

Installationshandbuch für NSX-T Data Center

Geändert am 23. APR. 2019

VMware NSX-T Data Center 2.3



vmware®

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

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

Die VMware-Website enthält auch die neuesten Produkt-Updates.

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 © 2018, 2019 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

NSX-T Data Center -Installationshandbuch 5

1 Übersicht über NSX-T Data Center 6

Managementebene 7

Steuerungskomponente 9

Datenebene 10

Logische Switches 11

Logische Router 12

Wichtige Konzepte 13

2 Vorbereitung für die Installation 17

Systemvoraussetzungen 17

Ports und Protokolle 21

Allgemeine Aufgaben für die Installation von NSX-T Data Center 27

3 Arbeiten mit KVM 29

Einrichten von KVM 29

Verwalten der Gast-VMs in der KVM-CLI 34

4 NSX Manager -Installation 36

Installieren Sie NSX Manager und die verfügbaren Appliances 38

Installieren von NSX Manager auf ESXi unter Verwendung des OVF-Befehlszeilentools 40

Installieren von NSX Manager auf KVM 43

Anmeldung beim neu erstellten NSX Manager 46

5 NSX Controller -Installation und -Clustering 48

Automatische Installation von Controller und Cluster über NSX Manager 50

Installieren von NSX Controller auf ESXi unter Verwendung einer grafischen Benutzeroberfläche 58

Installieren von NSX Controller auf ESXi unter Verwendung des OVF-Befehlszeilentools 60

Installieren von NSX Controller auf KVM 63

NSX Controller -Verbindung mit NSX Manager 65

Initialisieren des Controller-Clusters zum Erstellen eines Controller-Cluster-Masters 67

Verbinden von weiteren NSX Controllern mit dem Cluster-Master 68

6 NSX Edge -Installation 72

NSX Edge -Netzwerkeinrichtung 74

Automatische Bereitstellung von virtuellen NSX Edge -Maschinen aus NSX Manager 80

Installieren eines NSX Edge unter ESXi über eine grafische vSphere -Benutzeroberfläche 81

- Installieren von NSX Edge auf ESXi unter Verwendung des OVF-Befehlszeilentools 84
- Installieren von NSX Edge mithilfe der ISO-Datei mit einem PXE-Server 88
- Verbinden von NSX Edge mit der Managementebene 100

7 Hostvorbereitung 102

- Installieren von Drittanbieterpaketen auf einem KVM-Host oder Bare Metal-Server 102
- Überprüfung der Open vSwitch-Version auf RHEL KVM-Hosts 105
- Hinzufügen eines Hypervisor-Hosts oder Bare Metal-Servers zur NSX-T Data Center -Fabric 106
- Manuelle Installation von NSX-T Data Center -Kernel-Modulen 110
- Verbinden der Hypervisor-Hosts mit der Managementebene 115

8 Transportzonen und Transportknoten 118

- Grundlegende Informationen zu Transportzonen 118
- Erweiterter Datenpfad 120
- Erstellen eines IP-Pools für Tunnel-Endpoint-IP-Adressen 122
- Erstellen eines Uplink-Profiles 124
- Erstellen von Transportzonen 128
- Erstellen eines Hosttransportknotens 131
- Erstellen der Anwendungsschnittstelle für Bare-Metal Server-Arbeitslasten 150
- Konfigurieren von Network I/O Control-Profilen 150
- Erstellen eines NSX Edge -Transportknotens 160
- Erstellen eines NSX Edge -Clusters 163

9 Installation von NSX Cloud -Komponenten 165

- Architektur und Komponenten von NSX Cloud 165
- Übersicht über die Installation der NSX Cloud-Komponenten 166
- Installieren von CSM und Herstellen einer Verbindung zu NSX Manager 168
- Public Cloud mit lokaler Bereitstellung verbinden 171
- Ihr Public Cloud-Konto hinzufügen 175
- PCG bereitstellen 180
- Bereitstellung von PCG aufheben 186

10 Deinstallieren von NSX-T Data Center 191

- Aufheben einer NSX-T Data Center -Overlay-Konfiguration 191
- Entfernen eines Hosts von NSX-T Data Center oder komplette NSX-T Data Center -Deinstallation 191

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.

VMware Technical Publications – Glossar

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

Übersicht über NSX-T Data Center

1

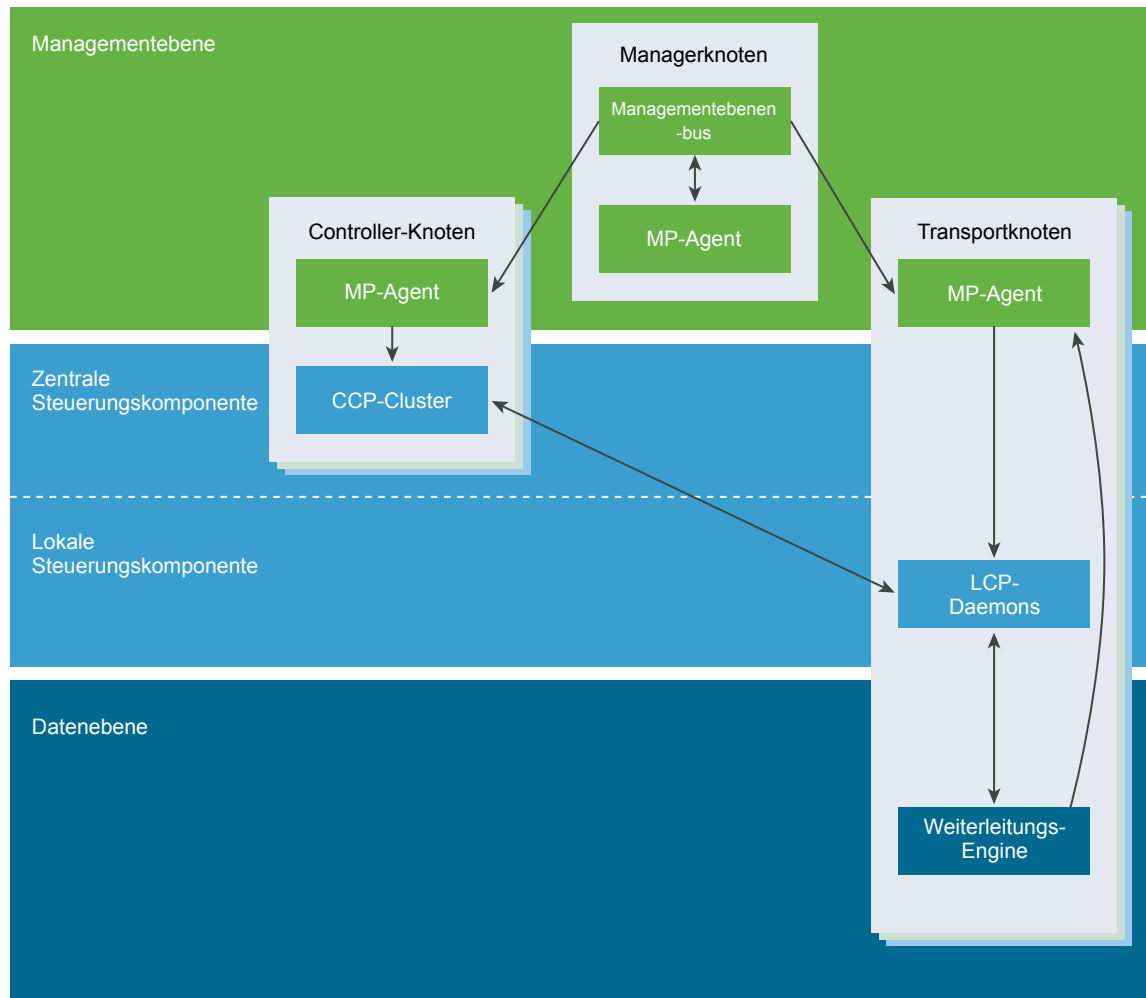
Mithilfe der Servervirtualisierung werden softwarebasierte virtuelle Maschinen (VMs) programmatisch erstellt, per Snapshot aufgenommen, gelöscht und wiederhergestellt. Auf die gleiche Weise lassen sich mit der NSX-T Data Center-Netzwerkvirtualisierung ganze softwarebasierte virtuelle Netzwerke programmatisch erstellen, löschen und wiederherstellen.

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. Die drei Ebenen werden als eine Reihe von Prozessen, Modulen und Agenten implementiert, die auf drei Typen von Knoten platziert sind: Manager-, Controller- und Transportknoten.

- Jeder Knoten hostet einen Managementebenen-Agenten.
- Der NSX Manager-Knoten hostet API-Dienste. Jede NSX-T Data Center-Installation unterstützt einen einzelnen NSX Manager-Knoten.
- NSX Controller-Knoten hosten die Cluster-Daemons der zentralen Steuerungskomponente.
- NSX Manager- und NSX Controller-Knoten können zusammen auf demselben physischen Server gehostet werden.

- Transportknoten hosten Daemons der lokalen Steuerungskomponente und Weiterleitungs-Engines.



Dieses Kapitel enthält die folgenden Themen:

- [Managementebene](#)
- [Steuerungskomponente](#)
- [Datenebene](#)
- [Logische Switches](#)
- [Logische Router](#)
- [Wichtige Konzepte](#)

Managementebene

Die Managementebene liefert einen einzelnen API-Einstiegspunkt in das System, speichert die Benutzerkonfiguration, verarbeitet Benutzerabfragen und führt Betriebsaufgaben auf allen Management-, Controller- und Datenebenenknoten im System aus.

Bei NSX-T Data Center fallen alle Handlungen zum Abfragen, Ändern und Speichern der Benutzerkonfiguration in den Aufgabenbereich der Managementebene, während die Verteilung dieser Konfiguration an die richtige Teilmenge aus Datenebenenelementen von der Steuerungskomponente durchgeführt wird. Das bedeutet, dass einige Daten zu mehreren Ebenen gehören (je nachdem, in welcher Phase sie sich befinden). Die Managementebene verarbeitet außerdem die Abfrage des letzten Status und Statistiken von der Steuerungskomponente und manchmal direkt von der Datenebene.

Die Managementebene ist die einzige Informationsquelle für das konfigurierte (logische) System, das vom Benutzer über die Konfiguration verwaltet wird. Änderungen werden entweder über eine RESTful-API oder die NSX-T Data Center-Benutzeroberfläche vorgenommen.

In NSX gibt es außerdem einen Managementebenen-Agenten (MPA), der auf allen Controllercluster- und Transportknoten ausgeführt wird. Auf den MPA kann sowohl lokal als auch remote zugegriffen werden. Auf Transportknoten kann er auch Datenebenenaufgaben ausführen.

Die Managementebene kann die folgenden Aufgaben umfassen:

- Speichern der Konfiguration (gewünschter logischer Zustand)
- Eingabevalidierung
- Benutzerverwaltung – Rollenzuweisungen
- Richtlinienverwaltung
- Verfolgung von Hintergrundaufgaben

NSX Manager

NSX Manager ist eine virtuelle Appliance, die die grafische Benutzeroberfläche (GUI) und die REST-APIs für die Erstellung, Konfiguration und Überwachung von NSX-T Data Center-Komponenten wie logischen Switches und NSX Edge-Dienst-Gateways bereitstellt.

NSX Manager ist die Managementebene für das NSX-T Data Center-Ökosystem. NSX Manager bietet die Gesamtübersicht über das System und ist die zentrale NSX-T Data Center-Komponente für das Netzwerkmanagement. Es bietet Konfiguration und Orchestrierung von:

- logischen Netzwerkkomponenten (logischem Switching und Routing)
- Netzwerk- und Edge-Diensten
- Sicherheitsdienste und verteilte Firewall

Mit NSX Manager wird die Überwachung von und Fehlerbehebung bei Arbeitslasten ermöglicht, die mit von NSX-T Data Center erstellten virtuellen Netzwerken verbunden sind. Dies ermöglicht die nahtlose Orchestrierung von integrierten und externen Diensten. Alle Sicherheitsdienste (ob integriert oder von einem Drittanbieter) werden von der NSX-T Data Center-Managementebene bereitgestellt und konfiguriert. Die Managementebene liefert ein zentrales Fenster für die Anzeige der Dienstverfügbarkeit. Sie erleichtert außerdem die richtlinienbasierte Dienstverkettung, Kontextfreigabe und Verarbeitung dienstinterner Ereignisse. Dadurch wird die Überwachung des Sicherheitszustands erleichtert und die Anwendung identitätsbasierter Kontrollen (z. B. AD und Mobilitätsprofile) wird optimiert.

NSX Manager liefert außerdem REST-API-Einstiegspunkte zur Automatisierung der Nutzung. Diese flexible Architektur ermöglicht die automatisierte Konfiguration und Überwachung über eine beliebige Cloud-Managementplattform, eine Sicherheitsanbieterplattform oder ein Automatisierungs-Framework.

Der NSX-T Data Center-Managementebenen-Agent (MPA) ist eine NSX Manager-Komponente, die auf jedem Knoten (Hypervisor) vorhanden ist. Der MPA speichert den gewünschten Systemzustand und kommuniziert NFC-Nachrichten (Non-Flow-Controlling), wie Konfiguration, Statistiken, Status und Echtzeitdaten, zwischen Transportknoten und der Managementebene.

NSX Policy Manager

NSX Policy Manager ist eine virtuelle Appliance, die ein absichtbasiertes System zur Vereinfachung der Nutzung von NSX-T Data Center-Diensten bereitstellt.

NSX Policy Manager bietet eine grafische Benutzeroberfläche (GUI) und REST-APIs, um die Absicht im Zusammenhang mit Netzwerken, Sicherheit und Verfügbarkeit anzugeben.

NSX Policy Manager akzeptiert die Absicht vom Benutzer in Form eines strukturbasierten Datenmodells und konfiguriert den NSX Manager für die Umsetzung dieser Absicht. Der NSX Policy Manager unterstützt eine Kommunikationsabsichtsspezifikation, mit der eine verteilte Firewall auf dem NSX Manager konfiguriert wird.

Cloud Service Manager

Cloud Service Manager (CSM) bietet einen zentralen Endpunkt für die Verwaltung aller Ihrer Public Cloud-Konstrukte.

CSM ist eine virtuelle Appliance, die die grafische Benutzeroberfläche (GUI) und die REST-APIs für das Onboarding, die Konfiguration und die Überwachung Ihrer Public Cloud-Bestandsliste bereitstellt.

Steuerungskomponente

Berechnet alle kurzlebigen Laufzeitzustände basierend auf der Konfiguration aus der Managementebene, verteilt Topologie-Informationen, die von den Datenebenenelementen gemeldet werden, und überträgt die zustandslose Konfiguration an Weiterleitungs-Engines.

Die Steuerungskomponente ist in NSX-T Data Center in zwei Teile aufgeteilt: die zentrale Steuerungskomponente (Central Control Plane; CCP), die auf den NSX Controller-Clusterknoten ausgeführt wird, und die lokale Steuerungskomponente (Local Control Plane; LCP), die auf den Transportknoten angrenzend an die gesteuerte Datenebene ausgeführt wird. Die zentrale Steuerungskomponente berechnet einige kurzlebige Laufzeitzustände basierend auf der Konfiguration aus der Managementebene und verteilt Topologieinformationen, die von den Datenebenenelementen über die lokale Steuerungskomponente gemeldet werden. Die lokale Steuerungskomponente überwacht den lokalen Linkstatus, berechnet die meisten kurzlebigen Laufzeitzustände basierend auf Aktualisierungen von Datenebene und CCP und überträgt die zustandslose Konfiguration an Weiterleitungs-Engines. Die LCP ist per Fate-Sharing an das Datenebenenelement gebunden, das sie hostet.

NSX Controller

Als zentrale Steuerungskomponente (Central Control Plane, CCP) aufgerufener NSX Controller ist ein erweitertes, verteiltes Zustandsverwaltungssystem, das virtuelle Netzwerke und Overlay-Transporttunnel steuert.

NSX Controller wird als Cluster aus hochverfügbaren virtuellen Appliances bereitgestellt, die für die programmgesteuerte Bereitstellung virtueller Netzwerke in der ganzen NSX-T Data Center-Architektur verantwortlich sind. Die zentrale NSX-T Data Center-Steuerungskomponente ist logisch vom gesamten Datenebenenverkehr getrennt. Das bedeutet, dass sich Fehler in der Steuerungskomponente nicht auf bestehende Datenebenenvorgänge auswirken. Der Datenverkehr verläuft nicht durch den Controller. Stattdessen stellt der Controller die Konfiguration für andere NSX Controller-Komponenten bereit, wie logische Switches, logische Router und Edge-Konfiguration. Stabilität und Zuverlässigkeit des Datentransports stellen wesentliche Aspekte beim Networking dar. Um Hochverfügbarkeit und Skalierbarkeit weiter zu verbessern, wird NSX Controller in einem Cluster aus drei Instanzen bereitgestellt.

Datenebene

Führt die zustandslose Weiterleitung/Transformation von Paketen anhand von Tabellen durch, die von der Steuerungskomponente aufgefüllt werden, meldet Topologie-Informationen an die Steuerungskomponente und pflegt Statistiken auf Paketebene.

Die Datenebene ist die Informationsquelle für die physische Topologie und den Status, wie z. B. VIF-Ort, Tunnelstatus usw. Wenn Sie Pakete von einem Ort zu einem anderen verschieben, befinden Sie sich in der Datenebene. Die Datenebene ist außerdem für den Status von und das Failover zwischen mehreren Links/Tunneln verantwortlich. Die Leistung pro Paket ist von höchster Wichtigkeit und es gelten besonders strenge Latenz- oder Jitter-Anforderungen. Die Datenebene ist nicht unbedingt gänzlich in Kernen, Treibern, im Benutzerbereich oder sogar in bestimmten Benutzerbereichsprozessen enthalten. Sie ist auf komplett zustandslose Weiterleitung anhand von Tabellen/Regeln beschränkt, die von der Steuerungskomponente aufgefüllt werden.

Die Datenebene kann auch Komponenten aufweisen, die gewisse Zustandsinformationen für Funktionen wie TCP-Beendigung pflegen. Dies unterscheidet sich von dem von der Steuerungskomponente verwalteten Zustand, wie MAC:IP-Tunnelzuordnungen, da der von der Steuerungskomponente verwaltete Zustand festlegt, wie die Pakete weitergeleitet werden sollen, während der von der Datenebene verwaltete Zustand auf die Bearbeitung der Nutzlast begrenzt ist.

NSX Edge

NSX Edge liefert Routing-Dienste und Konnektivität zu Netzwerken, die zur NSX-T Data Center-Bereitstellung extern sind.

NSX Edge kann als Bare-Metal-Knoten oder als virtuelle Maschine bereitgestellt werden.

NSX Edge ist erforderlich, um externe Konnektivität von der NSX-T Data Center-Domäne über einen Tier-0-Router per BGP oder statisches Routing aufzubauen. Außerdem muss NSX Edge bereitgestellt werden, wenn Sie NAT-Dienste (Network Address Translation) beim logischen Tier-0- oder Tier-1-Router benötigen.

Das NSX Edge-Gateway verbindet isolierte Stub-Netzwerke mit freigegebenen (Uplink-)Netzwerken durch die Bereitstellung von gängigen Gateway-Diensten wie NAT und dynamisches Routing. NSX Edge wird häufig in der DMZ und in Cloud-Umgebungen mit mehreren Mandanten bereitgestellt, in denen NSX Edge virtuelle Grenzen für jeden Mandanten erstellt.

Transportzonen

Eine Transportzone ist ein logisches Konstrukt, das steuert, welche Hosts ein logischer Switch erreichen kann. Sie kann einen oder mehrere Hostcluster umfassen. Transportzonen bestimmen, welche Hosts und damit auch welche VMs an der Verwendung eines bestimmten Netzwerks teilnehmen können.

Eine Transportzone definiert eine Sammlung von Hosts, die über eine physische Netzwerkinfrastruktur miteinander kommunizieren können. Diese Kommunikation findet über Schnittstellen statt, die als virtuelle Tunnel-Endpoints (VTEPs) definiert sind.

Die Transportknoten sind die Hosts, auf denen die Daemons der lokalen Steuerungskomponente und die Weiterleitungs-Engines ausgeführt werden, welche die NSX-T Data Center-Datenebene implementieren. Die Transportknoten bestehen aus einem NSX-T Data Center Virtual Distributed Switch (N-VDS), der dafür zuständig ist, Pakete gemäß der Konfiguration der verfügbaren Netzwerkdienste zu schalten.

Wenn sich zwei Transportknoten in derselben Transportzone befinden, können die auf diesen Transportknoten gehosteten VMs logische NSX-T Data Center-Switches, die sich ebenfalls in dieser Transportzone befinden, „sehen“ und daher mit diesen verknüpft werden. Dank dieser Verknüpfung können die VMs miteinander kommunizieren, vorausgesetzt, dass sie über Schicht-2-/Schicht-3-Erreichbarkeit verfügen. Wenn VMs mit Switches verknüpft sind, die sich in anderen Transportzonen befinden, können die VMs nicht miteinander kommunizieren. Transportzonen ersetzen keine Anforderungen zu Schicht-2-/Schicht-3-Erreichbarkeit, begrenzen die Erreichbarkeit aber. Anders ausgedrückt: Die Zugehörigkeit zu derselben Transportzone ist Voraussetzung für die Konnektivität. Wenn diese Voraussetzung erfüllt ist, wird die Erreichbarkeit möglich, ist aber nicht automatisch gegeben. Um wirklich erreichbar zu sein, muss Schicht-2- und (bei anderen Subnetzen) Schicht-3-Networking stattfinden.

Ein Host kann als Transportknoten fungieren, wenn er mindestens einen NSX-verwalteten Virtual Distributed Switch (N-VDS, ehemals als Host-Switch bekannt) enthält. Wenn Sie einen Hosttransportknoten erstellen und dann einer Transportzone hinzufügen, installiert NSX-T Data Center einen N-VDS auf dem Host. Für jede Transportzone, zu der der Host gehört, wird ein eigener N-VDS installiert. Über den N-VDS werden VMs mit logischen NSX-T Data Center-Switches verknüpft, und es werden logische NSX-T Data Center-Router-Uplinks und -Downlinks erstellt.

Logische Switches

Dank der logischen Switching-Funktion in der NSX-T Data Center-Plattform können Sie isolierte L2-Netzwerke mit derselben Flexibilität und Agilität wie der von virtuellen Maschinen erweitern.

Ein logischer Switch stellt Schicht-2-Switch-Konnektivität über zahlreiche Hosts hinweg mit Schicht-3-IP-Erreichbarkeit dazwischen dar. Wenn Sie einige logische Netzwerke auf wenige Hosts einschränken möchten oder individuelle Konnektivitätsanforderungen haben, müssen Sie eventuell zusätzliche logische Switches erstellen.

Diese Anwendungen und Mandanten müssen aus Sicherheitsgründen, für Fehlerisolierungszwecke und zur Vermeidung von Problemen durch sich überschneidende IP-Adressen voneinander isoliert werden. Endpoints (sowohl virtuell als auch physisch) können mit logischen Segmenten verbunden werden und unabhängig von ihrer physischen Position im Datencenter-Netzwerk Konnektivität aufbauen. Dies ist möglich, weil die Netzwerkinfrastruktur vom logischen Netzwerk, das durch die NSX-T Data Center-Netzwerkvirtualisierung bereitgestellt wird, entkoppelt wird (d. h. das Underlay-Netzwerk vom Overlay-Netzwerk).

Logische Router

Logische NSX-T Data Center-Router bieten Nord-Süd-Konnektivität, sodass Mandanten auf öffentliche Netzwerke zugreifen können, und Ost-West-Konnektivität zwischen verschiedenen Netzwerken in denselben Mandanten. Für Ost-West-Konnektivität sind logische Router über den Kernel der Hosts verteilt.

Mit NSX-T Data Center können Sie eine logische Router-Topologie mit zwei Ebenen erstellen: Der logische Router der obersten Ebene ist Tier-0 und der logische Router der unteren Ebene ist Tier-1. Mit dieser Struktur erhalten sowohl Anbieter- als auch Mandantenadministratoren vollständige Kontrolle über ihre Dienste und Richtlinien. Administratoren steuern und konfigurieren Tier-0-Routing und -Dienste und Mandantenadministratoren steuern und konfigurieren Tier-1. Das nördliche Ende von Tier-0 ist mit dem physischen Netzwerk verbunden. Dort können dynamische Routing-Protokolle konfiguriert werden, um Routing-Informationen mit physischen Routern auszutauschen. Das südliche Ende von Tier-0 ist mit mehreren Tier-1-Routing-Schichten verbunden und erhält Routing-Informationen von ihnen. Um die Ressourcennutzung zu optimieren, gibt die Tier-0-Schicht nicht alle Routen vom physischen Netzwerk an Tier-1 weiter, stellt aber Standardinformationen bereit.

In Richtung Süden ist die Tier-1-Routing-Schicht mit den logischen Switches verbunden, die von den Mandantenadministratoren definiert wurden, und liefert Ein-Hop-Routing dazwischen. Damit mit Tier-1 verknüpfte Subnetze vom physischen Netzwerk erreicht werden können, muss Route Redistribution zur Tier-0-Schicht aktiviert werden. Es wird allerdings kein klassisches Routing-Protokoll (wie OSPF oder BGP) zwischen der Tier-1-Schicht und der Tier-0-Schicht ausgeführt, und alle Routen verlaufen durch die NSX-T Data Center-Steuerungskomponente. Beachten Sie, dass die Routing-Topologie mit zwei Ebenen nicht obligatorisch ist. Wenn Anbieter und Mandant nicht getrennt werden müssen, kann eine Topologie mit nur einer Ebene erstellt werden. In diesem Szenario werden die logischen Switches direkt mit der Tier-0-Schicht verbunden, und es gibt keine Tier-1-Schicht.

Ein logischer Router besteht aus zwei optionalen Teilen: einem verteilten Router (Distributed Router; DR) und mindestens einem Dienstrouter (Service Router; SR).

Ein DR umfasst Hypervisors, deren VMs mit diesem logischen Router verbunden sind, sowie Edge-Knoten, an die der logische Router gebunden ist. Im Hinblick auf seine Funktion ist der DR für verteiltes Routing mit einem Hop zwischen logischen Switches und/oder logischen Routern zuständig, die mit diesem logischen Router verbunden sind. Der SR stellt Dienste wie zustandsbehaftete NAT.bereit, die derzeit nicht verteilt implementiert sind.

Ein logischer Router weist immer einen DR sowie SRs auf, wenn eine der folgenden Bedingungen zutrifft:

- Der logische Router ist ein Tier-0-Router, selbst wenn keine zustandsbehafteten Dienste konfiguriert sind.
- Der logische Router ist ein Tier-1-Router, der mit einem Tier-0-Router verknüpft ist und für den Dienste konfiguriert sind, die keine verteilte Implementierung aufweisen (wie NAT, LB, DHCP).

Die NSX-T Data Center-Managementebene (MP) erstellt automatisch die Struktur, die den Dienstrouter mit dem verteilten Router verbindet. Die MP erstellt einen logischen Transit-Switch und teilt ihm eine VNI zu. Dann erstellt sie einen Port auf jedem SR und DR, verbindet diese mit dem logischen Transit-Switch und teilt IP-Adressen für den SR und DR zu.

Wichtige Konzepte

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

Berechnungsmanager	Ein Berechnungsmanager ist eine Anwendung, die Ressourcen wie Hosts und virtuelle Maschinen verwaltet. Ein Beispiel ist vCenter Server.
Steuerungskomponente	Berechnet den Laufzeitzustand anhand der Konfiguration aus der Managementebene, verteilt Topologie-Informationen, die von den Datenebenenelementen gemeldet werden, und überträgt die zustandslose Konfiguration an Weiterleitungs-Engines.
Datenebene	Führt die zustandslose Weiterleitung oder Transformation von Paketen anhand von Tabellen durch, die von der Steuerungskomponente aufgefüllt werden. Die Datenebene meldet Topologie-Informationen an die Steuerungskomponente 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-Managementebene 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.

Ausgehender Datenverkehr am logischen Port	Ausgehender Netzwerkdatenverkehr, der die VM oder das logische Netzwerk verlässt, wird als ausgehend bezeichnet, weil der Datenverkehr das virtuelle Netzwerk verlässt und in das Datacenter eintritt.
Eingehender Datenverkehr am logischen Port	Eingehender Netzwerkdatenverkehr, der das Datacenter verlässt und in die VM eintritt, wird als eingehender Datenverkehr bezeichnet.
Logischer Router	NSX-T Data Center-Routing-Einheit
Logischer Routerport	Logischer Netzwerkport, mit dem Sie einen logischen Switch-Port oder einen Uplink-Port zu einem physischen Netzwerk verknüpfen können
Logischer Switch	<p>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 Hypervisoren umspannt, sodass VMs unabhängig von ihrer physischen Position verbunden werden.</p> <p>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.</p>
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.
Managementebene	Liefert einen einzelnen API-Einstiegspunkt in das System, speichert die Benutzerkonfiguration, verarbeitet Benutzerabfragen und führt Betriebsaufgaben auf allen Management-, Controller- und Datenebenenknoten im System aus. Die Managementebene ist außerdem für das Abfragen, Ändern und Speichern der Benutzerkonfiguration zuständig.
NSX Controller-Cluster	Wird als Cluster aus hochverfügbaren virtuellen Appliances bereitgestellt, die für die programmgesteuerte Bereitstellung virtueller Netzwerke in der ganzen NSX-T Data Center-Architektur verantwortlich sind.
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

Software, die auf dem Hypervisor ausgeführt wird und Datenverkehrsweiterleitung bereitstellt. Der NSX-verwaltete Virtual Distributed Switch (N-VDS, früher als Host-Switch bekannt) oder der OVS ist für den Administratoren des Mandantennetzwerks nicht sichtbar und bietet den zugrunde liegenden Weiterleitungsdienst, auf dem jeder logische Switch beruht. Um die Netzwerkvirtualisierung zu erreichen, muss ein Netzwerk-Controller den virtuellen Hypervisor-Switch mit Netzwerk-Flow-Tabellen konfigurieren, die die logischen Broadcast-Domänen bilden, die Mandantenadministratoren beim Erstellen und Konfigurieren der logischen Switches definiert haben.

Jede logische Broadcast-Domäne wird anhand von Tunneling von VM-zu-VM-Datenverkehr und Datenverkehr von VM zu logischen Routern implementiert. Dabei wird der Tunnelkapselungsmechanismus Geneve eingesetzt. Der Netzwerk-Controller verfügt über eine globale Ansicht des Datacenters und stellt sicher, dass die Netzwerk-Flow-Tabellen für den virtuellen Hypervisor-Switch beim Erstellen, Verschieben oder Entfernen von VMs aktualisiert werden.

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.

NSX Manager

Knoten, der die API-Dienste, die Managementebene und die Agent-Dienste hostet.

Einheitliche NSX-T Data Center-Appliance

Eine einheitliche NSX-T Data Center-Appliance ist eine Appliance, die im Installationspaket von NSX-T Data Center enthalten ist. Sie können die Appliance in der Rolle von NSX Manager, Policy Manager oder Cloud Service Manager bereitstellen. Die Appliance unterstützt derzeit nur jeweils eine Rolle gleichzeitig.

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.

Logischer Ebene-0-Router

Logischer Anbieter-Router wird auch als logischer Ebene-0-Router bezeichnet und ist mit dem physischen Netzwerk verbunden. Der logische Ebene-0-Router ist ein Router der obersten Ebene und kann als Aktiv/Aktiv- oder Aktiv/Standby-Cluster aus Diensten umgesetzt werden. Der logische Router führt BGP und Peers mit physischen Routern aus. Im Aktiv/Standby-Modus kann der logische Router auch zustandsbehaftete Dienste bereitstellen.

Logischer Ebene-1-Router	Der logische Ebene-1-Router ist der Router der zweiten Ebene, der mit einem logischen Ebene-0-Router für Northbound-Konnektivität und mit einem oder mehreren Overlay-Netzwerken für Southbound-Konnektivität verbunden ist. Der logische Ebene-1-Router kann ein Aktiv/Standby-Cluster aus Diensten sein, 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.
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-Endpunkt	Ermöglichen Hypervisor-Hosts die Teilnahme an einem NSX-T Data Center-Overlay. Das NSX-T Data Center-Overlay stellt ein Layer 2-Netzwerk über einer vorhandenen Layer 3-Netzwerk-Fabric bereit, indem Frames innerhalb von Paketen gekapselt und die Pakete über ein zugrunde liegendes Transportnetzwerk übertragen werden. Das zugrunde liegende Transportnetzwerk kann ein weiteres Layer 2-Netzwerk sein oder auch Layer 3-Grenzen überschreiten. Der VTEP ist der Verbindungspunkt, bei dem die Kapselung und Entkapselung stattfindet.

Vorbereitung für die Installation

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](#)
- [Allgemeine Aufgaben für die Installation von NSX-T Data Center](#)

Systemvoraussetzungen

NSX-T Data Center hat spezielle Anforderungen bezüglich der Hardwareressourcen und Softwareversionen.

Hypervisor-Anforderungen

Hypervisor	Version	CPU-Kerne	Arbeitsspeicher
vSphere	Unterstützte vSphere-Version	4	16 GB
RHEL KVM	7.5 und 7.4	4	16 GB
Ubuntu KVM	16.04.2 LTS	4	16 GB
CentOS-KVM	7,4	4	16 GB

NSX-T Data Center unterstützt die Hostvorbereitung unter RHEL 7.5, RHEL 7.4, Ubuntu 16.04 und CentOS 7.4. Die Bereitstellung von NSX Manager und NSX Controller wird unter RHEL 7.5 und CentOS 7.4 nicht unterstützt. Die Bereitstellung von NSX Edge-Knoten wird nur unter vSphere unterstützt.

Für ESXi-Hosts unterstützt NSX-T Data Center Hostprofile und Auto Deploy-Funktionen auf vSphere 6.7 U1 oder höher.



