

# Installationshandbuch für NSX-T Data Center

Geändert am 12. AUG. 2021  
VMware NSX-T Data Center 2.5

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

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

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

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

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

# Inhalt

NSX-T Data Center-Installationshandbuch	8
<b>1 Übersicht über NSX-T Data Center</b>	<b>9</b>
Wichtige Konzepte	10
Übersicht über NSX Manager	13
<b>2 Workflows für die Installation von NSX-T Data Center</b>	<b>17</b>
NSX-T Data Center-Workflow für vSphere	17
NSX-T Data Center-Installations-Workflow für KVM	18
NSX-T Data Center-Konfigurations-Workflow für Bare-Metal-Server	19
<b>3 Vorbereitung für die Installation</b>	<b>20</b>
Systemvoraussetzungen	20
Systemanforderungen für NSX Manager-VM und -Host-Transportknoten	20
Systemanforderungen für NSX Edge-VM	24
Anforderungen der NSX Edge-Bare-Metal-Bereitstellung	25
Bare Metal Server-Systemanforderungen	28
Bare Metal Linux-Container-Anforderungen	28
Ports und Protokolle	29
Von NSX Manager verwendete TCP- und UDP-Ports	29
Von NSX Edge verwendete TCP- und UDP-Ports	31
Von ESXi, KVM-Hosts und Bare-Metal-Server verwendete TCP- und UDP-Ports	32
<b>4 NSX Manager-Installation</b>	<b>35</b>
Ändern der standardmäßigen Ablaufzeit des Administratorkennworts	41
<b>5 Installieren von NSX-T Data Center auf vSphere</b>	<b>42</b>
Installieren Sie NSX Manager und die verfügbaren Appliances	42
Installieren von NSX Manager unter ESXi mithilfe des OVF-Befehlszeilentools	47
Konfigurieren von NSX-T Data Center zum Anzeigen des GRUB-Menü zum Startzeitpunkt	52
Anmeldung beim neu erstellten NSX Manager	53
Hinzufügen eines Compute Managers	53
Bereitstellen von NSX Manager-Knoten zur Bildung eines Clusters über die Benutzeroberfläche	56
Konfigurieren einer virtuellen IP-Adresse (VIP) für einen Cluster	64
Deaktivieren von Snapshots auf NSX-T-Appliances	65

## **6** Installieren von NSX-T Data Center auf KVM 67

Einrichten von KVM 67

Verwalten der Gast-VMs in der KVM-CLI 70

Installieren von NSX Manager auf KVM 71

Anmeldung beim neu erstellten NSX Manager 76

Installieren von Drittanbieterpaketen auf einem KVM-Host 77

Überprüfung der Open vSwitch-Version auf RHEL KVM-Hosts 78

Überprüfen der Open vSwitch-Version auf SUSE KVM-Hosts 79

Bereitstellen von NSX Manager-Knoten zur Bildung eines Cluster mithilfe der CLI 80

## **7** Konfigurieren des Bare-Metal-Servers zur Verwendung von NSX-T Data Center 82

Installieren von Drittanbieterpaketen auf einem Bare-Metal-Server 82

Erstellen der Anwendungsschnittstelle für Bare-Metal Server-Arbeitslasten 84

## **8** NSX Manager-Clusteranforderungen 86

NSX Manager-Clusteranforderungen für eine, zwei und mehrere Sites 86

## **9** Installieren von NSX Edge 90

NSX Edge-Installationsanforderungen 90

NSX Edge-Netzwerkeinrichtung 93

NSX Edge-Installationsmethoden 99

Erstellen eines NSX Edge-Transportknotens 101

Erstellen eines NSX Edge-Clusters 106

Installieren von NSX Edge unter ESXi mithilfe der grafischen vSphere-Benutzeroberfläche 107

Installieren von NSX Edge auf ESXi unter Verwendung des OVF-Befehlszeilentools 111

Installieren von NSX Edge per ISO-Datei als virtuelle Appliance 116

Bare-Metal-Installation von NSX Edge 120

Vorbereiten des PXE-Servers für NSX Edge 121

Automatisches Installieren von NSX Edge via ISO-Datei 126

Interaktives Installieren von NSX Edge via ISO-Datei 130

Verbinden von NSX Edge mit der Management Plane 132

Konfigurieren von NSX Edge als Transportknoten 134

## **10** Transportzonen und Transportknoten 137

Erstellen von Transportzonen 137

Erstellen eines IP-Pools für Tunnel-Endpoint-IP-Adressen 140

Erweiterter Datenpfad 141

Konfigurieren von Profilen 145

Erstellen eines Uplink-Profiles 145

Konfigurieren von Network I/O Control-Profilen 149

Hinzufügen eines NSX Edge-Cluster-Profiles	159
Hinzufügen eines NSX Edge-Bridge-Profiles	159
Hinzufügen eines Transportknotenprofils	160
VMkernel-Migration auf einen N-VDS-Switch	166
Fehler bei der VMkernel-Migration	172
Erstellen eines eigenständigen Hosts oder Bare-Metal-Server-Transportknotens	176
Konfigurieren eines verwalteten Host-Transportknotens	186
Konfigurieren von ESXi-Hosttransportknoten mit Linkaggregation (LAG)	191
Überprüfen des Transportknotenstatus	192
Migrieren von ESXi-VMkernel- und physischen Adaptern	195
NSX-Wartungsmodus	196
Optische Darstellung eines N-VDS	196
Integritätsprüfung für VLAN-ID-Bereiche und MTU-Einstellungen	198
Anzeigen des Erkennungsstatus für die bidirektionale Weiterleitung	201
Manuelle Installation von NSX-T Data Center-Kernel-Modulen	202
Manuelles Installieren von NSX-T Data Center-Kernel-Modulen auf ESXi-Hypervisors	202
Manuelles Installieren von NSX-T Data Center-Softwarepaketen auf Ubuntu-KVM-Hypervisors	206
Manuelles Installieren von NSX-T Data Center-Softwarepaketen auf RHEL- und CentOS-KVM-Hypervisors	207
Manuelles Installieren von NSX-T Data Center-Softwarepaketen auf SUSE-KVM-Hypervisors	208
Bereitstellung eines vollständig reduzierten vSphere-Clusters NSX-T	209

## 11 Integration des Hostprofils in NSX-T 222

Automatische Bereitstellung statusfreier Cluster	222
Allgemeine Aufgaben zum automatischen Bereitstellen statusfreier Cluster	222
Voraussetzungen und unterstützte Versionen	223
Erstellen eines benutzerdefinierten Image-Profiles für statusfreie Hosts	224
Zuordnen des benutzerdefinierten Images zu den Referenz- und Zielhosts	226
Einrichten der Netzwerkkonfiguration auf dem Referenzhost	227
Konfigurieren des Referenzhosts als Transportknoten in NSX-T	228
Extrahieren und Überprüfen des Hostprofils	230
Überprüfen der Hostprofilzuordnung mit dem statusfreien Cluster	231
Aktualisieren der Hostanpassung	232
Auslösen der automatischen Bereitstellung auf Zielhosts	233
Fehlerbehebung für das Host- und Transportknotenprofil	243
Statusorientierte Server	245
Unterstützte NSX-T- und ESXi-Versionen	246
Vorbereiten eines statusorientierten Zielclusters	246
VMkernel-Migration mit angewendetem Hostprofil	248
VMkernel-Migration ohne angewendetes Hostprofil	250

## 12 Deinstallieren von NSX-T Data Center von einem Host-Transportknoten 252

- Überprüfen der Host-Netzwerkzuordnungen für die Deinstallation 252
- Deinstallieren von NSX-T Data Center von einem vSphere-Cluster 254
- Deinstallieren von NSX-T Data Center von einem Host in einem vSphere-Cluster 256
- Deinstallieren von NSX-T Data Center von einem eigenständigen Host 257

## 13 Installieren von NSX Cloud-Komponenten 259

- Architektur und Komponenten von NSX Cloud 259
- Übersicht über das Bereitstellen von NSX Cloud 261
- Bereitstellen lokaler Komponenten von NSX-T Data Center 261
  - Installieren von CSM 262
  - Verbinden von CSM mit NSX Manager 262
  - Aktivieren des Zugriffs auf Ports und Protokolle 263
  - (Optional) Proxy-Server konfigurieren 264
  - (Optional) Einrichten von vDM für Cloud Service Manager 265
- Ihr Public Cloud-Konto hinzufügen 266
  - Ihr Microsoft Azure-Netzwerk mit Ihrer lokalen NSX-T Data Center-Bereitstellung verbinden 266
  - Ihr Amazon Web Services-Netzwerk (AWS-Netzwerk) mit Ihrer lokalen NSX-T Data Center-Bereitstellung verbinden 274
- Bereitstellen des NSX Public Cloud Gateway 280
  - Bereitstellen von PCG in einem VNet 283
  - Bereitstellen von PCG in einer VPC 285
  - Verknüpfung mit einer Transit-VPC oder einem Transit-VNet 288
  - Automatisch erstellte logische Entitäten und Cloud-native Sicherheitsgruppen 289
- (Optional) Installieren von NSX Tools auf Ihren Arbeitslast-VMs 296
- Aufheben der Bereitstellung oder Entfernen der Verknüpfung von PCGs 296
  - Entfernen des nsx.network-Tags in der Public Cloud 297
  - Deaktivieren der Quarantäne-Richtlinie, Bereitstellen einer Fallback-Sicherheitsgruppe 297
  - Vom Benutzer erstellte logische Elemente löschen 299
  - Bereitstellung aufheben oder Verknüpfung entfernen** von CSM 299
  - Beheben von Fehlern bei der Aufhebung der PCG-Bereitstellung 299

## 14 Installieren und Konfigurieren von NSX Intelligence 301

- Workflow zur NSX Intelligence-Installation und -Konfiguration 302
- Vorbereitung für die Installation von NSX Intelligence 302
  - Systemanforderungen für NSX Intelligence 303
  - Von NSX Intelligence verwendete TCP- und UDP-Ports 304
- Herunterladen und Entpacken des NSX Intelligence-Installationspakets 305
- Installieren der NSX Intelligence-Appliance 308
- Fehlerbehebung bei der Installation der NSX Intelligence-Appliance 311

Die Anmeldedaten waren falsch oder das angegebene Konto wurde gesperrt	311
Status „Fehlgeschlagen“ für die Appliance-Bereitstellung wird nicht gelöscht	311
Deinstallieren der NSX Intelligence-Appliance	312

## **15** Beheben von Installationsproblemen 313

Die Installation schlägt aufgrund unzureichenden Speicherplatzes in Bootbank auf dem ESXi-Host fehl	313
---	-----

# NSX-T Data Center-Installationshandbuch

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

## Zielgruppe

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

## Technische Veröffentlichungen – Glossar

VMware Technical Publications enthält ein Glossar mit Begriffen, die Ihnen möglicherweise unbekannt sind. Definitionen von Begriffen, wie sie in der technischen Dokumentation von VMware genutzt werden, finden Sie unter <https://www.vmware.com/topics/glossary>.



# Übersicht über NSX-T Data Center

# 1

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

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

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

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

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

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

Dieses Kapitel enthält die folgenden Themen:

- [Wichtige Konzepte](#)

## ■ Übersicht über NSX Manager

# Wichtige Konzepte

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

### Compute Manager

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

### Control Plane

Berechnet den Laufzeitzustand anhand der Konfiguration aus der Management Plane, verteilt Topologie-Informationen, die von den 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 Control Plane aufgefüllt werden. Die Datenebene meldet Topologie-Informationen an die Control Plane und pflegt Statistiken auf Paketebene.

### Externes Netzwerk

Ein physisches Netzwerk oder VLAN, das nicht von NSX-T Data Center verwaltet wird. Sie können Ihr logisches Netzwerk oder Overlay-Netzwerk über NSX Edge mit einem externen Netzwerk verknüpfen. Beispiel: Ein physisches Netzwerk in einem Kundendatencenter oder ein VLAN in einer physischen Umgebung.

### 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 Datencenter eintritt.

### Eingehender Datenverkehr am logischen Port

Eingehender Netzwerkdatenverkehr, der das Datencenter 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

Einheit, die virtuelles Layer 2-Switching für VM-Schnittstellen und Gateway-Schnittstellen bereitstellt. Ein logischer Switch bietet Mandantennetzwerk-Administratoren das logische Äquivalent eines physischen Layer 2-Switches, sodass Sie mehrere VMs mit einer gemeinsamen Broadcast-Domäne verbinden können. Ein logischer Switch ist eine logische Einheit, die von der physischen Hypervisor-Infrastruktur unabhängig ist und viele Hypervisors umspannt, sodass VMs unabhängig von ihrer physischen Position verbunden werden.

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

### **Port für den logischen Switch**

Verknüpfungspunkt für einen logischen Switch, mit dem eine Verbindung zu einer Netzwerkschnittstelle einer virtuellen Maschine oder zu einer logischen Router-Schnittstelle hergestellt werden kann. Der logische Switch-Port meldet das angewendete Switching-Profil, den Portstatus und den Linkstatus.

### **Management Plane**

Liefert einen einzelnen API-Einstiegspunkt in das System, speichert die Benutzerkonfiguration, verarbeitet Benutzerabfragen und führt Betriebsaufgaben auf allen Management-, Controller- und Datenebenenknoten im System aus. Die Management Plane ist außerdem für das Abfragen, Ändern und Speichern der Benutzerkonfiguration zuständig.

### **NSX Edge-Cluster**

Sammlung aus NSX Edge-Knoten-Appliances mit denselben Einstellungen wie Protokolle für die High Availability-Überwachung.

### **NSX Edge-Knoten**

Komponente, deren Funktionsziel es ist, Rechenleistung für die IP-Routing- und IP-Dienstfunktionen bereitzustellen.

### **NSX-verwalteter Virtual Distributed Switch oder KVM Open vSwitch**

Der NSX-verwaltete Virtual Distributed Switch (N-VDS, vormals Host-Switch) oder OVS wird für freigegebene NSX Edge- und Computing-Cluster verwendet. N-VDS ist für die Konfiguration des Overlay-Datenverkehrs erforderlich.

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, auf dem die API-Dienste, die Management Plane und die Agent-Dienste gehostet werden. NSX Manager ist eine Appliance, die im Installationspaket von NSX-T Data Center

enthalten ist. Sie können die Appliance mit der Rolle **NSX Manager** oder **nsx-cloud-service-manager** bereitstellen. Die Appliance unterstützt derzeit nur jeweils eine Rolle gleichzeitig.

### NSX Manager-Cluster

Ein Cluster aus NSX Managern, die Hochverfügbarkeit bereitstellen können.

### Open vSwitch (OVS)

Open Source-Software-Switch, der als virtueller Switch in XenServer, Xen, KVM und anderen Linux-basierten Hypervisoren fungiert.

### Logisches Overlay-Netzwerk

Logisches Netzwerk, das anhand von Layer 2-in-Layer 3-Tunneling implementiert wird, sodass die für VMs sichtbare Topologie von der des physischen Netzwerks entkoppelt wird

### Physische Schnittstelle (pNIC)

Netzwerkschnittstelle auf einem physischen Server, auf dem ein Hypervisor installiert ist

### Segment

Einheit, die virtuelles Layer 2-Switching für VM-Schnittstellen und Gateway-Schnittstellen bereitstellt. Ein Segment fungiert für Administratoren des Mandantennetzwerks als logisches Äquivalent eines physischen Layer 2-Switches, mit dem mehrere VMs mit einer gemeinsamen Broadcast-Domäne verbunden werden können. Ein Segment ist eine logische Einheit, die von der physischen Hypervisor-Infrastruktur unabhängig ist und viele Hypervisoren umspannt, sodass VMs unabhängig von ihrer physischen Position verbunden werden können. Ein Segment ist auch als logischer Switch bekannt.

In einer Cloud mit mehreren Mandanten können zahlreiche Segmente nebeneinander auf derselben Hypervisor-Hardware vorhanden sein, wobei jedes Layer 2-Segment von den anderen isoliert ist. Segmente können mithilfe von Gateways verbunden werden, die Konnektivität mit dem externen physischen Netzwerk bereitstellen können.

### Tier-0-Gateway oder logischer Tier-0 Router

Das Tier-0-Gateway auf der Registerkarte **Netzwerk und Sicherheit – Erweitert** als logischer Tier-0 Router bezeichnet. Er verbindet sich mit dem physischen Netzwerk und kann als Aktiv/Aktiv- oder Aktiv/Standby-Cluster dargestellt werden. Das Tier-0-Gateway führt BGP und Peers mit physischen Routern aus. Im Aktiv/Standby-Modus kann das Gateway auch zustandsbehaftete Dienste bereitstellen.

### Tier-1-Gateway oder logischer Tier-1 Router

Das Tier-1-Gateway auf der Registerkarte **Netzwerk und Sicherheit – Erweitert** als logischer Tier-1 Router bezeichnet. Er verbindet sich mit einem Tier-0-Gateway für Northbound-Konnektivität und einem oder mehreren Overlay-Netzwerken für Southbound-Konnektivität. Bei einem Tier-1-Gateway kann es sich um einen Aktiv/Standby-Cluster handeln, der zustandsbehaftete Dienste bereitstellt.

## Transportzone

Sammlung aus Transportknoten, die die maximale Reichweite für logische Switches definiert. Eine Transportzone stellt eine Reihe aus ähnlich bereitgestellten Hypervisors und die logischen Switches dar, die VMs auf diesen Hypervisors verbinden. Sie ist außerdem bei der NSX-T Data Center-Management Plane registriert und es sind NSX-T Data Center-Module auf ihr installiert. Damit ein Hypervisor-Host oder NSX Edge Teil des NSX-T Data Center-Overlays werden kann, muss er der NSX-T Data Center-Transportzone hinzugefügt werden.

## Transportknoten

Ein Knoten, der an einem NSX-T Data Center-Overlay oder NSX-T Data Center-VLAN-Netzwerk teilnehmen kann. Bei einem KVM-Host können Sie den N-VDS im Voraus konfigurieren oder die Konfiguration von NSX Manager durchführen lassen. Bei einem ESXi-Host wird der N-VDS immer von NSX Manager konfiguriert.

## Uplink-Profil

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

## VM-Schnittstelle (vNIC)

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

## Virtueller Tunnel-Endpoint

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

# Übersicht über NSX Manager

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

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

- Die Richtlinienchnittstelle: Registerkarten **Netzwerk**, **Sicherheit**, **Bestand** sowie **Planen und Fehler beheben**.

- Die erweiterte Schnittstelle: Registerkarte **Registerkarte Netzwerk und Sicherheit – Erweitert**.

## Zeitpunkt der Verwendung von Richtlinien- oder erweiterten Schnittstellen

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

- Wenn Sie eine neue Umgebung mit NSX-T Data Center 2.4 oder höher einsetzen, ist die Verwendung der neuen richtlinienbasierten Benutzeroberfläche zum Erstellen und Verwalten Ihrer Umgebung in den meisten Fällen die beste Wahl.
  - Einige Funktionen sind in der richtlinienbasierten Benutzeroberfläche nicht verfügbar. Wenn Sie diese Funktionen benötigen, verwenden Sie die erweiterte Benutzeroberfläche für alle Konfigurationen.
- Wenn Sie ein Upgrade auf NSX-T Data Center 2.4 oder höher durchführen, müssen Sie weiterhin Konfigurationsänderungen mithilfe der Benutzerschnittstelle **Netzwerk und Sicherheit – Erweitert** vornehmen.

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


Richtlinienschnittstelle	Erweiterte Schnittstelle
Für die meisten neuen Bereitstellungen sollte die richtlinienbasierte Schnittstelle verwendet werden.	Bereitstellungen, die mithilfe der erweiterten Schnittstelle erstellt wurden, z. B. Upgrades von Versionen, bevor die richtlinienbasierte Schnittstelle vorhanden war.
NSX Cloud-Bereitstellungen	Bereitstellungen, die in andere Plug-ins integriert werden. Beispiel: NSX Container Plug-in, OpenStack und andere Cloud Management-Plattformen.

**Tabelle 1-1. Zeitpunkt der Verwendung von Richtlinien- oder erweiterten Schnittstellen (Fortsetzung)**

Richtlinienschnittstelle	Erweiterte Schnittstelle
<p>Netzwerkfunktionen sind nur in der Richtlinienschnittstelle verfügbar:</p> <ul style="list-style-type: none"> <li>■ DNS-Dienste und -Zonen</li> <li>■ VPN</li> <li>■ Weiterleitungsrichtlinien für NSX Cloud</li> </ul>	<p>Netzwerkfunktionen sind nur in der erweiterten Schnittstelle verfügbar:</p> <ul style="list-style-type: none"> <li>■ Timer für die Weiterleitung der Aktiv-Benachrichtigung</li> <li>■ Statische Routen mit BFD und Schnittstelle als nächster Hop</li> <li>■ Metadaten-Proxy</li> <li>■ Der mit einem isolierten Segment verbundene DHCP-Server und die statische Bindung</li> </ul>
<p>Sicherheitsfunktionen, die nur in der Richtlinienschnittstelle verfügbar sind:</p> <ul style="list-style-type: none"> <li>■ Endpoint-Schutz</li> <li>■ Netzwerk-Introspektion (Ost-West-Service Insertion)</li> <li>■ Kontextprofile <ul style="list-style-type: none"> <li>■ L7-Anwendungen</li> <li>■ FQDN</li> </ul> </li> <li>■ Neue verteilte Firewall und neues Gateway-Firewall-Layout <ul style="list-style-type: none"> <li>■ Kategorien</li> <li>■ Automatische Dienstregeln</li> <li>■ Entwürfe</li> </ul> </li> </ul>	<p>Sicherheitsfunktionen, die nur in der erweiterten Schnittstelle verfügbar sind:</p> <ul style="list-style-type: none"> <li>■ Schwellenwerte von CPU und Arbeitsspeicher</li> <li>■ Bridge-Firewall</li> <li>■ Regeln für verteilte Firewalls basierend auf IPs in Quelle und Ziel</li> </ul>

## Verwenden der Richtlinienschnittstelle

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

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

## Wo Sie die Richtlinienschnittstellen und erweiterten Schnittstellen finden

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

Tabelle 1-2. Richtlinienchnittstellen und erweiterte Schnittstellen

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

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

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

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

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

Tabelle 1-3. Objektnamen

Mit der Richtlinienchnittstelle erstellte Objekte	Mit der erweiterten Schnittstelle erstellte Objekte
Segment	Logischer Switch
Tier-1-Gateway	Logischer Tier-1 Router
Tier-0-Gateway	Logischer Tier-0 Router
Gruppe	NSGroup, IP-Sets, MAC-Sets
Sicherheitsrichtlinie	Firewallabschnitt
Regel	Firewallregel
Gateway-Firewall	Edge-Firewall



# Workflows für die Installation von NSX-T Data Center

# 2

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

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

Dieses Kapitel enthält die folgenden Themen:

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

## NSX-T Data Center-Workflow für vSphere

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

Führen Sie die einzelnen Verfahren in der empfohlenen Reihenfolge durch.

- 1 Überprüfen der NSX Manager-Installationsanforderungen. Siehe [Kapitel 4 NSX Manager-Installation](#).
- 2 Konfigurieren der erforderlichen Ports und Protokolle. Siehe [Ports und Protokolle](#).
- 3 Installieren des NSX Manager. Siehe [Installieren Sie NSX Manager und die verfügbaren Appliances](#).
- 4 Anmelden beim neu erstellten NSX Manager. Siehe [Anmeldung beim neu erstellten NSX Manager](#).
- 5 Konfigurieren Sie einen Compute Manager. Siehe [Hinzufügen eines Compute Managers](#).
- 6 Bereitstellen weiterer NSX Manager-Knoten zum Erstellen eines Clusters. Siehe [Bereitstellen von NSX Manager-Knoten zur Bildung eines Clusters über die Benutzeroberfläche](#).
- 7 Überprüfen der NSX Edge-Installationsanforderungen. Siehe [NSX Edge-Installationsanforderungen](#).
- 8 Installieren von NSX Edges. Weitere Informationen finden Sie unter [Installieren von NSX Edge unter ESXi mithilfe der grafischen vSphere-Benutzeroberfläche](#).
- 9 Erstellen eines NSX Edge-Clusters. Siehe [Erstellen eines NSX Edge-Clusters](#).

- 10 Erstellen von Transportzonen. Siehe [Erstellen von Transportzonen](#).
- 11 Erstellen von Host-Transportknoten. Siehe [Erstellen eines eigenständigen Hosts oder Bare-Metal-Server-Transportknotens](#) oder [Konfigurieren eines verwalteten Host-Transportknotens](#).

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

## Nach der Installation

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

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

## NSX-T Data Center-Installations-Workflow für KVM

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

Führen Sie die einzelnen Verfahren in der empfohlenen Reihenfolge durch.

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

- 11 Erstellen von Transportzonen. Siehe [Erstellen von Transportzonen](#).
- 12 Erstellen von Host-Transportknoten. Siehe [Erstellen eines eigenständigen Hosts oder Bare-Metal-Server-Transportknotens](#).

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

## Nach der Installation

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

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

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

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

Führen Sie die einzelnen Verfahren in der empfohlenen Reihenfolge durch.

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

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

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

# Vorbereitung für die Installation

# 3

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

Dieses Kapitel enthält die folgenden Themen:

- [Systemvoraussetzungen](#)
- [Ports und Protokolle](#)

## Systemvoraussetzungen

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

## Systemanforderungen für NSX Manager-VM und -Host-Transportknoten

Stellen Sie vor der Installation von NSX Manager oder anderen NSX-T Data Center-Appliances sicher, dass die Umgebung die unterstützten Anforderungen erfüllt.

### Für Host-Transportknoten unterstützte Hypervisoren

Hypervisor	Version	CPU-Kerne	Arbeitsspeicher
vSphere	<a href="#">Unterstützte vSphere-Version</a>	4	16 GB
CentOS Linux-KVM	7.4, 7.5, 7.6	4	16 GB
Red Hat Enterprise Linux(RHEL)-KVM	7.6, 7.5 und 7.4	4	16 GB
SUSE Linux Enterprise Server-KVM	12 sp3, 12 sp4	4	16 GB
Ubuntu KVM	16.04, 18.04.2 LTS	4	16 GB

Tabelle 3-1. Unterstützte Hosts für NSX Manager

Beschreibung der Unterstützung	Hypervisor
ESXi	Die unterstützten Hosts finden Sie in der <a href="#">VMware-Produktkompatibilitätsmatrix</a> .
KVM	RHEL 7.4 und Ubuntu 18.04.2 LTS  <b>Hinweis</b> Ab NSX-T Data Center 2.5 kann ein Ubuntu-Host mit Version 18.04.2 LTS entweder von 16.04 aktualisiert werden oder es handelt sich um eine Neuinstallation.

