateway-Firewall (Nord-Süd)	Eine pro Transit-VPC/-VNet	cloud-<Transit VPC/VNet ID>	

Netzwerkentitäten

Die folgenden Entitäten werden in verschiedenen Onboarding-Phasen erstellt:

Abbildung 11-3. Automatisch erstellte Netzwerkentitäten von NSX-T Data Center nach der Bereitstellung von PCG

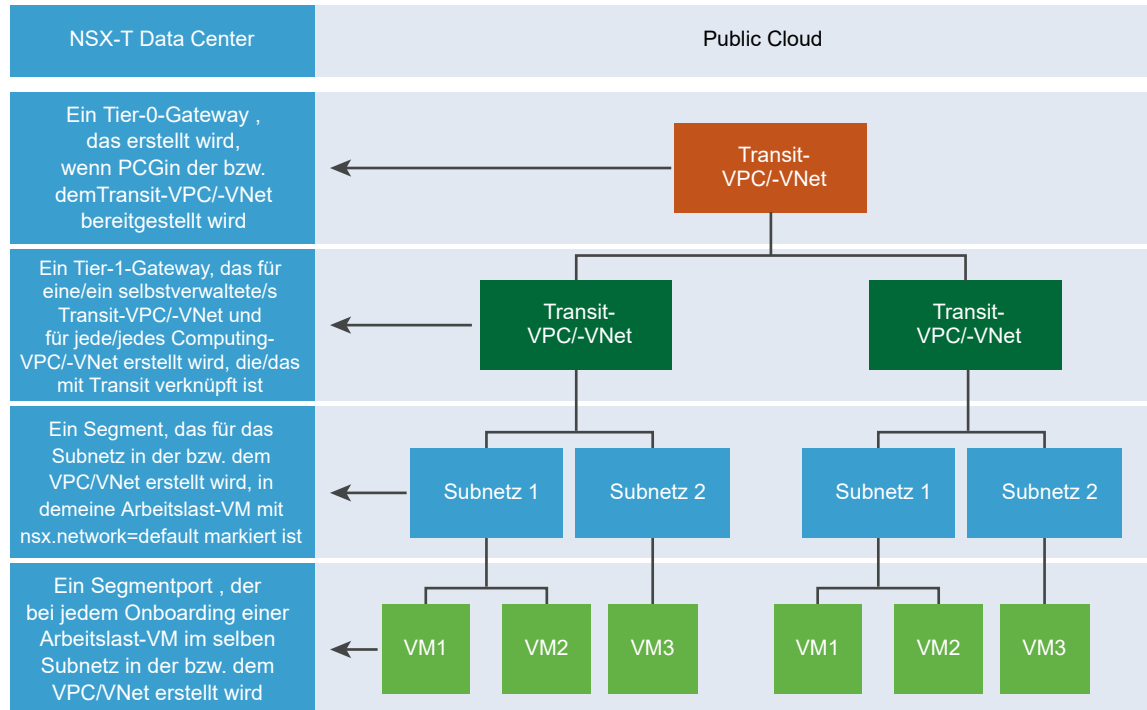


Tabelle 11-6. Automatisch erstellte Netzwerkentitäten

Onboarding-Aufgabe	Logische Entitäten, im NSX-T Data Center erstellt
PCG, auf Transit-VPC/-VNet bereitgestellt	<ul style="list-style-type: none"> ■ Tier-0-Gateway ■ Infrasegment (Standard-VLAN-Switch) ■ Tier-1-Router
Computing-VPC oder -VNet, die bzw. das mit dem Transit-VPC/-VNet verknüpft ist	<ul style="list-style-type: none"> ■ Tier-1-Router
Eine Workload-VM mit darauf installiertem NSX-Agent ist mit dem „ <code>nsx.network=default</code> “-Schlüssel:Wert in einem Subnetz einer Computing-VPC/eines Computing VNet oder einer selbstverwalteten VPC/eines selbstverwalteten VNet getaggt.	<ul style="list-style-type: none"> ■ Für dieses spezielle Subnetz der Computing-VPC oder des Computing-VNet oder der selbstverwalteten VPC oder des selbstverwalteten VNet wird ein Segment angelegt. ■ Hybrid-Ports werden für jede getaggte Workload-VM erstellt, auf der der NSX-Agent installiert ist
Weitere Workload-VMs werden im selben Subnetz der Computing-VPC/des Computing-VNet oder der selbstverwalteten VPC/des selbstverwalteten VNet getaggt.	<ul style="list-style-type: none"> ■ Hybrid-Ports werden für jede getaggte Workload-VM erstellt, auf der der NSX-Agent installiert ist