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.

Bare Metal Server-Anforderungen

Betriebssystem	Version	CPU-Kerne	Arbeitsspeicher
RHEL	7.5 und 7.4	4	16 GB
Ubuntu	16.04.2 LTS	4	16 GB
CentOS	7,4	4	16 GB

NSX Manager -Ressourcenanforderungen

Die Größe der virtuellen Thin-Festplatte beträgt 3,1 GB und die Größe der virtuellen Thick-Festplatte 200 GB.

Appliance	Arbeits- spei- cher	vCPU	Speicher	VM-Hardwareversion
NSX Manager Kleine VM	8 GB	2	200 GB	10 oder höher
NSX Manager Mittlere 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	32 GB	8	200 GB	10 oder höher
NSX Manager Besonders große VM	48 GB	12	200 GB	10 oder höher

Hinweis NSX Manager Kleine VM sollte in Bereitstellungen für Labor- und Testumgebungen verwendet werden.

Die Ressourcenanforderungen für den NSX Manager gelten auch für den NSX Policy Manager und den Cloud Service Manager.

NSX Controller -Ressourcenanforderungen

Appliance	Arbeitsspeicher	vCPU	Festplattenspeicher	Bereitstellungstyp
NSX Controller Kleine VM	8 GB	2	120 GB	Bereitstellungen für Labor- und Testumgebungen
NSX Controller Mittlere VM	16 GB	4	120 GB	Empfohlen für mittlere Bereitstellungsgröße
NSX Controller Große VM	32 GB	8	120 GB	Erforderlich für umfangreiche Bereitstellungen

Hinweis Stellen Sie drei NSX Controller bereit, um eine Hochverfügbarkeit zu gewährleisten und Ausfälle der NSX-T Data Center-Steuerungsebene zu vermeiden.

Jeder NSX Controller-Cluster muss auf drei separaten physischen Hypervisor-Hosts platziert werden, um die Beeinträchtigung der NSX-T Data Center-Steuerungsebene durch den Ausfall eines einzelnen physischen Hypervisor-Hosts zu vermeiden. Siehe dazu das Handbuch *NSX-T Data Center Reference Design*.

In Bereitstellungen für Labor- und Testumgebungen ohne Produktionsarbeitslasten ist ein einzelner NSX Controller zur Einsparung von Ressourcen akzeptabel.

Sie können nur kleine und große VM-Formfaktoren über die Benutzerschnittstelle der vSphere-OVF-Bereitstellung bereitstellen.

NSX Edge -VM-Ressourcenanforderungen

Bereitstellungsgröße	Arbeitsspeicher	vCPU	Festplattenspeicher	VM-Hardwareversion
Klein	4 GB	2	120 GB	10 oder höher (vSphere 5.5 oder höher)
Mittel	8 GB	4	120 GB	10 oder höher (vSphere 5.5 oder höher)
Groß	16 GB	8	120 GB	10 oder höher (vSphere 5.5 oder höher)

Hinweis Bei NSX Manager und NSX Edge dient die kleine Appliance für Proof-of-Concept-Bereitstellungen. Die mittlere Appliance eignet sich für eine typische Produktionsumgebung und kann bis zu 64 Hypervisoren unterstützen. Die große Appliance ist für große Bereitstellungen mit mehr als 64 Hypervisoren konzipiert.

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

CPU-Anforderungen für NSX Edge -VM und Bare-Metal NSX Edge

Hinweis 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.

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.

Hinweis Da die NSX-T Data Center-Datenebene Netzwerkfunktionen aus dem Intel Data Plane Development Kit (DPDK) verwendet, werden ausschließlich Intel-basierte CPUs unterstützt.

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

Systemvoraussetzungen für Bare Metal- NSX Edge

Prüfen Sie, ob die Bare Metal-Hardware für NSX Edge unter dieser URL aufgeführt ist: <https://certification.ubuntu.com/server/models/?release=16.04%20LTS&category=Server>. 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.

Spezifische Netzwerkkartenanforderungen für Bare Metal NSX Edge

Typ der Netzwerkkarte	Beschreibung	ID des PCI-Geräts
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_COM-BO_BACKPLANE	0x10F8
	IXGBE_DEV_ID_82599_COM-BO_BACKPLANE	0x000C
	IXGBE_SUBDEV_ID_82599_KX4_KR_MEZZ	0x10F9
	IXGBE_SUBDEV_ID_82599_KX4_KR_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

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

Arbeitsspeicher	CPU-Kerne	Festplattenspeicher
32 GB	8	200 GB

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 1.1.3-1OEM.670.0.0.8169922
Intel(R) Ethernet Controller XL710 for 40GbE QSFP+	

NSX Manager -Browserunterstützung

Browser	Windows 10	Windows 8.1	Ubuntu 14.04	Mac OS X 10.11 und 10.12
Internet Explorer 11	Ja	Ja		
Firefox 55			Ja	Ja
Chrome 60	Ja	Ja		Ja
Safari 10				Ja
Microsoft Edge 40	Ja			

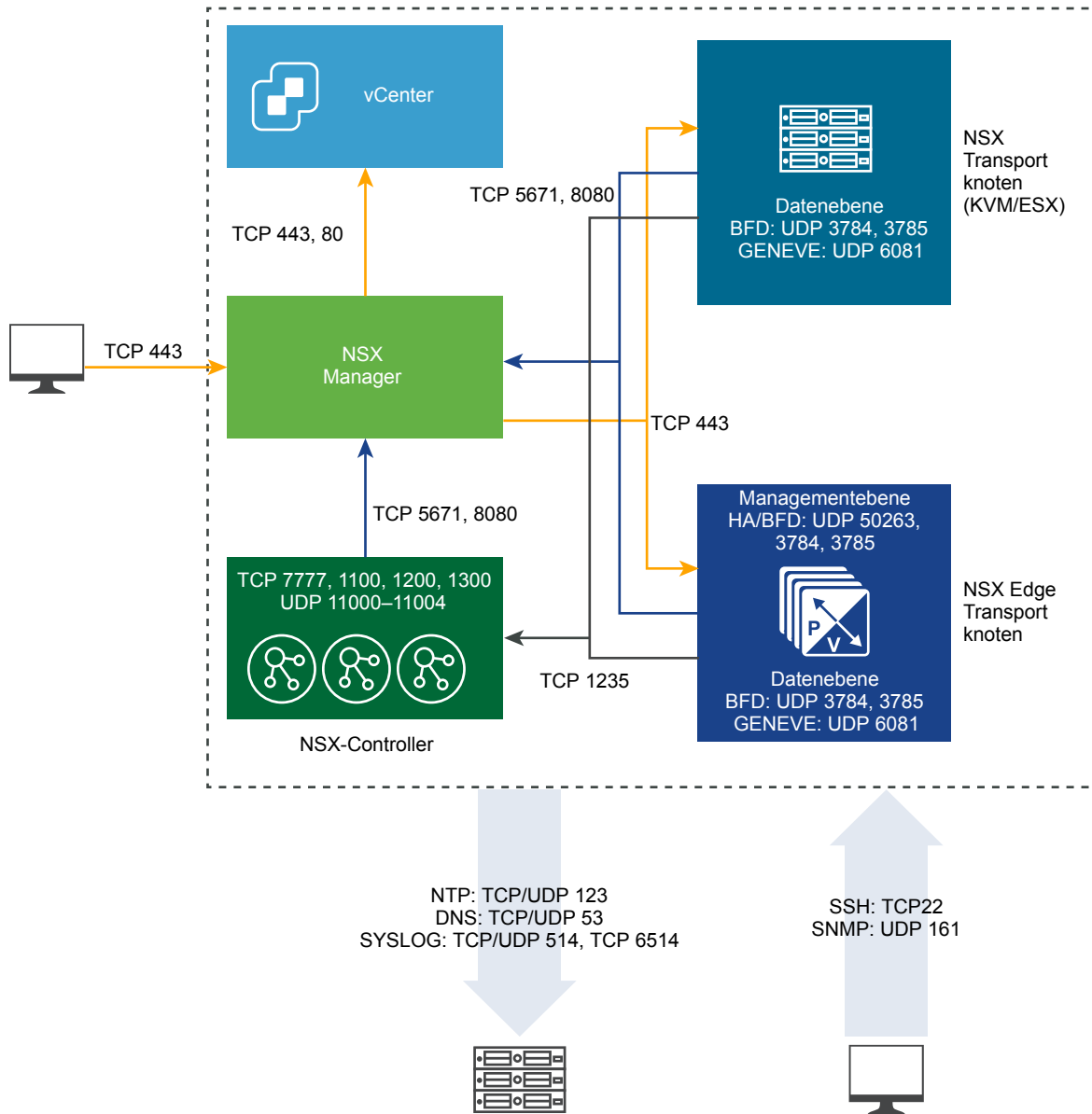
Hinweis Internet Explorer 11 im Kompatibilitätsmodus wird nicht unterstützt.

Die unterstützte Mindestauflösung des Browsers beträgt 1280 x 800 Pixel.

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.

Abbildung 2-1. 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
- ESX: netcpa, ESX-DP (im Kernel)


In der RMQ-Benutzerdatenbank (db) werden Kennwörter mit einer nicht umkehrbaren Hash-Funktion gehasht. $h(p1)$ ist also der Hash von Kennwort $p1$.

CCP Zentrale Steuerungskomponente

LCP Lokale Steuerungskomponente

MP	Managementebene
MPA	Managementebenen-Agent

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 Cloud erforderlich 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 2-1. Von NSX Manager verwendete TCP- und UDP-Ports

Quelle	Ziel	Port	Protokoll	Beschreibung
Verwaltungsclients	NSX Manager	22	TCP	SSH (standardmäßig deaktiviert)
NTP-Server	NSX Manager	123	UDP	NTP
Verwaltungsclients	NSX Manager	443	TCP	NSX-API-Server
SNMP-Server	NSX Manager	161	UDP	SNMP
NSX Controller, NSX Edge-Knoten, Transportknoten, vCenter Server	NSX Manager	8080	TCP	HTTP-Repository für Upgrade-Installation
NSX Controllers, NSX Edge-Knoten, Transportknoten	NSX Manager	5671	TCP	NSX-Messaging
NSX Manager	Management-SCP-Server	22	TCP	SSH (Hochladen von Support-Paketen, Sicherungen usw.)
NSX Manager	DNS-Server	53	TCP	DNS
NSX Manager	DNS-Server	53	UDP	DNS
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

Tabelle 2-1. Von NSX Manager verwendete TCP- und UDP-Ports (Fortsetzung)

Quelle	Ziel	Port	Protokoll	Beschreibung
NSX Manager	LogInsight-Server	9000	TCP	Log Insight-Agent
NSX Manager	Traceroute-Ziel	3343 4– 3352 3	UDP	Traceroute
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.

Von NSX Controller verwendete TCP- und UDP-Ports

NSX Controller 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 2-2. Von NSX Controller verwendete TCP- und UDP-Ports

Quelle	Ziel	Port	Protokoll	Beschreibung
Verwaltungsclients	NSX Controller	22	TCP	SSH (standardmäßig deaktiviert)
DNS-Server	NSX Controller	53	UDP	DNS
NTP-Server	NSX Controller	123	UDP	NTP
SNMP-Server	NSX Controller	161	UDP	SNMP
NSX Controllers	NSX Controller	1100	TCP	Zookeeper-Quorum
NSX Controllers	NSX Controller	1200	TCP	Zookeeper-Leaderauswahl
NSX Controllers	NSX Controller	1300	TCP	Zookeeper-Server
NSX Edge-Knoten, Transportknoten	NSX Controller	1235	TCP	CCP-netcpa-Kommunikation
NSX Controllers	NSX Controller	7777	TCP	Moot RPC
NSX Controllers	NSX Controller	11000–11004	UDP	Tunnel zu anderen Cluster-Knoten. Sie müssen weitere Ports öffnen, wenn das Cluster über mehr als 5 Knoten verfügt.
Traceroute-Ziel	NSX Controller	33434–33523	UDP	Traceroute
NSX Controllers	SSH-Ziel	22	TCP	SSH (standardmäßig deaktiviert)
NSX Controllers	DNS-Server	53	UDP	DNS
NSX Controllers	DNS-Server	53	TCP	DNS

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

Quelle	Ziel	Port	Protokoll	Beschreibung
NSX Controllers	NTP-Server	123	UDP	NTP
NSX Controllers	NSX Manager	5671	TCP	NSX-Messaging
NSX Controllers	LogInsight-Server	9000	TCP	Log Insight-Agent
NSX Controllers	NSX Controller	11000–11004	TCP	Tunnel zu anderen Cluster-Knoten. Sie müssen weitere Ports öffnen, wenn das Cluster über mehr als 5 Knoten verfügt.
NSX Controllers	NSX Manager	8080	TCP	NSX-Upgrade
NSX Controllers	Traceroute-Ziel	33434–33523	UDP	Traceroute
NSX Controllers	Syslog-Server	514	UDP	Syslog
NSX Controllers	Syslog-Server	514	TCP	Syslog
NSX Controllers	Syslog-Server	6514	TCP	Syslog

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 2-3. Von NSX Edge verwendete TCP- und UDP-Ports

Quelle	Ziel	Port	Protokoll	Beschreibung
Verwaltungsclients	NSX Edge-Knoten	22	TCP	SSH (standardmäßig deaktiviert)
NTP-Server	NSX Edge-Knoten	123	UDP	NTP
SNMP-Server	NSX Edge-Knoten	161	UDP	SNMP
NSX Edge-Knoten	NSX Edge-Knoten	1167	TCP	DHCP-Backend
NSX Edge-Knoten, Transportknoten	NSX Edge-Knoten	3784, 3785	UDP	BFD zwischen der TEP-IP-Adresse des Transportknotens in den Daten.
NSX Agent	NSX Edge-Knoten	5555	TCP	NSX Cloud: Agent der Instanz kommuniziert mit dem NSX Cloud-Gateway.
NSX Edge-Knoten	NSX Edge-Knoten	6666	TCP	NSX Cloud: lokale NSX Edge-Kommunikation.
NSX Edge-Knoten	NSX Manager	8080	TCP	NAPI, NSX-T Data Center-Upgrade
NSX Edge-Knoten	NSX Edge-Knoten	2480	TCP	Nestdb

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

Quelle	Ziel	Port	Protokoll	Beschreibung
NSX Edge-Knoten	Management-SCP- oder -SSH-Server	22	TCP	SSH
NSX Edge-Knoten	DNS-Server	53	UDP	DNS
NSX Edge-Knoten	NTP-Server	123	UDP	NTP
NSX Edge-Knoten	SNMP-Server	161, 162	UDP	SNMP
NSX Edge-Knoten	SNMP-Server	161, 162	TCP	SNMP
NSX Edge-Knoten	NSX Manager	443	TCP	HTTPS
NSX Edge-Knoten	Syslog-Server	514	TCP	Syslog
NSX Edge-Knoten	Syslog-Server	514	UDP	Syslog
NSX Edge-Knoten	NSX Edge-Knoten	1167	TCP	DHCP-Backend
NSX Edge-Knoten	NSX Controllers	1235	TCP	netcpa
NSX Edge-Knoten	OpenStack Nova-API-Server	3000–9000	TCP	Metadaten-Proxy
NSX Edge-Knoten	NSX Manager	5671	TCP	NSX-Messaging
NSX Edge-Knoten	Syslog-Server	6514	TCP	Syslog über TLS
NSX Edge-Knoten	Traceroute-Ziel	33434 – 33523	UDP	Traceroute
NSX Edge-Knoten	NSX Edge-Knoten	50263	UDP	Hohe Verfügbarkeit

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

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

Tabelle 2-4. Von vSphere ESXi - und KVM-Hosts verwendete TCP- und UDP-Ports

Quelle	Ziel	Port	Protokoll	Beschreibung
NSX Manager	vSphere ESXi-Host	443	TCP	Verwaltungs- und Bereitstellungsverbindung
NSX Manager	KVM-Host	443	TCP	Verwaltungs- und Bereitstellungsverbindung
vSphere ESXi-Host	NSX Manager	5671	TCP	AMQP-Kommunikationskanal zu NSX Manager

Tabelle 2-4. Von vSphere ESXi - und KVM-Hosts verwendete TCP- und UDP-Ports (Fortsetzung)

Quelle	Ziel	Port	Protokoll	Beschreibung
vSphere ESXi-Host	NSX Controller	123 5	TCP	Steuerungskomponente – Kommunikation von LCP zu CCP
KVM-Host	NSX Manager	567 1	TCP	AMQP-Kommunikationskanal zu NSX Manager
KVM-Host	NSX Controller	123 5	TCP	Steuerungskomponente – Kommunikation von LCP zu CCP
vSphere ESXi-Host	NSX Manager	808 0	TCP	Installation und Upgrade des HTTP-Repositorys
KVM-Host	NSX Manager	808 0	TCP	Installation und Upgrade des HTTP-Repositorys
GENEVE Terminierungsendpunkt (TEP)	GENEVE Terminierungsendpunkt (TEP)	608 1	UDP	Transportnetzwerk
NSX-T Data Center-Transportknoten	NSX-T Data Center-Transportknoten	378 4, 378 5	UDP	BFD-Sitzung zwischen TEPs, im Datenpfad unter Verwendung der TEP-Schnittstelle

Allgemeine Aufgaben für die Installation von NSX-T Data Center

Verfolgen Sie den Installationsprozess anhand der Prüfliste.

Führen Sie die einzelnen Verfahren in der empfohlenen Reihenfolge durch.

- 1 Installieren von NSX Manager, weitere Informationen finden Sie unter [Kapitel 4NSX Manager-Installation](#).
- 2 Installieren von NSX Controllern, weitere Informationen finden Sie unter [Kapitel 5NSX Controller-Installation und -Clustering](#).
- 3 Verbinden der NSX Controllers mit der Managementebene, weitere Informationen finden Sie unter [NSX Controller-Verbindung mit NSX Manager](#).
- 4 Erstellen eines Master-NSX Controllers zum Initialisieren des Steuerungsclusters, weitere Informationen finden Sie unter [Initialisieren des Controller-Clusters zum Erstellen eines Controller-Cluster-Masters](#).
- 5 Verbinden der NSX Controller innerhalb eines Steuerungsclusters, weitere Informationen finden Sie unter [Verbinden von weiteren NSX Controllern mit dem Cluster-Master](#).

NSX Manager installiert NSX-T Data Center-Module nach dem Hinzufügen der Hypervisor-Hosts.

Hinweis Beim Installieren von NSX-T Data Center-Modulen werden Zertifikate auf Hypervisor-Hosts erstellt.

- 6 Verbinden der Hypervisor-Hosts mit der Managementebene, weitere Informationen finden Sie unter [Verbinden der Hypervisor-Hosts mit der Managementebene](#).

Der Host sendet sein Hostzertifikat an die Managementebene.

- 7 Installieren der NSX Edges, weitere Informationen finden Sie unter [Kapitel 6 NSX Edge-Installation](#).
- 8 Verbinden der NSX Edges mit der Managementebene, weitere Informationen finden Sie unter [Verbinden von NSX Edge mit der Managementebene](#).
- 9 Erstellen von Transportzonen und Transportknoten, weitere Informationen finden Sie unter [Kapitel 8 Transportzonen und Transportknoten](#).

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.

Standardmäßig wird die Installation in der folgenden Reihenfolge durchgeführt:

- 1 NSX Manager wird zuerst installiert.
- 2 NSX Controller kann installiert und mit der Managementebene verbunden werden.
- 3 NSX-T Data Center-Module können auf einem Hypervisor-Host installiert werden, bevor dieser mit der Managementebene verbunden wird. Sie können aber auch beide Verfahren gleichzeitig über die Menüschnittflächen **Fabric > Hosts > Hinzufügen** in der Benutzeroberfläche ausführen.
- 4 NSX Controller, NSX Edges und Hosts mit NSX-T Data Center-Modulen können jederzeit mit der Managementebene verbunden werden.

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 Controllers, NSX Edges und Hosts der Managementebene beitreten, werden die logischen NSX-T Data Center-Einheiten und Konfigurationszustände automatisch an die NSX Controllers, NSX Edges und Hosts weitergegeben.

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

Arbeiten mit KVM

NSX-T Data Center unterstützt KVM auf zwei Arten: 1) als Hosttransportknoten und 2) als Host für NSX Manager und NSX Controller.

Tabelle 3-1. Unterstützte KVM-Versionen

Anforderungen	Beschreibung
Unterstützte Plattformen	<ul style="list-style-type: none"> ■ RHEL 7.5 ■ RHEL 7.4 ■ Ubuntu 16.04.2 LTS ■ CentOS 7.4

Dieses Kapitel enthält die folgenden Themen:

- [Einrichten von KVM](#)
- [Verwalten der Gast-VMs in der KVM-CLI](#)

Einrichten von KVM

Wenn Sie KVM als Transportknoten oder als Host für NSX Manager- und NSX Controller-Gast-VMs verwenden möchten, KVM aber noch nicht eingerichtet haben, können Sie wie hier beschrieben vorgehen.

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

Verfahren

- 1 Nur Red Hat: 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 planen, das NSX-T Container-Plug-In ausführen, für das bestimmte Kompatibilitätsanforderungen gelten.

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

Die unterstützte RHEL-Version ist 7.4.

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 vir- tinst virt-manager virt-viewer libguestfs-tools</pre>
RHEL	<pre>yum groupinstall "Virtualization Hypervisor" yum groupinstall "Virtualization Client" yum groupinstall "Virtualization Platform" yum groupinstall "Virtualization Tools"</pre>

5 Prüfen Sie die Hardware-Virtualisierungsfähigkeit.

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

Die Ausgabe sollte vmx enthalten.

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

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

- 7 Bereiten Sie für die Verwendung von KVM als Host für NSX Manager oder NSX Controller das Bridge-Netzwerk, die Management-Schnittstelle 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-Hosts Uplink-Schnittstellen zuweisen, sollten Sie sicherstellen, dass die von diesen Uplinks verwendeten Schnittstellenskripte 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	<p>Bearbeiten Sie <code>/etc/network/interfaces</code>:</p> <pre> 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 </pre> <p>Erstellen Sie eine XML-Netzwerkdefinitionsdatei für die Bridge. Erstellen Sie z. B. <code>/tmp/bridge.xml</code> mit den folgenden Zeilen:</p> <pre> <network> <name>bridge</name> <forward mode='bridge' /> <bridge name='br0' /> </network> </pre> <p>Definieren und starten Sie das Bridge-Netzwerk mit den folgenden Befehlen:</p> <pre> virsh net-define bridge.xml virsh net-start bridge virsh net-autostart bridge </pre>

Linux-Bereitstellung**Netzwerkkonfiguration**

Sie können den Status des Bridge-Netzwerks mit dem folgenden Befehl überprüfen:

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

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

RHEL

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

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


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

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

Nach diesem Schritt wird die Bridge-Schnittstelle „`nsx-vtep0.0`“ erstellt, sobald der KVM-Host als Transportknoten konfiguriert wurde. 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
```

- 9 Starten Sie den Netzwerkdienst `systemctl restart network` oder den Linux-Server neu, damit die Netzwerkänderungen in Kraft treten.

Verwalten der Gast-VMs in der KVM-CLI

NSX Manager und NSX Controller 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)

```

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.

Eine NSX-T Data Center-Bereitstellung kann nur über eine einzige Instanz von NSX Manager verfügen. Wenn NSX Manager auf einem ESXi-Host bereitgestellt wird, können Sie die Verfügbarkeit von NSX Manager mithilfe der Hochverfügbarkeitsfunktion (High Availability, HA) von vSphere sicherstellen.

Tabelle 4-1. Anforderung an die NSX Manager -Bereitstellung, -Plattform und -Installation

Anforderungen	Beschreibung
Unterstützte Bereitstellungsmethoden	<ul style="list-style-type: none"> ■ OVA/OVF ■ QCOW2
Unterstützte Plattformen	<p>Siehe Systemvoraussetzungen.</p> <p>Es wird empfohlen, die NSX Manager-Appliance unter ESXi auf freigegebenem Speicher zu installieren. Für die vSphere-Hochverfügbarkeit wird freigegebener Speicher benötigt, damit VMs auf einem anderen Host neu gestartet werden können, falls der ursprüngliche Host ausfällt.</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 acht Zeichen ■ mindestens ein Kleinbuchstabe ■ mindestens ein Großbuchstabe ■ mindestens eine Zahl ■ mindestens ein Sonderzeichen ■ mindestens fünf unterschiedliche Zeichen ■ keine Wörterbuchwörter ■ keine Palindrome
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. Weitere Informationen zu Hostnamenbeschränkungen finden Sie unter https://tools.ietf.org/html/rfc952 und https://tools.ietf.org/html/rfc1123.</p>

Tabelle 4-1. Anforderung an die NSX Manager -Bereitstellung, -Plattform und -Installation (Fortsetzung)

Anforderungen	Beschreibung
VMware Tools	Auf der unter ESXi ausgeführten NSX Manager-VM sind VMware Tools installiert. Entfernen oder aktualisieren Sie VMTools nicht.
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. ■ Erstellen Sie das Ziel-VM-Portgruppennetzwerk, wenn noch keines vorhanden ist. Es wird empfohlen, NSX-T Data Center-Appliances in einem VM-Verwaltungsnetzwerk zu platzieren. <p>Wenn Sie über mehrere Verwaltungsnetzwerke verfügen, können Sie statische Routen von der NSX-T Data Center-Appliance zu den anderen Netzwerken hinzufügen.</p> <ul style="list-style-type: none"> ■ Planen Sie das IPv4-IP-Adressschema. In dieser Version von NSX-T Data Center wird IPv6 nicht unterstützt.
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 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 Manager über SSH oder an der Konsole als die **admin**-Benutzer 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.

Dieses Kapitel enthält die folgenden Themen:

- [Installieren Sie NSX Manager und die verfügbaren Appliances](#)
- [Installieren von NSX Manager auf ESXi unter Verwendung des OVF-Befehlszeilentools](#)
- [Installieren von NSX Manager auf KVM](#)
- [Anmeldung beim neu erstellten NSX Manager](#)

Installieren Sie NSX Manager und die verfügbaren Appliances

Mithilfe von vSphere Web Client können Sie NSX Manager, NSX Policy Manager oder Cloud Service Manager als virtuelle Appliance bereitstellen.

Der NSX Policy Manager ist eine virtuelle Appliance zur Verwaltung von Richtlinien. Sie können Richtlinien konfigurieren, um Regeln für NSX-T Data Center-Komponenten wie logische Ports, IP-Adressen und VMs festzulegen. Mit NSX Policy Manager-Regeln können Sie allgemeine Nutzungs- und Ressourcenzugriffsregeln, die erzwungen werden, festlegen, ohne die genauen Details anzugeben.

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

Hinweis Es wird empfohlen, vSphere Web Client anstelle von vSphere Client zu verwenden. Wenn vCenter Server in Ihrer Umgebung nicht vorhanden ist, können Sie NSX Manager mit `ovftool` bereitstellen. Siehe [Installieren von NSX Manager auf ESXi unter Verwendung des OVF-Befehlszeilentools](#).

Verfahren

- 1 Suchen Sie die OVA- oder OVF-Datei der einheitlichen NSX-T Data Center-Appliance.
Kopieren Sie die Download-URL oder laden Sie die OVA-Datei auf Ihren Computer herunter.
- 2 Starten Sie in vSphere Web Client den Assistenten **OVF-Vorlage bereitstellen** und navigieren Sie zur .ova-Datei.

- 3 Geben Sie einen Namen für den NSX Manager ein und wählen Sie einen Ordner oder ein Datencenter.

Der eingegebene Name wird in der Bestandsliste angezeigt.

Der ausgewählte Ordner wird zum Anwenden von Berechtigungen für NSX Manager verwendet.

- 4 Wählen Sie einen Datenspeicher aus, in dem die Dateien der virtuellen NSX Manager-Appliance gespeichert werden sollen.
- 5 Wenn Sie die Installation in vCenter vornehmen, wählen Sie einen Host oder Cluster aus, auf dem die NSX Manager-Appliance bereitgestellt werden soll.
- 6 Wählen Sie die Portgruppe oder das Zielnetzwerk für NSX Manager.
- 7 Geben Sie die NSX Manager-Kennwörter und die IP-Einstellungen an.
- 8 Akzeptieren Sie die **nsx-manager**-Rolle.
 - Wählen Sie die **nsx-policy-manager**-Rolle aus dem Dropdown-Menü aus, um die NSX Policy Manager-Appliance zu installieren.
 - Wählen Sie die **nsx-cloud-service-manager**-Rolle aus dem Dropdown-Menü aus, um die NSX Cloud-Appliance zu installieren.

Hinweis Die Rolle **nsx-manager nsx-cloud-service-manager (multi-role)** wird nicht unterstützt.

- 9 (Optional) Reservieren Sie Arbeitsspeicher für die NSX-T Data Center-Komponente, um eine optimale Leistung zu erreichen.

Die Arbeitsspeicherreservierung ist eine garantierte Untergrenze für die Menge an physischem Arbeitsspeicher, die der Host für eine virtuelle Maschine reserviert, auch wenn der Arbeitsspeicher mehrfach vergeben wird. Legen Sie die Reservierung so fest, dass die NSX-T Data Center-Komponente über ausreichend Arbeitsspeicher für eine effiziente Ausführung verfügt. Siehe [Systemvoraussetzungen](#).

- 10 Öffnen Sie die Konsole der NSX-T Data Center-Komponente, um den Startvorgang zu verfolgen.
- 11 Melden Sie sich nach dem Start der NSX-T Data Center-Komponente als Administrator bei der Befehlszeilenschnittstelle an, und führen Sie den Befehl `get interface eth0` aus, um zu überprüfen, ob die IP-Adresse erwartungsgemäß angewendet wurde.

```
nsx-component> get interface eth0
Interface: eth0
  Address: 192.168.110.25/24
  MAC address: 00:50:56:86:7b:1b
  MTU: 1500
  Default gateway: 192.168.110.1
  Broadcast address: 192.168.110.255
  ...
```

12 Stellen Sie sicher, dass die NSX-T Data Center-Komponente über die erforderliche Konnektivität verfügt.

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

- Führen Sie für Ihre NSX-T Data Center-Komponente von einer anderen Maschine aus einen Ping-Vorgang aus.
- Die NSX-T Data Center-Komponente kann einen Ping-Vorgang für das zugehörige Standard-Gateway ausführen.
- Die NSX-T Data Center-Komponente kann mithilfe der Verwaltungsschnittstelle einen Ping-Vorgang für die Hypervisor-Hosts ausführen, die sich im selben Netzwerk wie die NSX-T Data Center-Komponente befinden.
- Die NSX-T Data Center-Komponente 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 Ihrer NSX-T Data Center-Komponente 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 bei der grafischen Benutzeroberfläche von NSX Manager an.

Die URL lautet `https://<IP-Adresse von NSX Manager>`. Beispiel: `https://10.16.176.10`.

Hinweis Sie müssen HTTPS verwenden. HTTP wird nicht unterstützt.

Installieren von NSX Manager auf ESXi unter Verwendung 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 beide 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, nsx_allowSSHRootLogin aber deaktiviert ist, können Sie eine SSH-Verbindung zu 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](#).

- Erstellen Sie das Ziel-VM-Portgruppennetzwerk, wenn noch keines vorhanden ist. Es wird empfohlen, NSX-T Data Center-Appliances in einem VM-Verwaltungsnetzwerk zu platzieren.

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

- Planen Sie das IPv4-IP-Adressschema. In dieser Version von NSX-T Data Center wird IPv6 nicht unterstützt.

Verfahren

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

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-manager
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--net="management"
--acceptAllEulas
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_role=nsx-manager
--prop:nsx_ip_0=192.168.110.75
--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|False>
--prop:nsx_allowSSHRootLogin=<True|False>
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-manager
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:<password>@192.168.110.51
Deploying to VI: vi://root:<password>@192.168.110.51
Transfer Completed
Powering on VM: nsx-manager
Task Completed
Completed successfully
```

- Führen Sie bei einem von vCenter Server verwalteten Host den `ovftool`-Befehl mit den jeweiligen Parametern aus. 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
--prop:nsx_ip_0=192.168.110.75
--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|False>
--prop:nsx_allowSSHRootLogin=<True|False>
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-manager
nsx-<component>.ova
vi://administrator@vsphere.local:<password>@192.168.110.24/?ip=192.168.110.51
```

```
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-manager
Task Completed
Completed successfully
```

- (Optional) Reservieren Sie Arbeitsspeicher für die NSX-T Data Center-Komponente, um eine optimale Leistung zu erreichen.

Die Arbeitsspeicherreservierung ist eine garantierte Untergrenze für die Menge an physischem Arbeitsspeicher, die der Host für eine virtuelle Maschine reserviert, auch wenn der Arbeitsspeicher mehrfach vergeben wird. Legen Sie die Reservierung so fest, dass die NSX-T Data Center-Komponente über ausreichend Arbeitsspeicher für eine effiziente Ausführung verfügt. Siehe [Systemvoraussetzungen](#).

- Öffnen Sie die Konsole der NSX-T Data Center-Komponente, um den Startvorgang zu verfolgen.