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

**Vorsicht** Auf RHEL und Ubuntu aktualisiert der Befehl `yum update` möglicherweise die Kernel-Version, die nicht größer als 4.14.x sein darf, und unterbricht die Kompatibilität mit NSX-T Data Center. Deaktivieren Sie das automatische Kernel-Update, wenn Sie `yum update` ausführen. Stellen Sie außerdem nach dem Ausführen des Befehls `yum install` sicher, dass NSX-T Data Center die Kernel-Version unterstützt.

## Netzwerkanforderungen für Hypervisor-Hosts

Die verwendete Netzwerkkarte muss mit der ESXi-Version kompatibel sein, auf der NSX-T Data Center ausgeführt wird. Informationen zu unterstützten Netzwerkkarten finden Sie im [VMware-Kompatibilitätshandbuch](#).

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

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

## NIC-Treiber mit erweitertem Datenpfad

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

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

## NSX Manager-VM-Ressourcenanforderungen

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

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

**Hinweis** NSX Manager stellt mehrere Rollen bereit, für die zuvor separate Appliances erforderlich waren. Dazu gehören die Richtlinienrolle, die Rolle der Management Plane und die Rolle der zentralen Control Plane. Die Rolle der zentralen Control Plane wurde zuvor von der NSX Controller-Appliance bereitgestellt.

- Sie können die besonders kleinen VM-Ressourcengröße nur für die Cloud Service Manager Appliance (CSM) verwenden. Stellen Sie CSM nach Bedarf in der besonders kleinen VM-Größe oder höher bereit. Weitere Informationen hierzu finden Sie unter [Übersicht über das Bereitstellen von NSX Cloud](#).
- Die kleine NSX Manager-VM-Appliance-Größe ist nur für Test- oder Proof-of-Concept-Bereitstellungen geeignet und darf nicht in der Produktion angewendet werden.
- Die mittlere NSX Manager-VM-Appliance-Größe ist für typische Produktionsumgebungen geeignet. Ein NSX-T-Verwaltungscluster, der mit dieser Appliance-Größe gebildet wird, kann bis zu 64 Hypervisoren unterstützen.
- Die große NSX Manager-VM-Appliance-Größe ist für große Bereitstellungen geeignet. Ein NSX-T-Verwaltungscluster, der mit dieser Appliance-Größe gebildet wird, kann über 64 Hypervisoren unterstützen.

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

## Sprachunterstützung

NSX Manager wurde in mehrere Sprachen lokalisiert: Englisch, Deutsch, Französisch, Japanisch, Chinesisch (vereinfacht), Koreanisch, Chinesisch (traditionell) und Spanisch.

## NSX Manager-Browserunterstützung

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

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

### Hinweis

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

## Anforderungen an die Netzwerklatenz

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

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

## Speicheranforderungen

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

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

## Systemanforderungen für NSX Edge-VM

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

**Hinweis** Die folgenden Bedingungen gelten für die Hosts für die NSX Edge-Knoten:

- NSX Edge-Knoten werden nur auf ESXi-basierten Hosts und nur mit Intel-basierten Chipsätzen unterstützt.

Andernfalls kann der EVC-Modus von vSphere verhindern, dass NSX Edge-Knoten gestartet werden, wobei eine Fehlermeldung in der Konsole angezeigt wird.

- Wenn der vSphere-EVC-Modus für den Host für die NSX Edge-VM aktiviert ist, muss die CPU Haswell oder eine neuere Generation aufweisen.
- Nur VMXNET3-vNIC wird nur für die NSX Edge-VM unterstützt.

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

### NSX Edge-VM-Ressourcenanforderungen

Appliance-Größe	Arbeitsspeicher	vCPU	Festplatte nspeicher	VM- Hardwareversion	Anmerkungen
NSX Edge Klein	4 GB	2	200 GB	11 oder höher (vSphere 6.0 oder höher)	Die kleine NSX Edge-VM-Appliance-Größe eignet sich für Test- oder Proof-of-Concept-Bereitstellungen.  <b>Hinweis</b> Die L7-Regeln werden auf einem Gateway der Ebene 1 nicht realisiert, wenn Sie eine kleine NSX Edge-VM bereitstellen.
NSX Edge Mittel	8 GB	4	200 GB	11 oder höher (vSphere 6.0 oder höher)	Die mittlere NSX Edge-Appliance-Größe ist für typische Produktionsumgebungen geeignet.
NSX Edge Groß	32 GB	8	200 GB	11 oder höher (vSphere 6.0 oder höher)	Die große NSX Edge-Appliance-Größe ist für Umgebungen mit Load Balancing konzipiert. Weitere Informationen finden Sie unter <a href="#">Skalieren von Load Balancer-Ressourcen</a> im <i>Administratorhandbuch für NSX-T Data Center</i> .



## CPU-Anforderungen für NSX Edge-VM

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

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

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

## Anforderungen der NSX Edge-Bare-Metal-Bereitstellung

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

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

Mindestanforderungen

Arbeitsspeicher	CPU-Kerne	Festplattenspeicher
32 GB	8	200 GB

Empfohlene Anforderungen

Arbeitsspeicher	CPU-Kerne	Festplattenspeicher
256 GB	24	200 GB

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

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

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

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

## Hardwareanforderungen für NSX Edge-Bare-Metal-Bereitstellungen

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

## Netzwerkkartenanforderungen für NSX Edge-Bare-Metal-Bereitstellungen

Typ der Netzwerkkarte	Beschreibung	ID des PCI-Geräts	Firmware-Version
Mellanox ConnectX-4 EN	PCI_DEVICE_ID_MELLANOX_CONNECTX4	0x1013	12.21.1000 und höher
Mellanox ConnectX-4 Lx EN	PCI_DEVICE_ID_MELLANOX_CONNECTX4LX	0x1015	14.21.1000 und höher
Mellanox ConnectX-5	PCI_DEVICE_ID_MELLANOX_CONNECTX5	0x1017	16.21.1000 und höher
Mellanox ConnectX-5 EX	PCI_DEVICE_ID_MELLANOX_CONNECTX5EX	0x1019	16.21.1000 und höher
Intel XXV710	I40E_DEV_ID_25G_B	0x158A	6.0.1
	I40E_DEV_ID_25G_SFP28	0x158B	6.0.1

Typ der Netzwerkkarte	Beschreibung	ID des PCI-Geräts	Firmware-Version
Intel X520/Intel 82599	IXGBE_DEV_ID_82599_KX4	0x10F7	Nicht verfügbar
	IXGBE_DEV_ID_82599_KX4_MEZZ	0x1514	Nicht verfügbar
		0x1517	Nicht verfügbar
	IXGBE_DEV_ID_82599_KR	0x10F8	Nicht verfügbar
	IXGBE_DEV_ID_82599_COMBO_BACKPLANE	0x000C	Nicht verfügbar
		0x10F9	Nicht verfügbar
	IXGBE_SUBDEV_ID_82599_KX4_KR_MEZZ	0x10FB	Nicht verfügbar
		0x11A9	Nicht verfügbar
	IXGBE_DEV_ID_82599_CX4	0x1F72	Nicht verfügbar
	IXGBE_DEV_ID_82599_SFP	0x17D0	Nicht verfügbar
	IXGBE_SUBDEV_ID_82599_SFP	0x0470	Nicht verfügbar
		0x1507	Nicht verfügbar
	IXGBE_SUBDEV_ID_82599_RNDC	0x154D	Nicht verfügbar
	IXGBE_SUBDEV_ID_82599_560FLR	0x154A	Nicht verfügbar
		0x1558	Nicht verfügbar
	IXGBE_SUBDEV_ID_82599_ECNA_DP	0x1557	Nicht verfügbar
		0x10FC	Nicht verfügbar
	IXGBE_DEV_ID_82599_SFP_EM	0x151C	Nicht verfügbar
	IXGBE_DEV_ID_82599_SFP_SF2		
	IXGBE_DEV_ID_82599_SFP_SF_QP		
	IXGBE_DEV_ID_82599_QSFP_SF_QP		
	IXGBE_DEV_ID_82599_EN_SFP		
	IXGBE_DEV_ID_82599_XAUI_LOM		
	IXGBE_DEV_ID_82599_T3_LOM		
Intel X540	IXGBE_DEV_ID_X540T	0x1528	Nicht verfügbar
	IXGBE_DEV_ID_X540T1	0x1560	Nicht verfügbar
Intel X550	IXGBE_DEV_ID_X550T	0x1563	Nicht verfügbar
	IXGBE_DEV_ID_X550T1	0x15D1	Nicht verfügbar
Intel X710	I40E_DEV_ID_SFP_X710	0x1572	6.0.1
	I40E_DEV_ID_KX_C	0x1581	6.0.1
	I40E_DEV_ID_10G_BASE_T	0x1586	6.0.1
Intel XL710	I40E_DEV_ID_KX_B	0x1580	6.0.1
	I40E_DEV_ID_QSFP_A	0x1583	6.0.1
	I40E_DEV_ID_QSFP_B	0x1584	6.0.1
	I40E_DEV_ID_QSFP_C	0x1585	6.0.1
Cisco VIC 1300er-Serie	Cisco UCS Virtual Interface Card 1300	0x0043	Nicht verfügbar

**Hinweis** Stellen Sie für alle oben aufgeführten unterstützten Netzwerkkarten sicher, dass die von Ihnen verwendeten Medienadapter und Kabel den unterstützten Medientypen des Anbieters entsprechen. Alle Medienadapter oder Kabel, die vom Anbieter nicht unterstützt werden, können zu unvorhersehbarem Verhalten führen. Dies kann sich beispielsweise dahingehend äußern, dass der Start aufgrund eines nicht erkannten Medienadapters nicht möglich ist. Informationen zu unterstützten Medienadaptern und Kabeln finden Sie in der Dokumentation des Netzwerkkartenanbieters.

## Bare Metal Server-Systemanforderungen

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

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

### Bare Metal Server-Anforderungen

Betriebssystem	Version	CPU-Kerne	Arbeitsspeicher
CentOS Linux	7.4 (1708) 7.5	4	16 GB
Red Hat Enterprise Linux (RHEL)	7.6 (Kernel: 3.10.0-957) 7.5 7.4 (Kernel: 3.10.0-6**)	4	16 GB
SUSE Linux Enterprise Server	12 sp3, 12 sp4	4	16 GB
Ubuntu	16.04.2 LTS (Kernel: 4.4.0-*) 18.04	4	16 GB

**Hinweis** Ab NSX-T Data Center 2.5 kann ein Ubuntu-Host mit Version 18.04.2 LTS entweder von Version 16.04 aktualisiert werden oder es handelt sich um eine Neuinstallation.

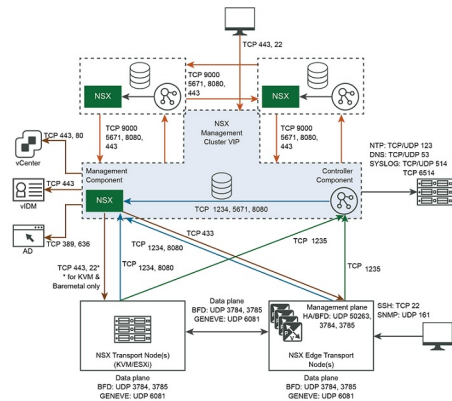
## Bare Metal Linux-Container-Anforderungen

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

## Ports und Protokolle

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

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



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

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

- KVM: MPA, netcpa, nsx-agent, OVS
- ESXi: netcpa, ESX-DP (im Kernel)

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

**NSX Cloud-Hinweis** Eine Liste der Ports, die für die Bereitstellung von NSX Cloud erforderlich sind, finden Sie unter [Aktivieren des Zugriffs auf Ports und Protokolle](#).

## Von NSX Manager verwendete TCP- und UDP-Ports

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

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

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

Quelle	Ziel	Port	Protokol	Beschreibung
NSX Manager, NSX Edge-Knoten, Transportknoten	NSX Manager	5671, 1234, 1235, 443	TCP	NSX-Messaging
NSX Manager, NSX Edge-Knoten, Transportknoten, vCenter Server	NSX Manager	8080	TCP	HTTP-Repository für Upgrade-Installation
NSX Manager	NSX Manager	9000, 5671, 1234, 443, 8080	TCP	Verteilter Datenspeicher
NSX Manager	DNS-Server	53	TCP	DNS
NSX Manager	DNS-Server	53	UDP	DNS
NSX Manager	Management-SCP-Server	22	TCP	SSH (Hochladen von Support-Paketen, Sicherungen usw.)
NSX Manager	NTP-Server	123	UDP	NTP
NSX Manager	SNMP-Server	161, 162	TCP	SNMP
NSX Manager	SNMP-Server	161, 162	UDP	SNMP
NSX Manager	Syslog-Server	514	TCP	Syslog
NSX Manager	Syslog-Server	514	UDP	Syslog
NSX Manager	Syslog-Server	6514	TCP	Syslog
NSX Manager	Syslog-Server	6514	UDP	Syslog
NSX Manager	Zwischen- und Root-CA-Server	80	TCP	Syslog (Export über TLS)  <b>Hinweis</b> Um zu überprüfen, welcher TCP-Port zum Abrufen der Zertifikatswiderrufslisten (CRLs) verwendet werden muss, überprüfen Sie die CRL Distribution Point(CDP)-URI der Zertifizierungsstelle.
NSX Manager	Traceroute-Ziel	3343-33523	UDP	Traceroute
NSX Manager	vCenter Server	80	TCP	NSX Manager zum Compute Manager-Kommunikation (vCenter Server), wenn konfiguriert.

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

Quelle	Ziel	Port	Protokoll	Beschreibung
NSX Manager	vCenter Server	443	TCP	NSX Manager zum Compute Manager-Kommunikation (vCenter Server), wenn konfiguriert.
NTP-Server	NSX Manager	123	UDP	NTP
Verwaltungsclients	NSX Manager	22	TCP	SSH (standardmäßig deaktiviert)
Verwaltungsclients	NSX Manager	443	TCP	NSX-API-Server
SNMP-Server	NSX Manager	161	UDP	SNMP

## Von NSX Edge verwendete TCP- und UDP-Ports

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

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

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

Quelle	Ziel	Port	Protokoll	Beschreibung
Verwaltungsclients	NSX Edge-Knoten	22	TCP	SSH (standardmäßig deaktiviert)
NSX Agent	NSX Edge-Knoten	5555	TCP	NSX Cloud: Agent der Instanz kommuniziert mit dem NSX Cloud-Gateway.
NSX Edge-Knoten	DNS-Server	53	UDP	DNS
NSX Edge-Knoten	Management-SCP- oder -SSH-Server	22	TCP	SSH
NSX Edge-Knoten	NSX Manager	1235	TCP	Kommunikation zwischen unterer Control Plane (LCP) und zentraler Control Plane (CCP)
NSX Edge-Knoten	NSX Edge-Knoten	1167	TCP	DHCP-Backend
NSX Edge-Knoten	NSX Edge-Knoten	2480	TCP	Nestdb
NSX Edge-Knoten	NSX Edge-Knoten	6666	TCP	NSX Cloud: lokale NSX Edge-Kommunikation.
NSX Edge-Knoten	NSX Edge-Knoten	50263	UDP	Hohe Verfügbarkeit
NSX Edge-Knoten	NSX Manager	443	TCP	HTTPS

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

Quelle	Ziel	Port	Protokoll	Beschreibung
NSX Edge-Knoten	NSX Manager	1234	TCP	NSX-Messaging-Kanal zu NSX Manager
NSX Edge-Knoten	NSX Manager	8080	TCP	NAPI, NSX-T Data Center-Upgrade
NSX Edge-Knoten	NTP-Server	123	UDP	NTP
NSX Edge-Knoten	OpenStack Nova-API- Server	3000– 9000	TCP	Metadaten-Proxy
NSX Edge-Knoten	SNMP-Server	161, 162	TCP	SNMP
NSX Edge-Knoten	SNMP-Server	161, 162	UDP	SNMP
NSX Edge-Knoten	Syslog-Server	514	TCP	Syslog
NSX Edge-Knoten	Syslog-Server	514	UDP	Syslog
NSX Edge-Knoten	Syslog-Server	6514	TCP	Syslog
NSX Edge-Knoten	Syslog-Server	6514	UDP	Syslog
NSX Edge-Knoten	Zwischen- und Root-CA- Server	80	TCP	Syslog (Export über TLS)  <b>Hinweis</b> Um zu überprüfen, welcher TCP-Port zum Abrufen der Zertifikatswiderrufslisten (CRLs) verwendet werden muss, überprüfen Sie die CRL Distribution Point(CDP)-URI der Zertifizierungsstelle.
NSX Edge-Knoten	Traceroute- Ziel	33434– 33523	UDP	Traceroute
NSX Edge-Knoten, Transportknoten	NSX Edge- Knoten	3784, 3785	UDP	BFD zwischen der TEP-IP-Adresse des Transportknotens in den Daten.
NTP-Server	NSX Edge- Knoten	123	UDP	NTP
SNMP-Server	NSX Edge- Knoten	161	UDP	SNMP

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

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



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

Quelle	Ziel	Port	Protokoll	Beschreibung
ESXi-Host	NSX Manager	1235	TCP	Kommunikation zwischen lokaler Control Plane (LCP) unter zentraler Control Plane (CCP)
ESXi-Host	NSX Manager	1234	TCP	NSX-Messaging-Kanal zu NSX Manager AMQP-Kommunikationskanal zu NSX Manager
ESXi-Host	NSX Manager	8080	TCP	Installation und Upgrade des HTTP-Repositorys
ESXi und KVM-Host	NSX Manager	443	TCP	Verwaltungs- und Bereitstellungsverbindung
ESXi und KVM-Host	NSX Manager	443	TCP	Installation und Upgrade des HTTP-Repositorys
GENEVE Terminierungsendpunkt (TEP)	GENEVE Terminierungsendpunkt (TEP)	6081	UDP	Transportnetzwerk
KVM-Host	NSX Manager	1234	TCP	NSX-Messaging-Kanal zu NSX Manager AMQP-Kommunikationskanal zu NSX Manager
Bare Metal-Serverhost	NSX Manager	5671, 1235, 1234, 8080	TCP	AMQP-Kommunikationskanal zu NSX Manager
KVM-Host	NSX Manager	1235	TCP	Kommunikation zwischen lokaler Control Plane (LCP) unter zentraler Control Plane (CCP)
KVM-Host	NSX Manager	8080	TCP	Installation und Upgrade des HTTP-Repositorys
NSX Manager	ESXi-Host	443	TCP	Verwaltungs- und Bereitstellungsverbindung
NSX Manager	KVM-Host	443	TCP	Verwaltungs- und Bereitstellungsverbindung
Host	Syslog-Server	514	TCP	Syslog (siehe Host-Syslog-Dokumentation)
Host	Syslog-Server	514	UDP	Syslog (siehe Host-Syslog-Dokumentation)
Host	Syslog-Server	6514	TCP	Syslog (siehe Host-Syslog-Dokumentation)
Host	Syslog-Server	6514	UDP	Syslog (siehe Host-Syslog-Dokumentation)

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

Quelle	Ziel	Port	Protokoll	Beschreibung
Host	Zwischen- und Root-CA-Server	80	TCP	<p>Syslog (Export über TLS)</p> <hr/> <p><b>Hinweis</b> Um zu überprüfen, welcher TCP-Port zum Abrufen der Zertifikatswiderrufslisten (CRLs) verwendet werden muss, überprüfen Sie die CRL Distribution Point(CDP)-URI der Zertifizierungsstelle.</p> <hr/>
NSX-T Data Center-Transportknoten	NSX-T Data Center-Transportknoten	3784, 3785	UDP	BFD-Sitzung zwischen TEPs, im Datenpfad unter Verwendung der TEP-Schnittstelle

# NSX Manager-Installation

# 4

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

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

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

In einer vSphere-Umgebung werden die folgenden Funktionen von NSX Manager unterstützt:

- vCenter Server kann die vMotion-Funktion zum Live-Migrieren von NSX Manager über Hosts und Cluster hinweg verwenden.
- vCenter Server kann die Storage vMotion-Funktion zum Live-Migrieren von NSX Manager über Hosts und Cluster hinweg verwenden.
- vCenter Server kann die Distributed Resource Scheduler-Funktion verwenden, um NSX Manager über Hosts und Cluster neu zu verteilen.
- vCenter Server kann die Anti-Affinitätsfunktion verwenden, um NSX Manager über Hosts und Cluster hinweg zu verwalten.

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

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

Anforderungen	Beschreibung
Unterstützte Bereitstellungsmethoden	<ul style="list-style-type: none"><li>■ OVA/OVF</li><li>■ QCOW2</li></ul>
Unterstützte Plattformen	Siehe <a href="#">Systemanforderungen für NSX Manager-VM und -Host-Transportknoten</a> . Es wird empfohlen, unter ESXi die NSX Manager-Appliance auf freigegebenem Speicher zu installieren.
IP-Adresse	Ein NSX Manager muss eine statische IP-Adresse aufweisen. Sie können die IP-Adresse nach der Installation nicht mehr ändern.

Anforderungen	Beschreibung
Kennwort für NSX-T Data Center-Appliance	<ul style="list-style-type: none"> <li>■ mindestens 12 Zeichen</li> <li>■ mindestens ein Kleinbuchstabe</li> <li>■ mindestens ein Großbuchstabe</li> <li>■ mindestens eine Zahl</li> <li>■ mindestens ein Sonderzeichen</li> <li>■ mindestens fünf unterschiedliche Zeichen</li> <li>■ Standard-Kennwortkomplexitätsregeln werden von den Argumenten des Linux PAM-Moduls erzwungen: <ul style="list-style-type: none"> <li>■ <code>retry=3</code>: die maximale Anzahl, wie oft ein neues Kennwort für dieses Argument eingegeben werden kann (maximal 3 mal), bevor eine Fehlermeldung zurückgegeben wird.</li> <li>■ <code>minlen=12</code>: die zulässige Mindestgröße für das neue Kennwort. Zusätzlich zur Anzahl von Zeichen im neuen Kennwort erfolgt eine Gutschrift (+ 1 für die Länge) für jede Art von Zeichen (sonstige, großgeschrieben, kleingeschrieben und Ziffer).</li> <li>■ <code>difok=0</code>: die minimale Anzahl von Bytes, die sich im neuen Kennwort unterscheiden müssen. Zeigt die Ähnlichkeit zwischen dem alten und dem neuen Kennwort an. Wenn <code>difok</code> der Wert 0 zugewiesen wird, müssen sich die Bytes des alten und des neuen Kennworts nicht unterscheiden. Eine genaue Übereinstimmung ist zulässig.</li> <li>■ <code>lcredit=1</code>: die maximale Gutschrift für die Verwendung von Kleinbuchstaben im neuen Kennwort. Wenn Sie weniger als oder 1 Kleinbuchstaben haben, zählt jeder Buchstabe + 1, um den aktuellen <code>minlen</code>-Wert zu erfüllen.</li> <li>■ <code>ucredit=1</code>: die maximale Gutschrift für die Verwendung von Großbuchstaben im neuen Kennwort. Wenn Sie weniger als oder 1 Großbuchstaben haben, zählt jeder Buchstabe + 1, um den aktuellen <code>minlen</code>-Wert zu erfüllen.</li> <li>■ <code>dcredit=1</code>: die maximale Gutschrift für die Verwendung von Ziffern im neuen Kennwort. Wenn Sie weniger als oder 1 Ziffer haben, zählt jede Ziffer + 1, um den aktuellen <code>minlen</code>-Wert zu erfüllen.</li> <li>■ <code>ocredit=1</code>: die maximale Gutschrift für die Verwendung von sonstigen Zeichen im neuen Kennwort. Wenn Sie weniger als oder 1 sonstiges Zeichen haben, zählt jedes Zeichen + 1, um den aktuellen <code>minlen</code>-Wert zu erfüllen.</li> <li>■ <code>enforce_for_root</code>: Das Kennwort ist für den Root-Benutzer festgelegt.</li> </ul> </li> </ul>
	<p><b>Hinweis</b> Weitere Einzelheiten zum Linux-PAM-Modul zum Abgleichen des Kennworts mit den Wörtern aus dem Wörterbuch finden Sie auf der Hauptseite.</p> <hr/> <p>Vermeiden Sie zum Beispiel einfache und systematische Kennwörter wie <b>VMware123!123</b> oder <b>VMware12345</b>. Kennwörter, die den Komplexitätsstandards entsprechen, sind nicht einfach und systematisch, sondern bestehen aus einer Kombination von Buchstaben, Sonderzeichen und Zahlen wie <b>VMware123!45</b>, <b>VMware1!2345</b> oder <b>VMware@1az23x</b>.</p>

Anforderungen	Beschreibung
Hostname	<p>Geben Sie beim Installieren von NSX Manager einen Hostnamen an, der keine ungültigen Zeichen wie einen Unterstrich oder Sonderzeichen wie den Punkt „.“ enthält. Wenn der Hostname ein ungültiges Zeichen oder Sonderzeichen enthält, wird der Hostname nach der Bereitstellung auf <b>nsx-manager</b> festgelegt.</p> <p>Weitere Informationen zu Hostnamenbeschränkungen finden Sie unter <a href="https://tools.ietf.org/html/rfc952">https://tools.ietf.org/html/rfc952</a> und <a href="https://tools.ietf.org/html/rfc1123">https://tools.ietf.org/html/rfc1123</a>.</p>
VMware Tools	<p>Auf der unter ESXi ausgeführten NSX Manager-VM sind VMware Tools installiert. Entfernen oder aktualisieren Sie VMTtools nicht.</p>
System	<ul style="list-style-type: none"> <li>■ Stellen Sie sicher, dass die Systemanforderungen erfüllt sind. Siehe <a href="#">Systemvoraussetzungen</a>.</li> <li>■ Stellen Sie sicher, dass die erforderlichen Ports geöffnet sind. Siehe <a href="#">Ports und Protokolle</a>.</li> <li>■ Stellen Sie sicher, dass auf dem ESXi-Host ein Datenspeicher konfiguriert und verfügbar ist.</li> <li>■ Stellen Sie sicher, dass Sie die IP-Adresse und das Gateway, die IP-Adressen des DNS-Servers, die Domänensuchliste und die IP-Adresse des NTP-Servers haben, die von NSX Manager verwendet werden.</li> <li>■ Erstellen Sie das Ziel-VM-Portgruppennetzwerk, wenn noch keines vorhanden ist. Platzieren Sie die NSX-T Data Center-Appliances in einem VM-Verwaltungsnetzwerk.</li> </ul> <p>Wenn Sie über mehrere Verwaltungsnetzwerke verfügen, können Sie statische Routen von der NSX-T Data Center-Apliance zu den anderen Netzwerken hinzufügen.</p> <ul style="list-style-type: none"> <li>■ Planen Sie das IPv4-IP-Adressschema für NSX Manager.</li> </ul>
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	<p>Das Client-Integrations-Plug-In muss installiert sein.</p>

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

## NSX Manager-Installationsszenarien

**Wichtig** Wenn Sie NSX Manager über eine OVA- oder OVF-Datei installieren (entweder über den vSphere-Client oder die Befehlszeile), werden OVA/OVF-Eigenschaftswerte wie Benutzernamen und Kennwörter erst beim Einschalten der virtuellen Maschine validiert. Das Feld mit der statischen IP-Adresse ist jedoch ein obligatorisches Feld zum Installieren von NSX Manager.