Weiterleitungsrichtlinien

Die folgenden drei Weiterleitungsregeln werden für eine Computing-VPC/ein Computing-VNet, einschließlich einer selbstverwalteten Transit-VPC/eines selbstverwalteten Transit-VNet eingerichtet:

- Zugriff auf alle CIDR von derselben Computing-VPC über das Public Cloud-Netzwerk (Underlay)
- Leiten von Datenverkehr über Public Cloud-Netzwerk an die Public Cloud-Metadatendienste (Underlay)
- Leiten Sie alles, was nicht in den CIDR-Block des Computing-VPC/VNet oder einen bekannten Dienst gehört, über das Netzwerk NSX-T Data Center (Overlay)

Automatisch erstellte Cloud-native SGs

Cloud-native Sicherheitsgruppen werden in Ihren Public Clouds erstellt.

Public-Cloud-Konfigurationen

In AWS:

- In der AWS VPC wird ein neuer Typ A-Datensatz mit dem Namen `nsx-gw.vmware.local` in eine private gehostete Zone in Amazon Route 53 hinzugefügt. Die diesem Datensatz zugeordnete IP-Adresse entspricht der Management-IP-Adresse von PCG, die vom AWS unter Verwendung von DHCP zugewiesen wird und für jede VPC unterschiedlich ist. Dieser DNS-Eintrag in der privat gehosteten Zone in Amazon Route 53 wird von NSX Cloud zur Auflösung der IP-Adresse von PCG verwendet.

Hinweis Wenn Sie benutzerdefinierte DNS-Domännennamen nutzen, die in einer privat gehosteten Zone in Amazon Route 53 definiert sind, müssen die **DNS-Auflösung**- und die **DNS-Hostnamen**-Attribute für Ihre VPC-Einstellungen im AWS auf **Ja** festgelegt sein.

- Eine sekundäre IP-Adresse für die Uplink-Schnittstelle für PCG wird erstellt. Dieser sekundären IP-Adresse ist eine elastische AWS-IP-Adresse zugeordnet. Diese Konfiguration gilt für SNAT.

In AWS und Microsoft Azure:

Die Sicherheitsgruppen **gw** werden auf die entsprechenden PCG-Schnittstellen angewendet.

Tabelle 11-7. Von NSX Cloud für PCG-Schnittstellen erstellte Public-Cloud-Sicherheitsgruppen

Name der Sicherheitsgruppe	Verfügbar in Microsoft Azure?	Verfügbar in AWS?	Vollständiger Name
gw-mgmt-sg	Ja	Ja	Gateway-Management-Sicherheitsgruppe
gw-uplink-sg	Ja	Ja	Gateway-Uplink-Sicherheitsgruppe
gw-vtep-sg	Ja	Ja	Gateway-Downlink-Sicherheitsgruppe

Tabelle 11-8. Von NSX Cloud für Workload-VMs erstellte Public Cloud-Sicherheitsgruppen

Name der Sicherheitsgruppe	Verfügbar in Microsoft Azure?	Verfügbar in AWS?	Beschreibung
quarantine	Ja	Nein	Quarantäne-Sicherheitsgruppe für Microsoft Azure
default	Nein	Ja	Quarantäne-Sicherheitsgruppe für AWS
vm-underlay-sg	Ja	Ja	Nicht-Overlay-VM-Sicherheitsgruppe
vm-override-sg	Ja	Ja	Überschreiben-VM-Sicherheitsgruppe
vm-overlay-sg	Ja	Ja	Overlay-VM-Sicherheitsgruppe (diese wird in der aktuellen Version nicht verwendet)
vm-outbound-bypass-sg	Ja	Ja	Ausgehende VM-Bypass-Sicherheitsgruppe (diese wird in der aktuellen Version nicht verwendet)
vm-inbound-bypass-sg	Ja	Ja	Eingehende VM-Bypass-Sicherheitsgruppe (diese wird in der aktuellen Version nicht verwendet)