- Melden Sie sich nach dem Start der NSX-T Data Center-Komponente als Administrator bei der Befehlszeilenschnittstelle an, und führen Sie den Befehl `get interface eth0` aus, um zu überprüfen, ob die IP-Adresse erwartungsgemäß angewendet wurde.

```
nsx-component> get interface eth0
Interface: eth0
Address: 192.168.110.25/24
MAC address: 00:50:56:86:7b:1b
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

- Stellen Sie sicher, dass die NSX-T Data Center-Komponente über die erforderliche Konnektivität verfügt.

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

- Führen Sie für Ihre NSX-T Data Center-Komponente von einer anderen Maschine aus einen Ping-Vorgang aus.
- Die NSX-T Data Center-Komponente kann einen Ping-Vorgang für das zugehörige Standard-Gateway ausführen.
- Die NSX-T Data Center-Komponente kann mithilfe der Verwaltungsschnittstelle einen Ping-Vorgang für die Hypervisor-Hosts ausführen, die sich im selben Netzwerk wie die NSX-T Data Center-Komponente befinden.
- Die NSX-T Data Center-Komponente 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 Ihrer NSX-T Data Center-Komponente 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 bei der grafischen Benutzeroberfläche von NSX Manager an.

Die URL lautet `https://<IP-Adresse von NSX Manager>`. Beispiel: `https://10.16.176.10`.

Hinweis Sie müssen HTTPS verwenden. HTTP wird nicht unterstützt.

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 [Kapitel 4 NSX Manager-Installation](#).

Verfahren

- 1 Laden Sie das QCOW2-Image für NSX Manager herunter, und kopieren Sie es per SCP oder Synchronisierung auf die KVM-Maschine, auf der der NSX Manager ausgeführt wird.
- 2 (Nur Ubuntu) Fügen Sie den derzeit angemeldeten Benutzer als libvirtd-Benutzer hinzu:

```
adduser $USER libvirtd
```

- 3 Erstellen Sie in dem Verzeichnis, in dem Sie das QCOW2-Image gespeichert haben, eine Datei mit dem Namen „guestinfo“ (ohne Dateierweiterung) und füllen Sie diese mit den Eigenschaften der NSX Manager-VM.

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_role" oe:value="nsx-manager"/>
    <Property oe:key="nsx_allowSSHRootLogin" oe:value="True"/>
    <Property oe:key="nsx_cli_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_dns1_0" oe:value="192.168.110.10"/>
    <Property oe:key="nsx_domain_0" oe:value="corp.local"/>
    <Property oe:key="nsx_gateway_0" oe:value="192.168.110.1"/>
    <Property oe:key="nsx_hostname" oe:value="nsx-manager1"/>
    <Property oe:key="nsx_ip_0" oe:value="192.168.110.19"/>
    <Property oe:key="nsx_isSSHEnabled" oe:value="True"/>
    <Property oe:key="nsx_netmask_0" oe:value="255.255.255.0"/>
    <Property oe:key="nsx_ntp_0" oe:value="192.168.110.10"/>
    <Property oe:key="nsx_passwd_0" oe:value="<password>"/>
  </PropertySection>
</Environment>
```

In diesem Beispiel sind `nsx_isSSHEnabled` und `nsx_allowSSHRootLogin` beide 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, `nsx_allowSSHRootLogin` aber deaktiviert ist, können Sie eine SSH-Verbindung zu NSX Manager herstellen, sich aber nicht als Root anmelden.

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

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

```
sudo guestfish --rw -i -a nsx-manager1-build.qcow2 upload guestinfo /config/guestinfo
```

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

```
user@ubuntu1604:/var/lib/libvirt/images$ sudo virt-install --import --name nsx-manager1 --ram 16348 --vcpus 4 --network=bridge:br0,model=e1000 --disk path=/var/lib/libvirt/images/nsx-manager-1.1.0.0.0.4446302.qcow2,format=qcow2 --nographics
```

```
Starting install...
Creating domain...      |    0 B    00:01
Connected to domain nsx-manager1
Escape character is ^]
```

```
nsx-manager1 login:
```

Nach dem NSX Manager-Start wird die NSX Manager-Konsole angezeigt.

- 6 (Optional) Reservieren Sie Arbeitsspeicher für die NSX-T Data Center-Komponente, um eine optimale Leistung zu erreichen.

Die Arbeitsspeicherreservierung ist eine garantierte Untergrenze für die Menge an physischem Arbeitsspeicher, die der Host für eine virtuelle Maschine reserviert, auch wenn der Arbeitsspeicher mehrfach vergeben wird. Legen Sie die Reservierung so fest, dass die NSX-T Data Center-Komponente über ausreichend Arbeitsspeicher für eine effiziente Ausführung verfügt. Siehe [Systemvoraussetzungen](#).

- 7 Öffnen Sie die Konsole der NSX-T Data Center-Komponente, um den Startvorgang zu verfolgen.
- 8 Melden Sie sich nach dem Start der NSX-T Data Center-Komponente als Administrator bei der Befehlszeilenschnittstelle an, und führen Sie den Befehl `get interface eth0` aus, um zu überprüfen, ob die IP-Adresse erwartungsgemäß angewendet wurde.

```
nsx-component> get interface eth0
Interface: eth0
Address: 192.168.110.25/24
MAC address: 00:50:56:86:7b:1b
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

- 9 Stellen Sie sicher, dass die NSX-T Data Center-Komponente über die erforderliche Konnektivität verfügt.

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

- Führen Sie für Ihre NSX-T Data Center-Komponente von einer anderen Maschine aus einen Ping-Vorgang aus.
- Die NSX-T Data Center-Komponente kann einen Ping-Vorgang für das zugehörige Standard-Gateway ausführen.
- Die NSX-T Data Center-Komponente kann mithilfe der Verwaltungsschnittstelle einen Ping-Vorgang für die Hypervisor-Hosts ausführen, die sich im selben Netzwerk wie die NSX-T Data Center-Komponente befinden.
- Die NSX-T Data Center-Komponente 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 Ihrer NSX-T Data Center-Komponente herstellen können.

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

- 10 Verlassen Sie die KVM-Konsole.

```
control-]
```

Nächste Schritte

Melden Sie sich über einen unterstützten Webbrowser bei der grafischen Benutzeroberfläche von NSX Manager an.

Die URL lautet `https://<IP-Adresse von NSX Manager>`. Beispiel: `https://10.16.176.10`.

Hinweis Sie müssen HTTPS verwenden. HTTP wird nicht unterstützt.

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, inklusive Informationen, wie Sie sich am Programm beteiligen und wieder abmelden können.

Voraussetzungen

Stellen Sie sicher, dass NSX Manager installiert ist.

Verfahren

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

NSX Controller -Installation und -Clustering

5

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

NSX Controller fungieren als zentraler Kontrollpunkt für alle logischen Switches innerhalb eines Netzwerks und verwalten Informationen zu allen Hosts, logischen Switches und logischen Routern.

NSX Controllers steuern die Geräte, die die Paketweiterleitung vornehmen. Diese Weiterleitungsgeräte werden als virtuelle Switches bezeichnet.

Virtuelle Switches wie der NSX-verwaltete Virtual Distributed Switch (N-VDS, früher als Host-Switch bekannt) und der Open vSwitch (OVS) befinden sich auf ESXi und anderen Hypervisoren wie KVM.

In einer Produktionsumgebung benötigen Sie einen NSX Controller-Cluster mit drei Mitgliedern, um Ausfallzeiten für die NSX-Steuerungsebene zu vermeiden. Jeder Controller muss auf einem eindeutigen Hypervisor-Host platziert werden (insgesamt drei physische Hypervisor-Hosts), um die Beeinträchtigung der NSX-Steuerungskomponente durch den Ausfall eines einzelnen physischen Hypervisors zu vermeiden. In Bereitstellungen für Labor- und Testumgebungen ohne Produktionsarbeitslasten ist die Ausführung eines einzelnen Controllers zur Einsparung von Ressourcen akzeptabel.

Tabelle 5-1. Anforderung an die NSX Controller -Bereitstellung, -Plattform und -Installation

Anforderungen	Beschreibung
Unterstützte Bereitstellungsmethoden	<ul style="list-style-type: none">■ OVA/OVF■ QCOW2 <p>Hinweis Die Bereitstellungsmethode für PXE Boot wird nicht unterstützt.</p>
Unterstützte Plattformen	<p>Siehe Systemvoraussetzungen.</p> <p>NSX Controller wird auf ESXi als VM und KVM unterstützt.</p> <p>Hinweis Die Bereitstellungsmethode für PXE Boot wird nicht unterstützt.</p>
IP-Adresse	<p>Ein NSX Controller muss eine statische IP-Adresse aufweisen. Sie können die IP-Adresse nach der Installation nicht mehr ändern.</p> <p>Planen Sie das IPv4-IP-Adressschema. In dieser Version von NSX-T Data Center wird IPv6 nicht unterstützt.</p>

Tabelle 5-1. Anforderung an die NSX Controller -Bereitstellung, -Plattform und -Installation (Fortsetzung)

Anforderungen	Beschreibung
Kennwort für NSX-T Data Center-Appliance	<ul style="list-style-type: none"> ■ mindestens acht Zeichen ■ mindestens ein Kleinbuchstabe ■ mindestens ein Großbuchstabe ■ mindestens eine Zahl ■ mindestens ein Sonderzeichen ■ mindestens fünf unterschiedliche Zeichen ■ keine Wörterbuchwörter ■ keine Palindrome
Hostname	Geben Sie beim Installieren von NSX Controller 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 Controller-VM sind VMware Tools installiert. Entfernen oder aktualisieren Sie VMTools nicht.
System	Stellen Sie sicher, dass die Systemanforderungen erfüllt sind. Siehe Systemvoraussetzungen .
Ports	Stellen Sie sicher, dass die erforderlichen Ports geöffnet sind. Siehe Ports und Protokolle .

NSX Controller -Installationsszenarien

Wichtig Wenn Sie NSX Controller 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 Controller über SSH oder an der Konsole als die **admin**-Benutzer 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 Controller 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 Controller 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

- Verwenden Sie keine Root-Berechtigungen, um Daemons oder Anwendungen zu installieren. Wenn Sie Root-Berechtigungen zum Installieren von Daemons oder Anwendungen verwenden, kann Ihr Supportvertrag ungültig werden. Verwenden Sie Root-Berechtigungen nur dann, wenn Sie durch das VMware-Supportteam dazu aufgefordert werden.
- Die Kerndienste der Appliance werden erst gestartet, wenn ein Kennwort mit ausreichender Komplexität festgelegt wurde.

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

Dieses Kapitel enthält die folgenden Themen:

- [Automatische Installation von Controller und Cluster über NSX Manager](#)
- [Installieren von NSX Controller auf ESXi unter Verwendung einer grafischen Benutzeroberfläche](#)
- [Installieren von NSX Controller auf ESXi unter Verwendung des OVF-Befehlszeilentools](#)
- [Installieren von NSX Controller auf KVM](#)
- [NSX Controller-Verbindung mit NSX Manager](#)
- [Initialisieren des Controller-Clusters zum Erstellen eines Controller-Cluster-Masters](#)
- [Verbinden von weiteren NSX Controllern mit dem Cluster-Master](#)

Automatische Installation von Controller und Cluster über NSX Manager

Sie können NSX Manager so konfigurieren, dass Controller automatisch auf vSphere ESXi-Hosts installiert werden. Nach der Bereitstellung werden diese Controller automatisch zu einem Controller-Cluster auf diesem vSphere ESXi-Host hinzugefügt, der von einem vCenter Server verwaltet wird. Zum automatischen Installieren von Controller-Clustern können Sie alternativ auch NSX Manager-REST APIs verwenden.

Mit NSX Manager können Sie automatisch zusätzliche Controller für einen vorhandenen Cluster bereitstellen, der manuell bereitgestellt wird. Allerdings müssen Sie, um einen manuell hinzugefügten Controller aus dem Cluster zu löschen, diesen manuell aus dem Cluster entfernen.

Unterstützte Anwendungsbeispiele

- Erstellen eines Clusters mit einem Knoten
- Erstellen eines Clusters mit mehreren Knoten
- Hinzufügen von Knoten zu einem vorhandenen Cluster
- Löschen eines automatisch bereitgestellten Controllers von einem funktionsfähigen Cluster

Konfigurieren der automatischen Installation von Controllern und Clustern unter Verwendung der Benutzeroberfläche von NSX Manager

Konfigurieren Sie NSX Manager für die automatische Installation von Controllern auf vSphere ESXi-Hosts, die von einem vCenter Server verwaltet werden. Nach der Installation werden diese Controller automatisch zu einem Controller-Cluster auf einem vSphere ESXi-Host hinzugefügt.

Voraussetzungen

- NSX Manager muss bereitgestellt sein.
- vCenter Server und vSphere ESXi-Hosts müssen bereitgestellt sein.
- Der vSphere ESXi-Host muss auf dem vCenter Server registriert sein.
- Der vSphere ESXi-Host muss über genügend CPU-, Arbeitsspeicher- und Festplattenspeicherressourcen verfügen, um 12 vCPUs, 48 GB RAM und 360 GB Speicher zu unterstützen.

Verfahren

- 1 Melden Sie sich beim NSX Manager an, <https://<nsxmanagerIPAddress>/>.
- 2 Wenn die NSX Manager-Benutzeroberfläche nicht über ein registriertes vCenter verfügt, wechseln Sie zum Bereich **Fabric**, klicken Sie auf **Berechnungsmanager** und fügen Sie einen Berechnungsmanager hinzu.
- 3 Klicken Sie auf der Seite „System“ auf **Controller hinzufügen**.
- 4 Geben Sie auf der Seite „Häufige Attribute“ die erforderlichen Werte ein.
- 5 Wählen Sie den **Berechnungsmanager** aus.
- 6 (Optional) Sie können SSH aktivieren.
- 7 (Optional) Sie können den Root-Zugriff aktivieren.
- 8 (Optional) Wenn Sie zu einem vorhandenen Cluster einen neuen Knoten hinzufügen, aktivieren Sie „Mit vorhandenem Cluster verbinden“.

- 9 Geben Sie den gemeinsamen geheimen Schlüssel ein, der für die Clusterinitialisierung und -bildung erforderlich ist, und bestätigen Sie ihn.

Hinweis Alle zu diesem Cluster hinzugefügten Controllerknoten müssen denselben gemeinsamen geheimen Schlüssel verwenden.

- 10 Geben Sie die Anmeldedaten für den Controller ein.
- 11 Klicken Sie auf **Weiter**.
- 12 Klicken Sie auf der Seite „Controller“ auf **Controller hinzufügen**.
- 13 Geben Sie für den Controllerknoten einen gültigen Hostnamen oder einen vollqualifizierten Domänennamen ein.
- 14 Wählen Sie den Cluster aus.
- 15 Optional: Wählen Sie den Ressourcenpool aus. Der Ressourcenpool enthält nur einen Pool mit Berechnungsressourcen für die Bereitstellung der Controllerknoten. Weisen Sie bestimmte Speicherressourcen zu.
- 16 Optional: Wählen Sie den Host aus.
- 17 Wählen Sie den Datenspeicher aus.
- 18 Wählen Sie die Verwaltungsschnittstelle aus, über die der Host mit verschiedenen Komponenten innerhalb des Hosts selbst kommuniziert.
- 19 Geben Sie eine statische IP-Adresse mit den Portdetails (*<IPAddress>/<PortNumber>*) und die Netzmaske ein.
- 20 Sie können mehrere Controller hinzufügen. Klicken Sie auf die Schaltfläche **+** und geben Sie die Controllerdetails ein, bevor Sie mit der Bereitstellung beginnen.
- 21 Klicken Sie auf **Fertigstellen**.

Die automatische Controller-Installation beginnt. Die Controller werden zuerst beim NSX Manager registriert, bevor der Cluster gebildet wird oder sie mit einem vorhandenen Cluster verbunden werden.

- 22 Überprüfen Sie, ob die Controller beim NSX Manager registriert sind.
 - a Melden Sie sich bei der NSX Manager-Konsole an.
 - b Geben Sie `# get management-cluster status` ein.

Der Status des Managementclusters muss „STABIL“ sein.
 - c Alternativ können Sie über die NSX Manager-Benutzeroberfläche prüfen, ob die Manager-Konnektivität „AKTIV“ lautet.
- 23 Überprüfen Sie den Status des Controller-Clusters.
 - a Melden Sie sich bei der CLI-Konsole des Controllers an.
 - b Geben Sie `# get control-cluster status` ein.

Der Status des Controller-Clusters muss „STABIL“ sein.

- c Alternativ können Sie über die NSX Manager-Benutzeroberfläche prüfen, ob die Cluster-Konnektivität „AKTIV“ lautet.

Nächste Schritte

Konfigurieren Sie NSX Manager für die automatische Installation von Controllern und Clustern mithilfe von APIs. Siehe [Konfigurieren der automatischen Installation von Controllern und Clustern unter Verwendung von APIs](#).

Konfigurieren der automatischen Installation von Controllern und Clustern unter Verwendung von APIs

Mithilfe von APIs konfigurieren Sie NSX Manager für die automatische Installation von Controllern auf vSphere ESXi-Hosts, die von einem vCenter Server verwaltet werden. Nach der Installation von Controllern werden diese automatisch zu einem Controller-Cluster auf vSphere ESXi-Hosts hinzugefügt.

Verfahren

- 1 Bevor Sie die automatische Erstellung des Controller-Clusters auslösen, müssen Sie die als Nutzlast der POST API erforderliche vCenter Server-ID, Berechnungs-ID, Speicher-ID und Netzwerk-ID abrufen.
- 2 Melden Sie sich beim vCenter Server an.
`https://<vCenterServer_IPAddress>/mob.`
- 3 Klicken Sie in der Spalte „Wert“ auf **Inhalt**.
- 4 Klicken Sie auf der Seite „Inhaltseigenschaften“ auf die Spalte „Wert“, suchen Sie nach „Datencenter“ und klicken Sie auf den Link „Gruppe“.
- 5 Klicken Sie auf der Seite „Gruppeneigenschaften“ auf die Spalte „Wert“ und klicken Sie auf den Link „Datencenter“.
- 6 Kopieren Sie auf der Seite „Datencenter-Eigenschaften“ den Datenspeicherwert und den Netzwerkwert, die Sie beim Erstellen des Controller-Clusters verwenden möchten.
- 7 Klicken Sie auf den Link **HostFolder**.
- 8 Kopieren Sie auf der Seite „Gruppeneigenschaften“ den Cluster-Wert, den Sie beim Erstellen des Controller-Clusters verwenden möchten.
- 9 Wechseln Sie zum Abrufen der vCenter Server-ID zur NSX Manager-Benutzeroberfläche und kopieren Sie ihre ID von der Seite „Berechnungsmanager“.
- 10 POST `https://<nsx-manager>/api/v1/cluster/nodes/deployments`

```
REQUEST
{
  "deployment_requests": [
    {
      "roles": ["CONTROLLER"],
      "user_settings": {
        "cli_password": "CLIp4$$w4rd",
```

```

        "root_password": "R00Tp4$$w4rd"
    },
    "deployment_config": {
        "placement_type": "VsphereClusterNodeVMDeploymentConfig",
        "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
        "management_network_id": "network-13",
        "hostname": "controller-0",
        "compute_id": "domain-s9",
        "storage_id": "datastore-12",
        "default_gateway_addresses": [
            "10.33.79.253"
        ],
        "management_port_subnets": [
            {
                "ip_addresses": [
                    "10.33.79.64"
                ],
                "prefix_length": "22"
            }
        ]
    }
},
{
    "roles": ["CONTROLLER"],
    "user_settings": {
        "cli_password": "VMware$123",
        "root_password": "VMware$123"
    },
    "deployment_config": {
        "placement_type": "VsphereClusterNodeVMDeploymentConfig",
        "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
        "management_network_id": "network-13",
        "hostname": "controller-1",
        "compute_id": "domain-s9",
        "storage_id": "datastore-12",
        "default_gateway_addresses": [
            "10.33.79.253"
        ],
        "management_port_subnets": [
            {
                "ip_addresses": [
                    "10.33.79.65"
                ],
                "prefix_length": "22"
            }
        ]
    }
}
],
        "deployment_config": {
            "placement_type": "VsphereClusterNodeVMDeploymentConfig",
            "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
            "management_network_id": "network-13",
            "hostname": "controller-0",

```

```

    "compute_id": "domain-s9",
    "storage_id": "datastore-12",
    "default_gateway_addresses": [
    "10.33.79.253"
    ],
    "management_port_subnets": [
    {
        "ip_addresses": [
        "10.33.79.66"
        ],
        "prefix_length": "22"
        }
    ]
    }
},

    "clustering_config": {
"clustering_type": "ControlClusteringConfig",
"shared_secret": "123456",
"join_to_existing_cluster": false
    }
}

Response
{
    "result_count": 2,
    "results": [
    {
        "user_settings": {
            "cli_password": "[redacted]",
            "root_password": "[redacted]",
            "cli_username": "admin"
        },
        "vm_id": "71f02260-644f-4482-aa9a-ab8570bb49a3",
        "roles": [
            "CONTROLLER"
        ],
        "deployment_config": {
            "placement_type": "VsphereClusterNodeVMDeploymentConfig",
            "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
            "management_network_id": "network-13",
            "default_gateway_addresses": [
                "10.33.79.253"
            ],
            "hostname": "controller-0",
            "compute_id": "domain-s9",
            "storage_id": "datastore-12",
            "management_port_subnets": [
                {
                    "ip_addresses": [
                        "10.33.79.64"
                    ],
                    "prefix_length": 22
                }
            ]
        }
    }
]

```

```

    },

    "form_factor": "SMALL"
  },

  {
    "user_settings": {
      "cli_password": "[redacted]",
      "root_password": "[redacted]",
      "cli_username": "admin"
    },

    "vm_id": "38029a2b-b9bc-467f-8138-aef784e802cc",
    "roles": [
      "CONTROLLER"
    ],
    "deployment_config": {
      "placement_type": "VsphereClusterNodeVMDeploymentConfig",
      "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
      "management_network_id": "network-13",
      "hostname": "controller-1",
      "compute_id": "domain-s9",
      "storage_id": "datastore-12"
    },
    "form_factor": "MEDIUM"
  }
]
}

```

- 11** Sie können den Status der Bereitstellung mit dem folgenden API-Aufruf anzeigen: GET <https://<nsx-manager>/api/v1/cluster/nodes/deployments>

```

{

  "result_count": 2,
  "results": [
    {
      "user_settings": {
        "cli_password": "[redacted]",
        "root_password": "[redacted]"
      },
      "vm_id": "12f563af-af9f-48f3-848e-e9257c8740b0",
      "roles": [
        "CONTROLLER"
      ],

      "deployment_config": {
        "placement_type": "VsphereClusterNodeVMDeploymentConfig",
        "vc_id": "15145422-47a1-4c55-81da-01d953151d1f",
        "management_network_id": "network-158",
        "hostname": "controller-0",
        "compute_id": "domain-c154",
        "storage_id": "datastore-157"
      },

```



```

    "form_factor": "SMALL",
  },
  {
    "user_settings": {
      "cli_password": "[redacted]",
      "root_password": "[redacted]"
    },
    "vm_id": "cc21854c-265b-42de-af5f-05448c00777a",
    "roles": [
      "CONTROLLER"
    ],
    "deployment_config": {
      "placement_type": "VsphereClusterNodeVMDeploymentConfig",
      "vc_id": "feb17651-49a7-4ce6-88b4-41d3f624e53b",
      "management_network_id": "network-158",
      "hostname": "controller-0",
      "compute_id": "domain-c154",
      "storage_id": "datastore-157"
    },
    "form_factor": "MEDIUM",
  }
]
}

```

Nächste Schritte

Löschen Sie einen Cluster. Siehe [NSX Controller löschen](#).

NSX Controller löschen

NSX Controller aus dem Cluster löschen.

Verfahren

- 1 Melden Sie sich auf **https://<nsx-manager-ip>/** an.
- 2 Klicken Sie auf **System > Komponenten**.
- 3 Identifizieren Sie unter „Controller-Cluster“ den NSX Controller.
- 4 Klicken Sie auf das Symbol **Einstellungen** und klicken Sie auf **Löschen**.
- 5 Klicken Sie auf **Bestätigen**.

NSX-T Data Center trennt den NSX Controller vom Cluster, hebt seine Registrierung im NSX Manager auf, schaltet ihn aus und löscht den NSX Controller.

Nächste Schritte

Installieren eines NSX Controller auf einem vSphere ESXi-Host unter Verwendung der GUI. Siehe [Installieren von NSX Controller auf ESXi unter Verwendung einer grafischen Benutzeroberfläche](#).

Installieren von NSX Controller auf ESXi unter Verwendung einer grafischen Benutzeroberfläche

Wenn Sie eine interaktive NSX Controller-Installation bevorzugen, können Sie ein VM-Managementtool mit einer Benutzeroberfläche verwenden, z. B. den mit vCenter Server verbundenen vSphere Client.

Die Installation verläuft auch dann erfolgreich, wenn das Kennwort die Anforderungen nicht erfüllt. Wenn Sie sich jedoch zum ersten Mal anmelden, werden Sie aufgefordert, das Kennwort zu ändern.

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

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

- Stellen Sie sicher, dass die Systemanforderungen erfüllt sind. Siehe [Systemvoraussetzungen](#).
- Stellen Sie sicher, dass die erforderlichen Ports geöffnet sind. Siehe [Ports und Protokolle](#).
- Erstellen Sie das Ziel-VM-Portgruppennetzwerk, wenn noch keines vorhanden ist. Es wird empfohlen, NSX-T Data Center-Appliances in einem VM-Verwaltungsnetzwerk zu platzieren.

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

- Planen Sie das IPv4-IP-Adressschema. In dieser Version von NSX-T Data Center wird IPv6 nicht unterstützt.
- 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 *nsx-controller* festgelegt.
- Ein Managementtool, das OVF-Vorlagen wie vCenter Server oder den vSphere-Client bereitstellen kann.

Das OVF-Bereitstellungstool muss Konfigurationsoptionen für manuelle Konfiguration unterstützen.

- Das Client-Integrations-Plug-In muss installiert sein.

Verfahren

- 1 Suchen Sie die OVA- oder OVF-Datei von NSX Controller.
Kopieren Sie die Download-URL oder laden Sie die OVA-Datei auf Ihren Computer herunter.
- 2 Starten Sie im Managementtool den Assistenten **OVF-Vorlage bereitstellen** und navigieren Sie zur OVA-Datei.

- 3 Geben Sie einen Namen für den NSX Controller ein und wählen Sie einen Ordner oder ein Datencenter.

Der eingegebene Name wird in der Bestandsliste angezeigt.

Der ausgewählte Ordner wird zum Anwenden von Berechtigungen für NSX Controller verwendet.

- 4 Wählen Sie einen Datenspeicher aus, in dem die Dateien der virtuellen NSX Controller-Appliance gespeichert werden sollen.
- 5 Wenn Sie vCenter verwenden, wählen Sie einen Host oder Cluster aus, auf dem die NSX Controller-Appliance bereitgestellt werden soll.
- 6 Wählen Sie die Portgruppe oder das Zielnetzwerk für NSX Controller.
- 7 Geben Sie die NSX Controller-Kennwörter und die IP-Einstellungen an.
- 8 (Optional) Reservieren Sie Arbeitsspeicher für die NSX-T Data Center-Komponente, um eine optimale Leistung zu erreichen.

Die Arbeitsspeicherreservierung ist eine garantierte Untergrenze für die Menge an physischem Arbeitsspeicher, die der Host für eine virtuelle Maschine reserviert, auch wenn der Arbeitsspeicher mehrfach vergeben wird. Legen Sie die Reservierung so fest, dass die NSX-T Data Center-Komponente über ausreichend Arbeitsspeicher für eine effiziente Ausführung verfügt. Siehe [Systemvoraussetzungen](#).

- 9 Öffnen Sie die Konsole der NSX-T Data Center-Komponente, um den Startvorgang zu verfolgen.
- 10 Melden Sie sich nach dem Start der NSX-T Data Center-Komponente als Administrator bei der Befehlszeilenschnittstelle an, und führen Sie den Befehl `get interface eth0` aus, um zu überprüfen, ob die IP-Adresse erwartungsgemäß angewendet wurde.

```
nsx-component> get interface eth0
Interface: eth0
Address: 192.168.110.25/24
MAC address: 00:50:56:86:7b:1b
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

- 11 Stellen Sie sicher, dass die NSX-T Data Center-Komponente über die erforderliche Konnektivität verfügt.

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

- Führen Sie für Ihre NSX-T Data Center-Komponente von einer anderen Maschine aus einen Ping-Vorgang aus.
- Die NSX-T Data Center-Komponente kann einen Ping-Vorgang für das zugehörige Standard-Gateway ausführen.

- Die NSX-T Data Center-Komponente kann mithilfe der Verwaltungsschnittstelle einen Ping-Vorgang für die Hypervisor-Hosts ausführen, die sich im selben Netzwerk wie die NSX-T Data Center-Komponente befinden.
- Die NSX-T Data Center-Komponente 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 Ihrer NSX-T Data Center-Komponente 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

Verbinden Sie NSX Controller mit der Managementebene. Siehe [NSX Controller-Verbindung mit NSX Manager](#).

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

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

Standardmäßig sind „nsx_isSSEnabled“ und „nsx_allowSSHRootLogin“ aus Sicherheitsgründen beide deaktiviert. Wenn diese Optionen deaktiviert sind, können Sie SSH nicht verwenden oder sich nicht bei der NSX Controller-Befehlszeile anmelden. Wenn Sie nsx_isSSEnabled aktivieren, nsx_allowSSHRootLogin aber deaktiviert ist, können Sie eine SSH-Verbindung zu NSX Controller 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](#).
- Erstellen Sie das Ziel-VM-Portgruppennetzwerk, wenn noch keines vorhanden ist. Es wird empfohlen, NSX-T Data Center-Appliances in einem VM-Verwaltungsnetzwerk zu platzieren.

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

- Planen Sie das IPv4-IP-Adressschema. In dieser Version von NSX-T Data Center wird IPv6 nicht unterstützt.
- OVF Tool Version 4.0 oder höher

Verfahren

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

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-controller
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--network="management"
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.210
--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|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-controller
<path/url to nsx component ova>
vi://root:<password>@192.168.110.51
```

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

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-controller
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--network="management"
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.210
--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|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-controller
<path/url to nsx component ova>
vi://administrator@vsphere.local:<vcenter_password>@192.168.110.24/?ip=192.168.110.51
```

- (Optional) Reservieren Sie Arbeitsspeicher für die NSX-T Data Center-Komponente, um eine optimale Leistung zu erreichen.

Die Arbeitsspeicherreservierung ist eine garantierte Untergrenze für die Menge an physischem Arbeitsspeicher, die der Host für eine virtuelle Maschine reserviert, auch wenn der Arbeitsspeicher mehrfach vergeben wird. Legen Sie die Reservierung so fest, dass die NSX-T Data Center-Komponente über ausreichend Arbeitsspeicher für eine effiziente Ausführung verfügt. Siehe [Systemvoraussetzungen](#).

- Öffnen Sie die Konsole der NSX-T Data Center-Komponente, um den Startvorgang zu verfolgen.
- Melden Sie sich nach dem Start der NSX-T Data Center-Komponente als Administrator bei der Befehlszeilenschnittstelle an, und führen Sie den Befehl `get interface eth0` aus, um zu überprüfen, ob die IP-Adresse erwartungsgemäß angewendet wurde.

```
nsx-component> get interface eth0
Interface: eth0
  Address: 192.168.110.25/24
  MAC address: 00:50:56:86:7b:1b
  MTU: 1500
  Default gateway: 192.168.110.1
  Broadcast address: 192.168.110.255
  ...
```

- Stellen Sie sicher, dass die NSX-T Data Center-Komponente über die erforderliche Konnektivität verfügt.

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

- Führen Sie für Ihre NSX-T Data Center-Komponente von einer anderen Maschine aus einen Ping-Vorgang aus.
- Die NSX-T Data Center-Komponente kann einen Ping-Vorgang für das zugehörige Standard-Gateway ausführen.
- Die NSX-T Data Center-Komponente kann mithilfe der Verwaltungsschnittstelle einen Ping-Vorgang für die Hypervisor-Hosts ausführen, die sich im selben Netzwerk wie die NSX-T Data Center-Komponente befinden.
- Die NSX-T Data Center-Komponente 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 Ihrer NSX-T Data Center-Komponente 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

Verbinden Sie NSX Controller mit der Managementebene. Siehe [NSX Controller-Verbindung mit NSX Manager](#).

Installieren von NSX Controller auf KVM

NSX Controller fungiert als zentraler Kontrollpunkt für alle logischen Switches innerhalb eines Netzwerks und pflegt Informationen zu allen Hosts, logischen Switches und verteilten logischen Routern.

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

Verfahren

- 1 Laden Sie das NSX Controller-QCOW2-Image in das Verzeichnisse `/var/lib/libvirt/images` herunter.
- 2 (Nur Ubuntu) Fügen Sie den derzeit angemeldeten Benutzer als `libvirtd`-Benutzer hinzu:

```
adduser $USER libvirtd
```

- 3 Erstellen Sie in dem Verzeichnis, in dem Sie das QCOW2-Image gespeichert haben, eine Datei namens `guestinfo` (ohne Dateierweiterung) und füllen Sie diese mit den Eigenschaften der NSX Controller-VM.

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_allowSSHRootLogin" oe:value="True"/>
    <Property oe:key="nsx_cli_audit_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_cli_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_dns1_0" oe:value="192.168.110.10"/>
    <Property oe:key="nsx_domain_0" oe:value="corp.local"/>
    <Property oe:key="nsx_gateway_0" oe:value="192.168.110.1"/>
    <Property oe:key="nsx_hostname" oe:value="nsx-Controller1"/>
    <Property oe:key="nsx_ip_0" oe:value="192.168.110.34"/>
    <Property oe:key="nsx_isSSHEnabled" oe:value="True"/>
    <Property oe:key="nsx_netmask_0" oe:value="255.255.255.0"/>
    <Property oe:key="nsx_ntp_0" oe:value="192.168.110.10"/>
  </PropertySection>
</Environment>
```

```
<Property oe:key="nsx_passwd_0" oe:value="<password>"/>
</PropertySection>
</Environment>
```

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

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

Wenn Sie mehrere NSX Controller erstellen, müssen Sie für jeden Controller eine eigene Kopie des QCOW2-Images erstellen. Nachdem die Informationen aus `guestinfo` in ein QCOW2-Image geschrieben wurden, können Sie nicht mehr überschrieben werden.