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

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

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

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

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

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

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

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

**Hinweis** Die Aktivierung der FQDN-Nutzung (DNS) auf NSX Managern ist für Multisite Lite und NSX Cloud und Bereitstellungen erforderlich. (Für alle anderen Bereitstellungstypen ist sie optional.) Weitere Informationen finden Sie unter *Bereitstellung von NSX-T Data Center für mehrere Sites* im *Administratorhandbuch für NSX-T Data Center* und [Kapitel 13 Installieren von NSX Cloud-Komponenten](#) in diesem Handbuch.

## Veröffentlichen der FQDNs der NSX Manager

Nach der Installation der NSX-T Data Center-Hauptkomponenten und CSM müssen Sie zum Aktivieren von NAT mithilfe des FQDN die Forward- und Reverse-Sucheinträge für die Manager-Knoten auf dem DNS-Server einrichten.

**Wichtig** Es wird dringend empfohlen, sowohl die Forward- als auch die Reverse-Sucheinträge für den FQDN der NSX Manager mit einer kurzen TTL zu konfigurieren, z. B. 600 Sekunden.

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

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

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

Beispielantwort:

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

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

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

## Validieren des Zugriffs über den FQDN durch Transportknoten

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



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

Beispielantwort:

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

Dieses Kapitel enthält die folgenden Themen:

- [Ändern der standardmäßigen Ablaufzeit des Administratorkennworts](#)

## Ändern der standardmäßigen Ablaufzeit des Administratorkennworts

Standardmäßig läuft das Administratorkennwort für die NSX Manager- und NSX Edge-Appliances nach 90 Tagen ab. Sie können jedoch den Ablaufzeitraum nach der Erstinstallation und -konfiguration zurücksetzen.

Wenn das Kennwort abläuft, können Sie sich nicht anmelden und keine Komponenten verwalten. Darüber hinaus schlagen alle Aufgaben oder API-Aufrufe fehl, für die das Administratorkennwort erforderlich ist. Wenn Ihr Kennwort abläuft, lesen Sie den Knowledgebase-Artikel 70691 zum [abgelaufenen NSX-T-Administratorkennwort](#).

### Verfahren

- 1 Verwenden Sie ein sicheres Programm, um eine Verbindung mit der NSX-CLI-Konsole herzustellen.
- 2 Setzen Sie den Ablaufzeitraum zurück.

Sie können den Ablaufzeitraum auf einen Wert zwischen 1 und 9999 Tagen festlegen.

```
nsxcli> set user admin password-expiration <1 - 9999>
```

**Hinweis** Alternativ können Sie API-Befehle verwenden, um den Ablaufzeitraum des Administratorkennworts festzulegen.

- 3 (Optional) Sie können den Ablauf des Kennworts deaktivieren, damit das Kennwort nie abläuft.

```
nsxcli> clear user audit password-expiration
```

# Installieren von NSX-T Data Center auf vSphere

# 5

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

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

Dieses Kapitel enthält die folgenden Themen:

- [Installieren Sie NSX Manager und die verfügbaren Appliances](#)
- [Konfigurieren einer virtuellen IP-Adresse \(VIP\) für einen Cluster](#)
- [Deaktivieren von Snapshots auf NSX-T-Appliances](#)

## Installieren Sie NSX Manager und die verfügbaren Appliances

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

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

### Voraussetzungen

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

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

- Planen Sie das IPv4-IP-Adressschema für NSX Manager.

## Verfahren

- 1 Suchen Sie im VMware-Download-Portal nach der NSX-T Data Center-OVA-Datei.  
Kopieren Sie die Download-URL oder laden Sie die OVA-Datei herunter.
- 2 Wählen Sie im Kontextmenü die Option **OVF-Vorlage bereitstellen** aus, um den Installationsassistenten zu starten.
- 3 Geben Sie die URL der herunterzuladenden OVA-Datei ein oder navigieren Sie zur OVA-Datei und klicken Sie auf **Weiter**.
- 4 Geben Sie einen Namen und einen Speicherort für die NSX Manager-VM ein und klicken Sie auf **Weiter**.  
Der eingegebene Name wird im vSphere- und im vCenter Server-Bestand angezeigt.
- 5 Wählen Sie eine Computing-Ressource für die NSX Manager-Appliance aus und klicken Sie auf **Weiter**.
  - ◆ Für die Installation auf einem von vCenter verwalteten ESXi-Host wählen Sie einen Host aus, auf dem die NSX Manager-Appliance bereitgestellt werden soll.
  - ◆ Für die Installation auf einem eigenständigen ESXi-Host wählen Sie den Host aus, auf dem die NSX Manager-Appliance bereitgestellt werden soll.
- 6 Überprüfen Sie die OVF-Vorlagendetails und klicken Sie auf **Weiter**.
- 7 Geben Sie die Bereitstellungsconfigurationsgröße an und klicken Sie auf **Weiter**.  
Im Bereich „Beschreibung“ auf der rechten Seite des Assistenten werden die Details der ausgewählten Konfiguration angezeigt.
- 8 Geben Sie den Speicher für die Konfigurations- und Festplattendateien an.
  - a Wählen Sie das Format für die virtuelle Festplatte aus.
  - b Wählen Sie die VM-Speicherrichtlinie aus.
  - c Geben Sie den Datenspeicher zum Speichern der NSX Manager-Appliance-Dateien an.
  - d Klicken Sie auf **Weiter**.
- 9 Wählen Sie ein Zielnetzwerk für jedes Quellnetzwerk aus.
- 10 Wählen Sie die Portgruppe oder das Zielnetzwerk für NSX Manager aus.
- 11 Konfigurieren Sie IP-Zuteilungseinstellungen.
  - a Geben Sie für die IP-Zuteilung **Statisch – Manuell** an.
  - b Wählen Sie für das IP-Protokoll **IPv4** aus.
- 12 Klicken Sie auf **Weiter**.

Die folgenden Schritte befinden sich alle im Abschnitt „Vorlage anpassen“ des Assistenten zum Bereitstellen der OVF-Vorlage.

- 13** Geben Sie im Bereich „Anwendung“ die System-Root-, CLI-Administrator- und Überwachungskennwörter für NSX Manager ein. Die Anmeldeinformationen für **root** und **admin** sind Pflichtfelder.

Ihre Kennwörter müssen den Einschränkungen zur Kennwortkomplexität entsprechen.

- mindestens 12 Zeichen
- mindestens ein Kleinbuchstabe
- mindestens ein Großbuchstabe
- mindestens eine Zahl
- mindestens ein Sonderzeichen
- mindestens fünf unterschiedliche Zeichen
- Standard-Kennwortkomplexitätsregeln werden von den Argumenten des Linux PAM-Moduls erzwungen:
  - `retry=3`: die maximale Anzahl, wie oft ein neues Kennwort für dieses Argument eingegeben werden kann (maximal 3 mal), bevor eine Fehlermeldung zurückgegeben wird.
  - `minlen=12`: die zulässige Mindestgröße für das neue Kennwort. Zusätzlich zur Anzahl von Zeichen im neuen Kennwort erfolgt eine Gutschrift (+ 1 für die Länge) für jede Art von Zeichen (sonstige, großgeschrieben, kleingeschrieben und Ziffer).
  - `difok=0`: die minimale Anzahl von Bytes, die sich im neuen Kennwort unterscheiden müssen. Zeigt die Ähnlichkeit zwischen dem alten und dem neuen Kennwort an. Wenn `difok` der Wert 0 zugewiesen wird, müssen sich die Bytes des alten und des neuen Kennworts nicht unterscheiden. Eine genaue Übereinstimmung ist zulässig.
  - `lcredit=1`: die maximale Gutschrift für die Verwendung von Kleinbuchstaben im neuen Kennwort. Wenn Sie weniger als oder 1 Kleinbuchstaben haben, zählt jeder Buchstabe + 1, um den aktuellen `minlen`-Wert zu erfüllen.
  - `ucredit=1`: die maximale Gutschrift für die Verwendung von Großbuchstaben im neuen Kennwort. Wenn Sie weniger als oder 1 Großbuchstaben haben, zählt jeder Buchstabe + 1, um den aktuellen `minlen`-Wert zu erfüllen.
  - `dcredit=1`: die maximale Gutschrift für die Verwendung von Ziffern im neuen Kennwort. Wenn Sie weniger als oder 1 Ziffer haben, zählt jede Ziffer + 1, um den aktuellen `minlen`-Wert zu erfüllen.
  - `ocredit=1`: die maximale Gutschrift für die Verwendung von sonstigen Zeichen im neuen Kennwort. Wenn Sie weniger als oder 1 sonstiges Zeichen haben, zählt jedes Zeichen + 1, um den aktuellen `minlen`-Wert zu erfüllen.

- `enforce_for_root`: Das Kennwort ist für den Root-Benutzer festgelegt.

---

**Hinweis** Weitere Einzelheiten zum Linux-PAM-Modul zum Abgleichen des Kennworts mit den Wörtern aus dem Wörterbuch finden Sie auf der Hauptseite.

---

Vermeiden Sie zum Beispiel einfache und systematische Kennwörter wie **VMware123!123** oder **VMware12345**. Kennwörter, die den Komplexitätsstandards entsprechen, sind nicht einfach und systematisch, sondern bestehen aus einer Kombination von Buchstaben, Sonderzeichen und Zahlen wie **VMware123!45**, **VMware1!2345** oder **VMware@1az23x**.

- 14 Lassen Sie im Abschnitt „Optionale Parameter“ die Kennwortfelder leer. Dadurch wird verhindert, dass Kennwörter für VMC-Rollen von einem Benutzer, der Zugriff auf die vCenter Server hat, kompromittiert werden. Beim Bereitstellen von VMC für NSX-T Data Center wird dieses Feld intern verwendet, um Kennwörter für Cloud Admin- und Cloud Audit-Rollen zu konfigurieren.
- 15 Geben Sie im Abschnitt „Netzwerkressourcen“ den Hostnamen von NSX Manager ein.

---

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

---

- 16 Wählen Sie einen **Rollenamen** für die Appliance aus. Die Standardrolle lautet **NSX Manager**.
  - Um eine NSX Manager-Appliance zu installieren, wählen Sie die Rolle **NSX Manager** aus.
  - Um eine Cloud Service Manager (CSM)-Appliance für eine NSX Cloud-Bereitstellung zu installieren, wählen Sie die Rolle **nsx-cloud-service-manager** aus.

Einzelheiten dazu finden Sie unter [Übersicht über das Bereitstellen von NSX Cloud](#).

- 17 (Erforderliche Felder) Geben Sie das Standard-Gateway, das Verwaltungsnetzwerk IPv4 und die Verwaltungsnetzwerkmaske ein.

---

**Wichtig** Wenn Sie das Feld für das Verwaltungsnetzwerk IPv4 leer lassen, ohne eine statische IP-Adresse einzugeben, wird NSX Manager während der Bereitstellung der Appliance keine IP-Adresse zugewiesen. Sie können nicht auf NSX Manager zugreifen, wenn er aktiviert wird. Um dieses Problem zu umgehen, müssen Sie die NSX Manager-Appliance erneut bereitstellen.

---

- 18 Geben Sie im Abschnitt „DNS“ die DNS-Serverliste und die Domänensuchliste ein.
- 19 Geben Sie im Abschnitt „Dienstkonfiguration“ die NTP-Serverliste ein.
 

Optional können Sie den SSH-Dienst aktivieren und die SSH-Root-Anmeldung zulassen. (Nicht empfohlen.)
- 20 Stellen Sie sicher, dass die gesamte Spezifikation der benutzerdefinierten OVF-Vorlage korrekt ist, und klicken Sie auf **Beenden**, um die Installation zu starten.

Die Installation kann 7 bis 8 Minuten dauern.

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

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

- 22** Öffnen Sie über den vSphere Client die VM-Konsole, um den Startvorgang zu verfolgen.

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

- 24** Geben Sie den Befehl `get services` ein, um sicherzustellen, dass alle Standarddienste ausgeführt werden.

Die folgenden Dienste sind standardmäßig nicht erforderlich und werden nicht automatisch gestartet.

- `liagent`
- `migration-coordinator`: Dieser Dienst wird nur verwendet, wenn der Migrations-Koordinator ausgeführt wird. Ziehen Sie den *Handbuch zum Migrations-Koordinator von NSX-T Data Center* zurate, bevor Sie diesen Dienst starten.
- `snmp`: Informationen zum Starten von SNMP finden Sie unter *Simple Network Management Protocol* im *Administratorhandbuch für NSX-T Data Center*.
- `nsx-message-bus`: Dieser Dienst wird in NSX-T Data Center 3.0 nicht verwendet.

- 25** Stellen Sie sicher, dass Ihr NSX Manager- oder Globaler Manager-Knoten über die erforderliche Konnektivität verfügt.

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

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

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

## Nächste Schritte

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

## Installieren von NSX Manager unter ESXi mithilfe des OVF-Befehlszeilentools

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

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

### Voraussetzungen

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

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

- Planen Sie das IPv4-IP-Adressschema für NSX Manager.

### Verfahren

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

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

- Bei einem eigenständigen Host:
  - Windows-Beispiel:

```
C:\Program Files\VMware\VMware OVF Tool>ovftool \
--sourceType=OVA \
--name=nsx-manager \
--deploymentOption=medium \
--X:injectOvfEnv \
--X:logFile=<filepath>\nsxovftool.log \
--allowExtraConfig \
--datastore=<datastore name> \
--network=<network name> \
```

```

--acceptAllEulas \
--noSSLVerify \
--diskMode=thin \
--powerOn \
--prop:"nsx_role=NSX Manager" \
--prop:"nsx_ip_0=10.168.110.75" \
--prop:"nsx_netmask_0=255.255.255.0" \
--prop:"nsx_gateway_0=10.168.110.1" \
--prop:"nsx_dns1_0=10.168.110.10" \
--prop:"nsx_domain_0=corp.local" \
--prop:"nsx_ntp_0=10.168.110.10" \
--prop:"nsx_isSSHEnabled=<True|False>" \
--prop:"nsx_allowSSHRootLogin=<True|False>" \
--prop:"nsx_passwd_0=<password>" \
--prop:"nsx_cli_passwd_0=<password>" \
--prop:"nsx_cli_audit_passwd_0=<password>" \
--prop:"nsx_hostname=nsx-manager" \
<nsx-unified-appliance-release>.ova \
vi://root:<password>@10.168.110.51

```

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

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

**Hinweis** Im obigen Beispiel ist „--deploymentOption“ auf die Standardgröße „Mittel“ festgelegt. Weitere Informationen zu anderen unterstützten Größen finden Sie unter [Systemanforderungen für NSX Manager-VM und -Host-Transportknoten](#).

■ Linux-Beispiel:

```

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

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

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

```



```

mgresxhost01="192.168.110.113"

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

```

Das Ergebnis sollte etwa wie folgt aussehen:

```

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

```

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

```

C:\Users\Administrator\Downloads>ovftool
--name=nsx-manager \
--deploymentOption=medium \
--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=10.168.110.75" \
--prop:"nsx_netmask_0=255.255.255.0" \
--prop:"nsx_gateway_0=10.168.110.1" \
--prop:"nsx_dns1_0=10.168.110.10" \
--prop:"nsx_domain_0=corp.local" \
--prop:"nsx_ntp_0=10.168.110.10" \
--prop:"nsx_isSSHEnabled=<True|False>" \
--prop:"nsx_allowSSHRootLogin=<True|False>" \
--prop:"nsx_passwd_0=<password>" \
--prop:"nsx_cli_passwd_0=<password>" \
--prop:nsx_cli_audit_passwd_0=$mgrpasswd \
--prop:"nsx_hostname=nsx-manager" \
<nsx-unified-appliance-release>.ova \
vi://administrator@vsphere.local:<password>@10.168.110.24/?ip=10.168.110.51

```

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

**Hinweis** Im obigen Beispiel ist „--deploymentOption“ auf die Standardgröße „Mittel“ festgelegt. Weitere Informationen zu anderen unterstützten Größen finden Sie unter [Systemanforderungen für NSX Manager-VM und -Host-Transportknoten](#).

■ Linux-Beispiel:

```

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

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

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

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

```

```

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

```

Das Ergebnis sollte etwa wie folgt aussehen:

```

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

```

- 2 Sie können auch das OVF-Tool im Prüfmodus durchführen, um den Inhalt einer Quelle anzuzeigen. OVA- und OVF-Pakete können unter einer Liste mit anderen unterstützten Quelltypen angezeigt werden. Sie können die im Prüfmodus zurückgegebenen Informationen verwenden, um Bereitstellungen zu konfigurieren.

```
$> \ovftool --allowExtraConfig <OVA path or URL>
```

Wobei „--allowExtraConfig“ der unterstützte Appliance Typ für Cloud Service Manager (CSM) ist.

- 3 Reservieren Sie Arbeitsspeicher für die Appliance, um eine optimale Leistung zu erreichen.

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

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

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

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

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

#### Nächste Schritte

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

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

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

---

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

---

#### Verfahren

- 1 Melden Sie sich bei der VM als Root-Benutzer an.

- 2 Ändern Sie den Wert für den Parameter GRUB\_HIDDEN\_TIMEOUT in der Datei `/etc/default/grub`.

`GRUB_HIDDEN_TIMEOUT=2`

- 3 (Optional) Ändern Sie das GRUB-Kennwort in der Datei `/etc/grub.d/40_custom`.

Das Standardkennwort lautet `VMware1`.

- 4 Aktualisieren Sie die GRUB-Konfiguration.

`update-grub`

## Anmeldung beim neu erstellten NSX Manager

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

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

### Voraussetzungen

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

### Verfahren

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

## Hinzufügen eines Compute Managers

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

NSX-T Data Center fragt Compute Managers ab, um Clusterinformationen von vCenter Server zu erfassen.

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

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

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

### Voraussetzungen

- Stellen Sie sicher, dass Sie die unterstützte vSphere-Version verwenden. Siehe [Unterstützte vSphere-Version](#).
- IPv6- und IPv4-Kommunikation mit vCenter Server.

- Stellen Sie sicher, dass Sie die empfohlene Anzahl an Compute Managers verwenden. Siehe <https://configmax.vmware.com/home>.

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

## Verfahren

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

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

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

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

- 4 Wenn sich das Symbol „Fortschritt“ von **In Bearbeitung** in **Nicht registriert** ändert, führen Sie die folgenden Schritte aus, um den Fehler zu beheben.
  - a Wählen Sie die Fehlermeldung und klicken Sie auf **Beheben**. Eine mögliche Fehlermeldung lautet:

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

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

Wenn eine bestehende Registrierung vorhanden ist, wird sie ersetzt.

## Ergebnisse

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

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

Nachdem der vCenter Server erfolgreich registriert wurde, schalten Sie die NSX Manager-VM nicht aus und löschen Sie sie nicht, ohne zuerst den Compute Manager zu löschen. Andernfalls können Sie bei der Bereitstellung eines neuen NSX Managers nicht mehr denselben vCenter Server registrieren. Sie erhalten eine Fehlermeldung mit dem Hinweis, dass der vCenter Server bereits bei einem anderen NSX Manager registriert ist.

---

**Hinweis** Nachdem ein vCenter Server (VC)-Compute Manager erfolgreich hinzugefügt wurde, kann er nicht mehr entfernt werden, wenn Sie eine der folgenden Aktionen erfolgreich ausgeführt haben:

- Dienst-VMs werden auf einem Host oder einem Cluster im VC mit NSX Service Insertion bereitgestellt.
- Sie verwenden die NSX Manager-Benutzeroberfläche für die Bereitstellung von NSX Edges, NSX Intelligence-VMs oder NSX Manager-Knoten auf einem Host oder Cluster im VC.

Wenn Sie versuchen, eine dieser Aktionen auszuführen, und ein Fehler auftritt (wenn z. B. die Installation fehlschlägt), können Sie den VC entfernen, wenn Sie keine der oben aufgeführten Aktionen erfolgreich ausgeführt haben.

Sie können den VC auch entfernen, nachdem:

- Die Vorbereitung aller Transportknoten zurückgesetzt wurde.
- Die Bereitstellung aller Dienst-VMs, der NSX Intelligence-VM, aller NSX Edge-VMs und NSX Manager-Knoten aufgehoben wurde.

Diese Einschränkung gilt für eine Neuinstallation von NSX-T Data Center 2.5.x sowie für ein Upgrade.

---

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

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

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

---

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

---

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

### Voraussetzungen

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



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

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

## Verfahren

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

Option	Beschreibung
<b>Compute Manager</b>	Der registrierte Ressourcen-Compute Manager wird mit Daten befüllt.
<b>SSH aktivieren</b>	Schalten Sie die Schaltfläche um, um eine SSH-Anmeldung am neuen NSX Manager-Knoten zu ermöglichen.
<b>Root-Zugriff aktivieren</b>	Schalten Sie die Schaltfläche um, um den Root-Zugriff auf den neuen NSX Manager-Knoten zu ermöglichen.

Option	Beschreibung
<b>CLI-Benutzername und Kennwortbestätigung</b>	<p>Legen Sie das CLI-Kennwort und die Kennwortbestätigung für den neuen Knoten fest.</p> <p>Ihr Kennwort muss den Einschränkungen zur Kennwortkomplexität entsprechen.</p> <ul style="list-style-type: none"> <li>■ mindestens 12 Zeichen</li> <li>■ mindestens ein Kleinbuchstabe</li> <li>■ mindestens ein Großbuchstabe</li> <li>■ mindestens eine Zahl</li> <li>■ mindestens ein Sonderzeichen</li> <li>■ mindestens fünf unterschiedliche Zeichen</li> <li>■ Standard-Kennwortkomplexitätsregeln werden von den Argumenten des Linux PAM-Moduls erzwungen: <ul style="list-style-type: none"> <li>■ <code>retry=3</code>: die maximale Anzahl, wie oft ein neues Kennwort für dieses Argument eingegeben werden kann (maximal 3 mal), bevor eine Fehlermeldung zurückgegeben wird.</li> <li>■ <code>minlen=12</code>: die zulässige Mindestgröße für das neue Kennwort. Zusätzlich zur Anzahl von Zeichen im neuen Kennwort erfolgt eine Gutschrift (+ 1 für die Länge) für jede Art von Zeichen (sonstige, großgeschrieben, kleingeschrieben und Ziffer).</li> <li>■ <code>difok=0</code>: die minimale Anzahl von Bytes, die sich im neuen Kennwort unterscheiden müssen. Zeigt die Ähnlichkeit zwischen dem alten und dem neuen Kennwort an. Wenn <code>difok</code> der Wert 0 zugewiesen wird, müssen sich die Bytes des alten und des neuen Kennworts nicht unterscheiden. Eine genaue Übereinstimmung ist zulässig.</li> <li>■ <code>lcredit=1</code>: die maximale Gutschrift für die Verwendung von Kleinbuchstaben im neuen Kennwort. Wenn Sie weniger als oder 1 Kleinbuchstaben haben, zählt jeder Buchstabe + 1, um den aktuellen <code>minlen</code>-Wert zu erfüllen.</li> <li>■ <code>ucredit=1</code>: die maximale Gutschrift für die Verwendung von Großbuchstaben im neuen Kennwort. Wenn Sie weniger als oder 1 Großbuchstaben haben, zählt jeder Buchstabe + 1, um den aktuellen <code>minlen</code>-Wert zu erfüllen.</li> <li>■ <code>dcredit=1</code>: die maximale Gutschrift für die Verwendung von Ziffern im neuen Kennwort. Wenn Sie weniger als oder 1 Ziffer haben, zählt jede Ziffer + 1, um den aktuellen <code>minlen</code>-Wert zu erfüllen.</li> <li>■ <code>ocredit=1</code>: die maximale Gutschrift für die Verwendung von sonstigen Zeichen im neuen Kennwort. Wenn Sie weniger als oder 1 sonstiges Zeichen haben, zählt jedes Zeichen + 1, um den aktuellen <code>minlen</code>-Wert zu erfüllen.</li> </ul> </li> <li>■ <code>enforce_for_root</code>: Das Kennwort ist für den Root-Benutzer festgelegt.</li> </ul>

**Hinweis** Weitere Einzelheiten zum Linux-PAM-Modul zum Abgleichen des Kennworts mit den Wörtern aus dem Wörterbuch finden Sie auf der Hauptseite.

Vermeiden Sie zum Beispiel einfache und systematische Kennwörter wie **VMware123!123** oder **VMware12345**. Kennwörter, die den Komplexitätsstandards entsprechen, sind nicht einfach und systematisch, sondern bestehen aus einer Kombination von Buchstaben, Sonderzeichen und Zahlen wie **VMware123!45**, **VMware1!2345** oder **VMware@1az23x**.

Option	Beschreibung
	Der CLI-Benutzername ist bereits auf Admin festgelegt.