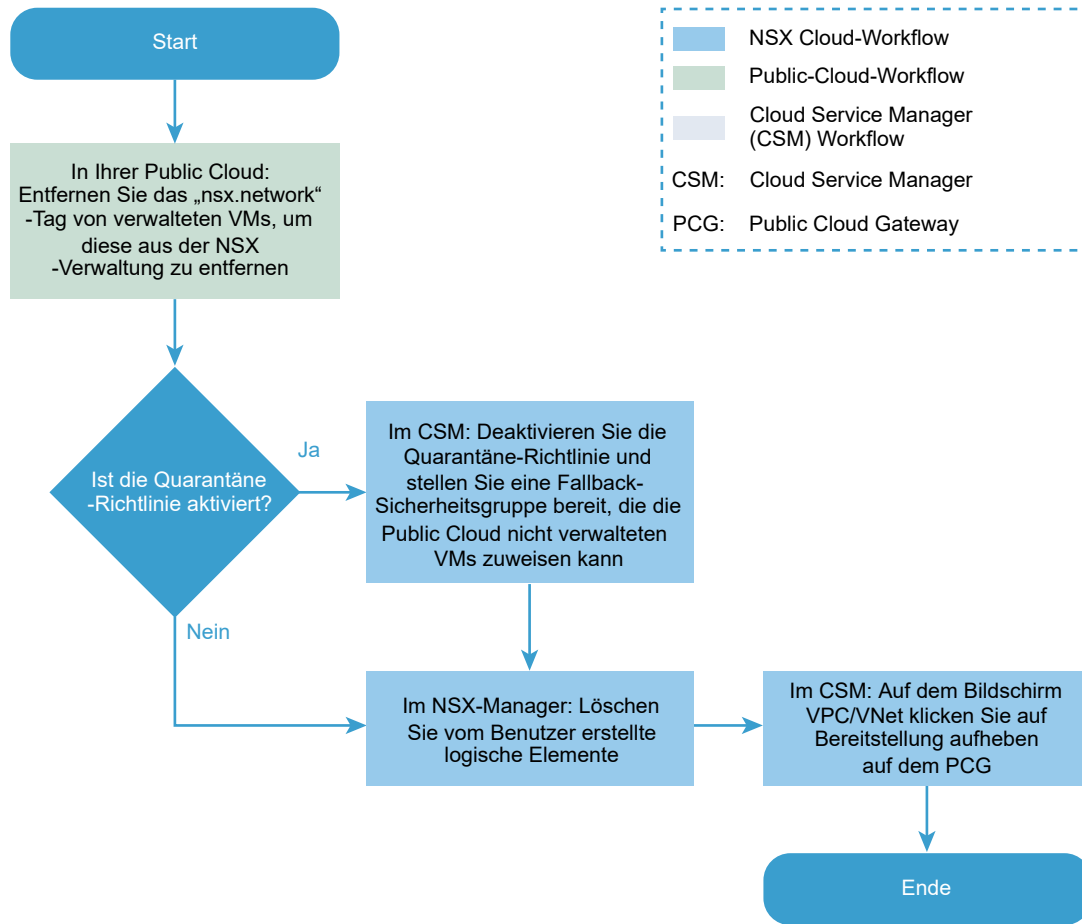
Bereitstellung von PCG aufheben

In diesem Flussdiagramm finden Sie die Schritte zum Aufheben der Bereitstellung von PCG.

Vor der Aufhebung der Bereitstellung des PCG müssen Sie Folgendes durchführen:

- Stellen Sie sicher, dass keine Workload-VMs in der VPC oder im VNet von NSX verwaltet werden.
- Deaktivieren Sie die Quarantäne-Richtlinie.
- Löschen Sie alle vom Benutzer erstellten logischen Elemente, die mit dem PCG verknüpft sind.

Abbildung 11-4. Aufheben der Bereitstellung von PCG



Verfahren

1 Tags für VMs in der Public Cloud entfernen

Bevor Sie die Bereitstellung von PCG aufheben können, müssen alle VMs nicht verwaltet sein.

2 Quarantäne-Richtlinie deaktivieren, falls aktiviert

Wenn sie zuvor aktiviert wurde, muss die Quarantäne-Richtlinie deaktiviert werden, um die Bereitstellung von PCG aufzuheben.

3 Vom Benutzer erstellte logische Elemente löschen

Alle vom Benutzer erstellten logischen Elemente, die mit PCG verknüpft sind, müssen gelöscht werden.

4 Bereitstellung aufheben von CSM

Um nach Erfüllung der Voraussetzungen die Bereitstellung von PCG aufzuheben, klicken Sie auf Bereitstellung Gateway aufheben von **Clouds** > **<Public_Cloud>** > **<VNet/VPC>** in CSM.

Tags für VMs in der Public Cloud entfernen

Bevor Sie die Bereitstellung von PCG aufheben können, müssen alle VMs nicht verwaltet sein.

Wechseln Sie zur VPC oder zum VNet in Ihrer Public Cloud und entfernen Sie das Tag `nsx.network` von den verwalteten VMs.

Quarantäne-Richtlinie deaktivieren, falls aktiviert

Wenn sie zuvor aktiviert wurde, muss die Quarantäne-Richtlinie deaktiviert werden, um die Bereitstellung von PCG aufzuheben.