```
sudo guestfish --rw -i -a nsx-controller1-build.qcow2 upload guestinfo /config/guestinfo
```

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

```
user@ubuntu1604:/var/lib/libvirt/images$ sudo virt-install --import --name nsx-controller1 --ram
16384 --vcpus 2 --network=bridge:br0,model=e1000 --disk path=/var/lib/libvirt/images/nsx-control-
ler-release_version_number.qcow2,format=qcow2 --nographics --noautoconsole
```

Nach dem NSX Controller-Start wird die NSX Controller-Konsole angezeigt.

- 6 (Optional) Reservieren Sie Arbeitsspeicher für die NSX-T Data Center-Komponente, um eine optimale Leistung zu erreichen.

Die Arbeitsspeicherreservierung ist eine garantierte Untergrenze für die Menge an physischem Arbeitsspeicher, die der Host für eine virtuelle Maschine reserviert, auch wenn der Arbeitsspeicher mehrfach vergeben wird. Legen Sie die Reservierung so fest, dass die NSX-T Data Center-Komponente über ausreichend Arbeitsspeicher für eine effiziente Ausführung verfügt. Siehe [Systemvoraussetzungen](#).

- 7 Öffnen Sie die Konsole der NSX-T Data Center-Komponente, um den Startvorgang zu verfolgen.
- 8 Melden Sie sich nach dem Start der NSX-T Data Center-Komponente als Administrator bei der Befehlszeilenschnittstelle an, und führen Sie den Befehl `get interface eth0` aus, um zu überprüfen, ob die IP-Adresse erwartungsgemäß angewendet wurde.

```
nsx-component> get interface eth0
Interface: eth0
Address: 192.168.110.25/24
MAC address: 00:50:56:86:7b:1b
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```


- 9 Stellen Sie sicher, dass die NSX-T Data Center-Komponente über die erforderliche Konnektivität verfügt.

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

- Führen Sie für Ihre NSX-T Data Center-Komponente von einer anderen Maschine aus einen Ping-Vorgang aus.
- Die NSX-T Data Center-Komponente kann einen Ping-Vorgang für das zugehörige Standard-Gateway ausführen.
- Die NSX-T Data Center-Komponente kann mithilfe der Verwaltungsschnittstelle einen Ping-Vorgang für die Hypervisor-Hosts ausführen, die sich im selben Netzwerk wie die NSX-T Data Center-Komponente befinden.
- Die NSX-T Data Center-Komponente 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 Ihrer NSX-T Data Center-Komponente 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

Verbinden Sie NSX Controller mit der Managementebene. Siehe [NSX Controller-Verbindung mit NSX Manager](#).

NSX Controller -Verbindung mit NSX Manager

Durch die NSX Controller-Verbindung mit NSX Manager wird sichergestellt, dass NSX Manager und NSX Controller miteinander kommunizieren können.

Voraussetzungen

- Stellen Sie sicher, dass NSX Manager installiert ist.
- Vergewissern Sie sich, dass Sie über Administratorberechtigungen zur Anmeldung bei den NSX Manager- und NSX Controller-Appliances verfügen.

Verfahren

- 1 Öffnen Sie eine SSH-Sitzung mit NSX Manager.
- 2 Öffnen Sie eine SSH-Sitzung mit jeder der NSX Controller-Appliances.
Beispiel: NSX-Controller1, NSX-Controller2 und NSX-Controller3
- 3 Führen Sie den Befehl `get certificate api thumbprint` auf NSX Manager aus.

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

- 4 Führen Sie auf jeder der NSX Controller-Appliances den Befehl **join management-plane** aus.

```
NSX-Controller1> join management-plane NSX-Manager-IP-address username admin thumbprint <NSX-Manager-thumbprint>
```

```
Password for API user: <NSX-Manager-password>
Node successfully registered and controller restarted
```

Führen Sie diesen Befehl auf jedem bereitgestellten NSX Controller-Knoten aus.

Geben Sie die folgenden Informationen an:

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

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

```
NSX-Controller1> get managers
- 192.168.110.47 Connected
```

- 6 Führen Sie auf der NSX Manager-Appliance den Befehl `get management-cluster status` aus und prüfen Sie, ob die NSX Controllers aufgelistet werden.

```
NSX-Manager> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.47 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.201 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086)
- 192.168.110.202 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086)
- 192.168.110.203 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086)
```

Nächste Schritte

Initialisieren Sie den Controller-Cluster. Siehe [Initialisieren des Controller-Clusters zum Erstellen eines Controller-Cluster-Masters](#).

Initialisieren des Controller-Clusters zum Erstellen eines Controller-Cluster-Masters

Nachdem Sie den ersten NSX Controller in der NSX-T Data Center-Bereitstellung installiert haben, können Sie den Controller-Cluster initialisieren. Die Initialisierung des Controller-Clusters ist auch dann erforderlich, wenn Sie eine kleine Proof of Concept-Umgebung (Machbarkeitsnachweis) mit nur einem Controller-Knoten einrichten. Wenn Sie den Controller-Cluster nicht initialisieren, kann der Controller nicht mit den Hypervisor-Hosts kommunizieren. Im Cluster brauchen Sie nur einen Controller zu initialisieren.

Voraussetzungen

- Installieren Sie mindestens einen NSX Controller.
- Verbinden Sie NSX Controller mit der Managementebene.
- Vergewissern Sie sich, dass Sie über Administratorberechtigungen zur Anmeldung bei der NSX Controller-Appliance verfügen.
- Weisen Sie ein gemeinsames geheimes Kennwort zu. Ein gemeinsames geheimes Kennwort ist ein benutzerdefinierter Schlüssel (z. B. „secret123“).

Verfahren

- 1 Öffnen Sie eine SSH-Sitzung für den NSX Controller.
- 2 Führen Sie den Befehl `set control-cluster security-model shared-secret secret <secret>` aus und geben Sie einen gemeinsamen geheimen Schlüssel ein, wenn Sie dazu aufgefordert werden.
- 3 Führen Sie den Befehl `initialize control-cluster` aus.

Durch diesen Befehl wird dieser Controller zum Controller-Cluster-Master.

Beispiel:

```
NSX-Controller1> initialize control-cluster
Control cluster initialization successful.
```

- 4 Führen Sie den Befehl `get control-cluster status verbose` aus.

Stellen Sie sicher, dass `is master` und `in majority true` sind, dass der Status `active` lautet und dass die Zookeeper Server IP als `reachable, ok` angegeben wird.

```
nsx-controller1> get control-cluster status verbose
NSX Controller Status:

uuid: 78d5b561-4f66-488d-9e53-089735eac1c1
is master: true
in majority: true
uuid                                address                        status
78d5b561-4f66-488d-9e53-089735eac1c1 192.168.110.34                active
```

Cluster Management Server Status:

uuid id	vpn address	rpc address status	rpc port	global
557a911f-41fd-4977-9c58-f3ef55b3efe7	192.168.110.34	7777		
1	169.254.1.1	connected		

Zookeeper Ensemble Status:

Zookeeper Server IP: 10.0.0.1, reachable, ok
 Zookeeper version: 3.5.1-alpha--1, built on 03/08/2016 01:18 GMT
 Latency min/avg/max: 0/0/1841
 Received: 212095
 Sent: 212125
 Connections: 5
 Outstanding: 0
 Zxid: 0x10000017a
 Mode: leader
 Node count: 33
 Connections: /10.0.0.1:51726[1] (queued=0, rec-
 ved=60324, sent=60324, sid=0x100000f14a10003, lop=PING, est=1459376913497, to=30000, lcxid=0x8, lzxid=0x10
 000017a, lresp=604617273, llat=0, minlat=0, avglat=0, maxlat=1088)
 /10.0.0.1:35462[0] (queued=0, recved=1, sent=0)
 /10.0.0.1:51724[1] (queued=0, rec-
 ved=45786, sent=45803, sid=0x100000f14a10001, lop=GETC, est=1459376911226, to=40000, lcxid=0x21e, lzxid=0x1
 0000017a, lresp=604620658, llat=0, minlat=0, avglat=0, maxlat=1841)
 /10.0.0.1:51725[1] (queued=0, rec-
 ved=60328, sent=60333, sid=0x100000f14a10002, lop=PING, est=1459376913455, to=30000, lcxid=0xc, lzxid=0x10
 000017a, lresp=604618294, llat=0, minlat=0, avglat=0, maxlat=1356)
 /10.0.0.1:51730[1] (queued=0, rec-
 ved=45315, sent=45324, sid=0x100000f14a10006, lop=PING, est=1459376914516, to=40000, lcxid=0x49, lzxid=0x1
 0000017a, lresp=604623243, llat=0, minlat=0, avglat=0, maxlat=1630)

Nächste Schritte

Fügen Sie dem Controller-Cluster weitere NSX Controllers hinzu. Siehe [Verbinden von weiteren NSX Controllern mit dem Cluster-Master](#).

Verbinden von weiteren NSX Controllern mit dem Cluster-Master

Durch Erstellung eines Clusters aus NSX Controllern mit mehreren Knoten können Sie sicherstellen, dass mindestens ein NSX Controller immer verfügbar ist.

Voraussetzungen

- Installieren Sie mindestens drei NSX Controller-Appliances.
- Vergewissern Sie sich, dass Sie über Administratorberechtigungen zur Anmeldung bei den NSX Controller-Appliances verfügen.
- Stellen Sie sicher, dass die NSX Controller-Knoten mit der Managementebene verbunden wurden. Siehe [NSX Controller-Verbindung mit NSX Manager](#).

- Initialisieren Sie den Controller-Cluster, um einen Controller-Cluster-Master zu erstellen. Sie müssen nur den ersten Controller initialisieren.
- Geben Sie im Befehl `join control-cluster` eine IP-Adresse und keinen Domännennamen an.
- Wenn Sie vCenter verwenden und NSX-T Data Center-Controller in demselben Cluster bereitstellen, achten Sie darauf, DRS-Anti-Affinitätsregeln zu konfigurieren. Mit DRS-Anti-Affinitätsregeln wird verhindert, dass mehrere Knoten in einen Host migriert werden.

Verfahren

- 1 Öffnen Sie eine SSH-Sitzung für jede der NSX Controller-Appliances.

Beispiel: NSX-Controller1, NSX-Controller2 und NSX-Controller3 In diesem Beispiel hat NSX-Controller1 den Controller-Cluster bereits initialisiert und ist der Controller-Cluster-Master.

- 2 Führen Sie auf den anderen NSX Controllern den Befehl `set control-cluster security-model` mit einem gemeinsamen geheimen Kennwort aus. Das für NSX-Controller2 und NSX-Controller3 eingegebene gemeinsame geheime Kennwort muss mit dem Kennwort übereinstimmen, das bei NSX-Controller1 eingegeben wurde.

Beispiel:

```
NSX-Controller2> set control-cluster security-model shared-secret secret <NSX-Controller1's-shared-secret-password>
```

```
Security secret successfully set on the node.
```

```
NSX-Controller3> set control-cluster security-model shared-secret secret <NSX-Controller1's-shared-secret-password>
```

```
Security secret successfully set on the node.
```

- 3 Führen Sie auf den Nicht-Master-NSX Controllern den Befehl `get control-cluster certificate thumbprint` aus.

Die Befehlsausgabe besteht aus einer Reihe von Zahlen, die für jeden NSX Controller eindeutig sind.

Beispiel:

```
NSX-Controller2> get control-cluster certificate thumbprint
...
```

```
NSX-Controller3> get control-cluster certificate thumbprint
...
```

- 4 Führen Sie auf dem Master-NSX Controller den Befehl **`join control-cluster`** aus.

Geben Sie die folgenden Informationen an:

- IP-Adresse mit einer optionalen Portnummer der Nicht-Master-NSX Controllern (NSX-Controller2 und NSX-Controller3 in diesem Beispiel)

- Zertifikatsfingerabdruck der Nicht-Master-NSX Controllers

Führen Sie die `join`-Befehle nicht für mehrere Controller gleichzeitig aus. Stellen Sie sicher, dass jede Verbindung abgeschlossen ist, bevor Sie einen weiteren Controller verbinden.

```
NSX-Controller1> join control-cluster <NSX-Controller2-IP> thumbprint <nsx-controller2's-thumbprint>
Node 192.168.210.48 has successfully joined the control cluster.
Please run 'activate control-cluster' command on the new node.
```

Stellen Sie sicher, dass NSX-Controller2 dem Cluster beigetreten ist, indem Sie den Befehl `get control-cluster status` ausführen.

```
NSX-Controller1> join control-cluster <NSX-Controller3-IP> thumbprint <nsx-controller3's-thumbprint>
Node 192.168.210.49 has successfully joined the control cluster.
Please run 'activate control-cluster' command on the new node.
```

Stellen Sie sicher, dass NSX-Controller3 dem Cluster beigetreten ist, indem Sie den Befehl `get control-cluster status` ausführen.

- 5 Führen Sie den Befehl `activate control-cluster` auf den zwei NSX Controller-Knoten aus, die dem Controller-Cluster-Master beigetreten sind.

Hinweis Führen Sie die `activate`-Befehle nicht auf mehreren NSX Controller-Controllern gleichzeitig aus. Stellen Sie sicher, dass jede Aktivierung abgeschlossen ist, bevor Sie einen weiteren Controller aktivieren.

Beispiel:

```
NSX-Controller2> activate control-cluster
Control cluster activation successful.
```

Führen Sie bei NSX-Controller2 den Befehl `get control-cluster status verbose` aus und stellen Sie sicher, dass für die Zookeeper Server IP `reachable, ok` angegeben ist.

```
NSX-Controller3> activate control-cluster
Control cluster activation successful.
```

Führen Sie bei NSX-Controller3 den Befehl `get control-cluster status verbose` aus und stellen Sie sicher, dass für die Zookeeper Server IP `reachable, ok` angegeben ist.

- 6 Überprüfen Sie das Ergebnis, indem Sie den Befehl `get control-cluster status` ausführen.

```
NSX-Controller1> get control-cluster status
uuid: db4aa77a-4397-4d65-ad33-9fde79ac3c5c
is master: true
in majority: true
```

uuid	address	status
0cfe232e-6c28-4fea-8aa4-b3518baef00d	192.168.210.47	active
bd257108-b94e-4e6d-8b19-7fa6c012961d	192.168.210.48	active
538be554-1240-40e4-8e94-1497e963a2aa	192.168.210.49	active

Die zuerst aufgeführte UUID gilt für den Controller-Cluster als Ganzes. Jeder NSX Controller-Knoten verfügt ebenfalls über eine UUID.

Wenn Sie versuchen, einen Controller mit einem Cluster zu verbinden, und der Befehl `set control-cluster security-model` oder `join control-cluster` fehlschlägt, sind die Clusterkonfigurationsdateien eventuell inkonsistent.

Um dieses Problem zu beheben, führen Sie die folgenden Schritte aus:

- Führen Sie den Befehl `deactivate control-cluster` auf dem NSX Controller aus, der dem Cluster beitreten soll.
- Wenn am Master-Controller der Befehl `get control-cluster status` oder `get control-cluster status verbose` Informationen zum fehlgeschlagenen Controller anzeigt, führen Sie den Befehl `detach control-cluster <IP address of failed controller>` aus.

Nächste Schritte

Stellen Sie NSX Edge bereit. Siehe [Kapitel 6 NSX Edge-Installation](#).

NSX Edge -Installation

NSX Edge liefert Routing-Dienste und Konnektivität zu Netzwerken, die zur NSX-T Data Center-Bereitstellung extern sind. Ein NSX Edge ist erforderlich, wenn Sie einen Tier-0- oder Tier-1-Router mit zu-standsbehafteten Diensten wie Netzwerkadressübersetzung (Network Address Translation, NAT), VPN usw. bereitstellen möchten.

Tabelle 6-1. 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.
Kennwort für NSX-T Data Center-Appliance	<ul style="list-style-type: none"> ■ mindestens acht Zeichen ■ mindestens ein Kleinbuchstabe ■ mindestens ein Großbuchstabe ■ mindestens eine Zahl ■ mindestens ein Sonderzeichen ■ mindestens fünf unterschiedliche Zeichen ■ keine Wörterbuchwörter ■ keine Palindrome
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.

Tabelle 6-1. Anforderung an die NSX Edge -Bereitstellung, -Plattformen und -Installation (Fortsetzung)

Anforderungen	Beschreibung
System	Stellen Sie sicher, dass die Systemanforderungen erfüllt sind. Siehe Systemvoraussetzungen .
NSX-Ports	Stellen Sie sicher, dass die erforderlichen Ports geöffnet sind. Siehe Ports und Protokolle . Erstellen Sie das Ziel-VM-Portgruppennetzwerk, wenn noch keines vorhanden ist. Es wird empfohlen, NSX-T Data Center-Appliances in einem VM-Verwaltungsnetzwerk zu platzieren.
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 das IPv4-IP-Adressschema. In dieser Version von NSX-T Data Center wird IPv6 nicht unterstützt. Das IPv6-Format wird nicht unterstützt.
OVF-Vorlage	<ul style="list-style-type: none"> ■ Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Bereitstellen einer OVF-Vorlage auf dem ES-Xi-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. <p>Das OVF-Bereitstellungstool muss Konfigurationsoptionen für manuelle Konfiguration unterstützen.</p> <ul style="list-style-type: none"> ■ 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.

Dieses Kapitel enthält die folgenden Themen:

- [NSX Edge-Netzwerkeinrichtung](#)
- [Automatische Bereitstellung von virtuellen NSX Edge-Maschinen aus NSX Manager](#)
- [Installieren eines NSX Edge unter ESXi über eine grafische vSphere-Benutzeroberfläche](#)
- [Installieren von NSX Edge auf ESXi unter Verwendung des OVF-Befehlszeilentools](#)
- [Installieren von NSX Edge mithilfe der ISO-Datei mit einem PXE-Server](#)
- [Verbinden von NSX Edge mit der Managementebene](#)

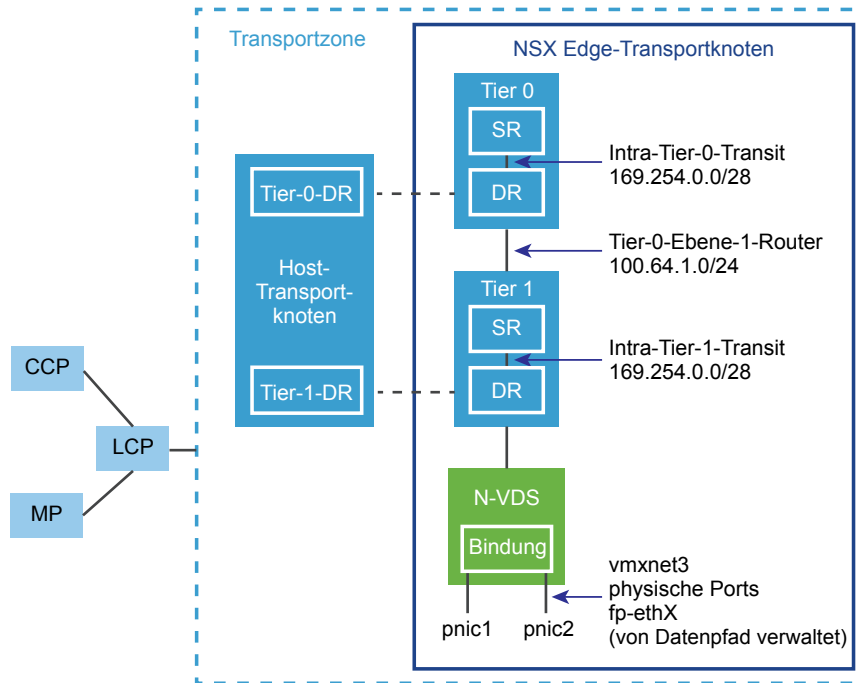
NSX Edge -Netzwerkeinrichtung

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

NSX Edge-Knoten sind Dienst-Appliances mit Kapazitätspools, die für die Durchführung von Netzwerkdiensten reserviert sind und nicht an die Hypervisoren verteilt werden können. Edge-Knoten können bei der ersten Bereitstellung als leere Container betrachtet werden.

Abbildung 6-1. Übersicht über NSX Edge



Ein NSX Edge-Knoten ist die Appliance, die physische Netzwerkkarten für die Verbindung mit der physischen Infrastruktur bereitstellt. Zu diesen Funktionen zählen:

- Konnektivität mit der physischen Infrastruktur
- NAT
- DHCP-Server
- Metadaten-Proxy
- Edge-Firewall

Wenn einer dieser Dienste konfiguriert ist oder wenn auf dem logischen Router ein Uplink definiert ist, um eine Verbindung mit der physischen Infrastruktur herzustellen, wird auf dem NSX Edge-Knoten ein SR instanziiert. Der NSX Edge-Knoten ist außerdem ein Transportknoten, wie die Computing-Knoten in NSX-T Data Center, und ähnlich wie Computing-Knoten kann sich NSX Edge mit mehr als einer Transportzone verbinden – eine für Overlay und weitere für Nord-Süd-Peering mit externen Geräten. Es gibt zwei Transportzonen in der NSX Edge:

Overlay-Transportzone – Jeder Datenverkehr, der von einer VM stammt, die an der NSX-T Data Center-Domäne teilnimmt, benötigt möglicherweise Erreichbarkeit von externen Geräten oder Netzwerken. Dies wird in der Regel als externer Nord-Süd-Datenverkehr bezeichnet. Der NSX Edge-Knoten ist zuständig für die Entkapselung des von Computing-Knoten empfangenen Overlay-Datenverkehrs sowie für die Kap-selung des an Computing-Knoten gesendeten Datenverkehrs.

VLAN-Transportzone – Neben der Funktion zur Kapselung oder Entkapselung des Datenverkehrs benötigen NSX Edge-Knoten außerdem eine VLAN-Transportzone, um Uplink-Konnektivität zur physischen Infrastruktur bereitzustellen.

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 eine NSX Edge 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.

Die Übersicht der NSX Edge-Abbildung zeigt 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.

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

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. Die primäre Komponente, die auf der Datenebene der Transportknoten beteiligt ist, ist der N-VDS. Der N-VDS leitet den Datenverkehr zwischen den Komponenten weiter, die auf dem Transportknoten ausgeführt werden; z. B. zwischen virtuellen Maschinen oder zwischen internen Komponenten und dem physischen Netzwerk. Im letzten Fall muss der N-VDS eine oder mehrere physische Schnittstellen (pNICs) auf dem Transportknoten besitzen. Wie andere virtuelle Switches kann ein N-VDS keine physische Schnittstelle mit einem anderen N-VDS gemeinsam nutzen. Er kann mit einem anderen N-VDS koexistieren, sofern ein separater Satz pNICs verwendet wird.

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.

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.

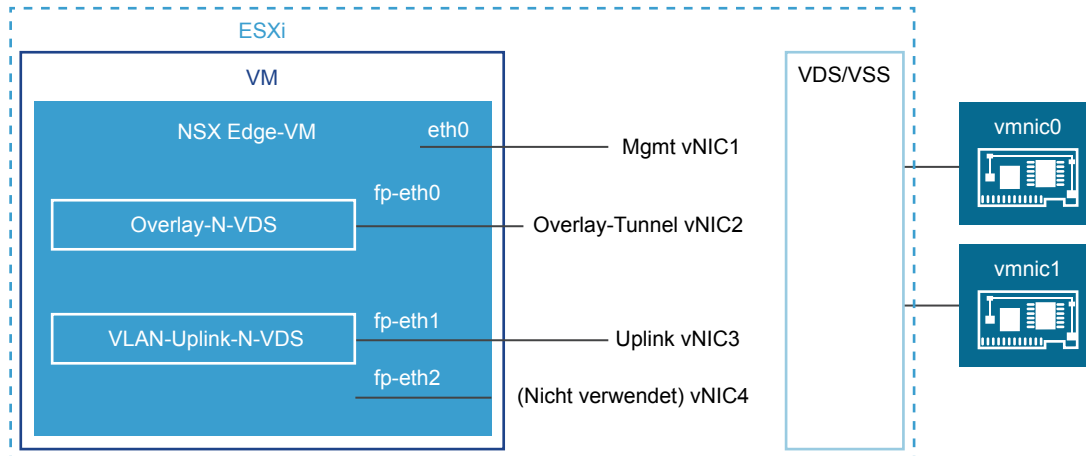
Weitere Informationen zu Transportzonen finden Sie unter [Grundlegende Informationen zu Transportzonen](#).

NSX Edge -Networking über virtuelle Appliance/VM

Eine NSX Edge-VM hat vier interne Schnittstellen: eth0, fp-eth0, fp-eth1 und fp-eth2. Eth0 ist für die Verwaltung reserviert, während die restlichen Schnittstellen DPDK-FastPath zugewiesen sind. Diese Schnittstellen werden für Uplinks zu Top-of-Rack(ToR-)Switches und für NSX-T Data Center-Overlay-Tunneling zugeteilt. Die Zuweisung der Schnittstellen entweder für Uplink oder Overlay ist flexibel. Beispiel: fp-eth0 kann für den Overlay-Datenverkehr fp-eth1, fp-eth2 oder beide für Uplink-Datenverkehr zugewiesen werden.

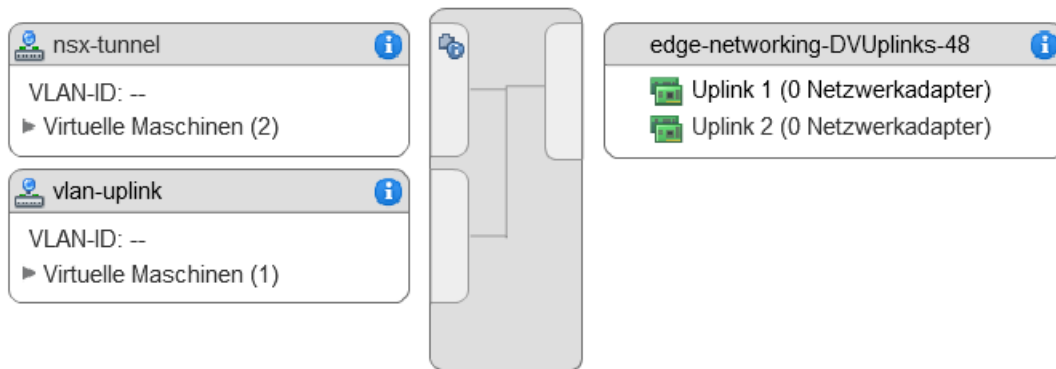
Auf dem vSphere Distributed Switch oder dem vSphere Standard Switch müssen Sie der NSX Edge mindestens zwei vmnics zuteilen, um Redundanz zu erhalten.

Im folgenden Beispiel für eine physische Topologie werden eth0 für das Verwaltungsnetzwerk, fp-eth0 für den NSX-T Data Center-Overlay-Datenverkehr und fp-eth1 für den VLAN-Uplink verwendet. fp-eth2 wird nicht verwendet. Wenn fp-eth2 nicht verwendet wird, müssen Sie die Verbindung trennen.

Abbildung 6-2. 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-uplink. Sie können die VM-Portgruppen beliebig benennen.

Bei einem Standard-vSwitch konfigurieren Sie beispielsweise die Trunk-Ports wie folgt: **Host > Konfiguration > Networking > Networking hinzufügen > Virtuelle Maschine > VLAN-ID Alle (4095)**.

Eine NSX Edge-VM kann auf dem vSphere Distributed Switch oder auf vSphere Standard Switches installiert werden.

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.

Mehrere NSX Edge-VMs können auf einem einzigen Host installiert werden, der dieselben Verwaltungs-, VLAN-und Overlay-Portgruppen nutzt.

Für eine auf einem ESXi-Host mit dem vSphere anstelle von N-VDS bereitgestellte NSX Edge-VM müssen Sie wie folgt vorgehen:

- Aktivieren Sie die gefälschte Übertragung für den DHCP-Server, der auf dieser NSX Edge ausgeführt wird.
- Aktivieren Sie den promiskuitiven Modus für die NSX Edge-VM, 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.

NSX Edge -Networking auf Bare-Metal-Bereitstellung

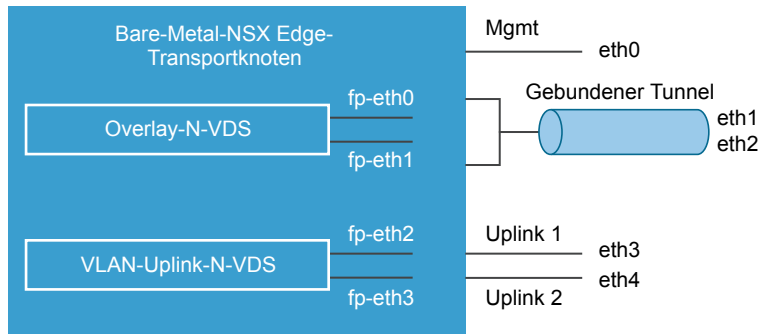
Die NSX-T Data Center Bare Metal-NSX Edge wird auf einem physischen Server ausgeführt und wird unter Verwendung einer ISO-Datei oder eines PXE-Startvorgangs installiert. Die Bare Metal-NSX Edge empfiehlt sich für Produktionsumgebungen, in denen neben der Layer-3-Unicast-Weiterleitung auch Dienste wie NAT, Firewall und Load Balancer benötigt werden. Eine Bare Metal-NSX Edge unterscheidet sich von der VM-Formfaktor-NSX Edge im Hinblick auf die Leistung. Sie bietet eine schnellere Konvergenz, ein schnelleres Failover und einen höheren Durchsatz.

Wenn ein Bare Metal-NSX Edge-Knoten installiert ist, wird eine dedizierte Schnittstelle für die Verwaltung beibehalten. Wenn Redundanz erwünscht wird, können zwei Netzwerkkarten für die Hochverfügbarkeit der Verwaltungsebene verwendet werden. Diese Verwaltungsschnittstellen können auch 1G sein.

Der Bare Metal-NSX Edge-Knoten unterstützt maximal 8 physische Netzwerkkarten für Overlay-Datenverkehr und Uplink-Datenverkehr zu den TOR-Switches. Für jede dieser 8 physischen Netzwerkkarten auf dem Server wird eine interne Schnittstelle mit einem Namen vom Typ „fp-ethX“ erstellt. Diese internen Schnittstellen werden DPDK-FastPath zugewiesen. Bei der Zuweisung von fp-eth-Schnittstellen für Overlay-oder Uplink-Konnektivität besteht vollständige Flexibilität.

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 6-3. Ein Vorschlag für die Linkeinrichtung für Bare-Metal- NSX Edge -Networking



Automatische Bereitstellung von virtuellen NSX Edge - Maschinen aus NSX Manager

Sie können eine NSX Edge in der NSX Manager-Benutzeroberfläche konfigurieren und NSX Edge automatisch in vCenter Server bereitstellen.

Voraussetzungen

- Siehe NSX Edge-Netzwerkanforderungen im Handbuch [NSX Edge-Netzwerkeinrichtung](#).
- Wenn ein vCenter Server in NSX-T Data Center als Berechnungsmanager registriert ist, können Sie über die Benutzeroberfläche von NSX Manager einen Host als NSX Edge-Knoten konfigurieren und ihn automatisch auf dem vCenter Server bereitstellen.
- Stellen Sie sicher, dass auf dem vCenter Server-Datenspeicher, auf dem die NSX Edge installiert wird, mindestens 120 GB verfügbar sind.
- Stellen Sie sicher, dass der vCenter Server-Cluster oder Host Zugriff auf die angegebenen Netzwerke und Datenspeicher in der Konfiguration hat.

Verfahren

- 1 Melden Sie sich über einen Browser bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Fabric > Knoten > Edges > 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 Wählen Sie eine Konfigurationsgröße aus: klein, mittel oder groß.

Die Systemanforderungen variieren je nach Konfigurationsgröße.

- 6 Geben Sie die Befehlszeilenschnittstelle (CLI) und die Root-Kennwörter für die Systeme an.

Die Einschränkungen für die Root- und CLI-Administratorkennwörter gelten auch für die automatische Bereitstellung.

- 7 Wählen Sie im Dropdown-Menü den Berechnungsmanager aus.

Der Berechnungsmanager entspricht der in der Managementebene registrierten vCenter Server.

- 8 Wählen Sie für den Berechnungsmanager einen Cluster im Dropdown-Menü aus, oder weisen Sie einen Ressourcenpool zu.

- 9 Wählen Sie einen Datenspeicher aus, in dem die Dateien der virtuellen NSX Edge-Maschine gespeichert werden sollen.

- 10 Wählen Sie den Cluster aus, auf dem die NSX Edge-VM bereitgestellt werden soll.

Es wird empfohlen, NSX Edge in einem Cluster hinzuzufügen, der Netzwerk-Management-Dienstprogramme zur Verfügung stellt.

- 11 Wählen Sie den Host oder Ressourcenpool aus. Es kann jeweils nur ein Host gleichzeitig hinzugefügt werden.

- 12 Wählen Sie die IP-Adresse aus, und geben Sie die IP-Adressen und Pfade des Verwaltungsnetzwerks ein, in dem die NSX Edge-Schnittstellen abgelegt werden sollen. Die IP-Adresse muss im CIDR-Format eingegeben werden.

Das Verwaltungsnetzwerk muss auf NSX Manager zugreifen können. Es muss seine IP-Adresse von einem DHCP-Server erhalten. Sie können die Netzwerke nach der NSX Edge-Bereitstellung ändern.

- 13 Fügen Sie ein Standard-Gateway hinzu, wenn die IP-Adresse des Verwaltungsnetzwerks nicht zu derselben Schicht 2 wie das NSX Manager-Netzwerk gehört.

Stellen Sie sicher, dass zwischen NSX Manager und dem NSX Edge-Verwaltungsnetzwerk eine Schicht-3-Konnektivität verfügbar ist.

Die NSX Edge-Bereitstellung nimmt 1 bis 2 Minuten in Anspruch. Sie können den Echtzeitstatus der Bereitstellung in der Benutzeroberfläche nachverfolgen.