Option	Beschreibung
<b>Root-Kennwort und Kennwortbestätigung</b>	<p>Legen Sie das Root-Kennwort und die Kennwortbestätigung für den neuen Knoten fest.</p> <p>Ihr Kennwort muss den Einschränkungen zur Kennwortkomplexität entsprechen.</p> <ul style="list-style-type: none"> <li>■ mindestens 12 Zeichen</li> <li>■ mindestens ein Kleinbuchstabe</li> <li>■ mindestens ein Großbuchstabe</li> <li>■ mindestens eine Zahl</li> <li>■ mindestens ein Sonderzeichen</li> <li>■ mindestens fünf unterschiedliche Zeichen</li> <li>■ Standard-Kennwortkomplexitätsregeln werden von den Argumenten des Linux PAM-Moduls erzwungen: <ul style="list-style-type: none"> <li>■ <code>retry=3</code>: die maximale Anzahl, wie oft ein neues Kennwort für dieses Argument eingegeben werden kann (maximal 3 mal), bevor eine Fehlermeldung zurückgegeben wird.</li> <li>■ <code>minlen=12</code>: die zulässige Mindestgröße für das neue Kennwort. Zusätzlich zur Anzahl von Zeichen im neuen Kennwort erfolgt eine Gutschrift (+ 1 für die Länge) für jede Art von Zeichen (sonstige, großgeschrieben, kleingeschrieben und Ziffer).</li> <li>■ <code>difok=0</code>: die minimale Anzahl von Bytes, die sich im neuen Kennwort unterscheiden müssen. Zeigt die Ähnlichkeit zwischen dem alten und dem neuen Kennwort an. Wenn <code>difok</code> der Wert 0 zugewiesen wird, müssen sich die Bytes des alten und des neuen Kennworts nicht unterscheiden. Eine genaue Übereinstimmung ist zulässig.</li> <li>■ <code>lcredit=1</code>: die maximale Gutschrift für die Verwendung von Kleinbuchstaben im neuen Kennwort. Wenn Sie weniger als oder 1 Kleinbuchstaben haben, zählt jeder Buchstabe + 1, um den aktuellen <code>minlen</code>-Wert zu erfüllen.</li> <li>■ <code>ucredit=1</code>: die maximale Gutschrift für die Verwendung von Großbuchstaben im neuen Kennwort. Wenn Sie weniger als oder 1 Großbuchstaben haben, zählt jeder Buchstabe + 1, um den aktuellen <code>minlen</code>-Wert zu erfüllen.</li> <li>■ <code>dcredit=1</code>: die maximale Gutschrift für die Verwendung von Ziffern im neuen Kennwort. Wenn Sie weniger als oder 1 Ziffer haben, zählt jede Ziffer + 1, um den aktuellen <code>minlen</code>-Wert zu erfüllen.</li> <li>■ <code>ocredit=1</code>: die maximale Gutschrift für die Verwendung von sonstigen Zeichen im neuen Kennwort. Wenn Sie weniger als oder 1 sonstiges Zeichen haben, zählt jedes Zeichen + 1, um den aktuellen <code>minlen</code>-Wert zu erfüllen.</li> </ul> </li> <li>■ <code>enforce_for_root</code>: Das Kennwort ist für den Root-Benutzer festgelegt.</li> </ul> <p><b>Hinweis</b> Weitere Einzelheiten zum Linux-PAM-Modul zum Abgleichen des Kennworts mit den Wörtern aus dem Wörterbuch finden Sie auf der Hauptseite.</p> <p>Vermeiden Sie zum Beispiel einfache und systematische Kennwörter wie <b>VMware123!123</b> oder <b>VMware12345</b>. Kennwörter, die den Komplexitätsstandards entsprechen, sind nicht einfach und systematisch, sondern bestehen aus einer Kombination von Buchstaben, Sonderzeichen und Zahlen wie <b>VMware123!45</b>, <b>VMware1!2345</b> oder <b>VMware@1az23x</b>.</p>

Option	Beschreibung
<b>DNS-Server</b>	Geben Sie die IP-Adresse des DNS-Servers ein, der im vCenter Server verfügbar ist.
<b>NTP-Server</b>	Geben Sie die IP-Adresse des NTP-Servers ein.

**4** Geben Sie die Knotendetails zu NSX Manager ein.

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

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

Wiederholen Sie die Schritte 3 bis 4.

**6** Klicken Sie auf **Fertigstellen**.

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

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

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

**Hinweis** Wenn der erste Knoten während der Bereitstellung eines neuen Knotens neu gestartet wird, kann der neue Knoten möglicherweise nicht beim Cluster registriert werden und die Meldung **Registrieren fehlgeschlagen** wird auf der Miniaturansicht des neuen Knotens angezeigt. Wenn Sie den Knoten im Cluster manuell erneut bereitstellen möchten, navigieren Sie zur Miniaturansicht des neuen Knotens, wählen Sie die vertikalen Ellipsen aus und klicken Sie auf **Wiederholen**.

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

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

Die folgenden Dienste sind standardmäßig nicht erforderlich und werden nicht automatisch gestartet.

- `liagent`
- `migration-coordinator`: Dieser Dienst wird nur verwendet, wenn der Migrations-Koordinator ausgeführt wird. Ziehen Sie den *Handbuch zum Migrations-Koordinator von NSX-T Data Center* zurate, bevor Sie diesen Dienst starten.
- `snmp`: Informationen zum Starten von SNMP finden Sie unter *Simple Network Management Protocol* im *Administratorhandbuch für NSX-T Data Center*.
- `nsx-message-bus`: Dieser Dienst wird in NSX-T Data Center 3.0 nicht verwendet.

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

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

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

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

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

### Nächste Schritte

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

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

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

### Voraussetzungen

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

## Verfahren

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

---

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

---

Geben Sie die folgenden NSX Manager-Informationen an:

- Hostname oder IP-Adressenknoten, dem Sie beitreten möchten
- Cluster-ID
- Benutzername
- Kennwort
- Certificate Thumbprint

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

- CLI-Befehl

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

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

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

- 6 Fügen Sie den dritten NSX Manager-Knoten zum Cluster hinzu.  
Wiederholen Sie Schritt 5.
- 7 Überprüfen Sie den Cluster-Status, indem Sie den Befehl `get cluster status` auf Ihren Hosts ausführen.
- 8 (NSX Manager-Benutzeroberfläche) Wählen Sie **System > Appliances > Übersicht** und überprüfen Sie die Cluster-Konnektivität.

## Nächste Schritte

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

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

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

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

---

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

---

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

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

---

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

---

### Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wechseln Sie zu **System > Übersicht**.
- 3 Klicken Sie im Feld „Virtuelle IP“ auf **Bearbeiten**.
- 4 Geben Sie die VIP für den Cluster ein. Stellen Sie sicher, dass die VIP Teil desselben Subnetzes wie die anderen Verwaltungsknoten ist.
- 5 Klicken Sie auf **Speichern**.



- Um den Clusterstatus und den API-Führer der HTTPS-Gruppe zu überprüfen, geben Sie den NSX Manager-CLI-Befehl `get cluster status verbose` in die NSX Manager-Konsole oder über SSH ein.

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

Group Type: HTTPS		
Group Status: STABLE		
Members:		
UUID	FQDN	IP
STATUS		
<b>cdb93642-ccba-fdf4-8819-90bf018cd727</b>	nsx-manager	192.196.197.84
UP		
51a13642-929b-8dfc-3455-109e6cc2a7ae	nsx-manager	192.196.198.156
UP		
d0de3642-d03f-c909-9cca-312fd22e486b	nsx-manager	192.196.198.54
UP		
Leaders:		
SERVICE	LEADER	LEASE
VERSION		
api	<b>cdb93642-ccba-fdf4-8819-90bf018cd727</b>	8

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

## Ergebnisse

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

## Deaktivieren von Snapshots auf NSX-T-Appliances

Als VMs können NSX Manager und NSX Edge so konfiguriert werden, dass ihre Snapshots erstellt und gespeichert werden. Klone und Snapshots von NSX-T-Appliances werden jedoch nicht unterstützt und können zu funktionellen und sonstigen Problemen führen. Aus diesem Grund wird dringend empfohlen, Snapshots von NSX-T-Appliance-VMs zu deaktivieren.

Führen Sie für jede NSX-T-Appliance-VM das folgende Verfahren aus.

### Verfahren

- Ermitteln Sie die Appliance-VMs im vSphere Client.
- Schalten Sie die VM aus.
- Klicken Sie mit der rechten Maustaste auf die VM und wählen Sie **Einstellungen bearbeiten** aus.
- Klicken Sie auf die Registerkarte **VM-Optionen** und erweitern Sie dann **Erweitert**.

- 5 Klicken Sie im Feld **Konfigurationsparameter** auf **Konfiguration bearbeiten...**
- 6 Klicken Sie im Fenster **Konfigurationsparameter** auf **Konfigurationsparameter hinzufügen**.
- 7 Geben Sie Folgendes ein:
  - Geben Sie als Namen **snapshot.MaxSnapshots** ein.
  - Geben Sie als Wert **-0** ein.
- 8 Klicken Sie auf **OK**, um die Änderungen zu speichern.
- 9 Schalten Sie die VM wieder ein.

# Installieren von NSX-T Data Center auf KVM

# 6

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

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

Dieses Kapitel enthält die folgenden Themen:

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

## Einrichten von KVM

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

---

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

---

### Verfahren

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

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

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

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

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

Zu den unterstützten RHEL-Versionen gehören 7.4 und 7.5.

- 4 Installieren Sie KVM und Bridge-Dienstprogramme.

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

- 5 Damit NSX Manager NSX-Softwarepakete automatisch auf dem KVM-Host installiert, bereiten Sie die Netzwerkkonfiguration der Uplink-/Datenschnittstelle vor.

Der KVM-Host kann über mehrere Netzwerkschnittstellen verfügen. Für die Netzwerkschnittstelle, die Sie als Uplink-Schnittstelle (Datenschnittstelle) für NSX-T-Zwecke bereitstellen möchten, ist es wichtig, dass die Netzwerkkonfigurationsdateien ordnungsgemäß gefüllt sind. NSX-T untersucht diese Netzwerkkonfigurationsdateien, um NSX-T-spezifische Netzwerkgeräte zu erstellen. Füllen Sie in Ubuntu die Datei `/etc/network/interfaces`. Füllen Sie in RHEL, CentOS oder SUSE die Datei `/etc/sysconfig/network-scripts/ifcfg-$uplinkdevice`.

In den folgenden Beispielen ist die Schnittstelle „ens32“ das Uplink-Gerät (Datenschnittstelle). Je nach Bereitstellungsumgebung kann diese Schnittstelle DHCP oder statische IP-Einstellungen verwenden.

---

**Hinweis** Schnittstellennamen können in verschiedenen Umgebungen variieren.

---

**Wichtig** Bei Ubuntu müssen alle Netzwerkkonfigurationen in `/etc/network/interfaces` angegeben werden. Erstellen Sie keine individuellen Netzwerkkonfigurationsdateien wie `/etc/network/ifcfg-eth1`, die ein Fehlschlagen der Transportknotenerstellung verursachen können.

---

Linux-Bereitstellung	Netzwerkkonfiguration
Ubuntu	<p>Bearbeiten Sie <code>/etc/network/interfaces</code>:</p> <pre> auto eth0 iface eth0 inet manual  auto ens32 iface ens32 inet manual </pre>
RHEL oder CentOS Linux	<p>Bearbeiten Sie <code>/etc/sysconfig/network-scripts/ifcfg-ens32</code>:</p> <pre> DEVICE="ens32" TYPE="Ethernet" NAME="ens32" UUID="&lt;something&gt;" BOOTPROTO="none" HWADDR="&lt;something&gt;" ONBOOT="yes" NM_CONTROLLED="no" </pre>
SUSE Linux Enterprise Server	<p>Wenn bereits ein SLES-Host vorhanden ist, stellen Sie sicher, dass die Datenschnittstellen bereits auf dem Host konfiguriert sind.</p> <p>Wenn Sie über keinen vorkonfigurierten SLES-Host verfügen, finden Sie weitere Informationen in der Referenzkonfiguration für die Verwaltungs- und Datenschnittstelle.</p> <p>Bearbeiten Sie <code>./etc/sysconfig/network-scripts/ifcfg-ens32</code>:</p> <pre> DEVICE="ens32" NAME="ens32" UUID="&lt;UUID&gt;" BOOTPROTO="none" LLADDR="&lt;HWADDR&gt;" STARTMODE="yes" </pre>

- 6 Starten Sie den Netzwerkdienst `systemctl restart network` oder den Linux-Server neu, damit die Netzwerkänderungen wirksam werden.
- 7 Nachdem der KVM-Host als Transportknoten konfiguriert wurde, wird die Bridge-Schnittstelle `nsx-vtep0.0` automatisch von NSX-T erstellt.

In Ubuntu enthält die Datei `/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) die Konfigurationsdatei `ifcfg-nsx-vtep0.0`, die in etwa folgende Einträge enthält:

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

In SUSE

```
DEVICE=nsx-vtep0.0
BOOTPROTO=static
NETMASK=255.255.255.0
IPADDR=192.168.13.119
MACADDR=ae:9d:b7:ca:20:4a
MTU=1600
USERCTL=no
STARTMODE=auto
```

- 8 Konfigurieren Sie die Syslog-Rotationsrichtlinie als zeitbasiert anstelle einer größenbasierten Richtlinie. Bei einer größenbasierten Syslog-Rotationsrichtlinie können die generierten Protokolldateien sehr groß sein.

## Verwalten der Gast-VMs in der KVM-CLI

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

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

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

```
# List running
virsh list

# List all
virsh list --all

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

```
virsh resume <instance>

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

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

```
ifconfig
...

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

## Installieren von NSX Manager auf KVM

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

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

### Voraussetzungen

- KVM-Einrichtung Siehe [Einrichten von KVM](#).
- Rechte zum Bereitstellen eines QCOW2-Images auf dem KVM-Host
- Vergewissern Sie sich, dass das Kennwort in der `guestinfo`-Datei die Anforderungen bezüglich der Kennwortkomplexität erfüllt, sodass Sie sich nach der Installation anmelden können. Siehe [Kapitel 4 NSX Manager-Installation](#).
- Machen Sie sich mit den NSX Manager-Ressourcenanforderungen vertraut. Siehe [Systemanforderungen für NSX Manager-VM und -Host-Transportknoten](#).
- Wenn Sie Ubuntu OS installieren möchten, wird empfohlen, vor der Installation von NSX Manager Ubuntu-Version 18.04 auf dem KVM-Host zu installieren.

### Verfahren

- 1 Laden Sie das NSX Manager-QCOW2-Image aus dem Ordner **nsx-unified-appliance > exports > kvm** herunter.
- 2 Kopieren Sie das Image auf die KVM-Maschine, die den NSX Manager mithilfe von SCP oder Synchronisierung ausführt.

- 3** (Nur Ubuntu) Fügen Sie den derzeit angemeldeten Benutzer als libvirtd-Benutzer hinzu:

```
adduser $USER libvirtd
```



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

Eigenschaft	Beschreibung
<ul style="list-style-type: none"> <li>■ <b>nsx_cli_passwd_0</b></li> <li>■ <b>nsx_cli_audit_passwd_0</b></li> <li>■ <b>nsx_passwd_0</b></li> </ul>	<p>Ihre Kennwörter müssen den Einschränkungen zur Kennwortkomplexität entsprechen.</p> <ul style="list-style-type: none"> <li>■ mindestens 12 Zeichen</li> <li>■ mindestens ein Kleinbuchstabe</li> <li>■ mindestens ein Großbuchstabe</li> <li>■ mindestens eine Zahl</li> <li>■ mindestens ein Sonderzeichen</li> <li>■ mindestens fünf unterschiedliche Zeichen</li> <li>■ Standard-Kennwortkomplexitätsregeln werden von den Argumenten des Linux PAM-Moduls erzwungen: <ul style="list-style-type: none"> <li>■ <b>retry=3</b>: die maximale Anzahl, wie oft ein neues Kennwort für dieses Argument eingegeben werden kann (maximal 3 mal), bevor eine Fehlermeldung zurückgegeben wird.</li> <li>■ <b>minlen=12</b>: die zulässige Mindestgröße für das neue Kennwort. Zusätzlich zur Anzahl von Zeichen im neuen Kennwort erfolgt eine Gutschrift (+ 1 für die Länge) für jede Art von Zeichen (sonstige, großgeschrieben, kleingeschrieben und Ziffer).</li> <li>■ <b>difok=0</b>: die minimale Anzahl von Bytes, die sich im neuen Kennwort unterscheiden müssen. Zeigt die Ähnlichkeit zwischen dem alten und dem neuen Kennwort an. Wenn <b>difok</b> der Wert 0 zugewiesen wird, müssen sich die Bytes des alten und des neuen Kennworts nicht unterscheiden. Eine genaue Übereinstimmung ist zulässig.</li> <li>■ <b>lcredit=1</b>: die maximale Gutschrift für die Verwendung von Kleinbuchstaben im neuen Kennwort. Wenn Sie weniger als oder 1 Kleinbuchstaben haben, zählt jeder Buchstabe + 1, um den aktuellen <b>minlen</b>-Wert zu erfüllen.</li> <li>■ <b>ucredit=1</b>: die maximale Gutschrift für die Verwendung von Großbuchstaben im neuen Kennwort. Wenn Sie weniger als oder 1 Großbuchstaben haben, zählt jeder Buchstabe + 1, um den aktuellen <b>minlen</b>-Wert zu erfüllen.</li> <li>■ <b>dcredit=1</b>: die maximale Gutschrift für die Verwendung von Ziffern im neuen Kennwort. Wenn Sie weniger als oder 1 Ziffer haben, zählt jede Ziffer + 1, um den aktuellen <b>minlen</b>-Wert zu erfüllen.</li> <li>■ <b>ocredit=1</b>: die maximale Gutschrift für die Verwendung von sonstigen Zeichen im neuen Kennwort. Wenn Sie weniger als oder 1 sonstiges Zeichen haben, zählt jedes Zeichen + 1, um den aktuellen <b>minlen</b>-Wert zu erfüllen.</li> <li>■ <b>enforce_for_root</b>: Das Kennwort ist für den Root-Benutzer festgelegt.</li> </ul> </li> </ul> <p><b>Hinweis</b> Weitere Einzelheiten zum Linux-PAM-Modul zum Abgleichen des Kennworts mit den Wörtern aus dem Wörterbuch finden Sie auf der Hauptseite.</p>

Eigenschaft	Beschreibung
	Vermeiden Sie zum Beispiel einfache und systematische Kennwörter wie <b>VMware123!123</b> oder <b>VMware12345</b> . Kennwörter, die den Komplexitätsstandards entsprechen, sind nicht einfach und systematisch, sondern bestehen aus einer Kombination von Buchstaben, Sonderzeichen und Zahlen wie <b>VMware123!45</b> , <b>VMware1!2345</b> oder <b>VMware@1az23x</b> .
<b>nsx_hostname</b>	Geben Sie den Hostnamen für den NSX Manager ein. Der Hostname muss ein gültiger Domänenname sein. Stellen Sie sicher, dass jeder Teil des Hostnamens (Domäne/Unterdomäne), der per Punkt getrennt ist, mit einem alphabetischen Zeichen beginnen muss.
<b>nsx_role</b>	<ul style="list-style-type: none"> <li>■ <i>nsx-manager</i>: Erforderlich. Mit diesem Rollennamen wird die NSX Manager-Appliance installiert.</li> <li>■ <i>nsx-cloud-service-manager</i>: Optional. Verwenden Sie nach Installation von NSX Manager diesen Rollennamen, um die Cloud Service Manager-Appliance für NSX Cloud zu installieren.</li> </ul>
<b>nsx_isSSEnabled</b>	Sie können die Eigenschaft aktivieren oder deaktivieren. Wenn diese Option aktiviert ist, können Sie sich mithilfe von SSH beim NSX Manager anmelden.
<b>nsx_allowSSHRootLogin</b>	Sie können die Eigenschaft aktivieren oder deaktivieren. Wenn diese Option aktiviert ist, können Sie sich mithilfe von SSH als root-Benutzer beim NSX Manager anmelden. Um diese Eigenschaft verwenden zu können, muss <b>nsx_isSSEnabled</b> aktiviert sein.
<ul style="list-style-type: none"> <li>■ <b>nsx_dns1_0</b></li> <li>■ <b>nsx_ntp_0</b></li> <li>■ <b>nsx_domain_0</b></li> <li>■ <b>nsx_gateway_0</b></li> <li>■ <b>nsx_netmask_0</b></li> <li>■ <b>nsx_ip_0</b></li> </ul>	Geben Sie die IP-Adresse des Standard-Gateways, die IPv4-Adresse und Netzmaske des Verwaltungsnetzwerks, die DNS- und NTP-IP-Adresse ein.

Beispiel:

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

```
<Property oe:key="nsx_ip_0" oe:value="10.168.110.19"/>
</PropertySection>
</Environment>
```

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

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

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

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

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

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

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

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

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

```
virsh list --all
```

Id	Name	State
18	nsx-manager1	running

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

```
virsh console 18
Connected to domain nsx-manager1
```

```
Escape character is ^]
```

```
nsx-manager1 login: admin
Password:
```

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

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

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

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

- 12 Verlassen Sie die KVM-Konsole.

```
control-]
```

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

## Anmeldung beim neu erstellten NSX Manager

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

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

### Voraussetzungen

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

## Verfahren

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

## Installieren von Drittanbieterpaketen auf einem KVM-Host

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

### Voraussetzungen

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

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

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

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

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

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

```
libcap-progs
```

## Verfahren

- ◆ Führen Sie unter 18.04.2 LTS den Befehl `apt-get install <package_name>` aus, um die folgenden Drittanbieterpakete manuell zu installieren.

```
traceroute
python-mako
python-simplejson
python-unittest2
python-yaml
python-netaddr
dkms
libc6-dev
libelf-dev
```

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

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

### RHEL 7.6, 7.5 und 7.4    CentOS Linux 7.5 und 7.4

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

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

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

### SUSE Linux Enterprise Server 12.0

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

## Überprüfung der Open vSwitch-Version auf RHEL KVM-Hosts

Überspringen Sie dieses Thema, wenn keine OVS-Pakete auf dem RHEL-Host vorhanden sind. Wenn OVS-Pakete bereits auf einem RHEL-Host vorhanden sind, müssen Sie entweder die vorhandenen OVS-Pakete entfernen und die von NSX-T unterstützten OVS-Pakete installieren oder die vorhandenen OVS-Pakete auf von NSX-T unterstützte Pakete aktualisieren.

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
```

---

**Wichtig** Wenn für die vorhandenen Open vSwitch-Pakete die neueste oder eine frühere Version ausgeführt wird, müssen Sie die vorhandenen Open vSwitch-Pakete durch die unterstützte Version ersetzen.

---

- 2 Löschen Sie die folgenden Open vSwitch-Pakete.

- kmod-openvswitch oder openvswitch-kmod
- openvswitch
- openvswitch-selinux-policy

- 3 Aktualisieren Sie alternativ die für NSX-T Data Center erforderlichen 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>-rhel75_x86_64.tar.gz
```

- d Gehen Sie zum Paketverzeichnis.

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

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

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

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

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

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

## Überprüfen der Open vSwitch-Version auf SUSE KVM-Hosts

Überspringen Sie dieses Thema, wenn keine OVS-Pakete auf dem SUSE-Host vorhanden sind. Wenn OVS-Pakete auf einem SUSE-Host vorhanden sind, müssen Sie entweder die vorhandenen OVS-Pakete entfernen und die von NSX-T unterstützten OVS-Pakete installieren oder die vorhandenen OVS-Pakete auf von NSX-T unterstützte Pakete aktualisieren.

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-vsitchd --version
```

---

**Wichtig** Wenn für die vorhandenen Open vSwitch-Pakete die neueste oder eine frühere Version ausgeführt wird, müssen Sie die vorhandenen Open vSwitch-Pakete durch die unterstützte Version ersetzen.

---

- 2 Löschen Sie die folgenden Open vSwitch-Pakete.

- kmod-openvswitch oder openvswitch-kmod
- openvswitch
- openvswitch-selinux-policy

- 3 Aktualisieren Sie alternativ die für NSX-T Data Center erforderlichen 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.

```
nsx-lcp-3.0.0.0.14335404-linux64-sles12sp3.tar.gz
```

- d Gehen Sie zum Paketverzeichnis.

```
nsx-lcp-linux64-sles12sp3/
```

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

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

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

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

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

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

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

**Voraussetzungen**

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

**Verfahren**

- 1 Öffnen Sie eine SSH-Sitzung für den ersten bereitgestellten NSX Manager-Knoten.
- 2 Melden Sie sich mit den Anmeldedaten des Administrators an.



- 3 Führen Sie auf dem NSX Manager-Knoten den Befehl `get certificate api thumbprint` aus.  
Die Befehlsausgabe besteht aus einer Reihe von Zahlen, die für diesen NSX Manager eindeutig sind.
- 4 Führen Sie den Befehl `get cluster config` aus, um die Kennung des ersten bereitgestellten NSX Manager-Clusters zu erhalten.
- 5 Fügen Sie den NSX Manager-Knoten zum Cluster hinzu.

---

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

---

Geben Sie die folgenden NSX Manager-Informationen an:

- Hostname oder IP-Adressenknoten, dem Sie beitreten möchten
- Cluster-ID
- Benutzername
- Kennwort
- Certificate Thumbprint

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

- CLI-Befehl

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

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

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

- 6 Fügen Sie den dritten NSX Manager-Knoten zum Cluster hinzu.  
Wiederholen Sie Schritt 5.
- 7 Überprüfen Sie den Cluster-Status, indem Sie den Befehl `get cluster status` auf Ihren Hosts ausführen.
- 8 (NSX Manager-Benutzeroberfläche) Wählen Sie **System > Appliances > Übersicht** und überprüfen Sie die Cluster-Konnektivität.

#### Nächste Schritte

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

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

# 7

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

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

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

---

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

---

Dieses Kapitel enthält die folgenden Themen:

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

## Installieren von Drittanbieterpaketen auf einem Bare-Metal-Server

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

### Voraussetzungen

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

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

## Verfahren

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

Ubuntu 18.04.2	Ubuntu 16.04
traceroute python-mako python-netaddr python-simplejson python-unittest2 python-yaml python-openssl dkms libvirt0 libelf-dev	libunwind8 libgflags2v5 libgoogle-perftools4 traceroute python-mako python-simplejson python-unittest2 python-yaml python-netaddr python-openssl libboost-filesystem1.58.0 libboost-chrono1.58.0 libgoogle-glog0v5 dkms libboost-date-time1.58.0 python-protobuf python-gevent libsnappy1v5 libleveldb1v5 libboost-program-options1.58.0 libboost-thread1.58.0 libboost-iostreams1.58.0 libvirt0 libelf-dev

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

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

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

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

## Erstellen der Anwendungsschnittstelle für Bare-Metal Server-Arbeitslasten

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

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

#### Verfahren

- 1 Installieren Sie die erforderlichen Drittanbieterpakete.