Wenn die Quarantäne-Richtlinie aktiviert ist, werden Ihren VMs Sicherheitsgruppen zugewiesen, die durch NSX Cloud definiert sind. Wenn Sie die Bereitstellung von PCG aufheben, müssen Sie die Quarantäne-Richtlinie deaktivieren und eine Fallback-Sicherheitsgruppe angeben, der die VMs zugeordnet werden können, wenn sie aus den NSX Cloud-Sicherheitsgruppen entfernt werden.

Hinweis Die Fallback-Sicherheitsgruppe muss eine vorhandene benutzerdefinierte Sicherheitsgruppe in Ihrer Public Cloud sein. Sie können keine der NSX Cloud-Sicherheitsgruppen als Fallback-Sicherheitsgruppe verwenden. Eine Liste der NSX Cloud Sicherheitsgruppen finden Sie unter [Automatisch erstellte logische Entitäten und Cloud-native Sicherheitsgruppen](#).

Deaktivieren Sie die Quarantäne-Richtlinie für die VPC oder das VNet, von der bzw. dem aus Sie die Bereitstellung von PCG aufheben:

- Navigieren Sie zur VPC oder zum VNet in CSM.
- Unter **Aktionen > Konfigurationen bearbeiten** > deaktivieren Sie die Einstellung für die **Standard-Quarantäne**.
- Geben Sie einen Wert für eine Fallback-Sicherheitsgruppe ein, der die VMs zugewiesen werden.

The screenshot shows the 'Edit VPC' configuration window. At the top, there's a title bar 'Edit VPC:'. Below it, the 'Default Quarantine' toggle is turned off. A yellow highlight is on the 'Fallback Security Group ID' field, which has a red asterisk indicating it's required. A tooltip points to this field with the text: 'Provide the ID of an existing Security Group in your VPC that NSX Cloud can assign unmanaged VMs to. This is required when the Quarantine Policy is disabled.' To the right of the field is a dropdown menu showing 'profile-1a'. At the bottom right, there are 'CANCEL' and 'SAVE' buttons.

- Alle VMs, die in dieser VPC oder diesem VNet nicht verwaltet werden oder unter Quarantäne gestellt werden, erhalten die ihnen zugewiesene Fallback-Sicherheitsgruppe.
- Wenn alle VMs nicht verwaltet werden, werden sie der Fallback-Sicherheitsgruppe zugewiesen.

- Wenn beim Deaktivieren der Quarantäne-Richtlinie verwaltete VMs vorhanden sind, behalten sie ihre mit NSX Cloud zugeordneten Sicherheitsgruppen. Wenn Sie zum ersten Mal das `nsx.network`-Tag von solchen VMs entfernen, um sie aus der NSX-Verwaltung zu entfernen, wird ihnen ebenfalls die Fallback-Sicherheitsgruppe zugewiesen.

Hinweis Unter **Verwalten der Quarantäne-Richtlinie** im *Administratorhandbuch für NSX-T Data Center* finden Sie Anweisungen und weitere Informationen zu den Auswirkungen der Aktivierung und Deaktivierung der Quarantäne-Richtlinie.

Vom Benutzer erstellte logische Elemente löschen

Alle vom Benutzer erstellten logischen Elemente, die mit PCG verknüpft sind, müssen gelöscht werden.

Ermitteln Sie Elemente, die dem PCG zugeordnet sind, und löschen Sie sie.

Hinweis Löschen Sie nicht die automatisch erstellten logischen Elemente. Diese werden automatisch gelöscht, nachdem Sie in CSM auf **Gateway-Bereitstellung aufheben** geklickt haben. Die Liste mit den automatisch erstellten logischen Elementen finden Sie unter [Automatisch erstellte logische Entitäten und Cloud-native Sicherheitsgruppen](#).

Bereitstellung aufheben von CSM

Um nach Erfüllung der Voraussetzungen die Bereitstellung von PCG aufzuheben, klicken Sie auf Bereitstellung Gateway aufheben von **Clouds** > **<Public_Cloud>** > **<VNet/VPC>** in CSM.

- 1 Melden Sie sich bei CSM an und gehen Sie zu Ihrer Public Cloud:
 - Klicken Sie bei Verwendung von AWS auf **Clouds** > **AWS** > **VPCs**. Klicken Sie auf die VPC, auf der ein oder zwei PCGs bereitgestellt wurden und ausgeführt werden.
 - Klicken Sie bei Verwendung von Microsoft Azure auf **Clouds** > **Azure** > **VNets**. Klicken Sie auf das VNet, in dem ein oder zwei PCGs bereitgestellt wurden und ausgeführt werden.
- 2 Klicken Sie auf Bereitstellung Gateway aufheben.

Die standardmäßig von NSX Cloud erstellten Entitäten werden automatisch entfernt, wenn die Bereitstellung von PCG aufgehoben wird.