Nächste Schritte

Wenn die NSX Edge-Bereitstellung fehlschlägt, navigieren Sie zu den Dateien `/var/log/cm-inventory/cm-inventory.log` und `/var/log/proton/nsxapi.log`, um das Problem zu beheben.

Bevor Sie NSX Edge einem NSX Edge-Cluster hinzufügen oder als Transportknoten konfigurieren, stellen Sie sicher, dass der neu erstellte NSX Edge-Knoten als „Knoten betriebsbereit“ angezeigt wird.

Installieren eines NSX Edge unter ESXi über eine grafische vSphere -Benutzeroberfläche

Wenn Sie eine interaktive NSX Edge-Installation bevorzugen, können Sie ein VM-Managementtool mit einer Benutzeroberfläche verwenden, z. B. den mit vCenter Server verbundenen vSphere Client.

In dieser Version von NSX-T Data Center wird IPv6 nicht unterstützt.

Voraussetzungen

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

Verfahren

- 1 Suchen Sie die OVA- oder OVF-Datei von NSX Edge.
Kopieren Sie die Download-URL oder laden Sie die OVA-Datei auf Ihren Computer herunter.
- 2 Starten Sie im Managementtool den Assistenten **OVF-Vorlage bereitstellen** und navigieren Sie zur OVA-Datei.
- 3 Geben Sie einen Namen für NSX Edge ein, und wählen Sie einen Ordner oder ein vCenter Server-Datencenter aus.
Der eingegebene Name wird in der Bestandsliste angezeigt.
Der ausgewählte Ordner wird zum Anwenden von Berechtigungen für NSX Edge verwendet.
- 4 Wählen Sie eine Konfigurationsgröße aus: klein, mittel oder groß.
Die Systemvoraussetzungen variieren abhängig von der konfigurierten Bereitstellungsgröße von NSX Edge. Siehe [Systemvoraussetzungen](#).
- 5 Wählen Sie einen Datenspeicher aus, in dem die Dateien der virtuellen NSX Edge-Appliance gespeichert werden sollen.
- 6 Wenn Sie die Installation in vCenter Server vornehmen, wählen Sie einen Host oder Cluster aus, auf dem die NSX Edge-Appliance bereitgestellt werden soll.
- 7 Wählen Sie die Netzwerke aus, in denen Sie die NSX Edge-Schnittstellen platzieren möchten.
Sie können die Netzwerke nach der NSX Edge-Bereitstellung ändern.
- 8 Geben Sie das NSX Edge-Kennwort und die IP-Einstellungen an.
- 9 (Optional) Reservieren Sie Arbeitsspeicher für die NSX-T Data Center-Komponente, um eine optimale Leistung zu erreichen.
Die Arbeitsspeicherreservierung ist eine garantierte Untergrenze für die Menge an physischem Arbeitsspeicher, die der Host für eine virtuelle Maschine reserviert, auch wenn der Arbeitsspeicher mehrfach vergeben wird. Legen Sie die Reservierung so fest, dass die NSX-T Data Center-Komponente über ausreichend Arbeitsspeicher für eine effiziente Ausführung verfügt. Siehe [Systemvoraussetzungen](#).
- 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 Melden Sie sich nach dem Starten des NSX Edge mit Administratorrechten bei der CLI an. Verwenden Sie dazu den Benutzernamen **admin** und das Kennwort **default**.

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

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

Interface: eth0
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
...
```

Führen Sie bei Bedarf den Befehl `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt` aus, um die Managementschnittstelle zu aktualisieren. Optional können Sie den SSH-Dienst mit dem Befehl `start service ssh` starten.

- 14 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.

- 15 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 DHCP die falsche Netzwerkkarte für die Verwaltung zuweist, führen Sie die Aufgaben zum Beheben des Problems aus.

- 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 eth0 dhcp plane mgmt** ein.

- c Platzieren Sie eth0 im DHCP-Netzwerk und warten Sie, bis eth0 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.

In dieser Version von NSX-T Data Center wird IPv6 nicht unterstützt.

Voraussetzungen

- Stellen Sie sicher, dass die Systemanforderungen erfüllt sind. Siehe [Systemvoraussetzungen](#).
- Stellen Sie sicher, dass die erforderlichen Ports geöffnet sind. Siehe [Ports und Protokolle](#).
- Erstellen Sie das Ziel-VM-Portgruppennetzwerk, wenn noch keines vorhanden ist. Es wird empfohlen, NSX-T Data Center-Appliances in einem VM-Verwaltungsnetzwerk zu platzieren.

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

- Planen Sie das IPv4-IP-Adressschema. In dieser Version von NSX-T Data Center wird IPv6 nicht unterstützt.
- Siehe NSX Edge-Netzwerkanforderungen im Handbuch [NSX Edge-Netzwerkeinrichtung](#).
- 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 4.0 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
```

- (Optional) Reservieren Sie Arbeitsspeicher für die NSX-T Data Center-Komponente, um eine optimale Leistung zu erreichen.

Die Arbeitsspeicherreservierung ist eine garantierte Untergrenze für die Menge an physischem Arbeitsspeicher, die der Host für eine virtuelle Maschine reserviert, auch wenn der Arbeitsspeicher mehrfach vergeben wird. Legen Sie die Reservierung so fest, dass die NSX-T Data Center-Komponente über ausreichend Arbeitsspeicher für eine effiziente Ausführung verfügt. Siehe [Systemvoraussetzungen](#).

- Öffnen Sie die Konsole von NSX Edge, um den Startvorgang zu verfolgen.
- Melden Sie sich nach dem Starten des NSX Edge mit Administratorrechten bei der CLI an. Verwenden Sie dazu den Benutzernamen **admin** und das Kennwort **default**.
- Führen Sie den Befehl `get interface eth0` aus, um zu überprüfen, ob die IP-Adresse wie erwartet angewendet wurde.

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

Interface: eth0
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
...
```

Führen Sie bei Bedarf den Befehl `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt` aus, um die Managementschnittstelle zu aktualisieren. Optional können Sie den SSH-Dienst mit dem Befehl `start service ssh` starten.

- 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 DHCP die falsche Netzwerkkarte für die Verwaltung zuweist, führen Sie die Aufgaben zum Beheben des Problems aus.

- 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 eth0 dhcp plane mgmt** ein.
- c Platzieren Sie eth0 im DHCP-Netzwerk und warten Sie, bis eth0 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 mithilfe der ISO-Datei mit einem PXE-Server

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

Hinweis Beachten Sie, dass die PXE-Boot-Installation für NSX Manager und NSX Controller nicht unterstützt wird. Sie können nicht zugleich Netzwerkeinstellungen, wie IP-Adresse, Gateway, Netzwerkmaske, NTP und DNS konfigurieren.

Vorbereiten des PXE-Servers für die NSX Edge -Installation

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-Netzwerkeinrichtung](#).

Verfahren

- (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 <mgr-ip> thumbprint <mgr-thumbprint> username <mgr-username> password <mgr-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[...]FcoHLijOuFD
```

- 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 unter Verwendung der Bare-Metal- oder der ISO-Datei. Siehe [Bare-Metal-Installation von NSX Edge](#) oder [Installieren von NSX Edge per ISO-Datei als virtuelle Appliance](#).

Bare-Metal-Installation von NSX Edge

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, Netzwerkmaske, 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-Netzwerkeinrichtung](#).

Verfahren

- 1 Erstellen Sie einen bootfähigen Datenträger mit der NSX Edge-ISO-Datei.
- 2 Starten Sie die physische Maschine von der Festplatte.
- 3 Wählen Sie **Automatisierte Installation**.

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

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**.

- 4 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.

- 5 Melden Sie sich nach dem Starten des NSX Edge mit Administratorrechten bei der CLI an. Verwenden Sie dazu den Benutzernamen **admin** und das Kennwort **default**.

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.

- 6 Nach dem Neustart können Sie sich entweder als Administrator oder als Root anmelden. Das Standardkennwort für die Root-Anmeldung lautet **vmware**.
- 7 Führen Sie den Befehl `get interface eth0` aus, um zu überprüfen, ob die IP-Adresse wie erwartet angewendet wurde.

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

Interface: eth0
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
...
```

Führen Sie bei Bedarf den Befehl `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt` aus, um die Managementschnittstelle zu aktualisieren. Optional können Sie den SSH-Dienst mit dem Befehl `start service ssh` starten.

- 8 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.

- 9 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 DHCP die falsche Netzwerkkarte für die Verwaltung zuweist, führen Sie die Aufgaben zum Beheben des Problems aus.

- 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 eth0 dhcp plane mgmt** ein.
- c Platzieren Sie eth0 im DHCP-Netzwerk und warten Sie, bis eth0 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 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-Netzwerkeinrichtung](#).

Verfahren

- 1 Erstellen Sie auf einem eigenständigen Host oder im vCenter Web Client eine VM und teilen Sie die folgenden Ressourcen zu:
 - Gastbetriebssystem: anderes (64-Bit)
 - 3 VMXNET3-Netzwerkkarten (NICs) Der e1000-NIC-Treiber wird von NSX Edge nicht unterstützt.
 - Die jeweiligen Systemressourcen für Ihre NSX-T Data Center-Bereitstellung

2 Binden Sie die NSX Edge-ISO-Datei an die VM.

Stellen Sie sicher, dass der Gerätestatus des CD/DVD-Laufwerks auf **Beim Einschalten verbinden** gesetzt ist.

edge-from-iso - Einstellungen bearbeiten	
Virtuelle Hardware VM-Optionen SDRS-Regeln vApp-Optionen	
CPU	1
Arbeitsspeicher	2048 MB
Festplatte 1	16 GB
SCSI-Controller 0	VMware Paravirtuell
*Netzwerkadapter 1	VM Network <input checked="" type="checkbox"/> Verbunden
*CD-/DVD-Laufwerk 1	Datenspeicher-ISO-Datei <input type="checkbox"/> Verbunden
Status	<input checked="" type="checkbox"/> Beim Einschalten verbinden
CD-/DVD-Medien	[datastore (2)]/nsx-edge-2.3 <input data-bbox="954 856 1145 888" type="button" value="Durchsuchen..."/>
Gerätemodus	Passthrough-CD-ROM
Knoten des virtuellen Geräts	SATA-Controller 0 SATA(0:0)
Diskettenlaufwerk 1	Clientgerät <input type="checkbox"/> Verbunden
Grafikkarte	Benutzerdefinierte Einstellungen angeben
SATA-Controller 0	
VMCI-Gerät	
Weitere Geräte	

3 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 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 acht Zeichen
- mindestens ein Kleinbuchstabe
- mindestens ein Großbuchstabe
- mindestens eine Zahl

- mindestens ein Sonderzeichen
- mindestens fünf unterschiedliche Zeichen
- keine Wörterbuchwörter
- keine Palindrome

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

- 4 (Optional) Reservieren Sie Arbeitsspeicher für die NSX-T Data Center-Komponente, um eine optimale Leistung zu erreichen.

Die Arbeitsspeicherreservierung ist eine garantierte Untergrenze für die Menge an physischem Arbeitsspeicher, die der Host für eine virtuelle Maschine reserviert, auch wenn der Arbeitsspeicher mehrfach vergeben wird. Legen Sie die Reservierung so fest, dass die NSX-T Data Center-Komponente über ausreichend Arbeitsspeicher für eine effiziente Ausführung verfügt. Siehe [Systemvoraussetzungen](#).

- 5 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.

- 6 Melden Sie sich nach dem Starten des NSX Edge mit Administratorrechten bei der CLI an. Verwenden Sie dazu den Benutzernamen **admin** und das Kennwort **default**.

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.

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

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

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

Interface: eth0
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
...
```

Führen Sie bei Bedarf den Befehl `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt` aus, um die Managementschnittstelle zu aktualisieren. Optional können Sie den SSH-Dienst mit dem Befehl `start service ssh` starten.

9 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.

10 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 DHCP die falsche Netzwerkkarte für die Verwaltung zuweist, führen Sie die Aufgaben zum Beheben des Problems aus.

- 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 eth0 dhcp plane mgmt** ein.
- c Platzieren Sie eth0 im DHCP-Netzwerk und warten Sie, bis eth0 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](#).

Zugriff auf die NSX Edge -Installation und deren Überprüfung

Sie können sich bei der NSX-T Data Center-VM oder dem Bare-Metal-Host von NSX-T Data Center anmelden, sich vergewissern, dass die Installation erfolgreich war und bei Bedarf Probleme beheben.

Voraussetzungen

- Stellen Sie sicher, dass Ihr PXE-Server für die Installation konfiguriert ist. Siehe [Vorbereiten des PXE-Servers für die NSX Edge-Installation](#).

- Stellen Sie sicher, dass NSX Edge unter Verwendung von Bare-Metal oder der ISO-Datei installiert wurde. Siehe [Bare-Metal-Installation von NSX Edge](#) oder [Installieren von NSX Edge per ISO-Datei als virtuelle Appliance](#).

Verfahren

- 1 Schalten Sie die NSX-T Data Center-VM oder den Bare-Metal-Host von NSX-T Data Center ein.

- 2 Wählen Sie im Boot-Menü **nsxedge**.

Das Netzwerk wird konfiguriert, Partitionen werden erstellt, und die NSX Edge-Komponenten werden installiert.

Wenn die NSX Edge-Anmeldeaufforderung angezeigt wird, können Sie sich als Admin oder Root anmelden.

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

- 3 (Optional) Reservieren Sie Arbeitsspeicher für die NSX-T Data Center-Komponente, um eine optimale Leistung zu erreichen.

Die Arbeitsspeicherreservierung ist eine garantierte Untergrenze für die Menge an physischem Arbeitsspeicher, die der Host für eine virtuelle Maschine reserviert, auch wenn der Arbeitsspeicher mehrfach vergeben wird. Legen Sie die Reservierung so fest, dass die NSX-T Data Center-Komponente über ausreichend Arbeitsspeicher für eine effiziente Ausführung verfügt. Siehe [Systemvoraussetzungen](#).

- 4 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.

- 5 Melden Sie sich nach dem Starten des NSX Edge mit Administratorrechten bei der CLI an. Verwenden Sie dazu den Benutzernamen **admin** und das Kennwort **default**.

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.

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

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

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

Interface: eth0
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
...
```

Führen Sie bei Bedarf den Befehl `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt` aus, um die Managementschnittstelle zu aktualisieren. Optional können Sie den SSH-Dienst mit dem Befehl `start service ssh` starten.

8 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.

9 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 DHCP die falsche Netzwerkkarte für die Verwaltung zuweist, führen Sie die Aufgaben zum Beheben des Problems aus.

- 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 eth0 dhcp plane mgmt** ein.
- c Platzieren Sie eth0 im DHCP-Netzwerk und warten Sie, bis eth0 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](#).

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.

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
```

In der NSX Manager-Benutzeroberfläche wird NSX Edge auf der Seite **Fabric > Knoten > Edges** angezeigt. 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](#).

Hostvorbereitung

Wenn Hypervisor-Hosts für den Betrieb mit NSX-T Data Center vorbereitet werden, gelten sie als Fabric-Knoten. Auf Hosts, die Fabric-Knoten darstellen, sind NSX-T Data Center-Module installiert und sie sind bei der NSX-T Data Center-Managementebene registriert.

Dieses Kapitel enthält die folgenden Themen:

- [Installieren von Drittanbieterpaketen auf einem KVM-Host oder Bare Metal-Server](#)
- [Überprüfung der Open vSwitch-Version auf RHEL KVM-Hosts](#)
- [Hinzufügen eines Hypervisor-Hosts oder Bare Metal-Servers zur NSX-T Data Center-Fabric](#)
- [Manuelle Installation von NSX-T Data Center-Kernel-Modulen](#)
- [Verbinden der Hypervisor-Hosts mit der Managementebene](#)

Installieren von Drittanbieterpaketen auf einem KVM-Host oder Bare Metal-Server

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

Voraussetzungen

- (Red Hat und CentOS) Bevor Sie die Drittanbieterpakete installieren, müssen Sie zuerst die Virtualisierungspakete installieren. Führen Sie auf dem Host die folgenden Befehle aus:

```
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:** Bevor Sie die Drittanbieterpakete installieren, müssen Sie zuerst die Virtualisierungspakete installieren. Führen Sie auf dem Ubuntu-Host die folgenden Befehle aus:

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

- **(Bare Metal-Server)** Für die Installation von Drittanbieterpaketen wird keine Virtualisierung vorausgesetzt.

Verfahren

- Stellen Sie unter Ubuntu 16.04.2 LTS sicher, dass die folgenden Drittanbieterpakete auf dem Host installiert sind.

```
libunwind8
libgflags2v5
libgoogle-perftools4
traceroute
python-mako
python-simplejson
python-unittest2
python-yaml
python-netaddr
libprotobuf9v5
libboost-chrono1.58.0
libgoogle-glog0v5
dkms
libboost-date-time1.58.0
libleveldb1v5
libsnappy1v5
python-gevent
python-protobuf
ieee-data
libyaml-0-2
python-linecache2
python-traceback2
libtcmalloc-minimal4
python-greenlet
python-markupsafe
libboost-program-options1.58.0
```

Wenn die Abhängigkeitspakete nicht auf Ubuntu 16.04.2 LTS installiert sind, führen Sie `apt-get install <package>` aus, um die Pakete manuell installieren.

- Stellen Sie sicher, dass die Red Hat- und CentOS-Hosts registriert sind und dass auf die entsprechenden Repositories zugegriffen werden kann.

Hinweis Wenn Sie den Host über die Benutzeroberfläche von NSX-T Data Center vorbereiten, müssen Sie die folgenden Abhängigkeiten auf dem Host installieren.

Installieren Sie Drittanbieterpakete unter RHEL 7.4 und CentOS 7.4.

```
yum-utils
wget
redhat-lsb-core
tcpdump
boost-filesystem
PyYAML
boost-iostreams
boost-chrono
python-mako
python-netaddr
python-six
gperftools-libs
libunwind
snappy
boost-date-time
c-ares
libev
python-gevent
python-greenlet
```

Installieren Sie Drittanbieterpakete unter RHEL 7.5.

```
PyYAML
c-ares
libev
libunwind
libyaml
python-beaker
python-gevent
python-greenlet
python-mako
python-markupsafe
python-netaddr
python-paste
python-tempita
```

- Wenn Sie den bereits bei RHEL und CentOS registrierten Host manuell vorbereiten, müssen Sie keine Abhängigkeiten auf dem Host installieren. Wenn der Host nicht registriert ist, installieren Sie die aufgelisteten Abhängigkeiten manuell mit dem Befehl `yum install <package>`.

- Installieren von Drittanbieterpaketen auf einem Bare Metal-Server
 - a Installieren Sie je nach Umgebung die hier aufgeführten Ubuntu-, RHEL- oder CentOS-Drittanbieterpakete.
 - b Installieren Sie die für den Bare Metal-Server spezifischen Drittanbieterpakete.
- Ubuntu – `apt-get install libvirt-libs`
- RHEL oder CentOS – `yum install libvirt-libs`

Überprüfung der Open vSwitch-Version auf RHEL KVM-Hosts

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

Die unterstützte Open vSwitch-Version lautet 2.9.1.8614397-1.

Verfahren

- 1 Überprüfen Sie, welche Version des Open vSwitch gegenwärtig 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.

- a Löschen Sie die folgenden Open vSwitch-Pakete.
 - `kmod-openvswitch`
 - `openvswitch`
 - `openvswitch-selinux-policy`
 - b Installieren Sie NSX-T Data Center entweder aus dem NSX Manager oder befolgen Sie das Verfahren für die manuelle Installation.
- 2 Aktualisieren Sie alternativ die von NSX-T Data Center verlangten Open vSwitch-Pakete.
 - 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>-rhel74_x86_64.tar.gz
```

- d Gehen Sie zum Paketverzeichnis.

```
cd nsx-lcp-rhel74_x86_64/
```

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

- Verwenden Sie für eine 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 eine 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
```

Nächste Schritte

Hinzufügen eines Hypervisor-Hosts zur NSX-T Data Center-Fabric. Siehe [Hinzufügen eines Hypervisor-Hosts oder Bare Metal-Servers zur NSX-T Data Center-Fabric](#).

Hinzufügen eines Hypervisor-Hosts oder Bare Metal-Servers zur NSX-T Data Center -Fabric

Ein Fabric-Knoten ist ein Knoten, der bei der NSX-T Data Center-Managementebene registriert wurde und auf dem NSX-T Data Center-Module installiert sind. Damit ein Hypervisor-Host oder ein Bare Metal-Server Teil des NSX-T Data Center-Overlays werden kann, muss er zunächst zur NSX-T Data Center-Fabric hinzugefügt werden.

Sie können dieses Verfahren überspringen, wenn Sie die Module manuell auf den Hosts installiert und die Hosts über die CLI mit der Managementebene verbunden haben.

Hinweis Zur Ausführung von Hostvorbereitungsaktivitäten für einen KVM-Host unter RHEL können Sie `sudo`-Anmeldedaten verwenden.

Voraussetzungen

- Erfassen Sie für jeden Host, den Sie der NSX-T Data Center-Fabric hinzufügen möchten, zunächst die folgenden Hostinformationen:
 - Hostname
 - Verwaltungs-IP-Adresse
 - Benutzername
 - Kennwort
 - Optional: (KVM) SHA-256-SSL-Fingerabdruck
 - Optional: (ESXi) SHA-256-SSL-Fingerabdruck

- Stellen Sie bei Ubuntu sicher, dass die erforderlichen Drittanbieterpakete installiert sind. Siehe [Installieren von Drittanbieterpaketen auf einem KVM-Host oder Bare Metal-Server](#).

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 vSphere 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:A2:4E: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 Stellen Sie in der NSX Manager-CLI sicher, dass der Service „install-upgrade“ ausgeführt wird.

```
nsx-manager-1> get service install-upgrade
```

```
Service name: install-upgrade
Service state: running
Enabled: True
```

- 3 Melden Sie sich über einen Browser bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 4 Wählen Sie **Fabric > Knoten > Hosts** und klicken Sie auf **Hinzufügen**.
- 5 Geben Sie den Hostnamen, die IP-Adresse, den Benutzernamen, das Kennwort und optional den Fingerabdruck ein.

Beispiel:

Host hinzufügen



Name *	comp-02b
IP-Adressen *	<div>192.168.210.54 ×</div>
Betriebssystem *	ESXi ▼
Benutzername *	root
Kennwort *	••••••••
SHA-256-Fingerabdruck	

[ABBRECHEN](#)[HINZUFÜGEN](#)

Für einen Bare Metal-Server können Sie im Dropdown-Menü „Betriebssystem“ **RHEL-Server**, **Ubuntu-Server** oder **CentOS-Server** auswählen.

Wenn Sie den Hostfingerabdruck nicht eingeben, werden Sie in der NSX-T Data Center-Benutzeroberfläche aufgefordert, den vom Host abgerufenen Standardfingerabdruck im Nur-Text-Format zu verwenden.

Beispiel:

Ungültiger Fingerabdruck



Der eingegebene Fingerabdruck war ungültig.

Möchten Sie diesen vom Server bereitgestellten Fingerabdruck verwenden?

fa984ff00d4856c1e8db1be005ff908a3f2335bcd67776447e926aba71a006b8

NEIN

HINZUFÜGEN

Wenn ein Host erfolgreich zur NSX-T Data Center-Fabric hinzugefügt wurde, wird auf der NSX Manager-Seite **Hosts** Folgendes angezeigt: **Bereitstellungsstatus: Installation erfolgreich** und **MPA-Konnektivität: Hochgefahren**.

LCP-Konnektivität wird erst dann verfügbar, wenn Sie den Fabric-Knoten in einen Transportknoten umgewandelt haben.

- 6 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.

Unter vSphere ESXi sind die Module als VIBs verpackt. Für KVM- oder Bare Metal-Server unter RHEL sind sie als RPMs verpackt. Für KVM- oder Bare Metal-Server unter Ubuntu sind sie als DEBs verpackt.

- Geben Sie unter ESXi den Befehl `esxcli software vib list | grep nsx` ein.

Das Datum ist der Tag, an dem Sie die Installation durchgeführt haben.

- Geben Sie unter RHEL den Befehl `yum list installed` oder den Befehl `rpm -qa` ein.
- Geben Sie unter Ubuntu den Befehl `dpkg --get-selections` ein.

- 7 (Optional) Zeigen Sie mit dem API-Aufruf `GET https://<nsx-mgr>/api/v1/fabric/nodes/<node-id>` den Fabric-Knoten an.
- 8 (Optional) Mit dem API-Aufruf `GET https://<nsx-mgr>/api/v1/fabric/nodes/<node-id>/status` können Sie den Status in der API überwachen.

- 9 (Optional) Ändern Sie die Abrufintervalle bestimmter Prozesse, wenn Sie über mindestens 500 Hypervisoren verfügen.

Im NSX Manager treten möglicherweise eine hohe CPU-Auslastung und Leistungsprobleme auf, wenn mehr als 500 Hypervisoren vorhanden sind.

- a Kopieren Sie mit dem NSX-T Data Center-CLI-Befehl `copy file` oder de 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 Manager IP address>' -u 'admin' -p '<password>' -i 900
```

- c (Optional) Setzen Sie die Abrufintervalle auf ihre Standardwerte zurück.

```
python aggsvc_change_intervals.py -m '<NSX Manager IP address>' -u 'admin' -p '<password>' -r
```

Nächste Schritte

Erstellen Sie eine Transportzone. Siehe [Grundlegende Informationen zu Transportzonen](#).

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-aggservice-<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.

Wenn Sie einen ESXi-Host zur NSX-T Data Center-Fabric hinzufügen, werden die folgenden VIBs auf dem Host installiert.

- **nsx-aggservice:** Liefert hostseitige Bibliotheken für den NSX-T Data Center-Aggregationsdienst. Der NSX-T Data Center-Zusammenfassungsdienst wird auf den Managementebenenknoten ausgeführt und ruft Laufzeitstatistiken von NSX-T Data Center-Komponenten ab.
- **nsx-da:** Erfasst Discovery Agent-(DA-)Daten zur Hypervisor-Betriebssystemversion, zu virtuellen Maschinen und zu Netzwerkschnittstellen. Stellt diese Daten der Managementebene bereit, damit sie in Fehlerbehebungstools verwendet werden können.
- **nsx-esx-datapath:** Liefert Funktionen für die Paketverarbeitung der NSX-T Data Center-Datenebene.
- **nsx-exporter:** Stellt Hostagents bereit, die Laufzeitstatistiken an den Zusammenfassungsdienst melden, der auf der Managementebene ausgeführt wird.
- **nsx-host:** Liefert Metadaten für das VIB-Paket, das auf dem Host installiert ist.
- **nsx-lldp:** Liefert Unterstützung für das Link Layer Discovery Protocol (LLDP). Dies ist ein Verbindungsschichtprotokoll, mit dem Netzwerkgeräte ihre Identität, Fähigkeiten und Nachbarn auf einem LAN ankündigen.
- **nsx-mpa:** Stellt Kommunikation zwischen NSX Manager und Hypervisor-Hosts bereit.
- **nsx-netcpa:** Stellt Kommunikation zwischen der zentralen Steuerungskomponente und Hypervisors bereit. Erhält den logischen Netzwerkzustand von der zentralen Steuerungskomponente und programmiert diesen Zustand in der Datenebene.

- `nsx-python-protobuf`: Liefert Python-Bindungen für Protokollpuffer.
- `nsx-sfhc`: Dienst-Fabric-Hostkomponente (Service Fabric Host Component; SFHC) Liefert einen Host-Agenten 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.
- `nsxa`: Führt Konfigurationen auf Hostebene durch, wie N-VDS-Erstellung und Uplink-Konfiguration.
- `nsxcli`: Stellt die NSX-T Data Center-CLI auf Hypervisor-Hosts bereit.
- `nsx-support-bundle-client`: Ermöglicht die Erfassung von Support-Paketen.

Zur Überprüfung können Sie den Befehl **`esxcli software vib list | grep nsx`** oder **`esxcli software vib list | grep <jjjj-mm-tt>`** auf dem ESXi-Host ausführen. Dabei ist das Datum der Tag, an dem Sie die Installation durchgeführt haben.

Nächste Schritte

Fügen Sie den Host der NSX-T Data Center-Managementebene hinzu. Siehe [Verbinden der Hypervisor-Hosts mit der Managementebene](#).

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 oder Bare Metal-Server](#).

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 [Verbinden der Hypervisor-Hosts mit der Managementebene](#).

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 [Verbinden der Hypervisor-Hosts mit der Managementebene](#).

Verbinden der Hypervisor-Hosts mit der Managementebene

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

Voraussetzungen

Die Installation der NSX-T Data Center-Module muss abgeschlossen sein.

Verfahren

- 1 Öffnen Sie eine SSH-Sitzung mit der NSX Manager-Appliance.
- 2 Melden Sie sich mit den Anmeldedaten des Administrators an.
- 3 Öffnen Sie eine SSH-Sitzung mit dem Hypervisor-Host.
- 4 Führen Sie auf der NSX Manager-Appliance den CLI-Befehl `get certificate api thumbprint` aus.

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

Beispiel:

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

- 5 Führen Sie auf dem Hypervisor-Host den Befehl **nsxcli** aus, um die NSX-T Data Center-CLI aufzurufen.

Hinweis Führen Sie den Befehl bei KVM als Superuser (sudo) aus.

```
[user@host:~] nsxcli
host>
```

Die Eingabeaufforderung ändert sich.

6 Führen Sie auf dem Hypervisor-Host 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

```
host> join management-plane NSX-Manager1 username admin thumbprint <NSX-Manager1's-thumbprint>
Password for API user: <NSX-Manager1's-password>
Node successfully joined
```

Überprüfen Sie das Ergebnis, indem Sie den Befehl `get managers` auf den Hosts ausführen.

```
host> get managers
- 192.168.110.47 Connected
```

Überprüfen Sie in der NSX Manager-Benutzeroberfläche unter **Fabric > Knoten > Hosts**, ob die MPA-Konnektivität als **Aktiv** angegeben wird.

Sie können den Zustand des Fabric-Hosts auch mit dem API-Aufruf **GET https://<nsx-mgr>/api/v1/fabric/nodes/<fabric-node-id>/state** anzeigen:

```
{
  "details": [],
  "state": "success"
}
```

Die Managementebene sendet die Hostzertifikate an die Steuerungskomponente und diese überträgt Informationen der Steuerungskomponente an die Hosts.

Sie sollten NSX Controller-Adressen in `/etc/vmware/nsx/controller-info.xml` auf jedem ESXi-Host sehen. Stattdessen können Sie auch mit dem Befehl `get controllers` die CLI aufrufen.

```
[root@host:~] cat /etc/vmware/nsx/controller-info.xml
<?xml version="1.0" encoding="utf-8"?>
<config>
  <connectionList>
    <connection id="0">
      <server>10.143.1.47</server>
      <port>1234</port>
      <sslEnabled>true</sslEnabled>
      <pemKey>-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----</pemKey>
    </connection>
    <connection id="1">
      <server>10.143.1.45</server>
      <port>1234</port>
      <sslEnabled>true</sslEnabled>
      <pemKey>-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----</pemKey>
    </connection>
```

```

    <connection id="2">
      <server>10.143.1.46</server>
      <port>1234</port>
      <sslEnabled>true</sslEnabled>
      <pemKey>-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----</pemKey>
    </connection>
  </connectionList>
</config>

```

Die Hostverbindung zu NSX-T Data Centers wird ausgelöst und verbleibt im Status „CLOSE_WAIT“, bis der Host zu einem Transportknoten hochgestuft wurde. Dies können Sie mit dem Befehl **esxcli network ip connection list | grep 1234** anzeigen.

```

# esxcli network ip connection list | grep 1234
tcp          0      0 192.168.210.53:45823      192.168.110.34:1234  CLOSE_WAIT    37256  newreno
netcpa

```

Bei KVM lautet der Befehl `netstat -anp --tcp | grep 1234`.

```

user@host:~$ netstat -anp --tcp | grep 1234
tcp  0  0 192.168.210.54:57794  192.168.110.34:1234  CLOSE_WAIT -

```

Nächste Schritte

Erstellen Sie eine Transportzone. Siehe [Grundlegende Informationen zu Transportzonen](#).

Transportzonen und Transportknoten

8

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

Dieses Kapitel enthält die folgenden Themen:

- [Grundlegende Informationen zu Transportzonen](#)
- [Erweiterter Datenpfad](#)
- [Erstellen eines IP-Pools für Tunnel-Endpoint-IP-Adressen](#)
- [Erstellen eines Uplink-Profiles](#)
- [Erstellen von Transportzonen](#)
- [Erstellen eines Hosttransportknotens](#)
- [Erstellen der Anwendungsschnittstelle für Bare-Metal Server-Arbeitslasten](#)
- [Konfigurieren von Network I/O Control-Profilen](#)
- [Erstellen eines NSX Edge-Transportknotens](#)
- [Erstellen eines NSX Edge-Clusters](#)

Grundlegende Informationen zu Transportzonen

Eine Transportzone ist ein Container, der die potenzielle Reichweite von Transportknoten definiert. Transportknoten sind Hypervisor-Hosts und NSX Edges, die an einem NSX-T Data Center-Overlay teilnehmen. Bei einem Hypervisor-Host bedeutet dies, dass er VMs hostet, die über logische NSX-T Data Center-Switches kommunizieren. Bei NSX Edges bedeutet es, dass logische Router-Uplinks und -Downlinks vorhanden sind.

Wenn Sie eine Transportzone erstellen, müssen Sie einen N-VDS-Modus angeben, entweder **Standard** oder **Optimierter Datenpfad**. Wenn Sie einer Transportzone einen Transportknoten hinzufügen, wird der der Transportzone zugeordnete N-VDS auf dem Transportknoten installiert. Jede Transportzone unterstützt genau einen N-VDS. Ein N-VDS mit optimiertem Datenpfad verfügt über geeignete Leistungsmerkmale, um NFV-Arbeitslasten (Network Functions Virtualization, Virtualisierung von Netzwerkfunktionen) zu unterstützen. Unterstützt werden sowohl VLANs als auch Overlay-Netzwerke. Hierfür ist ein ESXi-Host erforderlich, der N-VDS mit optimiertem Datenpfad unterstützt.