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

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

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

- 3 Fügen Sie einen Bare-Metal-Server zum NSX-T Data Center-Fabric hinzu und erstellen Sie einen Transportknoten.

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

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

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

# NSX Manager-Clusteranforderungen

# 8

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

Dieses Kapitel enthält die folgenden Themen:

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

## NSX Manager-Clusteranforderungen für eine, zwei und mehrere Sites

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

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

---

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

---

## Clusteranforderungen

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

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

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

---

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

---

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

## Anforderungen und Empfehlungen für einzelne Sites

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

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

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

Beispielszenario:

- Ein vSphere-Cluster, in dem alle drei NSX Manager bereitgestellt sind.
- Der vSphere-Cluster besteht aus vier oder mehr Hosts.
  - Host-01 mit bereitgestelltem nsxmgr-01
  - Host-02 mit bereitgestelltem nsxmgr-02
  - Host-03 mit bereitgestelltem nsxmgr-03

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

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

## Anforderungen und Empfehlungen für zwei Sites

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

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

Beispielszenario:

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

Site A:

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

Site B:

- Host-04 ohne Bereitstellung von NSX Manager
- Host-05 ohne Bereitstellung von NSX Manager
- Host-06 ohne Bereitstellung von NSX Manager
- vSphere HA ist so konfiguriert, dass alle verlorenen NSX Manager (z. B. nsxmgr-01) von allen Hosts (z. B. Host-01) in Site A auf einen der Hosts in Site B wiederhergestellt werden.



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

---

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

---

## Anforderungen und Empfehlungen für mehrere (drei oder mehr) Sites

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

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

Wenn Sie ohne vSphere HA bereitstellen:

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

Beispielsszenario (drei Sites):

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

Fehlerszenarien:

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

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

# Installieren von NSX Edge

# 9

Installieren Sie NSX Edge unter ESXi mithilfe der NSX-T-Benutzeroberfläche, des vSphere-Webclients oder des Befehlszeilen-OVF-Tools.

Dieses Kapitel enthält die folgenden Themen:

- [NSX Edge-Installationsanforderungen](#)
- [NSX Edge-Netzwerkeinrichtung](#)
- [NSX Edge-Installationsmethoden](#)
- [Erstellen eines NSX Edge-Transportknotens](#)
- [Erstellen eines NSX Edge-Clusters](#)
- [Installieren von NSX Edge unter ESXi mithilfe der grafischen vSphere-Benutzeroberfläche](#)
- [Bare-Metal-Installation von NSX Edge](#)
- [Verbinden von NSX Edge mit der Management Plane](#)
- [Konfigurieren von NSX Edge als Transportknoten](#)

## NSX Edge-Installationsanforderungen

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

---

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

---

Tabelle 9-1. Anforderung an die NSX Edge-Bereitstellung, -Plattformen und -Installation

Anforderungen	Beschreibung
Unterstützte Bereitstellungsmethoden	<ul style="list-style-type: none"> <li>■ OVA/OVF</li> <li>■ ISO mit PXE</li> <li>■ ISO ohne PXE</li> </ul>
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"> <li>■ mindestens 12 Zeichen</li> <li>■ mindestens ein Kleinbuchstabe</li> <li>■ mindestens ein Großbuchstabe</li> <li>■ mindestens eine Zahl</li> <li>■ mindestens ein Sonderzeichen</li> <li>■ mindestens fünf unterschiedliche Zeichen</li> <li>■ keine Wörterbuchwörter</li> <li>■ keine Palindrome</li> <li>■ mehr als vier monotone Zeichenfolgen ist nicht zulässig</li> </ul>
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 <b>localhost</b> festgelegt. Weitere Informationen zu Hostnamenbeschränkungen finden Sie unter <a href="https://tools.ietf.org/html/rfc952">https://tools.ietf.org/html/rfc952</a> und <a href="https://tools.ietf.org/html/rfc1123">https://tools.ietf.org/html/rfc1123</a> .
VMware Tools	Auf der unter ESXi ausgeführten NSX Edge-VM sind VMware Tools installiert. Entfernen oder aktualisieren Sie VMTools nicht.
System	Stellen Sie sicher, dass die Systemanforderungen erfüllt sind. Siehe <a href="#">Systemanforderungen für NSX Edge-VM</a> .
Ports	Stellen Sie sicher, dass die erforderlichen Ports geöffnet sind. Siehe <a href="#">Ports und Protokolle</a> .
IP-Adressen	<p>Wenn Sie über mehrere Verwaltungsnetzwerke verfügen, können Sie statische Routen von der NSX-T Data Center-Appliance zu den anderen Netzwerken hinzufügen.</p> <p>Planen Sie Ihr IPv4- oder IPv6-IP-Adressschema für NSX Edge.</p>

**Tabelle 9-1. Anforderung an die NSX Edge-Bereitstellung, -Plattformen und -Installation (Fortsetzung)**

Anforderungen	Beschreibung
OVF-Vorlage	<ul style="list-style-type: none"> <li>■ Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Bereitstellen einer OVF-Vorlage auf dem ESXi-Host verfügen.</li> <li>■ Stellen Sie sicher, dass Hostnamen keine Unterstriche enthalten. Andernfalls wird der Hostname auf <i>localhost</i> gesetzt.</li> <li>■ Ein Managementtool, das OVF-Vorlagen wie vCenter Server oder den vSphere-Client bereitstellen kann.</li> </ul> <p>Das OVF-Bereitstellungstool muss Konfigurationsoptionen für eine manuelle Konfiguration unterstützen.</p> <ul style="list-style-type: none"> <li>■ Das Client-Integrations-Plug-In muss installiert sein.</li> </ul>
NTP-Server	Auf allen NSX Edge-VMs bzw. Bare Metal-Edges in einem Edge-Cluster muss derselbe NTP-Server konfiguriert sein.

## Intel-basierte Chipsätze

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.

## NSX Edge-Unterstützung von vSphere-Geschäftskontinuitätsfunktionen

Ab NSX-T Data Center 2.5.1 werden vMotion, DRS und vSphere HA für NSX Edge-Knoten unterstützt.

## 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.

---

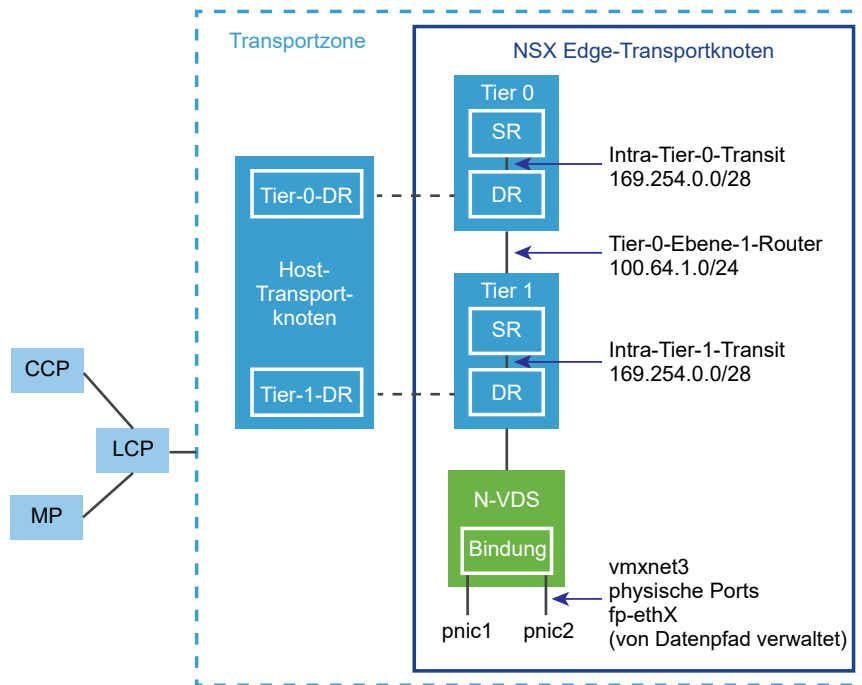
## NSX Edge-Netzwerkeinrichtung

NSX Edge kann über ISO, OVA/OVF oder PXE-Start installiert werden. Stellen Sie unabhängig von der Installationsmethode sicher, dass das Hostnetzwerk vor der Installation von NSX Edge vorbereitet ist.

## Übersicht über NSX Edge in einer Transportzone

Die Übersicht über NSX-T Data Center zeigt zwei Transportknoten in einer Transportzone. Ein Transportknoten ist ein Host. Der andere ist ein NSX Edge.

Abbildung 9-1. Übersicht über NSX Edge



Beim ersten Bereitstellen eines NSX Edge können Sie ihn sich als leeren Container vorstellen. Der NSX Edge führt erst dann Aktionen aus, wenn Sie logische Router erstellen. NSX Edge liefert die Rechenleistung für logische Tier-0 und Tier-1 Router. Jeder logische Router enthält einen Dienstrouter (Service Router; SR) und einen verteilten Router (Distributed Router; DR). Ein Router wird als verteilt bezeichnet, wenn er auf allen Transportknoten in derselben Transportzone repliziert wird. In dieser Abbildung enthält der Hosttransportknoten dieselben DRs, die auch in den Ebene-0- und Ebene-1-Routern enthalten sind. Ein Dienstrouter ist erforderlich, wenn der logische Router für die Ausführung von Diensten wie NAT konfiguriert wird. Alle logischen Tier-0 Router weisen einen Dienstrouter auf. Ein Ebene-1-Router kann bei Bedarf je nach Ihren Designüberlegungen einen Dienstrouter enthalten.

Standardmäßig verwenden die Links zwischen dem SR und dem DR das Subnetz 169.254.0.0/28. Diese routerübergreifenden Transit-Links werden automatisch erstellt, wenn Sie einen logischen Tier-0 oder Tier-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 Tier-1 Router ist der SR nur vorhanden, wenn Sie beim Erstellen des logischen Tier-1 Routers einen NSX Edge-Cluster auswählen.

Der Standard-Adressbereich für die Verbindungen von Ebene-0 zu Ebene-1 lautet 100.64.0.0/10. Jede Tier-0-zu-Tier-1-Peer-Verbindung erhält ein /31-Subnetz innerhalb des 100.64.0.0/10-Adressraums. Dieser Link wird automatisch erstellt, wenn Sie einen Ebene-1-Router erstellen und mit einem Ebene-0-Router verbinden. Sie müssen die Schnittstellen auf diesem Link nur dann ändern, wenn das Subnetz 100.64.0.0/10 bereits in Ihrer Bereitstellung verwendet wird.

Jede NSX-T Data Center-Bereitstellung verfügt über einen Management Plane-Cluster (Management Plane Cluster; MP) und einen Steuerungskomponentencluster (Control Plane Cluster; CCP). Der MP und der CCP geben Konfigurationen an die lokale Control Plane (LCP) jeder Transportzone weiter. Wenn ein Host oder NSX Edge der Management Plane beiträgt, baut der Management Plane-Agent (MPA) Konnektivität mit dem Host oder NSX Edge auf und der Host oder NSX Edge wird zu einem NSX-T Data Center-Fabric-Knoten. Wenn der Fabric-Knoten dann als Transportknoten hinzugefügt wird, wird LCP-Konnektivität mit dem Host oder NSX Edge aufgebaut.

Zuletzt zeigt die Abbildung ein Beispiel für zwei physikalische Netzwerkkarten (pNIC1 und pNIC2), die zur Gewährleistung hoher Verfügbarkeit verbunden sind. Der Datenpfad verwaltet die physischen Netzwerkkarten. Sie können entweder als VLAN-Uplinks zu einem externen Netzwerk oder als Tunnel-Endpoint-Links zu internen von NSX-T Data Center verwalteten VM-Netzwerken dienen.

Es wird empfohlen, mindestens zwei physische Links auf jeder NSX Edge zuzuteilen, die als virtuelle Maschine bereitgestellt wird. Optional können Sie die Portgruppen auf demselben pNIC mit unterschiedlichen VLAN-IDs überlappen. Der erste gefundene Netzwerkklink wird für das Management verwendet. Beispiel: Bei einer NSX Edge-VM kann zuerst der Link vnic1 gefunden werden. Bei einer Bare-Metal-Installation kann der erste gefundene Link eth0 oder em0 sein. Die restlichen Links werden für die Uplinks und Tunnel verwendet. Einer davon könnte z. B. für einen Tunnel-Endpoint für von NSX-T Data Center verwaltete VMs dienen. Der andere könnte als TOR-Uplink von NSX Edge zu extern verwendet werden.

Sie können die Informationen zum physischen Link der NSX Edge anzeigen, indem Sie sich bei der CLI als Administrator anmelden und die Befehle `get interfaces` und `get physical-ports` ausführen. In der API können Sie den API-Aufruf `GET fabric/nodes/<edge-node-id>/network/interfaces` verwenden. Im nächsten Abschnitt werden physische Links ausführlicher erläutert.

Unabhängig davon, ob Sie NSX Edge als VM-Appliance oder in einer Bare-Metal-Bereitstellung installieren, stehen Ihnen mehrere Optionen für die Netzwerkkonfiguration zur Verfügung, je nach Ihrer Bereitstellung.

## Transportzonen und N-VDS

Um das NSX Edge-Networking zu verstehen, müssen Sie sich etwas mit Transportzonen und N-VDS auskennen. Transportzonen steuern die Reichweite von Layer 2-Netzwerken in NSX-T Data Center. N-VDS ist ein Software-Switch, der auf einem Transportknoten erstellt wird. Ein N-VDS dient dazu, logische Router-Uplinks und -Downlinks an physische Netzwerkkarten (NICs) zu binden. Für jede Transportzone, zu der ein NSX Edge gehört, wird ein einzelner N-VDS auf dem NSX Edge installiert.

Es gibt zwei Arten von Transportzonen:

- Overlay für internes NSX-T Data Center-Tunneling zwischen Transportknoten.
- VLAN für Uplinks außerhalb von NSX-T Data Center.

Ein NSX Edge kann zu gar keinen oder zahlreichen VLAN-Transportzonen gehören. Ohne VLAN-Transportzonen kann der NSX Edge dennoch über Uplinks verfügen, da die NSX Edge-Uplinks denselben N-VDS verwenden können, der für die Overlay-Transportzone installiert wurde. Sie können dies tun, wenn Sie möchten, dass jeder NSX Edge nur einen N-VDS hat. Bei einer weiteren Designoption könnte der NSX Edge zu mehreren VLAN-Transportzonen gehören (einer für jeden Uplink).

Am häufigsten wird ein Design mit drei Transportzonen verwendet: eine Overlay- und zwei VLAN-Transportzonen für redundante Uplinks.

Um dieselbe VLAN-ID für ein Transportnetzwerk für Overlay-Datenverkehr und für anderen VLAN-Datenverkehr, beispielsweise einen VLAN-Uplink, zu verwenden, konfigurieren Sie die ID auf zwei verschiedenen N-VDS, einem für VLAN und dem anderen für Overlay.

## NSX Edge-Networking über virtuelle Appliance/VM

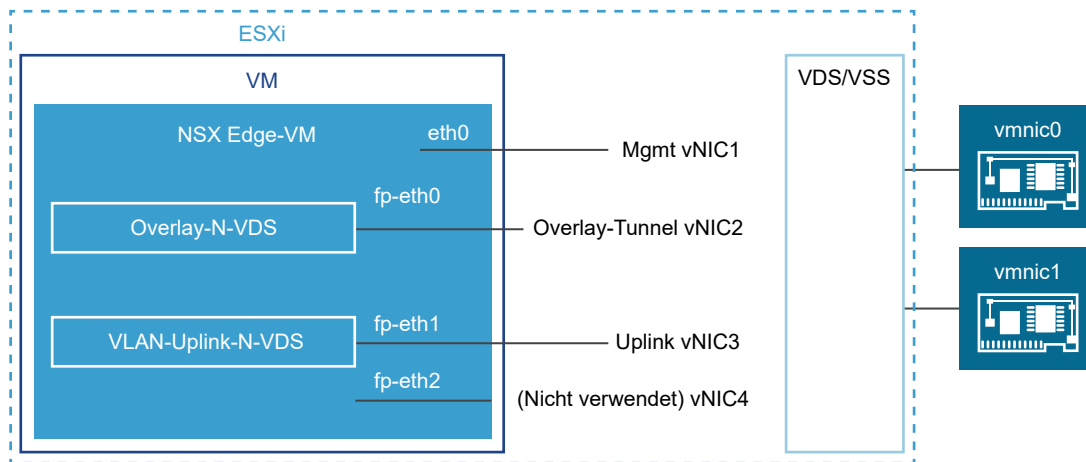
Wenn Sie NSX Edge als virtuelle Appliance oder VM installieren, werden interne Schnittstellen erstellt (mit dem Namen fp-ethX, wobei X für 0, 1, 2 und 3 steht). Diese Schnittstellen werden für Uplinks zu Top-of-Rack-(ToR-)Switches und für NSX-T Data Center-Overlay-Tunneling zugeteilt.

Beim Erstellen des NSX Edge-Transportknotens können Sie fp-ethX-Schnittstellen auswählen, die den Uplinks und dem Overlay-Tunnel zugeordnet werden. Sie können festlegen, wie die fp-ethX-Schnittstellen verwendet werden.

Auf dem vSphere Distributed Switch oder dem vSphere Standard Switch müssen Sie mindestens zwei vmnics zu NSX Edge zuordnen: einen für die NSX Edge-Verwaltung und einen für Uplinks und Tunnel.

In der folgenden physischen Beispieltopologie wird fp-eth0 für den NSX-T Data Center-Overlay-Tunnel verwendet. Fp-eth1 wird für den VLAN-Uplink verwendet. fp-eth2 und fp-eth3 werden nicht verwendet. vNIC1 wird dem Verwaltungsnetzwerk zugewiesen.

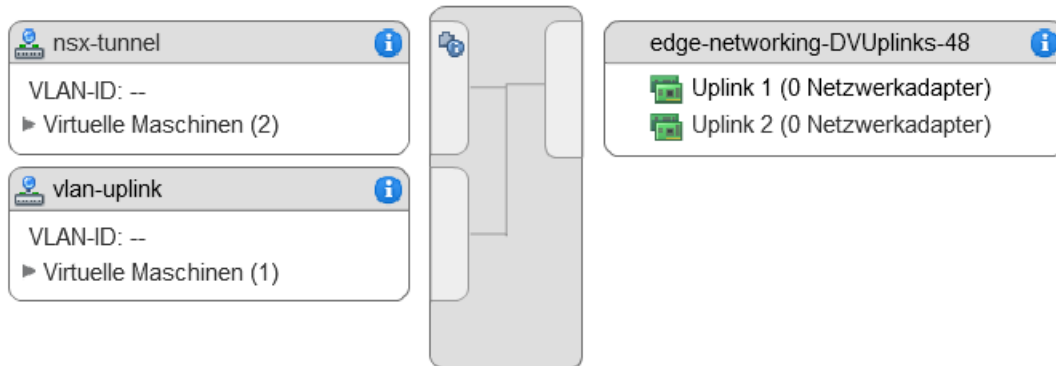
**Abbildung 9-2. Ein Vorschlag für die Linkeinrichtung zum NSX Edge-VM-Networking**





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.

Die für NSX Edge konfigurierten Tunnel- und Uplink-VM-Portgruppen müssen nicht den VMkernel-Ports oder bestimmten IP-Adressen zugeordnet sein. Dies liegt daran, dass sie nur auf Layer 2 verwendet werden. Wenn Ihre Bereitstellung DHCP verwendet, um eine Adresse zur Verwaltungsschnittstelle zur Verfügung zu stellen, müssen Sie sicherstellen, dass dem Verwaltungsnetzwerk nur eine Netzwerkkarte zugewiesen ist.

Beachten Sie, dass die VLAN- und Tunnel-Portgruppen als Trunk-Ports konfiguriert sind. Dies ist erforderlich. Bei einem Standard-vSwitch konfigurieren Sie beispielsweise die Trunk-Ports wie folgt: **Host > Konfiguration > Networking > Networking hinzufügen > Virtuelle Maschine > VLAN-ID Alle (4095).**

Wenn Sie einen Appliance-basierten oder VM-NSX Edge verwenden, können Sie Standard-vSwitches oder vSphere Distributed Switches verwenden.

Die NSX Edge-VM kann auf einem vorbereiteten NSX-T Data Center-Host installiert und als Transportknoten konfiguriert werden. Es gibt zwei Arten der Bereitstellung:

- Die NSX Edge-VM kann über VSS/VDS-Portgruppen bereitgestellt werden, wobei VSS/VDS separate PNIC(s) auf dem Host verbrauchen. Der Hosttransportknoten nutzt separate

PNIC(s) für den auf dem Host installierten N-VDS. Der N-VDS des Hosttransportknotens koexistiert mit einem VSS oder VDS, wobei beide separate PNICs nutzen. Der Host-TEP (Tunnelendpunkt) und der NSX Edge-TEP können im selben Subnetz oder in verschiedenen Subnetzen verfügbar sein.

- Die NSX Edge-VM kann über VLAN-unterstützte logische Switches auf dem N-VDS des Host-Transportknotens bereitgestellt werden. Der Host TEP und der NSX Edge-TEP müssen sich in unterschiedlichen Subnetzen befinden.

Optional können Sie mehrere NSX Edge-Appliances/-VMs auf einem einzelnen Host installieren und dieselben Portgruppen für Management, VLAN und Tunnel-Endpoint können von allen installierten NSX Edges verwendet werden.

Wenn die zugrunde liegenden physischen Links eingerichtet und die VM-Portgruppen konfiguriert sind, können Sie NSX Edge installieren.

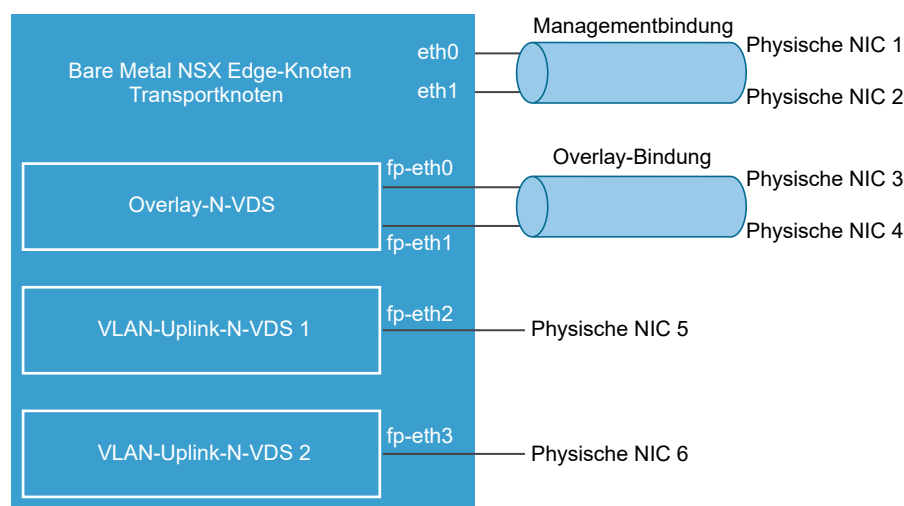
## NSX Edge-Networking auf Bare-Metal-Bereitstellung

Ein Bare-Metal-NSX Edge enthält interne Schnittstellen (mit dem Namen fp-ethX, wobei X für 0, 1, 2, 3 oder 4 steht). Wie viele fp-ethX-Schnittstellen erstellt werden, hängt davon ab, wie viele physische NICs im Bare-Metal-NSX Edge vorkommen. Bis zu vier dieser Schnittstellen können für Uplinks zu Top-of-Rack(ToR)-Switches und NSX-T Data Center-Overlay-Tunneling zugeteilt werden.

Beim Erstellen des NSX Edge-Transportknotens können Sie fp-ethX-Schnittstellen auswählen, die den Uplinks und dem Overlay-Tunnel zugeordnet werden.

Sie können festlegen, wie die fp-ethX-Schnittstellen verwendet werden. In der folgenden physischen Beispieltopologie werden fp-eth0 und fp-eth1 für den NSX-T Data Center-Overlay-Tunnel verwendet. fp-eth2 und fp-eth3 werden als redundante VLAN-Uplinks zu TORs eingesetzt.

Abbildung 9-3. Ein Vorschlag für die Linkeinrichtung für Bare-Metal-NSX Edge-Networking



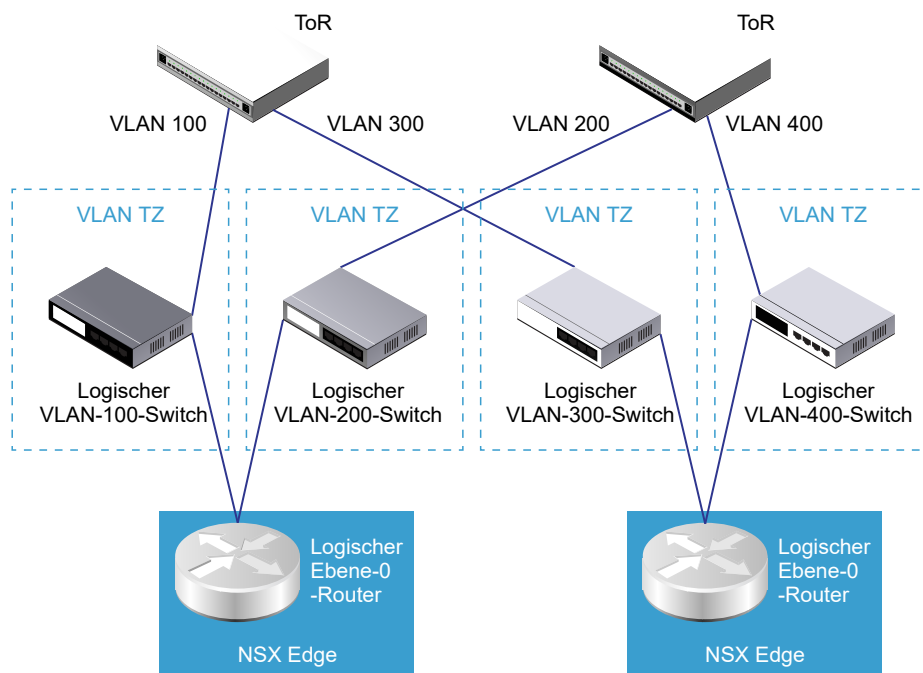
## NSX Edge-Uplink-Redundanz

Dank NSX Edge-Uplink-Redundanz können zwei VLAN-ECMP-Uplinks (Equal-Cost-MultiPath) in der TOR-Netzwerkverbindung von NSX Edge zu extern verwendet werden.