Mögliche Zugehörigkeiten eines Transportknotens:

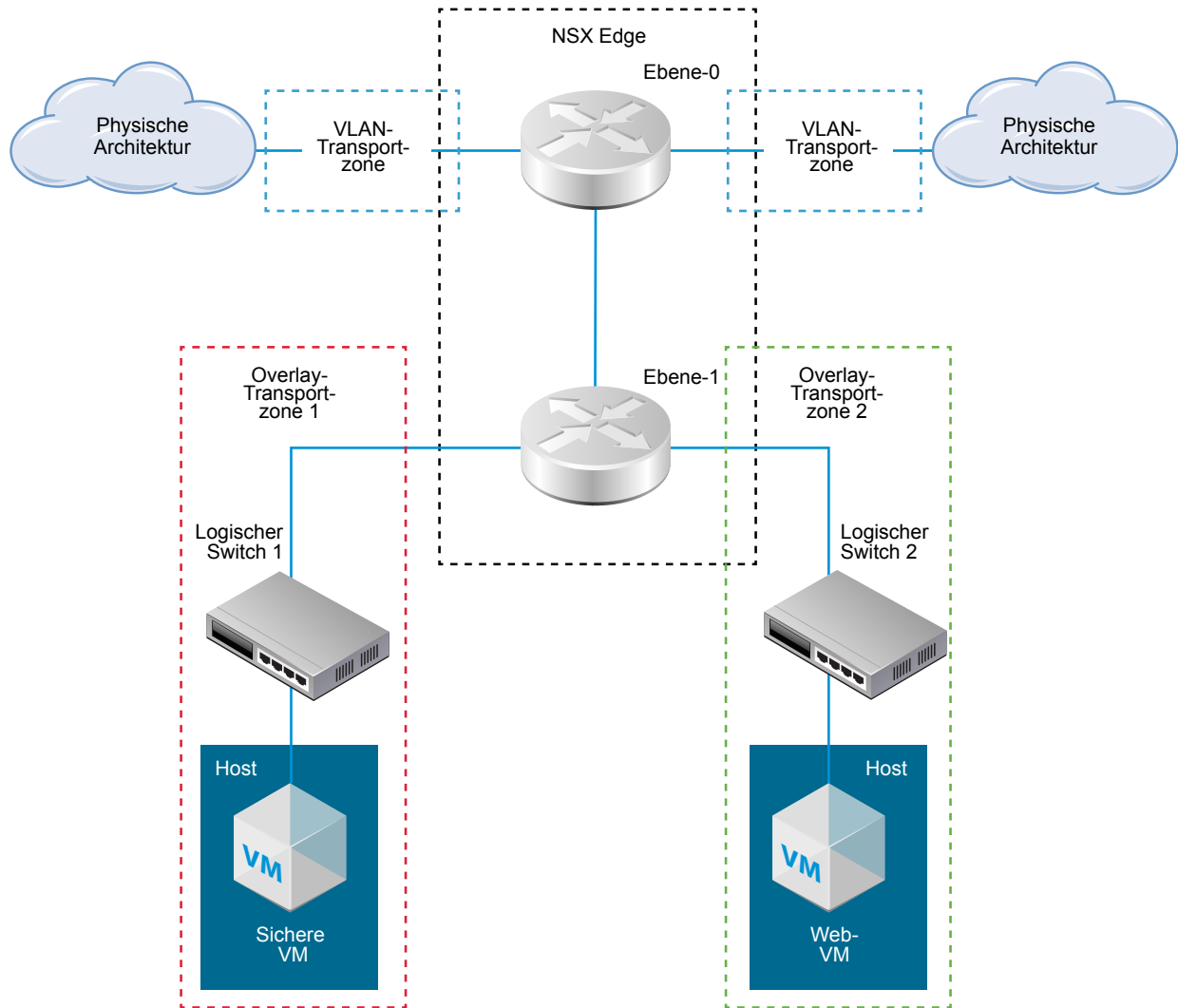
- Transportzonen mit mehreren VLANs.
- Maximal eine Overlay-Transportzone mit einem Standard-N-VDS.
- Mehrere Overlay-Transportzonen mit N-VDS mit erweitertem Datenpfad, wenn der Transportknoten auf einem ESXi-Host ausgeführt wird.

Wenn sich zwei Transportknoten in derselben Transportzone befinden, können die auf diesen Transportknoten gehosteten VMs mit logischen NSX-T Data Center-Switches verknüpft werden, die sich ebenfalls in dieser Transportzone befinden. Dank dieser Verknüpfung können die VMs miteinander kommunizieren, vorausgesetzt, dass sie über Schicht-2-/Schicht-3-Erreichbarkeit verfügen. Wenn VMs mit Switches verknüpft sind, die sich in anderen Transportzonen befinden, können die VMs nicht miteinander kommunizieren. Transportzonen ersetzen zwar keine Anforderungen an die Erreichbarkeit der zugrunde liegenden Ebene 2/3, sie begrenzen jedoch die Erreichbarkeit. Anders ausgedrückt: Die Zugehörigkeit zu derselben Transportzone ist Voraussetzung für die Konnektivität. Wenn diese Voraussetzung erfüllt ist, wird die Erreichbarkeit möglich, ist aber nicht automatisch gegeben. Um eine wirkliche Erreichbarkeit zu gewährleisten, muss das Netzwerk der zugrunde liegenden Ebene 2 und (bei unterschiedlichen Subnetzen) der Ebene 3 betriebsbereit sein.

Beispiel: Ein einzelner Transportknoten enthält sowohl reguläre VMs als auch VMs mit hoher Sicherheit. In Ihrem Netzwerkdesign müssen die regulären VMs in der Lage sein, einander zu erreichen, sollten aber nicht die VMs mit hoher Sicherheit erreichen können. Um dies zu erreichen, können Sie die sicheren VMs auf Hosts platzieren, die zur Transportzone `secure-tz` gehören. Die regulären VMs und die geschützten VMs dürfen sich nicht auf demselben Transportknoten befinden. Die regulären VMs werden dann auf einer anderen Transportzone mit dem Namen `general-tz` platziert. Die regulären VMs werden mit einem logischen NSX-T Data Center-Switch verknüpft, der sich ebenfalls in `general-tz` befindet. Die VMs mit hoher Sicherheit werden mit einem logischen NSX-T Data Center-Switch verknüpft, der sich in `secure-tz` befindet. Die VMs in unterschiedlichen Transportzonen können nicht miteinander kommunizieren, selbst wenn sie sich in demselben Subnetz befinden. Letztendlich wird die VM-Erreichbarkeit durch die Verbindung zwischen VM und logischem Switch gesteuert. Da sich zwei logische Switches in unterschiedlichen Transportzonen befinden, können sich „Web-VM“ und „Sichere VM“ nicht gegenseitig erreichen.

Die folgende Abbildung zeigt das Beispiel einer NSX Edge, die zu drei Transportzonen gehört: zwei VLAN-Transportzonen und Overlay-Transportzone 2. Overlay-Transportzone 1 enthält einen Host, einen logischen NSX-T Data Center-Switch und eine sichere VM. Da die NSX Edge nicht zur Overlay-Transportzone 1 gehört, hat die sichere VM keinen Zugriff auf die physische Architektur und umgekehrt. Die Web-VM in Overlay-Transportzone 2 kann dagegen mit der physischen Architektur kommunizieren, da die NSX Edge zur Overlay-Transportzone 2 gehört.

Abbildung 8-1. NSX-T Data Center -Transportzonen



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.

Im Modus „Erweiterter Datenpfad“ können Sie Folgendes konfigurieren:

- Overlay-Datenverkehr
- VLAN-Datenverkehr

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

- 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](#).

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

Siehe [Erstellen eines Hosttransportknotens](#).

„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 Netzwerkadaptertyp 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.

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 eindeutig 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 über einen Browser bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Bestand > Gruppen > IP-Pools** und klicken Sie auf **Hinzufügen**.

3 Geben Sie den Namen des IP-Pools, eine optionale Beschreibung und die Netzwerkeinstellungen ein.

Zu den Netzwerkeinstellungen gehören die folgenden:

- IP-Adressbereich
- Gateway
- Netzwerkadresse in CIDR-Notation
- (Optional) Durch Komma getrennte Liste mit DNS-Servern
- (Optional) DNS-Suffix

Beispiel:

Neuen IP-Pool hinzufügen



Name *

Beschreibung

Subnetze

[+ HINZUFÜGEN](#) [🗑 LÖSCHEN](#)

<input checked="" type="checkbox"/> IP-Bereiche *	Gateway	CIDR *	DNS-Server	DNS-Suffix
<input checked="" type="checkbox"/> 192.168.250.100 - 192.168.250.200	192.168.210.1	192.168.250.0/24		corp.local

[ABBRECHEN](#) [HINZUFÜGEN](#)

Sie können die IP-Pools auch mit dem API-Aufruf GET <https://<nsx-mgr>/api/v1/pools/ip-pools> anzeigen:

```
{
  "cursor": "0036e2d8c2e8-f6d7-498e-821b-b7e44d2650a9ip-pool-1",
  "sort_by": "displayName",
  "sort_ascending": true,
  "result_count": 1,
  "results": [
    {
      "id": "e2d8c2e8-f6d7-498e-821b-b7e44d2650a9",
      "display_name": "comp-tep",
      "resource_type": "IpPool",
      "subnets": [
        {
          "dns_nameservers": [
            "192.168.110.10"
          ]
        }
      ]
    }
  ]
}
```

```

    ],
    "allocation_ranges": [
      {
        "start": "192.168.250.100",
        "end": "192.168.250.200"
      }
    ],
    "gateway_ip": "192.168.250.1",
    "cidr": "192.168.250.0/24",
    "dns_suffix": "corp.local"
  }
],
"_last_modified_user": "admin",
"_last_modified_time": 1443649891178,
"_create_time": 1443649891178,
"_system_owned": false,
"_create_user": "admin",
"_revision": 0
}
]
}

```

Nächste Schritte

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

Erstellen eines Uplink-Profiles

Ein Uplink-Profil definiert Richtlinien für die Links von 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.

Mit Uplink-Profilen können Sie identische Funktionen für Netzwerkadapter über mehrere Hosts oder Knoten hinweg konsistent konfigurieren. Uplink-Profile sind Container für die Eigenschaften oder Funktionen, die Ihre Netzwerkadapter aufweisen sollen. Anstatt einzelne Eigenschaften oder Funktionen für jeden Netzwerkadapter zu konfigurieren, können Sie die Funktionen in Uplink-Profilen angeben. Diese können Sie dann beim Erstellen von NSX-T Data Center-Transportknoten anwenden.

Standby-Uplinks werden bei VM-/Appliance-basierten NSX Edges nicht unterstützt. Wenn Sie NSX Edge als eine virtuelle Appliance installieren, verwenden Sie das Standard-Uplink-Profil. Jedes für ein VM-basiertes NSX Edge erstellte Uplink-Profil darf nur einen aktiven Uplink und keinen Standby-Uplink angeben.

Hinweis NSX Edge-VMs ermöglichen mehrere Uplinks, wenn Sie einen eigenen N-VDS für jeden Uplink erstellen und ein anderes VLAN für jeden davon verwenden. Jeder Uplink benötigt eine eigene VLAN-Transportzone. So kann ein einzelner NSX Edge-Knoten unterstützt werden, der mit mehreren TOR-Switches verbunden wird.

Voraussetzungen

- Machen Sie sich mit dem NSX Edge-Netzwerk vertraut. Siehe [NSX Edge-Netzwerkeinrichtung](#).
- 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 über einen Browser bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Fabric > Profile > Uplink-Profile** aus und klicken Sie auf **Hinzufügen**.
- 3 Vervollständigen Sie die Details des Uplink-Profils.

Option	Beschreibung
Name	Geben Sie einen Uplink-Profilnamen ein.
Beschreibung	Fügen Sie eine optionale Beschreibung des Uplink-Profils hinzu.

Option	Beschreibung
LAGs	<p>(Optional) Linkaggregationsgruppen (LAGs) anhand von Link Aggregation Control Protocol (LACP) für das Transportnetzwerk</p> <p>Hinweis Für LACP werden mehrere LAGs auf KVM-Hosts nicht unterstützt.</p> <p>Fügen Sie eine kommasetrennte Liste mit Namen aktiver Uplinks hinzu.</p> <p>Fügen Sie eine kommasetrennte Liste mit Namen von Uplinks im Standby-Modus hinzu. 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>Klicken Sie im Abschnitt „Gruppierung“ auf Hinzufügen und geben Sie die Details ein. Die Gruppierungsrichtlinie definiert, wie der N-VDS seinen Uplink für Redundanz und Lastausgleich des Datenverkehrs verwendet. Für die Konfiguration der Gruppierungsrichtlinie stehen zwei verschiedene Gruppierungsrichtlinienmodi zur Verfügung:</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. ■ Lastausgleichsquelle: 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 Nur die Failover-Reihenfolge der Gruppierungsrichtlinie wird auf KVM-Hosts unterstützt. Die Lastausgleichsquellen-Gruppierungsrichtlinie wird nicht unterstützt.</p> <p>(Nur ESXi-Hosts) Sie können die folgenden Richtlinien für eine Transportzone definieren:</p> <ul style="list-style-type: none"> ■ Eine benannte Gruppierungsrichtlinie für jeden auf dem Switch konfigurierten logischen Switch. ■ Eine Standard-Gruppierungsrichtlinie für den gesamten Switch. <p>Benannte Gruppierungsrichtlinie: Eine benannte Gruppierungsrichtlinie bedeutet, dass Sie für jeden logischen Switch einen bestimmten Gruppierungsrichtlinienmodus und Uplinks definieren können. Dieser Richtlinientyp ermöglicht Ihnen die Flexibilität, Uplinks je nach Bedarf der Bandbreite auszuwählen.</p> <ul style="list-style-type: none"> ■ Wenn Sie eine benannte Gruppierungsrichtlinie definieren, verwendet N-VDS diese benannte Gruppierungsrichtlinie, wenn sie durch die angehängte Transportzone und den logischen Switch im Host angegeben ist. ■ Wenn Sie keine benannten Gruppierungsrichtlinien definieren, verwendet N-VDS die Standard-Gruppierungsrichtlinie.

4 Geben Sie einen Transport-VLAN-Wert ein.

5 Geben Sie den MTU-Wert ein.

Der Standardwert ist 1600.

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

```
{
  "result_count": 2,
  "results": [
    {
      "resource_type": "UplinkHostSwitchProfile",
      "id": "16146a24-122b-4274-b5dd-98b635e4d52d",
      "display_name": "comp-uplink",
      "transport_vlan": 250,
      "teaming": {
        "active_list": [
          {
            "uplink_type": "PNIC",
            "uplink_name": "uplink-1"
          }
        ],
        "standby_list": [ {
          "uplink_name": "uplink-2",
          "uplink_type": "PNIC"
        } ],
        "policy": "FAILOVER_ORDER"
      },
      "mtu": 1600,
      "_last_modified_time": 1457984399526,
      "_create_time": 1457984399526,
      "_last_modified_user": "admin",
      "_system_owned": false,
      "_create_user": "admin",
      "_revision": 0
    },
    {
      "resource_type": "UplinkHostSwitchProfile",
      "id": "c9e35cec-e9d9-4c51-b52e-17a5c1bd9a38",
      "display_name": "vlan-uplink",
      "transport_vlan": 100,
      "teaming": {
        "active_list": [
          {
            "uplink_type": "PNIC",
            "uplink_name": "uplink-1"
          }
        ],
        "standby_list": [],
        "policy": "FAILOVER_ORDER"
      },
      "named_teamings": [
        {
          "active_list": [
```

```

    {
      "uplink_type": "PNIC",
      "uplink_name": "uplink-2"
    }
  ],
  "standby_list": [
    {
      "uplink_type": "PNIC",
      "uplink_name": "uplink-1"
    }
  ],
  "policy": "FAILOVER_ORDER",
  "name": "named teaming policy"
}
]
"mtu": 1600,
"_last_modified_time": 1457984399574,
"_create_time": 1457984399574,
"_last_modified_user": "admin",
"_system_owned": false,
"_create_user": "admin",
"_revision": 0
}
]
}

```

Nächste Schritte

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

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 von NSX Edge 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 über einen Browser bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **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.

Die Optionen hierfür lauten **Standard** und **Optimierter Datenpfad**.

- 6 Wenn als Modus für den N-VDS „Standard“ gewählt wurde, müssen Sie einen Datenverkehrstyp auswählen.

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

- 7 Wenn als Modus für den N-VDS „Erweiterter Datenpfad“ gewählt wurde, müssen Sie einen Datenverkehrstyp auswählen.

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-ccbcbfe50b416",
  "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 Hosttransportknotens](#).

Erstellen eines Hosttransportknotens

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 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 bereits 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.

Voraussetzungen

- Der Host muss mit der Managementebene verbunden sein und MPA-Konnektivität muss auf der Seite **Fabric > Hosts** als aktiv markiert sein.
- 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.

Verfahren

- 1 Melden Sie sich über einen Browser bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Fabric > Knoten > Transportknoten > Hinzufügen** aus.

- 3 Geben Sie einen Namen für den Transportknoten ein.
- 4 Wählen Sie im Dropdown-Menü einen Knoten aus.
- 5 Wählen Sie die Transportzonen aus, zu denen dieser Transportknoten gehört.
- 6 Klicken Sie auf die Registerkarte **N-VDS**.
- 7 Wählen Sie bei einem KVM-Knoten den N-VDS-Typ aus.

Option	Beschreibung
Standard	NSX Manager erstellt den N-VDS. Diese Option ist standardmäßig ausgewählt.
Vorkonfiguriert	Der N-VDS ist bereits konfiguriert.

Bei einem Nicht-KVM-Knoten ist der N-VDS-Typ immer **Standard** oder **Erweiterter Datenpfad**.

- 8 Geben Sie bei einem Standard-N-VDS die folgenden Details an:

Option	Beschreibung
N-VDS-Name	Muss mit dem N-VDS-Namen der Transportzone identisch sein, zu der dieser Knoten gehört.
NIOC-Profil	Wählen Sie das NIOC-Profil im Dropdown-Menü aus.
Uplink-Profil	Wählen Sie ein Uplink-Profil im Dropdown-Menü aus.
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.
Physische Netzwerkkarten	Stellen Sie sicher, dass die physische Netzwerkkarte (NIC) noch nicht verwendet wird (z. B. von einem standardmäßigen vSwitch oder einem vSphere Distributed Switch). Andernfalls bleibt der Transportknotenstatus Teilweise erfolgreich , und die Fabric-Knoten-LCP-Konnektivität kann nicht hergestellt werden. Wählen Sie für den Bare Metal-Server die physische Netzwerkkarte aus, die als Uplink-1-Port konfiguriert werden kann. Der Uplink-1-Port wird im Uplink-Profil definiert. Wenn Sie in Ihrem Bare Metal-Server nur einen Netzwerkadapter haben, wählen Sie diese physische Netzwerkkarte aus, damit der Uplink-1-Port sowohl der Verwaltungs- als auch der Anwendungsschnittstelle zugewiesen wird.

9 Geben Sie bei einem N-VDS mit erweitertem Datenpfad die folgenden Details an.

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	Wählen Sie eine physische Netzwerkkarte (NIC), die erweiterte Datenpfade unterstützt. Stellen Sie sicher, dass die physische Netzwerkkarte (NIC) noch nicht verwendet wird (z. B. von einem standardmäßigen vSwitch oder einem vSphere Distributed Switch). Andernfalls bleibt der Transportknotenstatus Teilweise erfolgreich und die Fabric-Knoten-LCP-Konnektivität kann nicht hergestellt werden.
Uplink	Wählen Sie ein Uplink-Profil im Dropdown-Menü aus.
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.</p> <p>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</code> get 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>

10 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.

Nach dem Hinzufügen des Hosts als Transportknoten ändert sich die Host-Verbindung mit NSX Controller in einen aktiven Status.

11 Überprüfen Sie den Verbindungsstatus auf der Seite **Transportknoten**.

12 Alternativ können Sie den Verbindungsstatus mit CLI-Befehlen anzeigen.

- ◆ Geben Sie für ESXi den `esxcli network ip connection list | grep 1234`-Befehl 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 -
```

13 (Optional) Zeigen Sie den Transportknoten mit dem API-Aufruf `GET https://<nsx-mgr>/api/v1/transport-nodes/<node-id>` an.

```
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "95c8ce77-f895-43de-adc4-03a3ae2565e2",
  "display_name": "node-comp-01b",
  "tags": [],
  "transport_zone_endpoints": [
    {
      "transport_zone_id": "efd7f38f-c5da-437d-af03-ac598f82a9ec",
      "transport_zone_profile_ids": [
        {
          "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
          "resource_type": "BfdHealthMonitoringProfile"
        }
      ]
    }
  ],
  "host_switches": [
    {
      "host_switch_profile_ids": [
        {
          "value": "8abdb6c0-db83-4e69-8b99-6cd85bfcc61d",
          "key": "UplinkHostSwitchProfile"
        },
        {
          "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
          "key": "LldpHostSwitchProfile"
        }
      ]
    },
    {
      "host_switch_name": "overlay-hostswitch",
      "pnics": [
        {
          "device_name": "vmnic1",
          "uplink_name": "uplink-1"
        }
      ]
    }
  ],
}
```

```

    "static_ip_pool_id": "c78ac522-2a50-43fe-816a-c459a210127e"
  }
],
"node_id": "c551290a-f682-11e5-ae84-9f8726e1de65",
"_create_time": 1460051753373,
"_last_modified_user": "admin",
"_system_owned": false,
"_last_modified_time": 1460051753373,
"_create_user": "admin",
"_revision": 0
}

```

14 Fügen Sie den neu erstellten Transportknoten einer Transportzone hinzu.

- a Wählen Sie den Transportknoten aus.
- b Wählen Sie **Aktionen > Zur Transportzone hinzufügen** aus.
- c Wählen Sie im Dropdown-Menü die Transportzone aus.

Alle anderen Felder werden aufgefüllt.

Hinweis Wenn Sie für einen Standard-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 NSX-T Virtual Distributed Switch. Siehe [VMkernel-Migration auf einen N-VDS-Switch](#).

Konfigurieren der automatisierten Transportknotenerstellung

Wenn Sie einen vCenter Server-Cluster haben, können Sie die Installation und die Erstellung von Transportknoten auf allen NSX-T Data Center-Hosts in einzelnen oder mehreren Clustern automatisieren, anstatt eine manuelle Konfiguration vorzunehmen.

Hinweis Die automatisierte NSX-T Data Center-Transportknotenerstellung wird nur in vCenter Server 6.5 Update 1, 6.5 Update 2 und 6.7 unterstützt.

Wenn der Transportknoten bereits konfiguriert ist, ist die automatisierte Transportknotenerstellung für diesen Knoten nicht anwendbar.

Voraussetzungen

- Der Host muss Teil eines vCenter Server-Clusters sein.
- 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.
- vCenter Server sollte mindestens einen Cluster aufweisen.
- Ein Berechnungsmanager muss konfiguriert werden.

Verfahren

- 1 Melden Sie sich über einen Browser bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Fabric > Knoten > Hosts** aus.
- 3 Wählen Sie im Dropdown-Menü „Verwaltet“ einen vorhandenen Berechnungsmanager aus.
- 4 Wählen Sie einen Cluster aus, und klicken Sie auf **Cluster konfigurieren**.
- 5 Vervollständigen Sie die Details für die Clusterkonfiguration.

Option	Beschreibung
NSX automatisch installieren	Schalten Sie die Schaltfläche um, um die Installation von NSX-T Data Center auf allen Hosts im vCenter Server-Cluster zu aktivieren.
Transportknoten automatisch erstellen	<p>Schalten Sie die Schaltfläche um, um die Transportknotenerstellung auf allen Hosts im vCenter Server-Cluster zu aktivieren. Diese Einstellung muss festgelegt werden.</p> <p>Hinweis Wenn ein vorkonfigurierter Transportknoten im Cluster vorhanden ist oder in einen anderen Cluster verschoben wird, aktualisiert NSX-T Data Center den vorkonfigurierten Transportknoten nicht mit der Konfiguration, die in der Transportknotenvorlage des Clusters definiert ist. Damit alle Knoten dieselbe Konfiguration aufweisen, löschen Sie den vorkonfigurierten Transportknoten und fügen den betreffenden Host dem Cluster hinzu.</p>
Transportzone	Wählen Sie im Dropdown-Menü einen vorhandenen Transportknoten aus.
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>
IP-Zuweisung	<p>Wählen Sie im Dropdown-Menü DHCP verwenden oder IP-Pool verwenden aus.</p> <p>Wenn Sie IP-Pool verwenden auswählen, müssen Sie einen vorhandenen IP-Pool im Netzwerk aus dem Dropdown-Menü zuweisen.</p>
Physische Netzwerkkarten	<p>Stellen Sie sicher, dass die physische Netzwerkkarte (NIC) noch nicht verwendet wird (z. B. von einem standardmäßigen vSwitch oder einem vSphere Distributed Switch). Andernfalls lautet der Transportknotenzustand „Teilweise erfolgreich“, und die Fabric-Knoten-LCP-Konnektivität kann nicht hergestellt werden.</p> <p>Sie können den standardmäßigen Uplink verwenden oder einen vorhandenen Uplink aus dem Dropdown-Menü zuweisen.</p> <p>Klicken Sie auf PNIC hinzufügen, um die Anzahl der Netzwerkkarten in der Konfiguration zu erhöhen.</p>

Die NSX-T Data Center-Installation und Transportknotenerstellung auf den einzelnen Hosts im Cluster wird gleichzeitig gestartet. Der gesamte Vorgang hängt von der Anzahl Hosts im Cluster ab.

Wenn dem vCenter Server-Cluster ein neuer Host hinzugefügt wird, erfolgt die NSX-T Data Center-Installation und Transportknotenerstellung automatisch.

- 6 (Optional) Zeigen Sie den ESXi-Verbindungsstatus an.

```
# esxcli network ip connection list | grep 1234
tcp    0    0  192.168.210.53:20514  192.168.110.34:1234  ESTABLISHED  1000144459  newreno  netcpa
```

- 7 (Optional) Entfernen Sie eine NSX-T Data Center-Installation und einen Transportknoten von einem Host im Cluster.

- Wählen Sie einen Cluster aus, und klicken Sie auf **Cluster konfigurieren**.
- Schalten Sie die Schaltfläche „NSX automatisch installieren“ um, um die Option zu deaktivieren.
- Wählen Sie einen oder mehrere Hosts aus, und klicken Sie auf **NSX deinstallieren**.

Die Deinstallation dauert bis zu drei Minuten.

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 Hosttransportknotens](#).

Verfahren

- 1 Melden Sie sich über einen Browser bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Fabric > Profile > Uplink-Profile** aus und klicken Sie auf **Hinzufügen**.
- 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 hinzuzufügen.
Beispielsweise fügen Sie eine **lag1** genannte LAG mit 2 Uplinks hinzu.
- 5 Wählen Sie unter **Teamings** den Eintrag **Standard-Teaming** aus.

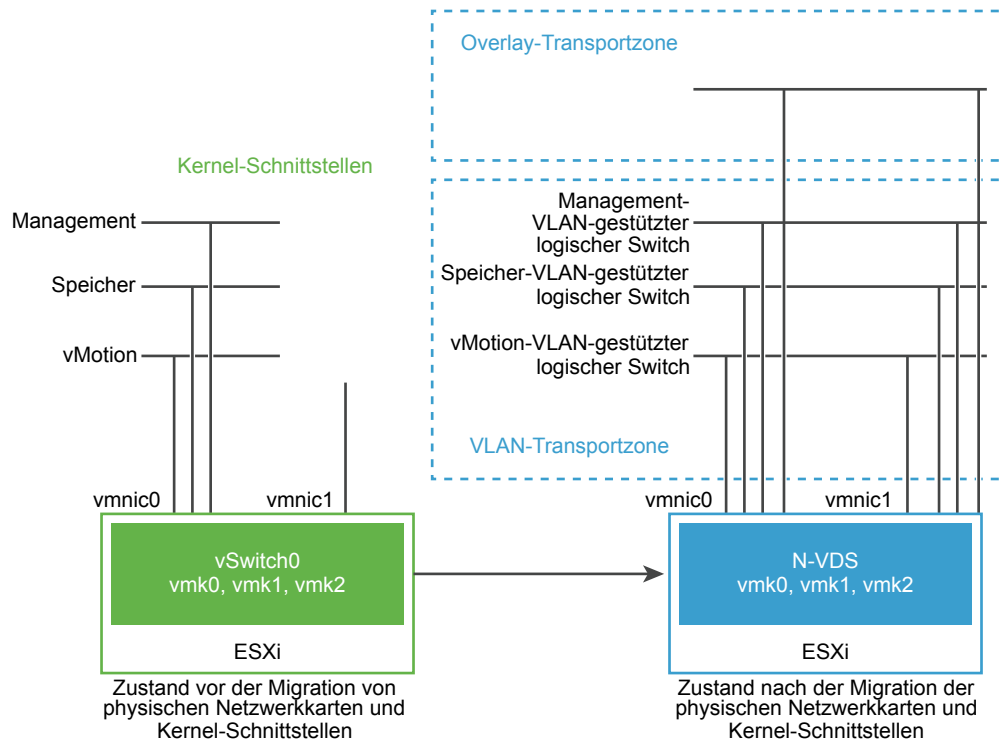
- 6 Geben Sie im Feld **Aktive Uplinks** den Namen der in Schritt 4 hinzugefügten LAG ein. In diesem Beispiel ist der Name **lag1**.
- 7 Klicken Sie unten im Dialogfeld auf **Hinzufügen**.
- 8 Geben Sie einen Wert für den **Transport-VLAN** und die **MTU** ein.
- 9 Klicken Sie unten im Fenster auf **Hinzufügen**.
- 10 Wählen Sie **Fabric > Knoten > Transportknoten > Hinzufügen** aus.
- 11 Geben Sie die auf der Registerkarte **Allgemein** die Daten ein.
- 12 Wählen Sie auf der Registerkarte **N-VDS** das in Schritt 3 erstellte Uplink-Profil **uplink-profile1** aus.
- 13 Im Feld **Physische Netzwerkkarten** sehen Sie eine Dropdown-Liste mit den physischen Netzwerkkarten und eine Dropdown-Liste mit den Uplinks, die Sie beim Erstellen des Uplink-Profiles festgelegt haben. Insbesondere sehen Sie die Uplinks **lag1-0** und **lag1-1**, in Übereinstimmung mit der in Schritt 4 erstellten LAG **lag1**. 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.

VMkernel-Migration auf einen N-VDS-Switch

Wenn Sie einen Transportknoten erstellen, kann es erforderlich sein, die physischen Netzwerkkarten und Kernel-Schnittstellen von einem vSphere Standard Switch (VSS) oder VDS zu einem NSX-T Data Center Virtual Distributed Switch (N-VDS) zu migrieren. Nach der Migration wickelt N-VDS den Datenverkehr auf dem VLAN-Netzwerk ab.

Die physischen Netzwerkkarten und ihre VMkernel-Schnittstellen werden anfänglich an einen VSS oder VDS auf einem vSphere ESXi-Host angehängt. Diese Kernel-Schnittstellen werden auf diesen Hosts definiert, um Konnektivität zur Verwaltungsschnittstelle, zum Speicher und zu anderen Schnittstellen bereitzustellen. Nach der Migration verbinden sich die VMkernel-Schnittstellen und ihre zugehörigen physischen NICs mit dem N-VDS und wickeln den Datenverkehr im VLAN und in den Overlay-Transportzonen ab.

Wenn in der folgenden Abbildung ein Host nur über zwei physische Netzwerkkarten verfügt, können Sie diese beiden Netzwerkkarten aus Redundanz Zwecken dem N-VDS zuweisen.

Abbildung 8-2. Vor und nach der Migration der Netzwerkschnittstellen zu einem N-VDS

Vor der Migration verfügt der vSphere 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 oder VDS angehängt, während `vmnic1` nicht verwendet wird. Darüber hinaus sind drei VMkernel-Schnittstellen vorhanden: `vmk0`, `vmk1` und `vmk2`.

VMkernel-Schnittstellen migrieren Sie mithilfe der NSX-T Data Center Manager-Benutzeroberfläche oder der NSX-T Data Center-APIs. 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 die Overlay-Transportzonen verbunden.

Migrieren von VMkernel-Schnittstellen zu einem N-VDS-Switch über die NSX-T Data Center Manager-Benutzeroberfläche

Die NSX-T Data Center Manager-Benutzeroberfläche ermöglicht Ihnen, alle Kernel-Schnittstellen, einschließlich der Verwaltungsschnittstelle, vom VSS- oder VDS- zum N-VDS-Switch zu migrieren.

Nehmen Sie für dieses Beispiel einen vSphere ESXi-Host mit zwei physischen Adapters, `vmnic0` und `vmnic1`, an. Der Standard-VSS- oder VDS-Switch auf dem Host ist mit einem einzelnen, `vmnic0` zugeordneten Uplink konfiguriert. Die VMkernel-Schnittstelle, `vmk0`, ist auch auf dem VSS oder VDS konfiguriert, um den Verwaltungsdatenverkehr auf dem Knoten auszuführen. Das Ziel ist es, `vmnic0` und `vmk0` zum N-VDS-Switch zu migrieren.

Als Teil der Hostvorbereitung werden VLAN- und Overlay-Transportzonen erstellt, um den Verwaltungs- bzw. den VM-Datenverkehr auszuführen. Außerdem wird ein N-VDS-Switch erstellt und mit einem `vmnic1` zugeordneten Uplink konfiguriert. Nach der Migration migriert NSX-T Data Center sowohl `vmnic0` als auch `vmk0` aus dem VSS- oder VDS-Switch zum N-VDS-Switch auf dem Knoten.

Voraussetzungen

- Vergewissern Sie sich, dass die physische Netzwerkinfrastruktur die gleiche LAN-Konnektivität für vmnic0 und vmnic1 bereitstellt.
- Vergewissern Sie sich, dass die nicht verwendete physische Netzwerkkarte vmnic1 über Layer 2-Konnektivität mit vmnic0 verfügt.
- Stellen Sie sicher, dass alle an dieser Migration beteiligten VMkernel-Schnittstellen zum gleichen Netzwerk gehören. Wenn Sie VMkernel-Schnittstellen auf einen Uplink migrieren, der mit einem anderen Netzwerk verbunden ist, ist der Host möglicherweise danach nicht mehr erreichbar oder nicht mehr funktionsfähig.

Verfahren

- 1 Wechseln Sie auf der NSX Manager-Benutzeroberfläche zu **Fabric** -> **Profil** -> **Uplink-Profile**.
- 2 Erstellen Sie ein Uplink-Profil mithilfe von vmnic0 als dem aktivem Uplink und vmnic1 als dem passivem Uplink.
- 3 Navigieren Sie zu **Fabric** -> **Transportzonen** -> **Hinzufügen**.
- 4 Erstellen Sie ein Overlay und VLAN-Transportzonen, um den VM-Datenverkehr bzw. den Verwaltungsdatenverkehr abzuwickeln.

Hinweis In der VLAN-Transportzone und in der OVERLAY-Transportzone muss derselbe N-VDS-Name verwendet werden.

- 5 Navigieren Sie zu **Fabric** -> **Knoten** -> **Transportknoten**.
- 6 Fügen Sie beide Transportzonen zum Transportknoten hinzu.
- 7 Fügen Sie auf der Registerkarte N-VDS ein N-VDS hinzu, indem Sie die von N-VDS zu verwendenden Uplinks und physischen Adapter definieren.

Der Transportknoten ist über einen einzelnen Uplink mit den Transportzonen verbunden.
- 8 Um sicherzustellen, dass vmk0 und vmnic0 nach der Migration Konnektivität zur VLAN-Transportzone erhalten, erstellen Sie einen logischen Switch für die entsprechende VLAN-Transportzone.
- 9 Wählen Sie den Transportknoten aus und klicken Sie auf **Aktionen** -> **ESX VMkernel und physische Adapter migrieren**.
- 10 Wählen Sie **Zu logischen Switches migrieren**.
- 11 Wählen Sie den N-VDS-Switch.
- 12 Fügen Sie die VMkernel-Adapter und die zugeordneten logischen Switches hinzu.
- 13 Fügen Sie den der VMkernel-Schnittstelle entsprechenden physischen Adapter hinzu. Stellen Sie sicher, dass mindestens ein physischer Adapter auf dem VSS- oder VDS-Switch verbleibt.
- 14 Klicken Sie auf **Speichern**.
- 15 Klicken Sie auf **Weiter**, um die Migration zu beginnen.

- 16 Testen der Konnektivität vom NSX Manager zu vmnic0 und vmk0.
- 17 Stellen Sie alternativ sicher, dass der VMkernel-Adapter in vCenter Server dem NSX-T Data Center-Switch zugeordnet ist.

VMkernel-Schnittstellen und ihre entsprechenden physischen Adapter werden zu N-VDS migriert.

Nächste Schritte

Sie können die VMkernel-Migration zu einem VSS oder einem VDS-Switch rückgängig machen.

Rückgängigmachen der VMkernel-Schnittstellen-Migration auf einen VSS- oder VDS-Switch unter Verwendung der NSX-T Data Center Manager-Benutzeroberfläche

Um die Migration von VMkernel-Schnittstellen auf einen VSS- oder VDS-Switch rückgängig zu machen, müssen Sie sicherstellen, dass eine Portgruppe auf dem ESXi-Host vorhanden ist.

NSX-T Data Center benötigt eine Portgruppe, um VMkernel-Schnittstellen vom N-VDS-Switch auf den VSS- oder VDS-Switch zu migrieren. Die Portgruppe akzeptiert die Netzwerkanforderung, diese Schnittstellen auf den VSS- oder VDS-Switch zu migrieren. Das an der Migration zu beteiligende Portmitglied wird aufgrund seiner Bandbreiten- und die Richtlinienkonfiguration bestimmt.

Stellen Sie sicher, dass die VMkernel-Schnittstellen funktionsfähig sind und Konnektivität auf dem N-VDS-Switch besteht, bevor Sie mit der Rückmigration des VMkernels auf den VSS- oder VDS-Switch beginnen.

Voraussetzungen

- Eine Port-Gruppe ist auf dem vSphere ESXi-Server vorhanden.

Verfahren

- 1 Navigieren Sie auf der NSX Manager-Benutzeroberfläche zu **Fabric -> Knoten -> Transportknoten**.
- 2 Wählen Sie den Transportknoten aus und klicken Sie auf **Aktionen -> ESX VMkernel und physische Adapter migrieren**.
- 3 Wählen Sie **Zu Portgruppen migrieren**.
- 4 Wählen Sie den N-VDS-Switch.
- 5 Fügen Sie die VMkernel-Adapter und die zugeordneten logischen Switches hinzu.
- 6 Fügen Sie den der VMkernel-Schnittstelle entsprechenden physischen Adapter hinzu. Stellen Sie sicher, dass mindestens ein physischer Adapter mit dem VSS- oder VDS-Switch verbunden bleibt.
- 7 Klicken Sie auf **Speichern**.
- 8 Klicken Sie auf **Weiter**, um die Migration zu beginnen.
- 9 Testen der Konnektivität vom NSX Manager zu vmnic0 und vmk0.
- 10 Stellen Sie alternativ dazu in vCenter Server sicher, dass der VMkernel-Adapter dem VSS- oder VDS-Switch zugeordnet ist.

VMkernel-Schnittstellen und ihre entsprechenden physischen Adapter werden zu N-VDS migriert.

Nächste Schritte

Sie möchten möglicherweise VMkernel-Schnittstellen über APIs migrieren. Siehe [Migrieren von Kernel-Schnittstellen auf einen N-VDS über APIs](#).

Migrieren von Kernel-Schnittstellen auf einen N-VDS über APIs

Wenn Sie NSX-T Data Center-APIs verwenden, müssen Sie vor der Migration der Management-Schnittstelle zunächst alle Kernel-Schnittstellen migrieren.

Nehmen Sie einen Host mit zwei Uplinks an, die mit entsprechenden physischen Netzwerkkarten verbunden sind. In diesem Verfahren können Sie mit einer Migration von der Speicher-Kernel-Schnittstelle vmk1 zu N-VDS beginnen. Nachdem diese Kernel-Schnittstelle erfolgreich auf N-VDS migriert wurde, können Sie die Kernel-Verwaltungsschnittstelle migrieren.

Siehe *Handbuch für die NSX-T Data Center-API*.

Voraussetzungen

- Vergewissern Sie sich, dass die physische Netzwerkinfrastruktur die gleiche LAN-Konnektivität für vmnic0 und vmnic1 bereitstellt.
- Vergewissern Sie sich, dass die nicht verwendete physische Netzwerkkarte vmnic1 über Layer 2-Konnektivität mit vmnic0 verfügt.
- Stellen Sie sicher, dass alle an dieser Migration beteiligten VMkernel-Schnittstellen zum gleichen Netzwerk gehören. Wenn Sie VMkernel-Schnittstellen auf einen Uplink migrieren, der mit einem anderen Netzwerk verbunden ist, wird der Host möglicherweise unerreichbar oder nicht funktionsfähig.

Verfahren

- 1 Erstellen Sie eine VLAN-Transportzone mit dem host_switch_name des N-VDS, der von der OVERLAY-Transportzone verwendet wird.
- 2 Erstellen Sie einen VLAN-gestützten logischen Switch in der VLAN-Transportzone mit einer VLAN-ID, die der von vmk1 auf dem VSS oder VDS verwendeten VLAN-ID entspricht.
- 3 Fügen Sie den vSphere ESXi-Transportknoten zur VLAN-Transportzone hinzu.

- 4 Rufen Sie die vSphere ESXi-Transportknotenkonfiguration ab.

```
GET /api/v1/transport-nodes/<transportnode-id>
```

Dabei ist *<transportnode-id>* die UUID des Transportknotens.

- 5 Migrieren Sie vmk1 zu N-VDS.

```
PUT https://<NSXmgr>/api/v1/transport-nodes/<transportnode-id> ?
if_id=<vmk>&esx_mgmt_if_migration_dest=<network>
```

Dabei ist *<transportnode-id>* die UUID des Transportknotens. *<vmk>* ist der Name der VMkernel-Schnittstelle vmk1. *<network>* ist die UUID des logischen Ziel-Switches.

- 6 Vergewissern Sie sich, dass die Migration erfolgreich abgeschlossen wurde.

```
GET /api/v1/transport-nodes/<transportnode-id>/state
```

Warten Sie, bis der Migrationsstatus als ERFOLG angezeigt wird. Sie können den Migrationsstatus der VMkernel-Schnittstelle auch im vCenter Server überprüfen.

Die VMkernel-Schnittstelle wird von einem VSS- oder VDS- zum N-VDS-Switch migriert.

Nächste Schritte

Sie können die verbleibenden VMkernel-Schnittstellen und die Kernel-Verwaltungsschnittstelle des VSS oder VDS zum N-VDS migrieren.

Migrieren der Verwaltungs-Kernel-Schnittstelle von einem VSS oder VDS zu einem N-VDS über APIs

Nachdem Sie alle anderen Kernel-Schnittstellen migriert haben, fahren Sie mit der Migration der Verwaltungs-Kernel-Schnittstelle fort. Bei der Migration der Kernel-Verwaltungsschnittstelle verschieben Sie vmnic0 und vmk0 von einem VSS oder VDS zu einem N-VDS.

Anschließend können Sie die vmnic0 und vmk0 für den physischen Uplink zusammen in einem Schritt zum N-VDS migrieren. Ändern Sie die Konfiguration des Transportknotens, sodass die vmnic0 jetzt als einer der Uplinks konfiguriert ist.

Hinweis Wenn Sie die vmnic0 für den Uplink und die vmk0 für die Kernel-Schnittstelle getrennt migrieren möchten, dann migrieren Sie zuerst vmk0 und dann vmnic0. Wenn Sie zuerst vmnic0 migrieren, bleibt vmk0 ohne unterstützende Uplinks auf dem VSS oder VDS und die Konnektivität zum Host geht verloren.

Voraussetzungen

- Überprüfen Sie die Konnektivität mit den bereits migrierten vmknics. Weitere Informationen finden Sie unter [Migrieren von Kernel-Schnittstellen auf einen N-VDS über APIs](#).
- Wenn vmk0 und vmk1 verschiedene VLANs verwenden, muss Trunk-VLAN auf dem physischen Switch verwendet werden, der mit den PNICs vmnic0 und vmnic1 verbunden ist, um beide VLANs zu unterstützen.
- Vergewissern Sie sich, dass ein externes Gerät die Schnittstellen vmk1 auf dem VLAN-gestützten logischen Switch für Speicher und vmk2 auf dem VLAN-gestützten logischen Switch für vMotion erreichen kann.

Verfahren

- 1 (Optional) Erstellen Sie eine zweite Kernel-Verwaltungsschnittstelle auf VSS oder VDS und migrieren Sie diese neu erstellte Schnittstelle zu N-VDS.
- 2 (Optional) Überprüfen Sie an einem externen Gerät die Konnektivität mit der Test-Verwaltungsschnittstelle.

- 3 Wenn vmk0 (Verwaltungsschnittstelle) ein anderes VLAN als vmk1 (Speicherschnittstelle) verwendet, erstellen Sie einen VLAN-gestützten logischen Switch in der VLAN-Transportzone mit einer VLAN-ID, die der von vmk0 auf dem VSS oder VDS verwendeten VLAN-ID entspricht.

- 4 Rufen Sie die vSphere ESXi-Transportknotenkonfiguration ab.

```
GET /api/v1/transport-nodes/<transportnode-id>
```

Dabei ist *<transportnode-id>* die UUID des Transportknotens.

- 5 Im `host_switch_spec:host_switches`-Element der Konfiguration fügen Sie die `vmnic0` zur `pnics`-Tabelle hinzu und weisen sie einem dedizierten Uplink, `uplink-2`, zu.

Hinweis Während der Migration der VM-Kernelschnittstellen haben wir `uplink-1` `vmnic1` zugewiesen. Die Zuweisung der Verwaltungsschnittstelle `vmnic0` zu einem dedizierten Uplink ist notwendig, damit die Migration erfolgreich durchgeführt und der Host nach der Migration erreicht werden kann.

```
"pnics": [
    {
        "device_name": "vmnic0",
        "uplink_name": "uplink-2"
    },
    {
        "device_name": "vmnic1",
        "uplink_name": "uplink-1"
    }
],
```

- 6 Migrieren Sie die Kernel-Verwaltungsschnittstelle `vmk0` anhand der aktualisierten Konfiguration zu N-VDS.

```
PUT api/v1/transport-nodes/<transportnode-id>?if_id=<vmk>&esx_mgmt_if_migration_dest=<network>
```

Dabei ist *<transportnode-id>* die UUID des Transportknotens. *<vmk>* ist der Name der VMkernel-Verwaltungsschnittstelle `vmk0`. *<Network>* ist die UUID des logischen Ziel-Switches.

- 7 Vergewissern Sie sich, dass die Migration erfolgreich abgeschlossen wurde.

```
GET /api/v1/transport-nodes/<transportnode-id>/state
```

Warten Sie, bis der Migrationsstatus als **ERFOLG** angezeigt wird. In vCenter Server können Sie überprüfen, ob die Kernel-Adapter dafür konfiguriert sind, den Namen des neuen logischen Switches anzuzeigen.

Nächste Schritte

Sie haben außerdem die Möglichkeit, die Migration der Kernelschnittstellen und der Verwaltungsschnittstelle von N-VDS auf einen VSS- oder VDS-Switch rückgängig zu machen.

Rückgängigmachen der VMkernel-Schnittstellen-Migration von einem N-VDS-Switch zu einem VSS- oder VDS-Switch über APIs

Wenn Sie VMkernel-Schnittstellen zurücksetzen, müssen Sie mit der Migration der Verwaltungs-Kernel-Schnittstelle beginnen. Migrieren Sie dann die anderen Kernel-Schnittstellen von einem N-VDS zu einem VSS- oder VDS-Switch.

Verfahren

- 1 Vergewissern Sie sich, dass der Zustand des Transportknotens erfolgreich ist.

```
GET /api/v1/transport-nodes/<transportnode-id>/state
```

- 2 Rufen Sie die Konfiguration des vSphere ESXi-Transportknotens ab, um die innerhalb des Elements „host_switch_spec“:„host_switches“ der physischen NICs zu suchen.

```
GET /api/v1/transport-nodes/<transportnode-id>
```

```
"pnics": [
  { "device_name": "vmnic0",
    "uplink_name": "uplink-2"
  },
  { "device_name": "vmnic1",
    "uplink_name": "uplink-1"
  }
],
```

- 3 Entfernen Sie vmnic0 aus dem Element „host_switch_spec“:„host_switches“ der Transportknotenkonfiguration, um die Managementschnittstelle für die Migration vorzubereiten.

```
"pnics": [
  { "device_name": "vmnic1",
    "uplink_name": "uplink-1"
  }
],
```

- 4 Migrieren Sie die Managementschnittstelle, vmnic0 und vmk0, von N-VDS zu VSS oder VDS und verwenden Sie dabei die geänderte Konfiguration.

```
PUT api/v1/transport-nodes/< transportnode-id>?if_id=vmk0&esx_mgmt_if_migration_dest=<vmk0_port_group_name>
```

Dabei gilt Folgendes: *<vmk0_port_group>* ist der Portgruppenname, der vmk0 vor der Migration auf den logischen Switch zugewiesen wurde.

- 5 Überprüfen Sie den Status der Migration.

```
GET /api/v1/transport-nodes/<transportnode-id>/state
```

Warten Sie, bis als Status „ERFOLG“ angezeigt wird.

- 6 Rufen Sie die vSphere ESXi-Transportknotenkonfiguration ab.

```
GET /api/v1/transport-nodes/<transportnode-id>
```

- 7 Migrieren Sie vmk1 von N-VDS zu VSS oder VDS und verwenden Sie dabei die vorgenannte Transportknotenkonfiguration.

```
PUT /api/v1/transport-nodes/<transportnode-id>?if_id=vmk1&esx_mgmt_if_migration_dest=<vmk1_port_group>
```

Dabei gilt Folgendes: *<vmk1_port_group>* ist der Portgruppenname, der vmk1 vor der Migration auf den logischen Switch zugewiesen wurde.

Hinweis vmk0 oder vmk1 müssen mit mindestens einer physischen Netzwerkkarte auf den VSS oder VDS migriert werden, da dem VSS oder VDS keine physische Netzwerkkarte zugewiesen ist.

- 8 Vergewissern Sie sich, dass der Zustand des Transportknotens erfolgreich ist.
GET /api/v1/transport-nodes/<transportnode-id>/state.
- 9 Führen Sie nach der Migration eine Überprüfung durch, um etwaige Probleme zu vermeiden.
 - a Die Management-Kernel-Schnittstelle, vmk0, darf erst migriert werden, wenn eine Uplink-Schnittstelle an den VSS oder VDS angehängt wurde.
 - b Stellen Sie sicher, dass vmk0 seine IP-Adresse von vmnic0 erhält. Andernfalls könnte sich das IP ändern und andere Komponenten wie VC könnten die Konnektivität mit dem Host über das alte IP verlieren.

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 Öffnen Sie die 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 in 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 konstruktionsbedingt.

```

# 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 Rufen Sie Zustandsinformationen mit der API ab.

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"
}
```

Hinzufügen eines Berechnungsmanagers

Ein Berechnungsmanager, z. B. vCenter Server, ist eine Anwendung, die Ressourcen wie Hosts und virtuellen Maschinen verwaltet. NSX-T Data Center fragt Berechnungsmanager 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 Berechnungsmanager hinzuzufügen, denn NSX-T erhält Bestandslisteninformationen auch ohne Berechnungsmanager, zum Beispiel von eigenständigen Hosts und VMs.

In dieser Version unterstützt diese Funktion Folgendes:

- vCenter Server Version 6.5 Update 1, Version 6.5 Update 2 und Version 6.7.
- IPv6- und IPv4-Kommunikation mit vCenter Server.

- Maximal 5 Berechnungsmanager.

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

Verfahren

- 1 Melden Sie sich über einen Browser bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie im Navigationsbereich **Fabric > Berechnungsmanager** aus.
- 3 Klicken Sie auf **Hinzufügen**.
- 4 Vervollständigen Sie die Details zum Berechnungsmanager.

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 Server beschreiben.
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.

- 5 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.

Im Bereich des Berechnungsmanagers wird eine Liste der Berechnungsmanager angezeigt. Sie können auf den Namen des Managers klicken, um Details zu dem Manager anzuzeigen oder zu bearbeiten oder um Tags zu verwalten, die für den Manager gelten.

Erstellen der Anwendungsschnittstelle für Bare-Metal Server-Arbeitslasten

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

Verfahren

- 1 Installieren Sie die erforderlichen Drittanbieterpakete.

Siehe [Installieren von Drittanbieterpaketen auf einem KVM-Host oder Bare Metal-Server](#).

- 2 Konfigurieren Sie die TCP- und UDP-Ports.

Siehe [Von vSphere ESXi, KVM-Hosts und Bare-Metal-Server verwendete TCP- und UDP-Ports](#).

- 3 Fügen Sie dem NSX-T Data Center-Fabric einen Bare-Metal-Server hinzu.

Siehe [Hinzufügen eines Hypervisor-Hosts oder Bare Metal-Servers zur NSX-T Data Center-Fabric](#).

- 4 Erstellen Sie einen KVM-Transportknoten.

Siehe [Erstellen eines Hosttransportknotens](#).

- 5 Erstellen Sie eine Anwendungsschnittstelle mit dem Ansible-Playbook.

Siehe <https://github.com/vmware/bare-metal-server-integration-with-nsxt>.

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 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 usw. Systemdatenverkehr ist strikt einem vSphere 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 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-Switch

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

Verfahren

- 1 Melden Sie sich bei NSX Manager Manager an: <https://<nsx-manager-IP-address>>.
 - 2 Navigieren Sie zu **Fabric > Profile**.
 - 3 Wählen Sie **NIOC-Profile** aus.
 - 4 Klicken Sie auf **+ HINZUFÜGEN**.
 - 5 Geben Sie die gewünschten Details über den Bildschirm „Neues NIOC-Profil“ ein.
 - a Geben Sie einen Namen für das NIOC-Profil ein.
 - b Schalten Sie den Status in **Aktiviert** um.
 - c Wählen Sie im Abschnitt „Ressource für Host-Infrastrukturdatenverkehr“ einen Datenverkehrstyp aus und geben Sie Werte für „Grenzwert“, „Anteile“ und „Reservierung“ ein.
 - 6 Klicken Sie auf **Hinzufügen**.
- Der Liste der NIOC-Profile wird ein neues NIOC-Profil hinzugefügt.

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

    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 re-
    sources.",
    "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 neues 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-c577aefe563a",
            "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 im Abschnitt `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/niocVnicInfo
```

```
Vnic NIOC Info
{
  Uplink reserved on:vmnic4
  Reservation in Mbps:200
  Shares:50
  Limit in Mbps:4294967295
  World ID:1001400726
  vNIC Index:0
  Respool Tag:0
  NIOC Version:3
  Active Uplink Bit Map:15
  Parent Respool ID:netsched.pools.persist.vm
}
```

- 7 # [root@ host:] /get /net/portsets/DvsPortset-1/uplinks/vmnic4/niocInfo

```
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
}

```

Das NIOC-Profil wird mit der vordefinierten Bandbreitenzuteilung für Anwendungen konfiguriert, die auf NSX-T Data Center-Hosts ausgeführt werden.

Erstellen eines NSX Edge -Transportknotens

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. Diese Knoten umfassen unter anderem auch NSX Edges. Im Folgenden wird beschrieben, wie Sie ein NSX Edge als Transportknoten hinzufügen.

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 neues Zertifikat, wenn bereits ein Zertifikat vorhanden ist.

Voraussetzungen

- Das NSX Edge muss mit der Managementebene verbunden sein und MPA-Konnektivität muss auf der Seite **Fabric > Edges** als aktiv markiert sein. Siehe [Verbinden von NSX Edge mit der Managementebene](#).
- Transportzonen müssen konfiguriert sein.
- 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 über einen Browser bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Fabric > Knoten > Transportknoten > Hinzufügen** aus.
- 3 Geben Sie einen Namen für den NSX Edge-Transportknoten ein.

- 4 Wählen Sie einen NSX Edge-Fabric-Knoten in der Dropdown-Liste aus.
- 5 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.

- 6 Klicken Sie auf die Registerkarte **N-VDS** und geben Sie die N-VDS-Informationen ein.

Option	Beschreibung
N-VDS-Name	Muss mit den Namen übereinstimmen, die Sie beim Erstellen der Transportzonen konfiguriert haben.
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.
IP-Pool	Wenn Sie IP-Pool verwenden für die IP-Zuweisung ausgewählt haben, geben Sie den Namen des IP-Pools an.
Physische Netzwerkkarten	Im Gegensatz zu einem Host-Transportknoten, bei dem vmnic als physische Netzwerkkarte verwendet wird, kommt bei einem NSX Edge-Transportknoten fp-ethX zum Einsatz.

- 7 (Optional) Zeigen Sie den Transportknoten mit dem API-Aufruf GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>` an.

```
GET https://<nsx-mgr>/api/v1/transport-nodes/78a03020-a3db-44c4-a8fa-f68ad4be6a0c
```

```
{
  "resource_type": "TransportNode",
  "id": "78a03020-a3db-44c4-a8fa-f68ad4be6a0c",
  "display_name": "node-comp-01b",
  "transport_zone_endpoints": [
    {
      "transport_zone_id": "efd7f38f-c5da-437d-af03-ac598f82a9ec",
      "transport_zone_profile_ids": [
        {
          "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
          "resource_type": "BfdHealthMonitoringProfile"
        }
      ]
    }
  ],
  "host_switches": [
    {
      "host_switch_profile_ids": [
        {
          "value": "8abdb6c0-db83-4e69-8b99-6cd85bfcc61d",
          "key": "UplinkHostSwitchProfile"
        }
      ]
    }
  ]
}
```

```

    },
    {
      "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
      "key": "LldpHostSwitchProfile"
    }
  ],
  "host_switch_name": "overlay-hostswitch",
  "pnics": [
    {
      "device_name": "vmnic1",
      "uplink_name": "uplink-1"
    }
  ],
  "static_ip_pool_id": "c78ac522-2a50-43fe-816a-c459a210127e"
}
],
"node_id": "c551290a-f682-11e5-ae84-9f8726e1de65",
"_create_time": 1459547122893,
"_last_modified_user": "admin",
"_last_modified_time": 1459547126740,
"_create_user": "admin",
"_revision": 1
}

```

- 8 (Optional) Statusinformationen werden über den API-Aufruf GET <https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/status> angezeigt.

```

{
  "control_connection_status": {
    "degraded_count": 0,
    "down_count": 0,
    "up_count": 1,
    "status": "UP"
  },
  "tunnel_status": {
    "down_count": 0,
    "up_count": 0,
    "status": "UNKNOWN",
    "bfd_status": {
      "bfd_admin_down_count": 0,
      "bfd_up_count": 0,
      "bfd_init_count": 0,
      "bfd_down_count": 0
    }
  },
  "bfd_diagnostic": {
    "echo_function_failed_count": 0,
    "no_diagnostic_count": 0,
    "path_down_count": 0,
    "administratively_down_count": 0,
    "control_detection_time_expired_count": 0,
    "forwarding_plane_reset_count": 0,
    "reverse_concatenated_path_down_count": 0,

```

```

    "neighbor_signaled_session_down_count": 0,
    "concatenated_path_down_count": 0
  }
},
"pnic_status": {
  "degraded_count": 0,
  "down_count": 0,
  "up_count": 4,
  "status": "UP"
},
"mgmt_connection_status": "UP",
"node_uuid": "cd4a8501-0ffc-44cf-99cd-55980d3d8aa6",
"status": "UNKNOWN"
}

```

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.
- Optional können Sie ein NSX Edge-Clusterprofil für High Availability (HA) unter **Fabric > Profile > Edge-Clusterprofile** erstellen. Sie können aber auch das standardmäßige NSX Edge-Clusterprofil verwenden.

Verfahren

- 1 Melden Sie sich über einen Browser bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Navigieren Sie zu **Fabric > Knoten > Edge-Cluster > Hinzufügen**.

- 3 Geben Sie einen Namen für den NSX Edge-Cluster ein.
- 4 Wählen Sie ein NSX Edge-Clusterprofil.
- 5 Klicken Sie auf **Bearbeiten**, und wählen Sie entweder **Physische Maschine** oder **Virtuelle Maschine** aus.

Der Begriff „physische Maschine“ bezieht sich auf NSX Edges, die auf einer Bare-Metal-Bereitstellung installiert sind. Der Begriff „virtuelle Maschine“ bezieht sich auf NSX Edges, die als virtuelle Maschinen/Appliances installiert sind.

- 6 Wählen Sie für die „Virtuelle Maschine“ im Dropdown-Menü „Mitgliedstyp“ entweder NSX Edge-Knoten oder **Public Cloud-Gateway-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.

- 7 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*.

Installation von NSX Cloud - Komponenten

9

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.

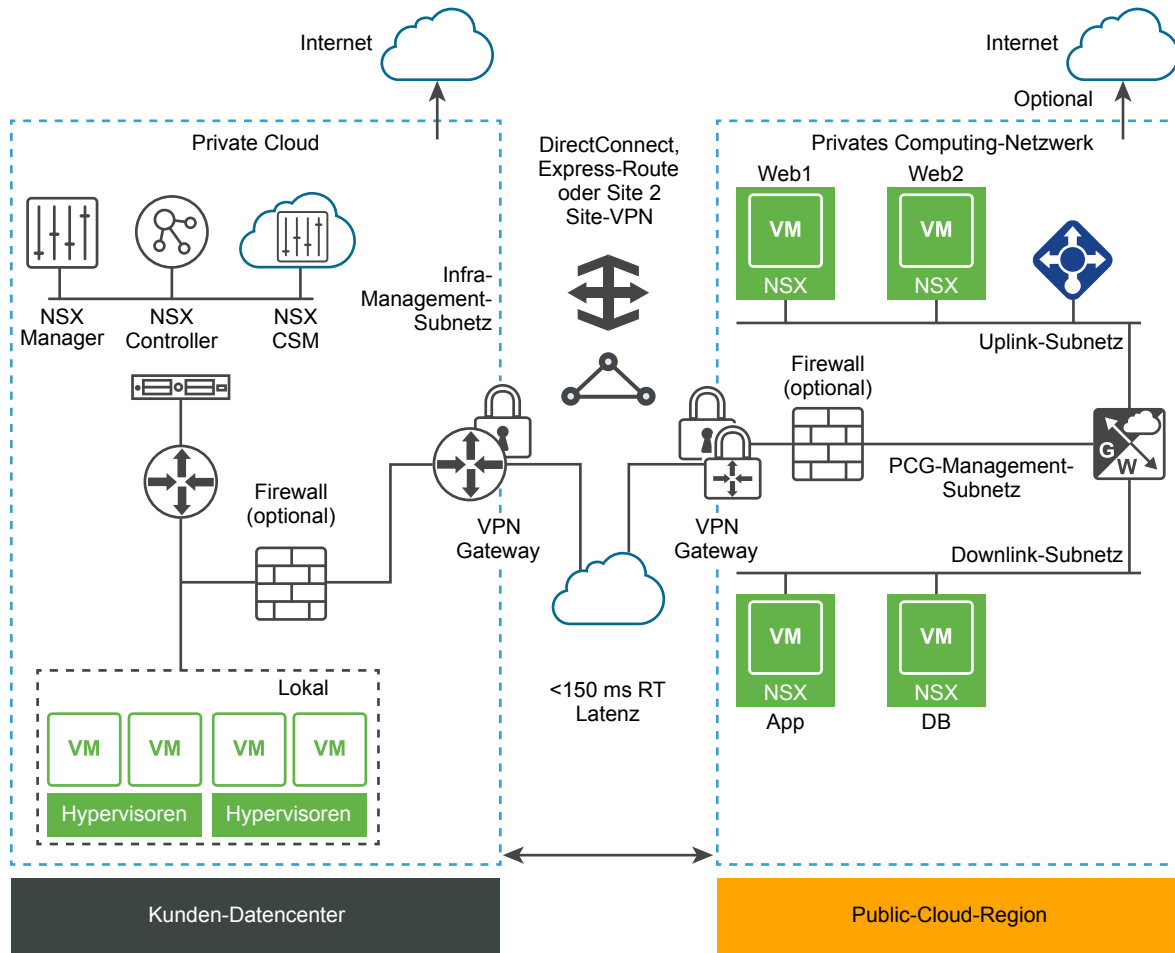
Dieses Kapitel enthält die folgenden Themen:

- [Architektur und Komponenten von NSX Cloud](#)
- [Übersicht über die Installation der NSX Cloud-Komponenten](#)
- [Installieren von CSM und Herstellen einer Verbindung zu NSX Manager](#)
- [Public Cloud mit lokaler Bereitstellung verbinden](#)
- [Ihr Public Cloud-Konto hinzufügen](#)
- [PCG bereitstellen](#)
- [Bereitstellung von PCG aufheben](#)

Architektur und Komponenten von NSX Cloud

NSX Cloud integriert die NSX-T Data Center-Hauptkomponenten, NSX Manager und NSX Controller, in Ihre Public Cloud, um Netzwerkfunktionalität und Sicherheit in allen Ihren Implementierungen bereitzustellen.

Abbildung 9-1. Die Architektur von NSX Cloud



Die Hauptkomponenten von NSX Cloud sind:

- *NSX Manager* für die Managementebene mit definierter rollenbasierter Zugriffssteuerung (RBAC).
- *NSX Controller* für die Steuerungsebene und den Laufzeitzustand.
- *Cloud Service Manager* für die Integration mit NSX Manager, um der Managementebene Public Cloud-spezifische Informationen zur Verfügung zu stellen.
- *NSX Public Cloud Gateway* für Konnektivität zu den NSX-Verwaltungs- und -Steuerungsebenen, für NSX Edge-Gateway-Dienste und für die API-basierte Kommunikation mit den Public-Cloud-Entitäten.
- *NSX Agent*-Funktionalität, die einen NSX-verwalteten Datenpfad für Workload-VMs bereitstellt.