Wenn Sie über zwei ECMP-VLAN-Uplinks verfügen, müssen für eine hohe Verfügbarkeit und eine vollständig vernetzte Konnektivität auch über zwei TOR-Switches verfügen. Jedem logischen VLAN-Switch ist eine VLAN-ID zugeordnet.

Wenn Sie einen NSX Edge zu einer VLAN-Transportzone hinzufügen, wird ein neuer N-VDS installiert. Wenn Sie beispielsweise, wie in der Abbildung gezeigt, einen NSX Edge-Knoten zu vier VLAN-Transportzonen hinzufügen, werden vier N-VDS auf dem NSX Edge installiert.

Abbildung 9-4. Ein Vorschlag für eine ECMP-VLAN-Einrichtung für NSX Edges zu TORs



**Hinweis** Für eine auf einem ESXi-Host mit dem vSphere Distributed Switch (vDS) anstelle von N-VDS bereitgestellte virtuelle Edge-Maschine müssen Sie wie folgt vorgehen:

- Aktivieren Sie die gefälschte Übertragung, damit DHCP funktioniert.
- Aktivieren Sie den promiskuitiven Modus für die virtuelle Edge-Maschine, um unbekannte Unicast-Pakete zu empfangen, da MAC Learning standardmäßig deaktiviert ist. Für vDS 6.6 oder höhere Versionen ist dies nicht notwendig, da MAC Learning für diese Versionen standardmäßig aktiviert ist.

## NSX Edge-Installationsmethoden

Installieren Sie NSX Edge auf einem ESXi-Host mithilfe der NSX Manager-Benutzeroberfläche (empfohlene Methode), des vSphere-Webclients oder des vSphere-Befehlszeilen-OVF-Tools.

## NSX Edge-Installationsmethoden

Installationsmethode	Anweisungen
NSX Manager (Methode wird nur zum Installieren einer NSX Edge-VM-Appliance empfohlen)	<ul style="list-style-type: none"> <li>■ Stellen Sie sicher, dass die NSX Edge-Netzwerkanforderungen erfüllt werden. Siehe <a href="#">NSX Edge-Installationsanforderungen</a>.</li> <li>■ Erstellen Sie einen NSX Edge-Transportknoten. Siehe <a href="#">Erstellen eines NSX Edge-Transportknotens</a>.</li> <li>■ Erstellen eines NSX Edge-Clusters. Siehe <a href="#">Erstellen eines NSX Edge-Clusters</a>.</li> </ul>
vSphere-WebClient oder vSphere-Befehlszeilen-OVF-Tool	<ul style="list-style-type: none"> <li>■ Stellen Sie sicher, dass die NSX Edge-Netzwerkanforderungen erfüllt werden. Siehe <a href="#">NSX Edge-Installationsanforderungen</a>.</li> <li>■ Wählen Sie vSphere-WebClient oder vSphere-Befehlszeilen-OVF-Tool aus, um NSX Edge zu installieren. <ul style="list-style-type: none"> <li>■ (WebClient) Installieren Sie NSX Edge unter ESXi. Siehe <a href="#">Installieren von NSX Edge unter ESXi mithilfe der grafischen vSphere-Benutzeroberfläche</a>.</li> <li>■ (Befehlszeilen-OVF-Tool) Installieren Sie NSX Edge unter ESXi. Siehe <a href="#">Installieren von NSX Manager unter ESXi mithilfe des OVF-Befehlszeilentools</a>.</li> </ul> </li> <li>■ Verbinden Sie NSX Edge mit der Management Plane. Siehe <a href="#">Verbinden von NSX Edge mit der Management Plane</a>.</li> <li>■ Konfigurieren Sie NSX Edge als Transportknoten. Siehe <a href="#">Konfigurieren von NSX Edge als Transportknoten</a>.</li> <li>■ Erstellen eines NSX Edge-Clusters. Siehe <a href="#">Erstellen eines NSX Edge-Clusters</a>.</li> </ul>
(Bare Metal-Server) ISO (automatischer oder interaktiver Modus über ISO-Datei) oder als NSX Edge-VM-Appliance	<p>Sie können die automatische Installation von NSX Edge auf einem Bare Metal-Server konfigurieren oder NSX Edge als VM-Appliance mithilfe von PXE installieren. Beachten Sie, dass das PXE-Boot-Installationsverfahren in NSX Manager nicht unterstützt wird.</p> <ul style="list-style-type: none"> <li>■ Stellen Sie sicher, dass die NSX Edge-Netzwerkanforderungen erfüllt werden. Siehe <a href="#">NSX Edge-Installationsanforderungen</a>.</li> <li>■ Bereiten Sie den PXE-Server vor. Siehe <a href="#">Vorbereiten des PXE-Servers für NSX Edge</a>. Wählen Sie eine der unterstützten Installationsmethoden aus: <ul style="list-style-type: none"> <li>■ (Automatisierte Installation) Installieren Sie NSX Edge per ISO-Datei einer Bare-Metal-Bereitstellung. Siehe <a href="#">Automatisches Installieren von NSX Edge via ISO-Datei</a>.</li> <li>■ (Automatisierte Installation) Installieren Sie NSX Edge per ISO-Datei als virtuelle Appliance. Siehe <a href="#">Installieren von NSX Edge per ISO-Datei als virtuelle Appliance</a>.</li> <li>■ (Manuelle Installation) Installieren Sie NSX Edge manuell per ISO-Datei. Siehe <a href="#">Interaktives Installieren von NSX Edge via ISO-Datei</a>.</li> </ul> </li> <li>■ Verbinden Sie NSX Edge mit der Management Plane. Siehe <a href="#">Verbinden von NSX Edge mit der Management Plane</a>.</li> <li>■ Konfigurieren Sie NSX Edge als Transportknoten. Siehe <a href="#">Konfigurieren von NSX Edge als Transportknoten</a>.</li> <li>■ Erstellen eines NSX Edge-Clusters. Siehe <a href="#">Erstellen eines NSX Edge-Clusters</a>.</li> </ul>

## Erstellen eines NSX Edge-Transportknotens

Sie können eine NSX Edge-VM der NSX-T Data Center-Fabric hinzufügen und sie dann als NSX Edge-Transportknoten-VM konfigurieren.

Ein NSX Edge-Knoten ist ein Transportknoten, der die lokalen Control Plane-Daemons und Weiterleitungs-Engines ausführt, die die NSX-T-Data Plane implementieren. Er führt eine Instanz des virtuellen NSX-T-Switches mit dem Namen NSX Virtual Distributed Switch oder N-VDS aus. Die Edge-Knoten sind Dienst-Appliances, die für die Durchführung zentralisierter Netzwerkdienste vorgesehen sind, die nicht an die Hypervisoren verteilt werden können. Sie können als Bare Metal-Appliance oder als VM-Formfaktor instanziiert werden. Sie sind in mindestens einem Clustern gruppiert und stellen einen Kapazitätspool dar.

Ein NSX Edge kann zu einer Overlay-Transportzone und mehreren VLAN-Transportzonen gehören. Ein NSX Edge gehört zu mindestens einer VLAN-Transportzone, um den Uplink-Zugriff bereitzustellen.

---

**Hinweis** Wenn Sie Transportknoten aus einer Vorlagen-VM erstellen möchten, achten Sie darauf, dass keine Zertifikate für den Host in `/etc/vmware/nsx/` vorhanden sind. Der netcpa-Agent erstellt kein Zertifikat, wenn bereits ein Zertifikat vorhanden ist.

---

### Voraussetzungen

- Transportzonen müssen konfiguriert sein. Siehe [Erstellen von Transportzonen](#).
- Stellen Sie sicher, dass der Compute Manager konfiguriert ist. Siehe [Hinzufügen eines Compute Managers](#).
- Ein Uplink-Profil muss konfiguriert sein. Alternativ können Sie auch das standardmäßige Uplink-Profil für NSX Edge-Knoten verwenden. Siehe [Erstellen eines Uplink-Profiles](#).
- Ein IP-Pool muss konfiguriert sein, oder in der Netzwerkbereitstellung verfügbar sein. Siehe [Erstellen eines IP-Pools für Tunnel-Endpoint-IP-Adressen](#).

### Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **System > Fabric > Knoten > Edge-Transportknoten > Edge-VM hinzufügen** aus.
- 3 Geben Sie einen Namen für NSX Edge ein.
- 4 Geben Sie den Hostnamen oder FQDN von vCenter Server ein.
- 5 Reservieren Sie Arbeitsspeicher für die NSX Edge-Appliance, um eine optimale Leistung zu erreichen.

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

**6** Geben Sie die Befehlszeilenschnittstelle (CLI) und die Root-Kennwörter für den NSX Edge an.

Ihre Kennwörter müssen den Einschränkungen zur Kennwortkomplexität entsprechen.

- mindestens 12 Zeichen
- mindestens ein Kleinbuchstabe
- mindestens ein Großbuchstabe
- mindestens eine Zahl
- mindestens ein Sonderzeichen
- mindestens fünf unterschiedliche Zeichen
- Standard-Kennwortkomplexitätsregeln werden von den Argumenten des Linux PAM-Moduls erzwungen:
  - `retry=3`: die maximale Anzahl, wie oft ein neues Kennwort für dieses Argument eingegeben werden kann (maximal 3 mal), bevor eine Fehlermeldung zurückgegeben wird.
  - `minlen=12`: die zulässige Mindestgröße für das neue Kennwort. Zusätzlich zur Anzahl von Zeichen im neuen Kennwort erfolgt eine Gutschrift (+ 1 für die Länge) für jede Art von Zeichen (sonstige, großgeschrieben, kleingeschrieben und Ziffer).
  - `difok=0`: die minimale Anzahl von Bytes, die sich im neuen Kennwort unterscheiden müssen. Zeigt die Ähnlichkeit zwischen dem alten und dem neuen Kennwort an. Wenn `difok` der Wert 0 zugewiesen wird, müssen sich die Bytes des alten und des neuen Kennworts nicht unterscheiden. Eine genaue Übereinstimmung ist zulässig.
  - `lcredit=1`: die maximale Gutschrift für die Verwendung von Kleinbuchstaben im neuen Kennwort. Wenn Sie weniger als oder 1 Kleinbuchstaben haben, zählt jeder Buchstabe + 1, um den aktuellen `minlen`-Wert zu erfüllen.
  - `ucredit=1`: die maximale Gutschrift für die Verwendung von Großbuchstaben im neuen Kennwort. Wenn Sie weniger als oder 1 Großbuchstaben haben, zählt jeder Buchstabe + 1, um den aktuellen `minlen`-Wert zu erfüllen.
  - `dcredit=1`: die maximale Gutschrift für die Verwendung von Ziffern im neuen Kennwort. Wenn Sie weniger als oder 1 Ziffer haben, zählt jede Ziffer + 1, um den aktuellen `minlen`-Wert zu erfüllen.
  - `ocredit=1`: die maximale Gutschrift für die Verwendung von sonstigen Zeichen im neuen Kennwort. Wenn Sie weniger als oder 1 sonstiges Zeichen haben, zählt jedes Zeichen + 1, um den aktuellen `minlen`-Wert zu erfüllen.
  - `enforce_for_root`: Das Kennwort ist für den Root-Benutzer festgelegt.

---

**Hinweis** Weitere Einzelheiten zum Linux-PAM-Modul zum Abgleichen des Kennworts mit den Wörtern aus dem Wörterbuch finden Sie auf der Hauptseite.

---

Vermeiden Sie zum Beispiel einfache und systematische Kennwörter wie **VMware123!123** oder **VMware12345**. Kennwörter, die den Komplexitätsstandards entsprechen, sind nicht einfach und systematisch, sondern bestehen aus einer Kombination von Buchstaben, Sonderzeichen und Zahlen wie **VMware123!45**, **VMware1!2345** oder **VMware@1az23x**.

## 7 Geben Sie die Details zum NSX Edge ein.

Option	Beschreibung
<b>Compute Manager</b>	Wählen Sie im Dropdown-Menü den Compute Manager aus. Der Compute Manager entspricht der in der Management Plane registrierten vCenter Server.
<b>Cluster</b>	Weisen Sie den Cluster zu, den der NSX Edge aus dem Dropdown-Menü verknüpfen wird.
<b>Ressourcenpool oder Host</b>	Weisen Sie entweder einen Ressourcenpool oder einen bestimmten Host für den NSX Edge aus dem Dropdown-Menü zu.
<b>Datenspeicher</b>	Wählen Sie einen Datenspeicher für die NSX Edge-Dateien aus dem Dropdown-Menü.

## 8 Geben Sie die Details zur NSX Edge-Schnittstelle ein.

Option	Beschreibung
<b>IP-Zuweisung</b>	Dies ist die dem NSX Edge-Knoten zugewiesene IP-Adresse, die für die Kommunikation mit NSX Manager und NSX Controller erforderlich ist. Wählen Sie für die IP-Adresse <b>DHCP</b> oder <b>Statisch</b> aus. Wenn Sie <b>Statisch</b> auswählen, geben Sie die Werte für Folgendes ein: <ul style="list-style-type: none"> <li>■ Verwaltungs-IP: Geben Sie die IP-Adresse von NSX Edge in die CIDR-Notation ein.</li> <li>■ Standard-Gateway: Geben Sie die Gateway-IP-Adresse von NSX Edge ein.</li> </ul>
<b>Verwaltungsschnittstelle</b>	Wählen Sie im Dropdown-Menü die Verwaltungsnetzwerkschnittstelle aus. Diese Schnittstelle muss entweder von NSX Manager aus erreichbar sein oder sich in derselben Verwaltungsschnittstelle befinden wie NSX Manager und NSX Controller. Die NSX Edge-Verwaltungsschnittstelle stellt die Kommunikation mit der NSX Manager-Verwaltungsschnittstelle her.

**9** Wählen Sie die Transportzonen aus, zu denen dieser Transportknoten gehört.

Ein NSX Edge-Transportknoten gehört zu mindestens zwei Transportzonen, einem Overlay für NSX-T Data Center-Konnektivität und einem VLAN für Uplink-Konnektivität.

---

**Hinweis** NSX Edge-Knoten unterstützen mehrere Overlay-Tunnel (Multi-TEP), wenn die folgenden Voraussetzungen erfüllt sind:

- Die TEP-Konfiguration darf nur auf einem N-VDS durchgeführt werden.
  - Alle TEPs müssen dasselbe Transport-VLAN für den Overlay-Datenverkehr verwenden.
  - Alle TEP-IPs müssen sich im selben Subnetz befinden und dasselbe Standard-Gateway verwenden.
- 

**10** Geben Sie die N-VDS-Informationen ein.

Option	Beschreibung
Edge-Switchname	Wählen Sie im Dropdown-Menü einen VLAN- oder Overlay-Switch aus.
Uplink-Profil	Wählen Sie ein Uplink-Profil im Dropdown-Menü aus. Die verfügbaren Uplinks hängen von der Konfiguration im gewählten Uplink-Profil ab.

---



Option	Beschreibung
<b>IP-Zuweisung</b>	<p>Die IP-Adresse wird dem konfigurierten NSX Edge-Switch zugewiesen. Sie wird zum Weiterleiten von Paketen in einem Overlay- oder VLAN-Netzwerk verwendet.</p> <p>Wählen Sie <b>IP-Pool verwenden</b> oder <b>Liste statischer IPs verwenden</b> für den Overlay-N-VDS aus.</p> <ul style="list-style-type: none"> <li>■ Wenn Sie <b>Liste statischer IPs verwenden</b> auswählen, geben Sie Folgendes an: <ul style="list-style-type: none"> <li>■ Statische IP-Liste: Geben Sie eine Liste mit durch Kommas getrennte IP-Adressen ein, die vom NSX Edge-Switch verwendet werden sollen.</li> <li>■ Gateway: Geben Sie die standardmäßige Gateway-IP-Adresse ein, die zum Weiterleiten von Paketen zwischen NSX Edge-Transportknoten in einem Overlay-Netzwerk verwendet wird.</li> <li>■ Subnetzmaske: Geben Sie die Subnetzmaske für das konfigurierte Gateway ein.</li> </ul> </li> <li>■ Wenn Sie <b>IP-Pool verwenden</b> für die IP-Zuweisung ausgewählt haben, geben Sie den Namen des IP-Pools an.</li> </ul>
<b>DPDK-Fastpath-Schnittstellen/ virtuelle Netzwerkkarten (NICs)</b>	<p>Wählen Sie den Datenpfadnamen für die Uplink-Schnittstelle aus.</p> <p><b>Hinweis</b> Wenn das auf den Edge-Knoten angewendete Uplink-Profil eine benannte Gruppierungsrichtlinie verwendet, stellen Sie sicher, dass die folgende Bedingung erfüllt ist:</p> <ul style="list-style-type: none"> <li>■ Alle Uplinks in der Standard-Gruppierungsrichtlinie müssen den physischen Netzwerkschnittstellen auf der Edge-VM zugeordnet werden, damit der Datenverkehr über einen logischen Switch übermittelt wird, der die benannten Gruppierungsrichtlinien verwendet.</li> </ul>

### Hinweis

- Das LLDP-Profil wird auf einer NSX Edge-VM-Appliance nicht unterstützt.
- Uplink-Schnittstellen werden als **DPDK-Fastpath-Schnittstellen** angezeigt, wenn NSX Edge mithilfe von NSX Manager oder auf einem Bare Metal-Server installiert wird.
- Uplink-Schnittstellen werden als **Virtuelle Netzwerkkarten** angezeigt, wenn NSX Edge manuell mithilfe von vCenter Server installiert wird.

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

Nach dem Hinzufügen des NSX Edge als Transportknoten ändert sich der Verbindungsstatus in 10-12 Minuten in Aktiv.

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

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

- 14** Nachdem ein NSX Edge-Knoten mithilfe von vCenter Server auf einen neuen Host migriert wurde, kann es vorkommen, dass die NSX Manager-UI veraltete Konfigurationsdetails (Berechnung, Datenspeicher, Netzwerk, SSH, NTP, DNS, Suchdomänen) der NSX Edge meldet. Um die aktuellsten Konfigurationsdetails von NSX Edge auf dem neuen Host zu erhalten, führen Sie den folgenden API-Befehl aus.

```
POST api/v1/transport-nodes/<transport-node-id>?
action=refresh_node_configuration&resource_type=EdgeNode
```

#### 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.
- Stellen Sie sicher, dass der NSX Edge-Knoten stabil ist, dass alle Dienste ausgeführt werden und alle Gruppen stabil sind, bevor Sie den Knoten dem Cluster hinzufügen.
- Verbinden Sie die NSX Edges mit der Management Plane.
- Fügen Sie die NSX Edges als Transportknoten hinzu.
- Erstellen Sie optional ein NSX Edge-Clusterprofil für Hochverfügbarkeit (HA). Sie können aber auch das standardmäßige NSX Edge-Clusterprofil verwenden.

#### Verfahren

- 1** Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2** Wählen Sie **System > Fabric > Knoten > Edge-Cluster > Hinzufügen** aus.
- 3** Geben Sie einen Namen für den NSX Edge-Cluster ein.

- 4 Wählen Sie ein NSX Edge-Clusterprofil im Dropdown-Menü aus.
- 5 Wählen Sie im Dropdown-Menü „Mitgliedstyp“ entweder **Edge-Knoten** aus, wenn die virtuelle Maschine lokal bereitgestellt wird oder wählen Sie **Public Cloud-Gateway** aus, wenn die virtuelle Maschine in einer Public Cloud bereitgestellt wird.
- 6 Wählen Sie in der Spalte **Verfügbar** die NSX Edges aus und klicken Sie auf den Pfeil nach rechts, um diese in die Spalte **Ausgewählt** zu verschieben.

#### Nächste Schritte

Jetzt können Sie logische Netzwerktopologien erstellen und Dienste konfigurieren. Siehe *Administratorhandbuch für NSX-T Data Center*.

## Installieren von NSX Edge unter ESXi mithilfe der grafischen vSphere-Benutzeroberfläche

Sie können den vSphere-Webclient oder den vSphere-Client verwenden, um NSX Edge auf ESXi interaktiv zu installieren.

---

**Hinweis** Ab NSX-T Data Center 2.5.1 unterstützt die NSX Edge-VM vMotion.

---

#### Voraussetzungen

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

#### Verfahren

- 1 Suchen Sie im VMware-Download-Portal nach der OVA-Datei der NSX Edge-Appliance.  
Kopieren Sie die Download-URL oder laden Sie die OVA-Datei auf Ihren Computer herunter.
- 2 Wählen Sie im vSphere Client den Host aus, auf dem die NSX Edge-Appliance installiert werden soll.
- 3 Wählen Sie im Kontextmenü die Option **OVF-Vorlage bereitstellen** aus, um den Installationsassistenten zu starten.
- 4 Geben Sie die URL der herunterzuladenden OVA-Datei ein oder navigieren Sie zur gespeicherten OVA-Datei.
- 5 Geben Sie einen Namen für die NSX Edge-VM ein.  
Der eingegebene Name wird in der Bestandsliste angezeigt.
- 6 Wählen Sie eine Computing-Ressource für die NSX Edge-Appliance aus.
- 7 Reservieren Sie Arbeitsspeicher für die NSX Edge-Appliance, um eine optimale Leistung zu erreichen.  
  
Legen Sie die Reservierung so fest, dass NSX Edge über ausreichend Arbeitsspeicher verfügt, um eine effiziente Ausführung sicherzustellen. Siehe [Systemanforderungen für NSX Edge-VM](#).
- 8 Überprüfen Sie die Details der OVF-Vorlage.

**9** Wählen Sie einen Datenspeicher für die Dateien der NSX Edge-Appliance aus.

**10** Akzeptieren Sie die Standardnetzwerkschnittstelle für die Quelle und das Ziel.

Sie können das Ziel des Standardnetzwerks für die restlichen Netzwerke übernehmen und die Netzwerkkonfiguration ändern, nachdem die NSX Edge bereitgestellt wurde.

**11** Wählen Sie im Dropdown-Menü die IP-Zuteilung aus.

**12** Geben Sie die System-Root-, CLI-Admin- und Audit-Kennwörter für die NSX Edge ein.

---

**Hinweis** Ignorieren Sie im Fenster „Vorlage anpassen“ die Meldung **Alle Eigenschaften haben gültige Werte**, die noch vor der Eingabe von Werten in einem der Felder angezeigt wird. Diese Meldung wird angezeigt, weil alle Parameter optional sind. Die Validierung wird durchgeführt, da Sie in keinem der Felder Werte eingegeben haben.

---

Ihre Kennwörter müssen den Einschränkungen zur Kennwortkomplexität entsprechen.

- mindestens 12 Zeichen
- mindestens ein Kleinbuchstabe
- mindestens ein Großbuchstabe
- mindestens eine Zahl
- mindestens ein Sonderzeichen
- mindestens fünf unterschiedliche Zeichen
- Standard-Kennwortkomplexitätsregeln werden von den Argumenten des Linux PAM-Moduls erzwungen:
  - `retry=3`: die maximale Anzahl, wie oft ein neues Kennwort für dieses Argument eingegeben werden kann (maximal 3 mal), bevor eine Fehlermeldung zurückgegeben wird.
  - `minlen=12`: die zulässige Mindestgröße für das neue Kennwort. Zusätzlich zur Anzahl von Zeichen im neuen Kennwort erfolgt eine Gutschrift (+ 1 für die Länge) für jede Art von Zeichen (sonstige, großgeschrieben, kleingeschrieben und Ziffer).
  - `difok=0`: die minimale Anzahl von Bytes, die sich im neuen Kennwort unterscheiden müssen. Zeigt die Ähnlichkeit zwischen dem alten und dem neuen Kennwort an. Wenn `difok` der Wert 0 zugewiesen wird, müssen sich die Bytes des alten und des neuen Kennworts nicht unterscheiden. Eine genaue Übereinstimmung ist zulässig.
  - `lcredit=1`: die maximale Gutschrift für die Verwendung von Kleinbuchstaben im neuen Kennwort. Wenn Sie weniger als oder 1 Kleinbuchstaben haben, zählt jeder Buchstabe + 1, um den aktuellen `minlen`-Wert zu erfüllen.
  - `ucredit=1`: die maximale Gutschrift für die Verwendung von Großbuchstaben im neuen Kennwort. Wenn Sie weniger als oder 1 Großbuchstaben haben, zählt jeder Buchstabe + 1, um den aktuellen `minlen`-Wert zu erfüllen.

- `dcredit=1`: die maximale Gutschrift für die Verwendung von Ziffern im neuen Kennwort. Wenn Sie weniger als oder 1 Ziffer haben, zählt jede Ziffer + 1, um den aktuellen `minlen`-Wert zu erfüllen.
- `ocredit=1`: die maximale Gutschrift für die Verwendung von sonstigen Zeichen im neuen Kennwort. Wenn Sie weniger als oder 1 sonstiges Zeichen haben, zählt jedes Zeichen + 1, um den aktuellen `minlen`-Wert zu erfüllen.
- `enforce_for_root`: Das Kennwort ist für den Root-Benutzer festgelegt.

---

**Hinweis** Weitere Einzelheiten zum Linux-PAM-Modul zum Abgleichen des Kennworts mit den Wörtern aus dem Wörterbuch finden Sie auf der Hauptseite.

---

Vermeiden Sie zum Beispiel einfache und systematische Kennwörter wie **VMware123!123** oder **VMware12345**. Kennwörter, die den Komplexitätsstandards entsprechen, sind nicht einfach und systematisch, sondern bestehen aus einer Kombination von Buchstaben, Sonderzeichen und Zahlen wie **VMware123!45**, **VMware1!2345** oder **VMware01az23x**.

- 13** (Optional) Wenn Sie über einen verfügbaren NSX Manager verfügen und NSX Edge während der OVA-Bereitstellung bei der Management Plane registrieren möchten, füllen Sie die Felder „Manager-IP“, „Fingerabdruck“ und „Token“ aus.
- a Geben Sie die IP-Adresse und den Fingerabdruck des übergeordneten NSX Manager-Knotens ein
  - b Führen Sie den API-Aufruf `POST https://<nsx-manager>/api/v1/aaa/registration-token` aus, um das NSX Manager-Token abzurufen.

```
{
  "token": "4065a7c0-9658-4058-bb01-c149f20f238a",
  "roles": [
    "enterprise_admin"
  ],
  "user": "admin"
}
```

- c Geben Sie das NSX Manager-Token ein.

---

**Hinweis** Das Feld für die Knoten-UUID ist nur für die interne Verwendung bestimmt. Lassen Sie das Feld leer.

---

- 14** Geben Sie den Hostnamen der NSX Edge-VM ein.
- 15** Geben Sie das Standard-Gateway, die IPv4-Adresse und Netzmaske des Verwaltungsnetzwerks, die DNS- und NTP-IP-Adresse ein.

---

**Hinweis** Ignorieren Sie die VMC-Einstellungen. Geben Sie nur Werte für VMC-Bereitstellungen ein.

---

- 16** (Optional) Aktivieren Sie SSH nicht, wenn Sie über die Konsole auf NSX Edge zugreifen möchten. Wenn Sie jedoch die Root-SSH-Anmeldung und die CLI-Anmeldung an der NSX Edge-Befehlszeile verwenden möchten, aktivieren Sie die SSH-Option.

Standardmäßig ist der SSH-Zugriff aus Sicherheitsgründen deaktiviert.

- 17** Stellen Sie sicher, dass die gesamte Spezifikation der benutzerdefinierten OVA-Vorlage korrekt ist, und klicken Sie auf **Beenden**, um die Installation zu starten.

Die Installation kann 7 bis 8 Minuten dauern.

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

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

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

---

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

---

- 20** Führen Sie den Befehl `get interface eth0` (ohne VLAN) oder `get interface eth0.<vlan_ID>` (mit einem VLAN) aus, um zu überprüfen, ob die IP-Adresse erwartungsgemäß angewendet wurde.

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

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

---

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

---

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

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

- 22** Wenn NSX Edge nicht bei der Management Plane registriert ist, schlagen Sie unter [Verbinden von NSX Edge mit der Management Plane](#) nach.

**23** 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.

**24** Beheben Sie Konnektivitätsprobleme.

---

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

---

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

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

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

**Nächste Schritte**

Konfigurieren Sie NSX Edge als Transportknoten. Siehe [Konfigurieren von NSX Edge als Transportknoten](#).

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

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

**Voraussetzungen**

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

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

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

- Planen Sie das IPv4-IP-Adressschema für NSX Manager.
- Siehe NSX Edge-Netzwerkanforderungen im Handbuch [NSX Edge-Installationsanforderungen](#).
- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Bereitstellen einer OVF-Vorlage auf dem ESXi-Host verfügen.
- Stellen Sie sicher, dass Hostnamen keine Unterstriche enthalten. Andernfalls wird der Hostname auf *localhost* gesetzt.
- OVF Tool Version 4.3 oder höher
- Kennen Sie die Parameter, die Sie verwenden können, um eine NSX Edge-VM bereitzustellen und sie der Management Plane hinzuzufügen.

Feldname	OVF-Parameter	Feldtyp
System-Root-Kennwort	nsx_passwd_0	Für die Installation von NSX Edge erforderlich.
CLI-Administratorkennwort	nsx_cli_passwd_0	Für die Installation von NSX Edge erforderlich.
CLI-Überwachungskennwort	nsx_cli_audit_passwd_0	Optional
CLI-Administratorbenutzername	nsx_cli_username	Optional
CLI-Überwachungsbenutzername	nsx_cli_audit_username	Optional
IP von NSX Manager	mpIp	Erforderlich für die Verknüpfung der NSX Edge-VM mit NSX Manager.
Token von NSX Manager	mpToken	Erforderlich für die Verknüpfung der NSX Edge-VM mit NSX Manager. Führen Sie für die Token-Ausführung in NSX Manager POST <code>https://&lt;nsx-manager&gt;/api/v1/aaa/registration-token</code> aus.



Feldname	OVF-Parameter	Feldtyp
Fingerabdruck von NSX Manager	mpThumbprint	Erforderlich für die Verknüpfung der NSX Edge-VM mit NSX Manager. Führen Sie zum Abrufen des Fingerabdrucks auf dem NSX Manager-Knoten <code>get certificate api thumbprint</code> aus.
Knoten-ID	mpNodeId	Nur für die interne Verwendung.
Hostname	nsx_hostname	Optional
Standard-IPv4-Gateway	nsx_gateway_0	Optional
IP-Adresse für das Verwaltungsnetzwerk	nsx_ip_0	Optional
Netzmaske für das Verwaltungsnetzwerk	nsx_netmask_0	Optional
DNS-Server	nsx_dns1_0	Optional
Suffixe für die Domänensuche	nsx_domain_0	Optional
NTP-Server	nsx_ntp_0	Optional
Ist der SSH-Dienst aktiviert	nsx_isSSHEnabled	Optional
Ist SSH für die Root-Anmeldung aktiviert	nsx_allowSSHRootLogin	Optional

## 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
--prop:mpIp=<NSXManager-IP>
--prop:mpToken=<NSXManager-Token>
--prop:mpThumbprint=<NSXManager-Thumbprint>
<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
--prop:mpIp=<NSXManager-IP>
```

```
--prop:mpToken=<NSXManager-Token>
--prop:mpThumbprint=<NSXManager-Thumbprint>
<path/url to nsx component ova>
vi://administrator@vsphere.local:<password>@192.168.110.24/?ip=192.168.210.53
```

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

- ◆ Reservieren Sie Arbeitsspeicher für die Appliance, um eine optimale Leistung zu erreichen. Legen Sie die Reservierung so fest, dass NSX Manager über ausreichend Arbeitsspeicher verfügt, um eine effiziente Ausführung sicherzustellen. Siehe [Systemanforderungen für NSX Manager-VM und -Host-Transportknoten](#).
- ◆ Öffnen Sie die Konsole von NSX Edge, um den Startvorgang zu verfolgen.
- ◆ Nachdem der NSX Edge gestartet ist, melden Sie sich bei der CLI mit Admin-Anmeldedaten an.
- ◆ Führen Sie den Befehl `get interface eth0` (ohne VLAN) oder `get interface eth0.<vlan_ID>` (mit einem VLAN) aus, um zu überprüfen, ob die IP-Adresse erwartungsgemäß angewendet wurde.

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

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

---

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

---

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

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

---

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

---

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

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

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

#### Nächste Schritte

Wenn Sie NSX Edge nicht mit der Management Plane verknüpft haben, schlagen Sie unter [Verbinden von NSX Edge mit der Management Plane](#) nach.

## 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-Installationsanforderungen](#).

## Verfahren

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

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

- 5 Wählen Sie in der Bestandsliste von vSphere Client den Host aus, auf den Sie die ISO-Datei hochgeladen haben. Stattdessen können Sie auch im vSphere Client
- 6 einen Rechtsklick ausführen und **Neue virtuelle Maschine** auswählen.
- 7 Wählen Sie eine Computing-Ressource für die NSX Edge-Appliance aus.
- 8 Wählen Sie einen Datenspeicher für die Dateien der NSX Edge-Appliance aus.
- 9 Akzeptieren Sie die Standardkompatibilität für Ihre NSX Edge-VM.
- 10 Wählen Sie die unterstützten ESXi-Betriebssysteme für Ihre NSX Edge-VM aus.
- 11 Konfigurieren Sie die virtuelle Hardware.
  - Neue Festplatte – **200 GB**
  - Neues Netzwerk – **VM-Netzwerk**
  - Neues CD/DVD-Laufwerk – **ISO-Datei für Datenspeicher**

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

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

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

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

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

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

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

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

---

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

---

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

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

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

---

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

---

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

---

**Hinweis** Wenn der Server Mellanox-Netzwerkkarten verwendet, konfigurieren Sie den Edge nicht in der In-Band-Verwaltungsschnittstelle.

---

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

(DHCP) `set interface eth0 dhcp plane mgmt`

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

- Schnittstelle mit Tagging.

`set interface eth0 vlan <vlan_ID> plane mgmt`

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

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

- In-Band-Schnittstelle.

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

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

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

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

**18** Führen Sie den Befehl `get interface eth0` (ohne VLAN) oder `get interface eth0.<vlan_ID>` (mit einem VLAN) aus, um zu überprüfen, ob die IP-Adresse erwartungsgemäß angewendet wurde.

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

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

---

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

---

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

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

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

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

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

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

## 21 Beheben Sie Konnektivitätsprobleme.

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

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

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

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

### Nächste Schritte

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

## Bare-Metal-Installation von NSX Edge

Verwenden Sie den PXE-Server, um die Installation von NSX Edge auf einem Bare Metal-Server zu automatisieren oder verwenden Sie die ISO-Datei, um NSX Edge als VM-Appliance oder auf einem Bare Metal-Server zu installieren.

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

### Voraussetzungen

- Wenn der NSX Edge-Bare Metal-Server Version 6.7u3 oder früher ausgeführt wird, führen Sie kein Upgrade von NSX Edge `virtualHW.version` auf **14** oder höher in vCenter Server durch. Für `virtualHW.version` ist standardmäßig **13** festgelegt.
- NSX Edge-Bare Metal-Bond-Geräte, die Ethernetgeräte zu einer LAG aggregieren, werden standardmäßig für das Load Balancing optimiert. So verwendet ein Bond-Gerät nur Netzwerkgeräte, die sich auf einem lokalen NUMA-Knoten befinden, dessen CPU Pakete überträgt. Wenn die den Bond bildenden Geräte mehrere NUMA-Knoten umfassen, die



der Paketverarbeitung zugeteilten CPUs jedoch zu einer Teilmenge der NUMA-Knoten gehören, versenden nur einige der Geräte Datenverkehr. Es werden also nicht alle Geräte für den Ausgleich des Datenverkehrs verwendet, der vom Bond-Gerät gesendet wird. Die Standardoptimierung kann nicht deaktiviert werden.

Wenn Sie jedoch alle Ethernetgeräte des Bonds für den Ausgleich des Datenverkehrs verwenden möchten, müssen Sie alle Ethernetgeräte auf die NUMA-Knoten verschieben, an die die CPUs für die Paketverarbeitung angehängt sind.

---

**Hinweis** Ein Failover ist exklusiv für Load Balancing. Wenn das an den lokalen NUMA-Knoten angehängte Ethernetgerät ausfällt, sendet der Bond den Datenverkehr an das andere Gerät, auch wenn es nicht NUMA-lokal ist. Die Optimierung des Lastausgleichs hat keine Auswirkung auf die Failover-Funktionalität.

---

## Vorbereiten des PXE-Servers für NSX Edge

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-Installationsanforderungen](#).

## Verfahren

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

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

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

```
nsxcli.install
```

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

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

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

Um das Kennwort des Admin-Benutzers zu ändern:

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

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

So verbinden Sie NSX Edge mit der Management Plane:

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

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

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

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

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

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

```

dns-nameservers 192.168.110.10

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

```

- 3 Installieren Sie DHCP-Serversoftware.

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

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

```
INTERFACES="eth1"
```

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

```

...
authoritative;
...

```

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

Beispiel:

```

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

```

- 7 Starten Sie den DHCP-Dienst.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```
d-i passwd/root-password-crypted password $6$tmLNLMP$9BuAHn...
```

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

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

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

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

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

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

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

```
allow booting;
allow bootp;

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

- 19** Starten Sie den DHCP-Dienst neu.

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

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

#### Nächste Schritte

Installieren Sie NSX Edge mithilfe einer ISO-Datei auf einer Bare-Metal-Bereitstellung. Siehe [Automatisches Installieren von NSX Edge via ISO-Datei](#).

## Automatisches Installieren von NSX Edge via ISO-Datei

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-Installationsanforderungen](#).

#### Verfahren

- 1** Wechseln Sie zu Ihrem MyVMware-Konto ([myvmware.com](https://myvmware.com)) und navigieren Sie zu **VMware NSX-T Data Center > Downloads**.
- 2** Suchen Sie die ISO-Datei für NSX Edge für Bare Metal und laden Sie sie herunter.
- 3** Sie können sich bei der Out-of-Band-Verwaltungsschnittstelle von Bare Metal anmelden (z. B. Integrated Lights Out (ILO) auf HP Servern).
- 4** Klicken Sie in der Vorschau der virtuellen Konsole auf **Starten**.
- 5** Wählen Sie **Virtuelle Medien > Virtuelle Medien verbinden** aus.

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

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

**7** Wählen Sie **Nächster Start > Virtuelle CD/DVD/ISO** aus.

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

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

**9** Wählen Sie **Automatisierte Installation**.

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

**10** Wählen Sie die anwendbare primäre Netzwerkschnittstelle aus.

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

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

**11** 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.

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

---

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

---

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

**14** Es gibt drei Möglichkeiten, eine Verwaltungsschnittstelle zu konfigurieren.

---

**Hinweis** Wenn der Server Mellanox-Netzwerkkartenkarten verwendet, konfigurieren Sie den Edge nicht in der In-Band-Verwaltungsschnittstelle.

---

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

(DHCP) `set interface eth0 dhcp plane mgmt`

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

- Schnittstelle mit Tagging.

`set interface eth0 vlan <vlan_ID> plane mgmt`

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

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

- In-Band-Schnittstelle.

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

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

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

- (Optional) Erstellen Sie eine **bond0**-Schnittstelle für die Verwaltungs-/HA-Schnittstelle mit mehreren Schnittstellen.

Sie können mithilfe der folgenden Befehlszeilenanweisung eine Verwaltungsschnittstelle für die Bindung einer NSX Edge konfigurieren. Verwenden Sie die Konsole, um die vorhandene Verwaltungs-IP zu löschen, bevor Sie eine Bindung erstellen und ihr eine Schnittstelle hinzufügen.

**Hinweis** Bei Bond-Schnittstellen ist nur der aktive Sicherungsmodus zulässig. Sie können VLAN nicht konfigurieren. Daher müssen Sie VLAN auf eine Zugriffs-VLAN konfigurieren, die sich näher am physischen Switch befindet.

```
set interface bond0 ip x.x.x.x/mask gateway x.x.x.x plane mgmt mode active-backup members eth0, eth1 primary eth0
```

- 15 Führen Sie den Befehl `get interface eth0` (ohne VLAN) oder `get interface eth0.<vlan_ID>` (mit einem VLAN) aus, um zu überprüfen, ob die IP-Adresse erwartungsgemäß angewendet wurde.

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

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

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

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

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

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

- 17 Legen Sie in der Liste der verfügbaren PCI-Geräte die von der NSX-T Data Center-Datenebene zu verwendenden physischen Netzwerkkarten fest.

```
a get dataplace device list
```



- b `set dataplane device list <NIC1>, <NIC2>, <NIC3>`
- c `restart service dataplane`
- d `get physical-port`

Starten Sie nach der Auswahl der physischen Netzwerkkarten die Dienste auf NSX-T Data Center-Datenebene neu, damit die Änderungen wirksam werden.

---

**Hinweis** Beanspruchen Sie bis zu 16 physische Netzwerkkarten.

---

- 18** Stellen Sie zur Vermeidung von Netzwerkkonfigurationsfehlern sicher, dass die ausgewählten physischen Netzwerkkarten mit den in den Transportknotenprofilen konfigurierten NICs übereinstimmen.

- 19** Bevor Sie NSX Edge als Transportknoten erstellen, setzen Sie die NIC-Liste auf Datenebene zurück.

`reset dataplane nic list`

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

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

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

- 21** Beheben Sie Konnektivitätsprobleme.

---

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

---

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

- a Melden Sie sich bei der Befehlszeilenschnittstelle (CLI) an, und geben Sie den Befehl **stop service dataplane** ein.
- b Geben Sie den Befehl **set interface *Schnittstelle* dhcp plane mgmt** ein.

- c Platzieren Sie die *Schnittstelle* im DHCP-Netzwerk und warten Sie, bis dieser *Schnittstelle* eine IP-Adresse zugewiesen wurde.
- d Geben Sie den Befehl **start service dataplane** ein.

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

### Nächste Schritte

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

## Interaktives Installieren von NSX Edge via ISO-Datei

Installieren Sie NSX Edge-Geräte auf Bare Metal mithilfe einer ISO-Datei im interaktiven Modus.

### Voraussetzungen

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

### Verfahren

- 1 Wechseln Sie zu Ihrem MyVMware-Konto ([myvmware.com](https://myvmware.com)) und navigieren Sie zu **VMware NSX-T Data Center > Downloads**.
- 2 Suchen Sie die ISO-Datei für NSX Edge für Bare Metal und laden Sie sie herunter.
- 3 Melden Sie sich beim ILO der Bare-Metal-Bereitstellung an.
- 4 Klicken Sie in der Vorschau der virtuellen Konsole auf **Starten**.
- 5 Wählen Sie **Virtuelle Medien > Virtuelle Medien verbinden** aus.  
Warten Sie einige Sekunden, bis die virtuellen Medien eine Verbindung hergestellt haben.
- 6 Wählen Sie **Virtuelle Medien > CD/DVD zuordnen** aus und navigieren Sie zur ISO-Datei.
- 7 Wählen Sie **Nächster Start > Virtuelle CD/DVD/ISO** aus.
- 8 Wählen Sie **Einschalten > System zurücksetzen (Warmstart)** aus.  
Die Installationsdauer richtet sich nach der Bare-Metal-Umgebung.
- 9 Wählen Sie **Interaktives Installieren** aus.  
Nach dem Drücken der Eingabetaste kann es zu einer Verzögerung von 10 Sekunden kommen.
- 10 Wählen Sie im Fenster „Tastatur konfigurieren“ **Ja** aus, wenn das Installationsprogramm die Tastatur automatisch erkennen muss oder wählen Sie **Nein** aus, wenn die Tastatur nicht von der Konsole erkannt werden darf.

- 11 Wählen Sie „Deutsch“ als Sprache aus.
- 12 Wählen Sie im Fenster „Netzwerk konfigurieren“ die entsprechende primäre Netzwerkschnittstelle aus.
- 13 Geben Sie den Hostnamen ein, der mit der ausgewählten primären Schnittstelle verbunden wird und klicken Sie auf **OK**.

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**.

- 14 Im Fenster „NSX-Appliance mit Kickstart konfigurieren“:
  - Geben Sie die URL der NSX-Kickstart-Konfigurationsdatei ein, wenn Sie die NSX-Konfiguration auf dem Bare Metal-Server automatisieren möchten.
  - Lassen Sie das Feld leer, wenn Sie NSX auf dem Bare Metal-Server manuell konfigurieren möchten.
- 15 Wählen Sie im Fenster „Partitionsdatenträger“ eine der folgenden Optionen aus:
  - Wählen Sie **Ja** aus, wenn Sie die Bereitstellung vorhandener Partitionen aufheben möchten, sodass neue Partitionen auf Datenträgern erstellt werden können.
  - Wählen Sie **Nein** aus, wenn Sie vorhandene Partitionen verwenden möchten.
- 16 Nachdem der NSX Edge gestartet ist, melden Sie sich bei der CLI mit Admin-Anmeldedaten an.

---

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

---

- 17 Führen Sie den Befehl `get interface eth0` (ohne VLAN) oder `get interface eth0.<vlan_ID>` (mit einem VLAN) aus, um zu überprüfen, ob die IP-Adresse erwartungsgemäß angewendet wurde.

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

```
Interface: eth0.100
Address: 192.168.110.37/24
MAC address: 00:50:56:86:62:4d
```

```
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

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

## 18 Beheben Sie Konnektivitätsprobleme.

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

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

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

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

### Nächste Schritte

Wenn Sie NSX Edge nicht mit der Management Plane verknüpft haben, schlagen Sie unter [Verbinden von NSX Edge mit der Management Plane](#) nach.

## Verbinden von NSX Edge mit der Management Plane

Durch Verbinden der NSX Edges mit der Management Plane 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 oder Konsolensitzung mit einer der NSX Manager-Appliances.
- 2 Öffnen Sie eine SSH- oder Konsolensitzung auf der NSX Edge-Knoten-VM.
- 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
659442c1435350edbbcb0e87ed5a6980d892b9118f851c17a13ec76a8b985f57
```

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

Geben Sie die folgenden Informationen an:

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

```
NSX-Edge1> join management-plane <Manager-IP> thumbprint <Manager-thumbprint> username admin
```

Wiederholen Sie diesen Befehl auf jeder NSX Edge-Knoten-VM.

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

```
nsx-edge-1> get managers
- 10.173.161.17 Connected (NSX-RPC)
- 10.173.161.140 Connected (NSX-RPC)
- 10.173.160.204 Connected (NSX-RPC)
```

- 6 Navigieren Sie in der NSX Manager-Benutzeroberfläche zu **System > Fabric > Knoten > Edge-Transportknoten**.

Auf der Seite „NSX Edge-Transportknoten“:

- In der Spalte **Konfigurationszustand** wird **NSX konfigurieren** angezeigt. Klicken Sie auf **NSX konfigurieren**, um mit der Konfiguration auf dem Knoten zu beginnen. Wenn in der Spalte **NSX-Version** die auf dem Knoten installierte Versionsnummer nicht angezeigt wird, versuchen Sie, das Browserfenster zu aktualisieren.

- Bevor Sie NSX auf dem NSX Edge-Knoten konfigurieren, wird in den Spalten **Knotenstatus** und **Tunnelstatus** der Zustand **Nicht verfügbar** angezeigt. In den Spalten **Transportzonen** und **N-VDS-Switches** wird der Wert **0** angezeigt. Dies deutet darauf hin, dass keine Transportzonen angehängt oder keine N-VDS-Switches auf dem NSX Edge-Knoten konfiguriert sind.

### Nächste Schritte

Schlagen Sie bei der Installation von NSX Edge mit NSX Manager unter [Erstellen eines NSX Edge-Transportknotens](#) nach.

Wenn Sie NSX Edge manuell installieren, schlagen Sie unter [Konfigurieren von NSX Edge als Transportknoten](#) nach.

## Konfigurieren von NSX Edge als Transportknoten

Nach der manuellen Installation von NSX Edge für ESXi oder Bare Metal konfigurieren Sie ein NSX Edge auf dem NSX-T Data Center-Fabric als Transportknoten.

Ein Transportknoten ist ein Knoten, der an einem NSX-T Data Center-Overlay oder NSX-T Data Center-VLAN-Networking teilnehmen kann. Jeder Knoten kann als Transportknoten dienen, wenn er einen N-VDS enthält. Solche Knoten umfassen, sind jedoch nicht beschränkt auf NSX Edges.

Ein NSX Edge kann zu einer Overlay-Transportzone und mehreren VLAN-Transportzonen gehören. Wenn eine VM Zugriff auf die Außenwelt erfordert, muss das NSX Edge zu derselben Transportzone gehören, zu der auch der logische Switch der VM gehört. Im Allgemeinen gehört das NSX Edge zu mindestens einer VLAN-Transportzone, um den Uplink-Zugriff bereitzustellen.

### Voraussetzungen

- Transportzonen müssen konfiguriert sein.
- Stellen Sie sicher, dass der Compute Manager konfiguriert ist. Siehe [Hinzufügen eines Compute Managers](#).
- Ein Uplink-Profil muss konfiguriert sein. Alternativ können Sie auch das standardmäßige Uplink-Profil für Bare-Metal-NSX Edge-Knoten verwenden.
- Ein IP-Pool muss konfiguriert sein, oder in der Netzwerkbereitstellung verfügbar sein.
- Mindestens eine nicht verwendete physische Netzwerkkarte (NIC) muss auf dem Host- oder NSX Edge-Knoten verfügbar sein.

### Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **System > Fabric > Knoten > Edge-Transportknoten > Edge bearbeiten** aus.
- 3 Wählen Sie den Edge-Knoten aus und klicken Sie auf **Bearbeiten**.

- 4 Wählen Sie die Transportzonen aus, zu denen dieser Transportknoten gehört.

Ein NSX Edge-Transportknoten gehört zu mindestens zwei Transportzonen, einem Overlay für NSX-T Data Center-Konnektivität und einem VLAN für Uplink-Konnektivität.

**Hinweis** Mehrere VTEPs in einer Transportzone müssen für dasselbe Netzwerksegment konfiguriert sein. Wenn VTEPs in einer Transportzone für unterschiedliche Netzwerksegmente konfiguriert sind, können keine BFD-Sitzungen zwischen den VTEPs eingerichtet werden.

- 5 Geben Sie die N-VDS-Informationen ein.

Option	Beschreibung
<b>Edge-Switchname</b>	Wählen Sie im Dropdown-Menü einen VLAN-Switch aus.
<b>Uplink-Profil</b>	Wählen Sie ein Uplink-Profil im Dropdown-Menü aus. Die verfügbaren Uplinks hängen von der Konfiguration im gewählten Uplink-Profil ab.
<b>IP-Zuweisung</b>	Wählen Sie <b>IP-Pool verwenden</b> oder <b>Liste statischer IPs verwenden</b> für den Overlay-N-VDS aus. Diese IP-Adressen werden dem NSX Edge-Transportknoten als VTEPs zugewiesen. Mehrere VTEPs auf einem NSX Edge müssen sich im selben Subnetz befinden. <ul style="list-style-type: none"> <li>■ Wenn Sie <b>Liste statischer IPs verwenden</b> auswählen, müssen Sie eine Liste mit durch Kommas getrennte IP-Adressen, ein Gateway und eine Subnetzmaske angeben.</li> <li>■ Wenn Sie <b>IP-Pool verwenden</b> für die IP-Zuweisung ausgewählt haben, geben Sie den Namen des IP-Pools an.</li> </ul>
<b>DPDK-Fastpath-Schnittstellen/ virtuelle Netzwerkkarten (NICs)</b>	Wählen Sie den Datenpfadnamen für die Uplink-Schnittstelle aus.  <b>Hinweis</b> Um sicherzustellen, dass der Datenverkehr über logische Switches läuft, die mit benannten Teaming-Richtlinien konfiguriert sind, ordnen Sie alle Uplinks in der Standard-Teaming-Richtlinie physischen Netzwerkschnittstellen auf der NSX Edge-VM zu.

- 6 Überprüfen Sie den Verbindungsstatus auf der Seite **Transportknoten**.

Nach dem Hinzufügen des NSX Edge als Transportknoten ändert sich der Verbindungsstatus in 10-12 Minuten in Aktiv.

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

- 9 Nachdem ein NSX Edge-Knoten mithilfe von vCenter Server auf einen neuen Host migriert wurde, kann es vorkommen, dass die NSX Manager-UI veraltete Konfigurationsdetails (Berechnung, Datenspeicher, Netzwerk, SSH, NTP, DNS, Suchdomänen) der NSX Edge meldet. Um die aktuellsten Konfigurationsdetails von NSX Edge auf dem neuen Host zu erhalten, führen Sie den folgenden API-Befehl aus.