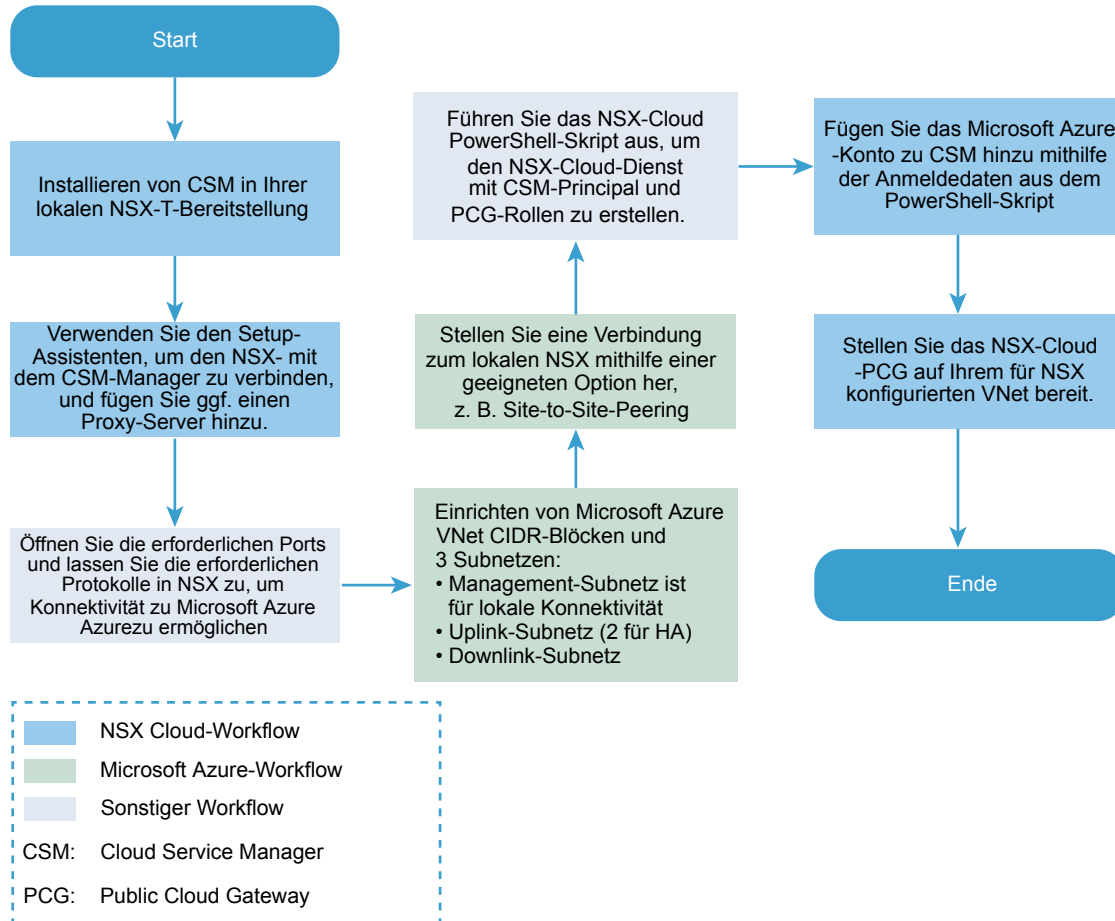
Übersicht über die Installation der NSX Cloud-Komponenten

In diesen Flussdiagrammen finden Sie eine Übersicht über Tag-0-Vorgänge für die Aktivierung von NSX-T Data Center, um Ihre Workload-VMs in der Public Cloud zu verwalten.

Tag-O-Workflow für Microsoft Azure

Dieses Flussdiagramm bietet eine Übersicht über die erforderlichen Schritte zum Hinzufügen eines Microsoft Azure-VNet zu NSX Cloud.

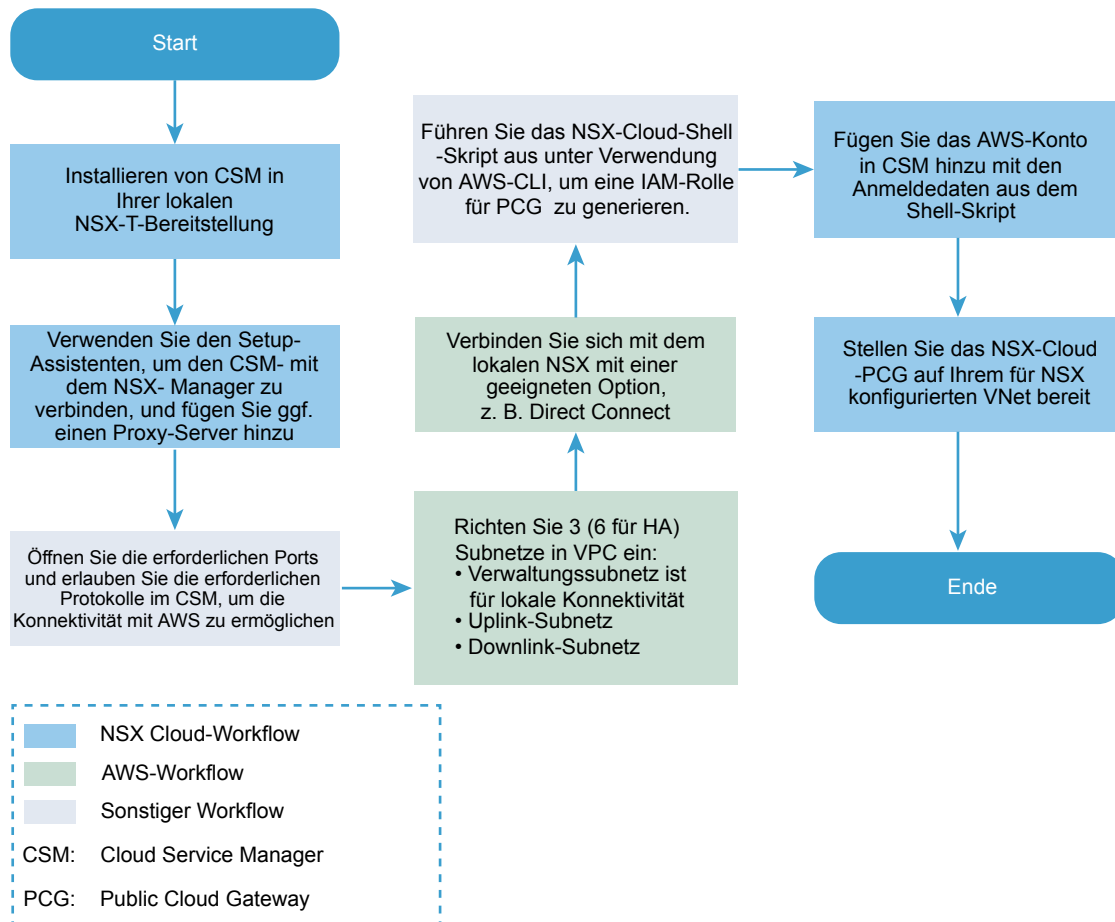
Abbildung 9-2. NSX Cloud – Tag-O-Workflow für Microsoft Azure



Tag-O-Workflow für AWS

Dieses Flussdiagramm bietet eine Übersicht über die Schritte zum Hinzufügen einer AWS VPC zu NSX Cloud.

Abbildung 9-3. NSX Cloud -Tag-O-Workflow für AWS



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](#).

Veröffentlichung von FQDN von 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 des FQDN von NSX Manager 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*.

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 müssen über Admin-Berechtigungen verfügen, um sich bei NSX Manager anzumelden.
- CSM muss installiert sein, und Ihnen muss in CSM die Rolle „Enterprise-Administrator“ zugewiesen sein.

Verfahren

- 1 Öffnen Sie eine SSH-Sitzung mit NSX Manager.
- 2 Führen Sie den Befehl `get certificate api thumbprint` auf NSX Manager aus.

```
NSX-Manager> get certificate api thumbprint
```

Die Ausgabe des Befehls besteht aus einer Reihe von Zahlen, die für diesen NSX Manager eindeutig sind.

- 3 Melden Sie sich bei CSM mit der Rolle „Enterprise-Administrator“ an.

- 4 Klicken Sie auf **System > Einstellungen**. Klicken Sie dann auf **Konfigurieren** im Bereich mit dem Titel **Verknüpfter NSX-Knoten**.

Hinweis Sie können diese Details auch bereitstellen, wenn Sie den CSM-Setup-Assistenten verwenden, der bei der Erstinstallation von CSM verfügbar ist.

- 5 Geben Sie Details zu NSX Manager 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 einen Benutzernamen und ein Kennwort bei der Rolle „Enterprise-Administrator“ an.
Manager-Fingerabdruck	Geben Sie den Fingerabdruckwert von NSX Manager ein, den Sie in Schritt 2 abgerufen haben.

- 6 Klicken Sie auf **Verbinden**.

CSM überprüft den NSX Manager-Fingerabdruck und stellt eine Verbindung her.

(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.

Proxyeinstellungen für PCG sind unabhängig von Proxyeinstellungen 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 „Konfigurieren der Proxyserver“ 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.

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 9-1.

Von	Zu	Protokoll/Port	Beschreibung
PCG	NSX Manager	TCP/5671	Eingehender Datenverkehr von Public Cloud zu lokalem NSX-T Data Center für Kommunikation auf Managementebene
PCG	NSX Manager	TCP/8080	Eingehender Datenverkehr von Public Cloud zu lokalem NSX-T Data Center für Upgrade
PCG	NSX Controller	TCP/1234, TCP/1235	Eingehender Datenverkehr von Public Cloud zu lokalem NSX-T Data Center für 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
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-Appliance 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 routingfähige 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.

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, Downlink-Subnetz, da Sie die Subnetze auswählen müssen, wenn Sie PCG in dieser VPC bereitstellen.

- 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.

Aktivieren Sie CSM , um auf Ihre Microsoft Azure-Bestandsliste zuzugreifen.

Ihr Microsoft Azure-Abonnement enthält ein oder mehrere VNets, die unter NSX-T Data Center-Management gestellt werden sollen.

Hinweis Wenn Sie bereits ein AWS-Konto zu CSM hinzugefügt haben, aktualisieren Sie den MTU-Wert in **NSX Manager > Fabric > Profil > Uplink-Profil > PCG-Uplink-Host-Switch-Profil** auf 1500, bevor Sie das Microsoft Azure-Konto hinzufügen. Dies kann auch über die NSX Manager-REST-APIs erfolgen.

Damit NSX Cloud im Rahmen Ihres Abonnements funktioniert, müssen Sie einen neuen Service Principal erstellen, um den erforderlichen Zugriff auf NSX-T Data Center zu gewähren. Sie müssen auch MSI-Rollen für CSM und PCG erstellen.

NSX Cloud stellt ein PowerShell-Skript zum Generieren des Service Principals bereit.

Dies ist ein zweistufiger Prozess:

- 1 Verwenden Sie das PowerShell-Skript NSX Cloud:
 - Erstellen Sie ein Service Principal-Konto für NSX Cloud.
 - Erstellen Sie eine Rolle für CSM und fügen Sie diese dem Service Principal hinzu.
 - Erstellen Sie eine Rolle für PCG und fügen Sie diese dem Service Principal hinzu.
- 2 Fügen Sie das Microsoft Azure-Abonnement zu CSM hinzu.

Erforderliche Rollen generieren

NSX Cloud nutzt die Managed Service Identity-(MSI-)Funktion von Microsoft Azure, um die Authentifizierung zu verwalten und gleichzeitig die Sicherheit Ihrer Microsoft-Zugangsdaten zu gewährleisten.

Damit NSX Cloud in Ihrem Microsoft Azure-Abonnement ausgeführt werden kann, müssen Sie MSI-Rollen für CSM und PCG und einen Service Principal für NSX Cloud einrichten.

Dies wird erreicht, indem Sie das NSX Cloud-PowerShell-Skript ausführen. Zusätzlich benötigen Sie zwei Dateien im JSON-Format als Parameter. Wenn Sie das PowerShell-Skript mit den erforderlichen Parametern ausführen, 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.

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.

Voraussetzungen

- Sie müssen PowerShell 5.0 + mit dem AzureRM-Modul installiert haben.
- Sie müssen der Besitzer des Microsoft Azure-Abonnements sein, für das Sie das Skript ausführen möchten, um den NSX Cloud Service Principal zu generieren.

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:

Dateiname	Beschreibung
CreateNSXRoles.ps1	Dies ist das PowerShell-Skript zum Generieren der NSX Cloud Service-Principal- und MSI-Rollen für CSM und PCG
nsx_csm_role.JSON	Diese Datei enthält den CSM-Rollenamen und Berechtigungen für diese Rolle in Microsoft Azure. Dies ist eine Eingabe in das PowerShell-Skript und muss sich im selben Ordner wie das Skript befinden.
nsx_pcg_role.JSON	Diese Datei enthält den PCG-Rollenamen und Berechtigungen für diese Rolle in Microsoft Azure. Dies ist eine Eingabe in das PowerShell-Skript und muss sich im selben Ordner wie das Skript befinden. Der PCG-(Gateway-)Rollename ist standardmäßig <code>nsx-pcg-role</code> .

Hinweis Wenn Sie Rollen für mehrere Abonnements in Ihrem Microsoft Azure Active Directory erstellen, müssen Sie die CSM- und PCG-Rollenamen für jedes Abonnement in den entsprechenden JSON-Dateien ändern und das Skript erneut ausführen.

- 3 Führen Sie das Skript mit Ihrer Microsoft Azure-Abonnement-ID als Parameter aus. Der Parametername ist `subscriptionId`.

Beispiel:

```
.\CreateNSXRoles.ps1 -subscriptionId <your_subscription_ID>
```

Dadurch wird ein Service Principal für NSX Cloud sowie eine Rolle mit entsprechenden Privilegien für CSM und PCG erstellt, und die Rollen CSM und PCG werden an den Service Principal NSX Cloud angehängt.

- 4 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

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](#)

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.

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.
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 wenigen Minuten können Sie es im Bereich **Konten** sehen.

Nächste Schritte

[Bereitstellen eines PCGs in Microsoft Azure VNet](#)

Aktivieren Sie CSM , um auf Ihre AWS-Bestandsliste zuzugreifen

Ihr AWS-Konto enthält eine oder mehrere VPCs, die Sie unter NSX-T Data Center-Management stellen möchten.

Dies ist ein dreistufiger Prozess.

- 1 Verwenden Sie das NSX Cloud-Skript, das AWS-CLI für folgende Aufgaben benötigt:
 - Ein Uplink-Profil erstellen.
 - Eine Rolle für PCG erstellen.
- 2 Das AWS-Konto in CSM hinzufügen.

Erforderliche Rollen generieren

NSX Cloud nutzt den AWS-IAM, um eine an das NSX Cloud-Profil angehängte Rolle zu generieren, welche die notwendigen Berechtigungen an PCG liefert, um auf Ihr AWS-Konto zuzugreifen.

Damit NSX Cloud in Ihrem AWS-Konto funktionieren kann, müssen Sie ein IAM-Profil und eine Rolle für PCG generieren.

Dies wird erreicht, indem das NSX Cloud-Shell-Skript unter Verwendung des AWS-CLI ausgeführt wird, das die folgenden Konstrukte erzeugt:

- ein IAM-Profil für NSX Cloud.
- eine Rolle für PCG, um die Arbeit an Ihrem Public-Cloud-Bestand zu ermöglichen.

Voraussetzungen

- Sie müssen die AWS-CLI mit dem Zugriffsschlüssel und dem geheimen Schlüssel Ihres AWS-Kontos installiert und konfiguriert haben.
- Sie müssen einen eindeutigen IAM-Profilnamen für das Skript ausgewählt haben. Der Gateway-Rollenname ist diesem IAM-Profil zugeordnet.
-

Verfahren

- 1 Laden Sie auf einem Linux- oder kompatiblen Desktop oder Server das SHELL-Skript mit dem Namen `AWS_create_credentials.sh` von der NSX-T Data Center **Download-Seite > Treiber & Tools > NSX Cloud Skripts > AWS** herunter.
- 2 Führen Sie das Skript aus und geben Sie einen Namen für das IAM-Profil ein, wenn Sie dazu aufgefordert werden. Beispiel:

```
bash AWS_create_NSXCloud_credentials.sh
```

- 3 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 im selben Verzeichnis gespeichert, in dem Sie das Skript ausgeführt haben. Der Dateiname lautet `aws_details.txt`.

Hinweis Der PCG-(Gateway-)Rollenname ist standardmäßig `nsx_pcg_service`. Sie können ihn im Skript ändern, wenn Sie einen anderen Wert für den Namen der Gateway-Rolle verwenden möchten. Dieser Wert wird zum Hinzufügen des AWS-Kontos in CSM benötigt, daher müssen Sie ihn notieren, wenn Sie den Standardwert ändern.

Nächste Schritte

[Ihr AWS-Konto zu CSM hinzufügen](#)

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.

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

[PCG in AWS VPC bereitstellen](#)

PCG bereitstellen

Ein NSX Public Cloud Gateway (PCG) ermöglicht Nord-Süd-Konnektivität zwischen der Public Cloud und den lokalen Verwaltungskomponenten von NSX-T Data Center

Voraussetzungen

- Ihre Public Cloud-Konten müssen bereits in CSM hinzugefügt worden sein.
- Für die VPC oder das VNet, auf denen Sie PCG bereitstellen, müssen die erforderlichen Subnetze entsprechend der Hochverfügbarkeit angepasst sein: *Uplink*, *Downlink* und *Verwaltung*.

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 eines PCG s in Microsoft Azure VNet

Folgen Sie diesen Anweisungen, um PCG in Ihrem Microsoft Azure-Abonnement bereitzustellen.

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	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. 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.
VHD-URL	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.
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, oder wählen Sie einen anderen Proxy-Server aus CSM, oder wählen Sie Kein Proxy-Server . Weitere Informationen zur Konfiguration von Proxy-Servern in CSM finden Sie unter (Optional) Proxy-Server konfigurieren .
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.
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-Netzwerkarte (Mgmt NIC)	Wählen Sie Neue IP-Adresse zuteilen , um der Management-Netzwerkarte 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-Netzwerkarte (NIC)	Wählen Sie Neue IP-Adresse zuteilen , um der Uplink-Netzwerkarte (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*.

PCG in AWS VPC bereitstellen

Befolgen Sie die Anweisungen zur Bereitstellung von PCG in Ihrem AWS-Konto.

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	Die Standardeinstellung ist aktiviert. Dies wird für die Greenfield-Bereitstellungen empfohlen. Wenn Sie in Ihrer VPC bereits VMs gestartet haben, deaktivieren Sie die Quarantäne-Richtlinie. Weitere Informationen finden Sie unter Verwalten der Quarantäne-Richtlinie im <i>Administratorhandbuch für NSX-T Data Center</i> .

Option	Beschreibung
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.
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-Netzwerkarte (Mgmt NIC)	Wählen Sie Neue IP-Adresse zuteilen , um der Management-Netzwerkarte 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-Netzwerkarte (NIC)	Wählen Sie Neue IP-Adresse zuteilen , um der Uplink-Netzwerkarte (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*.

Nach der Bereitstellung von PCG erstellte Konstrukte

Wesentliche NSX-T Data Center-Entitäten werden erstellt und in NSX Manager konfiguriert und Sicherheitsgruppen werden in Ihrer Public Cloud erstellt, nachdem PCG erfolgreich bereitgestellt wurde.

NSX Manager -Konfigurationen

Die folgenden Entitäten werden automatisch im NSX Manager erstellt:

- Ein Edge-Knoten mit dem Namen **Public Cloud Gateway** (PCG) wird erstellt.
- Der PCG-Knoten wird dem Edge-Cluster hinzugefügt. Bei einer Hochverfügbarkeitsbereitstellung gibt es zwei PCG.
- Das PCG (oder PCGs) wird als Transportknoten mit zwei erstellten Transportzonen registriert.
- Zwei logische Standard-Switches werden erstellt.
- Ein logischer Ebene-0-Router wird erstellt.
- Ein IP-Ermittlungsprofil wird erstellt. Dies wird für logische Overlay-Switches verwendet.
- Ein DHCP-Profil wird erstellt. Dies wird für DHCP-Server verwendet.
- Es wird eine standardmäßige NS-Gruppe mit dem Namen **PublicCloudSecurityGroup** erstellt, die die folgenden Mitglieder hat:
 - Der logische Standard-VLAN-Switch
 - Logische Ports, jeweils einer für die PCG-Uplink-Ports, wenn Sie HA aktiviert haben
 - IP-Adresse
- Es werden drei Regeln für verteilte Firewalls erstellt:
 - LogicalSwitchToLogicalSwitch
 - LogicalSwitchToAnywhere
 - AnywhereToLogicalSwitch

Hinweis Diese DFW-Regeln blockieren den gesamten Datenverkehr und müssen entsprechend Ihren spezifischen Anforderungen angepasst werden.

Verifizieren Sie diese Konfigurationen in NSX Manager:

- 1 Klicken Sie im NSX Cloud-Dashboard auf **NSX Manager**.
- 2 Navigieren Sie zu **Fabric > Knoten > Edge**. Public Cloud Gateway sollte als Edge-Knoten aufgeführt sein.
- 3 Verifizieren Sie, dass Bereitstellungsstatus, Manager-Verbindung und Controller-Verbindung verbunden sind (Status zeigt **Up** mit einem grünen Punkt).
- 4 Navigieren Sie zu **Fabric > Knoten > Edge-Cluster** und stellen Sie sicher, dass die Edge-Cluster und PCG als Teil des Clusters hinzugefügt wurden.
- 5 Navigieren Sie zu **Fabric > Knoten > Transportknoten** und stellen Sie sicher, dass PCG als Transportknoten registriert ist und mit zwei Transportzonen verbunden ist, die während der Bereitstellung von PCG automatisch erstellt wurden:
 - Datenverkehrstyp VLAN – dies stellt eine Verbindung mit dem PCG-Uplink her
 - Datenverkehrstyp Overlay – dies ist für die logische Overlay-Vernetzung
- 6 Verifizieren Sie, ob die logischen Switches und der logische Ebene-0-Router erstellt wurden und der logische Router dem Edge-Cluster hinzugefügt wurde.

Wichtig Löschen Sie keine der durch NSX erstellten Elemente.

Public-Cloud-Konfigurationen

In AWS:

- In der AWS VPC wird ein neuer Typ-A-Datensatz mit dem Namen `nsx-gw.vmware.local` hinzugefügt. Die diesem Datensatz zugeordnete IP-Adresse entspricht der Verwaltungs-IP-Adresse von PCG. Diese wird von AWS unter Verwendung von DHCP vergeben und ist für jede VPC unterschiedlich.
- 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 9-2. 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 9-3. 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)

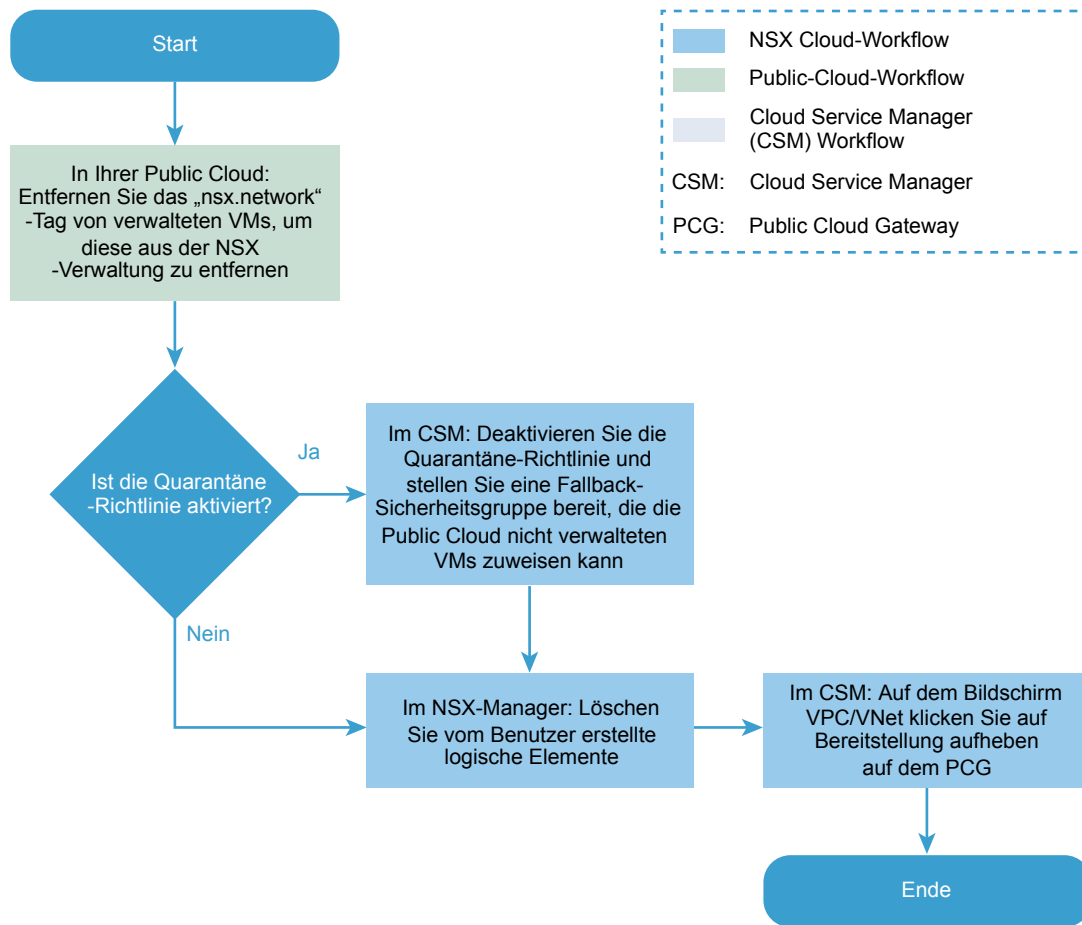
Bereitstellung von PCG aufheben

In diesem Flussdiagramm finden Sie die Schritte zum Aufheben der Bereitstellung von PCG.

- Um die Bereitstellung von PCG aufzuheben, müssen die folgenden Bedingungen erfüllt sein: keine Arbeitslast-VMs in der VPC oder im VNet dürfen von NSX verwaltet werden.
- Quarantäne-Richtlinie muss deaktiviert sein.

- Alle vom Benutzer erstellten logischen Elemente, die mit PCG verknüpft sind, müssen gelöscht werden.

Abbildung 9-4. Aufheben der Bereitstellung von PCG



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

Löschen Sie alle logischen Elemente, die Sie in NSX Manager erstellt haben.

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 [Nach der Bereitstellung von PCG erstellte Konstrukte](#).

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.

Edit VPC: [Redacted]

Default Quarantine ☐ Off

Fallback Security Group ID * ⓘ

Proxy Ser [Redacted]

profile-1a

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.

ANCEL SAVE

- 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

Löschen Sie alle logischen Elemente, die Sie in NSX Manager erstellt haben.

Schlagen Sie in der folgenden Liste nach, um die von Ihnen zu löschenden Entitäten zu finden:

Hinweis Löschen Sie die automatisch erstellten logischen Elemente nicht, wenn PCG bereitgestellt wird. Siehe [Nach der Bereitstellung von PCG erstellte Konstrukte](#)

- Public Cloud-DNS-Eintrag
- DDI: DHCP-Profil
- Routing: SNAT-Regel
- Routing: statischer Router
- Routing: logischer Routerport
- Routing: logischer Router
- Fabric-Knoten: Edge-Cluster
- Fabric-Knoten: Transportknoten
- Fabric-Knoten: Edges
- Fabric-Profile: PCG-Uplink-Host-Switch-Profil
- Switching: logische Switch-Ports
- Switching: logische Switches
- Fabric-Transportzonen: Transportzonen
- Switching: PublicCloud-Global-SpoofGuardProfile

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.

Deinstallieren von NSX-T Data Center

10

Sie können Elemente eines NSX-T Data Center-Overlays entfernen, einen Hypervisor-Host von NSX-T Data Center entfernen oder NSX-T Data Center komplett deinstallieren.

Dieses Kapitel enthält die folgenden Themen:

- [Aufheben einer NSX-T Data Center-Overlay-Konfiguration](#)
- [Entfernen eines Hosts von NSX-T Data Center oder komplette NSX-T Data Center-Deinstallation](#)

Aufheben einer NSX-T Data Center -Overlay-Konfiguration

Gehen Sie wie folgt vor, wenn Sie ein Overlay löschen, aber die Transportknoten beibehalten möchten.

Verfahren

- 1 Melden Sie sich beim vSphere Client an.
- 2 Trennen Sie in Ihrem VM-Managementtool alle VMs von allen logischen Switches, und verbinden Sie die VMs mit Netzwerken, die keine NSX-T Data Center-Netzwerke sind.
- 3 Bei KVM-Hosts senden Sie SSH auf die Hosts und schalten Sie die virtuellen Maschinen aus.
`shutdown -h now`
- 4 Löschen Sie in der NSX Manager-Benutzeroberfläche oder -API alle logischen Router.
- 5 Löschen Sie in der NSX Manager-Benutzeroberfläche oder -API alle logischen Switch-Ports und dann alle logischen Switches.
- 6 Löschen Sie in der NSX Manager-Benutzeroberfläche oder -API alle NSX Edges und dann alle NSX Edge-Cluster.
- 7 Konfigurieren Sie bei Bedarf einen neuen NSX-T Data Center-Overlay.

Entfernen eines Hosts von NSX-T Data Center oder komplette NSX-T Data Center -Deinstallation

Gehen Sie wie folgt vor, wenn Sie NSX-T Data Center vollständig deinstallieren oder nur einen Hypervisor-Host von NSX-T Data Center entfernen möchten, damit der Host nicht mehr am NSX-T Data Center-Overlay teilnehmen kann.

Im Folgenden wird eine vollständige Deinstallation von NSX-T Data Center beschrieben.

Voraussetzungen

Wenn das VM-Managementtool vCenter Server ist, versetzen Sie den vSphere-Host in den Wartungsmodus.

Verfahren

- 1 Wählen Sie im NSX Manager die Optionen **Fabric > Knoten > Transportknoten** und löschen Sie die Hosttransportknoten.

Durch das Löschen des Transportknotens wird der N-VDS vom Host entfernt. Dies können Sie mit dem folgenden Befehl überprüfen.

```
[root@host:~] esxcli network vswitch dvs vmware list
```

Bei KVM lautet der Befehl:

```
ovs-vsctl show
```

- 2 Stellen Sie in der NSX Manager-CLI sicher, dass der Dienst „install-upgrade“ von NSX-T Data Center ausgeführt wird.

```
nsx-manager-1> get service install-upgrade
Service name: install-upgrade
Service state: running
Enabled: True
```

- 3 Deinstallieren Sie den Host auf Managementebene, und entfernen Sie die NSX-T Data Center-Module.

Es kann bis zu 5 Minuten dauern, bis alle NSX-T Data Center-Module entfernt wurden.

Sie können die NSX-T Data Center-Module auf mehrere Arten entfernen:

- Wählen Sie im NSX Manager **Fabric > Knoten > Hosts > Löschen** aus.

Stellen Sie sicher, dass das Kontrollkästchen **NSX-Komponenten deinstallieren** aktiviert ist. Dadurch werden die NSX-T Data Center-Module auf dem Host deinstalliert.

Entfernen Sie die RHEL 7.4-Abhängigkeitspakete – json_spirit, python-greenlet, libev, protobuf, leveldb, python-gevent, python-simplejson, glog.

Entfernen Sie die Ubuntu 16.04.x-Abhängigkeitspakete – nicira-ovs-hypervisor-node, openvswitch-switch, openvswitch-datapath-dkms, openvswitch-pki, python-openvswitch, openvswitch-common, libjson-spirit.

Hinweis: Die Verwendung von **Fabric > Knoten > Hosts > Löschen** bei deaktivierter Option **NSX-Komponenten deinstallieren** dient nicht dazu, die Registrierung eines Hosts aufzuheben. Dies dient lediglich als Problemumgehung für Hosts in einem fehlerhaften Zustand.

- Von einem Berechnungsmanager verwaltete Hosts: Wählen Sie in NSX Manager den Menübefehl **Fabric > Knoten > Hosts > Transportknoten > Host löschen** aus.

Wählen Sie in NSX Manager den Menübefehl **Fabric > Knoten > Hosts > Berechnungsmanager > Clustermanager konfigurieren** aus und deaktivieren Sie die Option **NSX automatisch installieren**. Wählen Sie „Knoten“ aus und klicken Sie auf **NSX deinstallieren**.

Stellen Sie sicher, dass das Kontrollkästchen **NSX-Komponenten deinstallieren** aktiviert ist. Dadurch werden die NSX-T Data Center-Module auf dem Host deinstalliert.

- Verwenden Sie die API DELETE `/api/v1/fabric/nodes/<node-id>`.

Hinweis Diese API entfernt nicht die Abhängigkeitspakete aus dem nsx-lcp-Paket.

Entfernen Sie die RHEL 7.4-Abhängigkeitspakete – `json_spirit`, `python-greenlet`, `libev`, `protobuf`, `leveldb`, `python-gevent`, `python-simplejson`, `glog`.

Entfernen Sie die Ubuntu 16.04.x-Abhängigkeitspakete – `nicira-ovs-hypervisor-node`, `openvswitch-switch`, `openvswitch-datapath-dkms`, `openvswitch-pki`, `python-openvswitch`, `openvswitch-common`, `libjson-spirit`.

- Verwenden Sie die Befehlszeilenschnittstelle (CLI) für vSphere.

- a Rufen Sie den Manager-Fingerabdruck ab.

```
manager> get certificate api thumbprint
```

- b Führen Sie in der NSX-T Data Center-CLI des Hosts den im Folgenden aufgeführten Befehl aus, um den Host von der Managementebene zu trennen.

```
host> detach management-plane <MANAGER> username <ADMIN-USER> password <ADMIN-PASSWORD>
thumbprint <MANAGER-THUMBPRINT>
```

- c Führen Sie auf dem Host den nachfolgenden Befehl zum Entfernen von Filtern aus.

```
[root@host:~] vsipioctl clearallfilters
```

- d Führen Sie auf dem Host den nachfolgenden Befehl zum Anhalten von netcpa aus.

```
[root@host:~] /etc/init.d/netcpad stop
```

- e Schalten Sie die VMs auf dem Host aus oder migrieren Sie sie zu einem anderen Host.

- f Führen Sie auf dem Host den folgenden Befehl aus, um die Konfiguration und die Module von NSX-T Data Center manuell zu deinstallieren. Dieser Befehl wird auf allen Hosttypen unterstützt.

```
[root@host:~] clear management-plane
```

Nächste Schritte

Nach dieser Änderung wird der Host von der Managementebene entfernt und kann nicht mehr am NSX-T Data Center-Overlay teilnehmen.

Wenn Sie NSX-T Data Center gänzlich entfernen, fahren Sie NSX Manager, NSX Controllers und NSX Edges im VM-Managementtool herunter und löschen Sie diese von der Festplatte.