```
POST api/v1/transport-nodes/<transport-node-id>?
action=refresh_node_configuration&resource_type=EdgeNode
```

#### Nächste Schritte

Fügen Sie den NSX Edge-Knoten zu einem NSX Edge-Cluster hinzu. Siehe [Erstellen eines NSX Edge-Clusters](#).



# Transportzonen und Transportknoten

# 10

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

Dieses Kapitel enthält die folgenden Themen:

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

## Erstellen von Transportzonen

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

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

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

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

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

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

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

## Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **System > Fabric > Transportzonen > Hinzufügen** aus.
- 3 Geben Sie einen Namen für die Transportzone und optional eine Beschreibung ein.
- 4 Geben Sie einen Namen für den N-VDS ein.
- 5 Wählen Sie einen N-VDS-Modus aus.
  - **Standard**-Modus, der für alle unterstützten Hosts gilt
  - **Erweiterter Datenpfad** ist ein Netzwerk-Stack-Modus, der nur für Transportknoten des ESXi-Hosts in der Version 6.7 und höher gilt und zu einer Transportzone gehören kann.
- 6 Wenn der N-VDS-Modus „Standard“ gewählt wurde, wählen Sie einen Datenverkehrstyp. Die Optionen hierfür lauten **Overlay** und **VLAN**.
- 7 Wenn der N-VDS-Modus „Erweiterter Datenpfad“ gewählt wurde, wählen Sie einen Datenverkehrstyp. Die Optionen hierfür lauten **Overlay** und **VLAN**.

---

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

---

- 8 Geben Sie mindestens einen Namen für eine Uplink-Gruppierungsrichtlinie ein. Diese benannten Gruppierungsrichtlinien können von logischen Switches verwendet werden, die mit der Transportzone verbunden sind. Wenn die logischen Switches keine passende Gruppierungsrichtlinie finden, wird die standardmäßige Uplink-Gruppierungsrichtlinie verwendet.
- 9 Die neue Transportzone können Sie auf der Seite **Transportzonen** anzeigen.
- 10 (Optional) Stattdessen können Sie zum Anzeigen der neuen Transportzone auch den API-Aufruf GET `https://<nsx-mgr>/api/v1/transport-zones` verwenden.

```
{
  "cursor": "00369b661aed-1eaa-4567-9408-ccbcfe50b416tz-vlan",
```

```

"result_count": 2,
"results": [
  {
    "resource_type": "TransportZone",
    "description": "comp overlay transport zone",
    "id": "efd7f38f-c5da-437d-af03-ac598f82a9ec",
    "display_name": "tz-overlay",
    "host_switch_name": "overlay-hostswitch",
    "transport_type": "OVERLAY",
    "transport_zone_profile_ids": [
      {
        "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
        "resource_type": "BfdHealthMonitoringProfile"
      }
    ],
    "_create_time": 1459547126454,
    "_last_modified_user": "admin",
    "_system_owned": false,
    "_last_modified_time": 1459547126454,
    "_create_user": "admin",
    "_revision": 0,
    "_schema": "/v1/schema/TransportZone"
  },
  {
    "resource_type": "TransportZone",
    "description": "comp vlan transport zone",
    "id": "9b661aed-1eaa-4567-9408-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 eigenständigen Hosts oder Bare-Metal-Server-Transportknotens](#).

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

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

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

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

Kernel-IP-Routing-Tabelle:

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

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

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

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

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

## Verfahren

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

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

## Ergebnisse

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

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

## Nächste Schritte

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

# Erweiterter Datenpfad

Der erweiterte Datenpfad ist ein Netzwerk-Stack-Modus, der, wenn er konfiguriert ist, eine ausgezeichnete Netzwerkleistung bietet. Er ist in erster Linie NFV-Arbeitslasten vorgesehen, die durch die Nutzung der DPDK-Funktion Leistungsvorteile bieten.

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

Im Modus „Erweiterter Datenpfad“ werden beide Datenverkehrsmodi unterstützt:

- Overlay-Datenverkehr

## ■ VLAN-Datenverkehr

### Unterstützte VMkernel-Netzwerkarten

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

### Allgemeines Verfahren zum Konfigurieren des erweiterten Datenpfads

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

Die allgemeinen Schritte sind wie folgt:

- 1 Verwenden Sie NIC-Karten, welche den erweiterten Datenpfad unterstützen.  
Finden Sie im [VMware-Kompatibilitäts-Handbuch](#) Netzwerkarten, die den erweiterten Datenpfad unterstützen.  
Wählen Sie auf der Seite „VMware-Kompatibilitäts-Handbuch“ unter der Kategorie **E/A-Geräte ESXi 6.7**, E/A-Gerätetyp als **Netzwerk** und Funktion als **Erweiterter N-VDS-Datenpfad**.
- 2 Laden Sie die aktuellen NIC-Treiber von der [Seite „My VMware“](#) herunter und installieren Sie sie.
  - a Wechseln Sie zu **Treiber und Tools > Treiber-CDs**.
  - b Laden Sie Netzwerkkartentreiber herunter:  
 VMware ESXi 6.7 ixgben-ens 1.1.3 NIC Driver for Intel Ethernet Controllers 82599, x520, x540, x550, and x552 family  
 VMware ESXi 6.7 i40en-ens 1.1.3 NIC Driver for Intel Ethernet Controllers X710, XL710, XXV710, and X722 family
  - c Um den Host als ENS-Host zu verwenden, muss mindestens eine ENS-fähige NIC auf dem System verfügbar sein. Wenn keine ENS-fähigen NICs vorhanden sind, lässt die Management Plane nicht zu, dass den ENS-Transportzonen Hosts hinzugefügt werden.
  - d Listet den ENS-Treiber auf.  

```
esxcli software vib list | grep -E "i40|ixgben"
```
  - e Überprüfen Sie, ob die NIC den ENS-Datenpfadverkehr verarbeiten kann.

`esxcfg-nics -e`

Name	Driver	ENS Capable	ENS Driven	MAC Address	Description
vmnic0	ixgben	True	False	e4:43:4b:7b:d2:e0	Intel(R) Ethernet Controller X550
vmnic1	ixgben	True	False	e4:43:4b:7b:d2:e1	Intel(R) Ethernet Controller X550
vmnic2	ixgben	True	False	e4:43:4b:7b:d2:e2	Intel(R) Ethernet Controller X550
vmnic3	ixgben	True	False	e4:43:4b:7b:d2:e3	Intel(R) Ethernet Controller X550
vmnic4	i40en	True	False	3c:fd:fe:7c:47:40	Intel(R) Ethernet Controller X710/X557-AT 10GBASE-T
vmnic5	i40en	True	False	3c:fd:fe:7c:47:41	Intel(R) Ethernet Controller X710/X557-AT 10GBASE-T
vmnic6	i40en	True	False	3c:fd:fe:7c:47:42	Intel(R) Ethernet Controller X710/X557-AT 10GBASE-T
vmnic7	i40en	True	False	3c:fd:fe:7c:47:43	Intel(R) Ethernet Controller X710/X557-AT 10GBASE-T

- f Installieren Sie den ENS-Treiber.

```
esxcli software vib install -v file:///<DriverInstallerURL> --no-sig-check
```

- g Laden Sie alternativ den Treiber auf das System herunter und installieren Sie ihn.

```
wget <DriverInstallerURL>
```

```
esxcli software vib install -v file:///<DriverInstallerURL> --no-sig-check
```

- h Starten Sie den Host neu, um den Treiber zu laden. Fahren Sie mit dem nächsten Schritt fort.

- i Führen Sie zum Laden des Treibers die folgenden Schritte aus:

```
vmkload_mod -u i40en
```

```
ps | grep vmkdevmgr
```

```
kill -HUP "$(ps | grep vmkdevmgr | awk {'print $1'})"
```

```
ps | grep vmkdevmgr
```

```
kill -HUP <vmkdevmgrProcessID>
```

```
kill -HUP "$(ps | grep vmkdevmgr | awk {'print $1'})"
```

- j Um den ENS-Treiber zu deinstallieren, `esxcli software vib remove --vibname=i40en-ens --force --no-live-install`.

- 3 Erstellen Sie eine Uplink-Richtlinie.

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

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

Siehe [Erstellen von Transportzonen](#).

---

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

---

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

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

## „Load Balanced Source“-Teaming-Richtlinienmodus erkennt NUMA

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

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

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

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

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

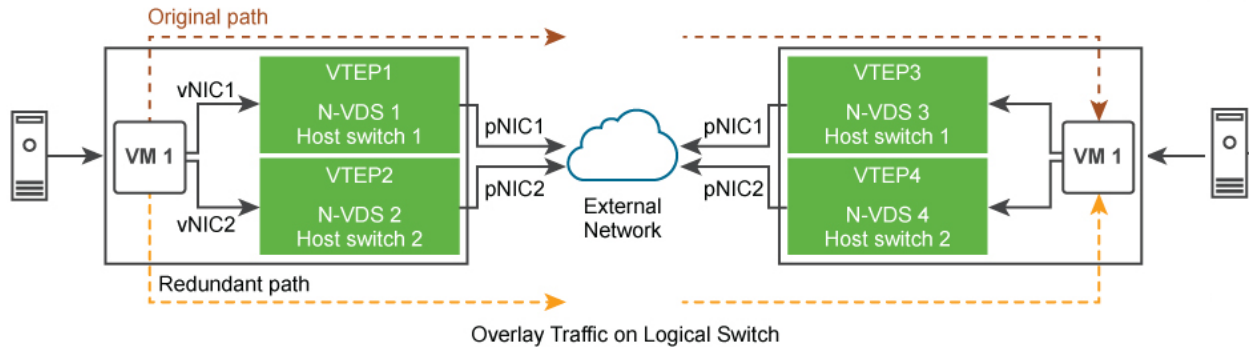
## ENS-Unterstützung für Anwendungen, für die ein zuverlässiger Datenverkehr erforderlich ist

NFV-Arbeitslasten verwenden möglicherweise Multi-Homing- und Redundanzfunktionen, die von SCTP (Stream Control Transmission Protocol) zur Verfügung gestellt werden, um die Stabilität und Zuverlässigkeit des Datenverkehrs für Anwendungen zu erhöhen. Multihoming ist die Fähigkeit, redundante Pfade von einer Quell-VM zu einem Ziel-VM zu unterstützen.



Je nach Anzahl der verfügbaren physischen Netzwerkkarten, die als Uplink für ein Overlay oder VLAN-Netzwerk verwendet werden sollen, sind viele redundante Netzwerkpfade für eine VM zum Senden von Datenverkehr über die Ziel-VM verfügbar. Die redundanten Pfade werden verwendet, wenn die angeheftete pNIC mit einem logischen Switch fehlschlägt. Der Switch im Modus „Erweiterter Datenpfad“ bietet redundante Netzwerkpfade zwischen den Hosts.

**Abbildung 10-1. Multi-Homing und Redundanz des Datenverkehrs über ENS**



Die allgemeinen Aufgaben sehen wie folgt aus:

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

Der N-VDS im erweiterten Datenpfad-Modus gewährleistet, dass bei einem Ausfall von pNIC1 Datenverkehr von VM 1 über den redundanten Pfad (vNIC 1 → Tunnel-Endpoint 2 → pNIC 2 → VM 2) geleitet wird.

## Konfigurieren von Profilen

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

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 Profilen angeben. Diese können Sie dann über mehrere Hosts oder Knoten hinweg anwenden.

## Erstellen eines Uplink-Profiles

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

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

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

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

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

#### Voraussetzungen

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

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

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

#### Verfahren

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

### 3 Vervollständigen Sie die Details des Uplink-Profiles.

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

Option	Beschreibung
	<ul style="list-style-type: none"> <li>■ <b>MAC-Adresse der Load Balance-Quelle:</b> Es wird ein Uplink basierend auf einem Hash des Quell-Ethernets ausgewählt.</li> </ul>
	<p><b>Hinweis</b></p> <ul style="list-style-type: none"> <li>■ Auf KVM-Hosts: Nur die Teaming-Richtlinie für die Failover-Reihenfolge wird unterstützt, während die Teaming-Richtlinien für die Load Balance-Quelle und die MAC der Load Balance-Quelle nicht unterstützt werden.</li> <li>■ Auf NSX Edge: Für die Standard-Teaming-Richtlinie werden die Teaming-Richtlinien für die Load Balance-Quelle und die Failover-Reihenfolge unterstützt. Für die benannte Teaming-Richtlinie wird nur die Richtlinie für die Failover-Reihenfolge unterstützt.</li> <li>■ Auf ESXi-Hosts: Die Teaming-Richtlinien für die MAC der Load Balance-Quelle, die Load Balance-Quelle und die Failover-Reihenfolge werden unterstützt.</li> </ul>
	<p>(ESXi-Hosts und NSX Edge) Sie können die folgenden Richtlinien für eine Transportzone definieren:</p> <ul style="list-style-type: none"> <li>■ Eine benannte Gruppierungsrichtlinie für jeden VLAN-basierten, logischen Switch oder das Segment.</li> <li>■ Eine Standard-Gruppierungsrichtlinie für den gesamten N-VDS.</li> </ul> <p>Benannte Gruppierungsrichtlinie: Eine benannte Gruppierungsrichtlinie bedeutet, dass Sie für jeden VLAN-basierten, logischen Switch bzw. für jedes VLAN-basierte, logische Segment einen bestimmten Gruppierungsrichtlinienmodus und Uplink-Namen definieren können. Dieser Richtlinientyp bietet Ihnen die Möglichkeit, bestimmte Uplinks je nach Richtlinie zur Datenverkehrslenkung auszuwählen, z. B. basierend auf der Bandbreitenanforderung.</p> <ul style="list-style-type: none"> <li>■ Wenn Sie eine benannte Gruppierungsrichtlinie definieren, verwendet N-VDS diese benannte Gruppierungsrichtlinie, wenn sie an die VLAN-basierte Transportzone angehängt und schließlich für den spezifischen VLAN-basierten, logischen Switch bzw. das VLAN-basierte, logische Segment im Host ausgewählt wird.</li> <li>■ Wenn Sie keine benannten Gruppierungsrichtlinien definieren, verwendet N-VDS die Standard-Gruppierungsrichtlinie.</li> </ul>

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

- 5 Geben Sie den MTU-Wert ein.

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

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

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

## Ergebnisse

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

## Nächste Schritte

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

## Konfigurieren von Network I/O Control-Profilen

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

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

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

---

**Hinweis** NIOC-Profile können nicht auf NSX Edge-Transportknoten angewendet werden.

---

## Bandbreitengarantie für Systemdatenverkehr

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

## Bandbreitenzuteilung für Systemdatenverkehr

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

- Verwaltungsdatenverkehr: Datenverkehr für die Hostverwaltung

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

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

## Bandbreitenzuteilungsparameter für Systemdatenverkehr

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

Zuteilungsparameter für Systemdatenverkehr

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

---

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

---

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

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

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

### Verfahren

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

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

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

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

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

### Verfahren

- 1 Stellen Sie eine Anfrage an den Host, um sowohl system- als auch benutzerdefinierte Host-Switch-Profile anzuzeigen.

**2** GET [https://<nsx-mgr>/api/v1/host-switch-profiles?include\\_system\\_owned=true](https://<nsx-mgr>/api/v1/host-switch-profiles?include_system_owned=true).

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

```
{
  "description": "This profile is created for Network I/O Control (NIOC).",
  "extends": {
    "$ref": "BaseHostSwitchProfile"+
  },
  "id": "NiocProfile",
  "module_id": "NiocProfile",
  "polymorphic-type-descriptor": {
    "type-identifier": "NiocProfile"
  },
  "properties": {
    "_create_time": {
      "$ref": "EpochMsTimestamp"+,
      "can_sort": true,
      "description": "Timestamp of resource creation",
      "readonly": true
    },
    "_create_user": {
      "description": "ID of the user who created this resource",
      "readonly": true,
      "type": "string"
    },
    "_last_modified_time": {
      "$ref": "EpochMsTimestamp"+,
      "can_sort": true,
      "description": "Timestamp of last modification",
      "readonly": true
    },
    "_last_modified_user": {
      "description": "ID of the user who last modified this resource",
      "readonly": true,
      "type": "string"
    },
    "_links": {
      "description": "The server will populate this field when returning the resource. Ignored on PUT
and POST.",
      "items": {
        "$ref": "ResourceLink"+
      },
      "readonly": true,
      "title": "References related to this resource",
      "type": "array"
    },
    "_protection": {
      "description": "Protection status is one of the following:
        PROTECTED – the client who retrieved the entity is not allowed to modify it.
        NOT_PROTECTED – the client who retrieved the entity is allowed to modify it
        REQUIRE_OVERRIDE – the client who retrieved the entity is a super user and can modify it,
```



```

    but only when providing the request header X-Allow-Overwrite=true.
    UNKNOWN – the _protection field could not be determined for this entity.",
    "readonly": true,
    "title": "Indicates protection status of this resource",
    "type": "string"
  },

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

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

  "_self": {
    "$ref": "SelfResourceLink+",
    "readonly": true,
    "title": "Link to this resource"
  },

  "_system_owned": {
    "description": "Indicates system owned resource",
    "readonly": true,
    "type": "boolean"
  },

  "description": {
    "can_sort": true,
    "maxLength": 1024,
    "title": "Description of this resource",
    "type": "string"
  },

  "display_name": {
    "can_sort": true,
    "description": "Defaults to ID if not set",
    "maxLength": 255,
    "title": "Identifier to use when displaying entity in logs or GUI",
    "type": "string"
  },

  "enabled": {
    "default": true,
    "description": "The enabled property specifies the status of NIOC feature.

```

When enabled is set to true, NIOC feature is turned on and the bandwidth allocations specified for the traffic resources are enforced.

When enabled is set to false, NIOC feature is turned off and no bandwidth allocation is guaranteed.

By default, enabled will be set to true.",

```

    "nsx_feature": "Nioc",
    "required": false,
    "title": "Enabled status of NIOC feature",
    "type": "boolean"
  },

  "host_infra_traffic_res": {
    "description": "host_infra_traffic_res specifies bandwidth allocation for various traffic
resources.",
    "items": {
      "$ref": "ResourceAllocation"+
    },
    "nsx_feature": "Nioc",
    "required": false,
    "title": "Resource allocation associated with NiocProfile",
    "type": "array"
  },

  "id": {
    "can_sort": true,
    "readonly": true,
    "title": "Unique identifier of this resource",
    "type": "string"
  },

  "required_capabilities": {
    "help_summary":
      "List of capabilities required on the fabric node if this profile is
used.
      The required capabilities is determined by whether specific features are enabled in the
profile.",
    "items": {
      "type": "string"
    },
    "readonly": true,
    "required": false,
    "type": "array"
  },

  "resource_type": {
    "$ref": "HostSwitchProfileType"+,
    "required": true
  },

  "tags": {
    "items": {
      "$ref": "Tag"+

```

```

    },

    "maxItems": 30,
    "title": "Opaque identifiers meaningful to the API user",
    "type": "array"
  }
},
"title": "Profile for Nioc",
"type": "object"
}

```

### 3 Erstellen Sie ein NIOC-Profil, wenn kein NIOC-Profil vorhanden ist.

POST <https://<nsx-mgr>/api/v1/host-switch-profiles>

```

{
  "description": "Specify limit, shares and reservation for all kinds of traffic.
  Values for limit and reservation are expressed in percentage. And for shares,
  the value is expressed as a number between 1-100.\n\nThe overall reservation among all traffic
  types should not exceed 75%.
  Otherwise, the API request will be rejected.",
  "id": "ResourceAllocation",
  "module_id": "NiocProfile",
  "nsx_feature": "Nioc",
  "properties": {
    "limit": {
      "default": -1.0,
      "description": "The limit property specifies the maximum bandwidth allocation for a given
      traffic type and is expressed in percentage. The default value for this
      field is set to -1 which means the traffic is unbounded for the traffic
      type. All other negative values for this property is not supported\n\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-c577aefe563a",
            "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 in der Datei `com.vmware.common.respools.cfg` aktualisiert wurden.

```
# [root@ host:] net-dvs -l
```

```

switch 1d 73 f5 58 99 7a 46 6a-9c cc d0 93 17 bb 2a 48 (vswitch)
max ports: 2560
global properties:

com.vmware.common.opaqueDvs = true ,      propType = CONFIG
com.vmware.nsx.kcp.enable = true ,        propType = CONFIG
com.vmware.common.alias = nsxvswitch ,    propType = CONFIG
com.vmware.common.uplinkPorts: uplink1   propType = CONFIG
com.vmware.common.portset.mtu = 1600, propType = CONFIG

```

```

com.vmware.etherswitch.cdp = LLDP, listen propType = CONFIG
com.vmware.common.respools.version = version3, propType = CONFIG
com.vmware.common.respools.cfg:
netsched.pools.persist.ft:0:50:-1:255
netsched.pools.persist.hbr:0:50:-1:255
netsched.pools.persist.vmotion:0:50:-1:255
netsched.pools.persist.vm:0:100:-1:255
netsched.pools.persist.iscsi:0:50:-1:255
netsched.pools.persist.nfs:0:50:-1:255
netsched.pools.persist.mgmt:0:50:-1:255
netsched.pools.persist.vdp:0:50:-1:255
netsched.pools.persist.vsan:0:50:-1:255
propType = CONFIG

```

## 6 Überprüfen Sie die NIOC-Profile im Host-Kernel.

```
# [root@ host:] /get /net/portsets/DvsPortset-1/ports/50335755/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 Überprüfen Sie die NIOC-Profilinformationen.

```
# [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
}

```

## Ergebnisse

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

## Hinzufügen eines NSX Edge-Cluster-Profiles

Das NSX Edge-Cluster-Profil definiert die Richtlinien für den NSX Edge-Transportknoten.

### Voraussetzungen

Stellen Sie sicher, dass der NSX Edge-Cluster verfügbar ist.

### Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **System > Fabric > Profile > Edge-Clusterprofile > Hinzufügen** aus.
- 3 Geben Sie die NSX Edge-Cluster-Profildetails ein.

Option	Beschreibung
<b>Name und Beschreibung</b>	Geben Sie einen Profilnamen für den NSX Edge-Cluster ein. Sie können optional die Profildetails wie z. B. die Einstellung für die bidirektionale Weiterleitungserkennung (BFD) eingeben.
<b>BFD-Prüfintervall</b>	Akzeptieren Sie die Standardeinstellung. BFD ist das Erkennungsprotokoll, das zur Identifizierung der Weiterleitungspfadfehler verwendet wird. Sie können das Intervall für BFD so festlegen, dass ein Weiterleitungspfadfehler erkannt wird.
<b>Für BFD zulässige Hops</b>	Akzeptieren Sie die Standardeinstellung. Sie können die Anzahl der Multihop-BFD-Sitzungen festlegen, die für das Profil zulässig sind.
<b>Dead Multiple für BFD deklarieren</b>	Akzeptieren Sie die Standardeinstellung. Sie können die Anzahl der Vorkommnisse festlegen, bei denen das BFD-Paket nicht eingegangen ist, bevor die Sitzung als ausgefallen markiert wird.
<b>Schwellenwert für Standby-Verlagerung</b>	Akzeptieren Sie die Standardeinstellung.

## Hinzufügen eines NSX Edge-Bridge-Profiles

Das NSX Edge-Bridge-Profil definiert die Richtlinien für den ESXi-Bridge-Cluster.

Ein Bridge-Cluster ist eine Sammlung von ESXi-Host-Transportknoten.

### Voraussetzungen

- Stellen Sie sicher, dass der NSX Edge-Cluster verfügbar ist.
- Stellen Sie sicher, dass der ESXi-Bridge-Cluster verfügbar ist.

### Verfahren

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

- 2 Wählen Sie **System > Fabric > Profile > Edge-Bridge-Profile > Hinzufügen** aus.
- 3 Geben Sie die NSX Edge-Cluster-Profildetails ein.

Option	Beschreibung
<b>Name und Beschreibung</b>	Geben Sie einen Profilnamen für den NSX Edge-Bridge-Cluster ein. Sie können optional die Profildetails wie z. B. die primären und die Backup-Knotendetails eingeben.
<b>Edge-Cluster</b>	Wählen Sie den NSX Edge-Cluster aus, den Sie verwenden möchten.
<b>Primärer Knoten</b>	Weisen Sie den bevorzugten NSX Edge-Knoten aus dem Cluster zu.
<b>Sicherungsknoten</b>	Weisen Sie den Backup-NSX Edge-Knoten zu, wenn der primäre Knoten fehlschlägt.
<b>Failover-Modus</b>	Wählen Sie entweder den Modus <b>Vorbeugend</b> oder <b>Nicht vorbeugend</b> aus. Die Standard-HA-Modus ist vorbeugend, wodurch der Datenverkehr verlangsamt werden kann, wenn der bevorzugte NSX Edge-Knoten wieder online geht. Der nicht vorbeugende Modus bewirkt keine Verlangsamung des Datenverkehrs.

## Hinzufügen eines Transportknotenprofils

Ein Transportknotenprofil erfasst die Konfiguration, die zum Erstellen eines Transportknotens erforderlich ist. Das Transportknotenprofil kann auf einen vorhandenen vCenter Server-Cluster zum Erstellen von Transportknoten für die Mitglieder-Hosts angewendet werden. Transportknotenprofile definieren Transportzonen, Mitglieder-Hosts, N-VDS-Switch-Konfiguration einschließlich Uplink-Profil, IP-Zuweisung, Zuordnung von physischen Netzwerkkarten zu virtuellen Uplink-Schnittstellen usw.

**Hinweis** Transportknoten-Profile müssen nicht auf NSX Edge-Transportknoten angewendet werden.

Die Transportknotenerstellung beginnt, wenn ein Transportknotenprofil auf ein vCenter Server-Cluster angewendet wird. NSX Manager bereitet die Hosts im Cluster vor und installiert die NSX-T Data Center-Komponenten auf allen Hosts. Transportknoten für die Hosts werden basierend auf der Konfiguration erstellt, die im Transportknotenprofil angegeben ist.

Um ein Transportknotenprofil zu löschen, müssen Sie zuerst das Profil vom zugehörigen Cluster trennen. Die bestehenden Transportknoten sind nicht betroffen. Neue Hosts, die zum Cluster hinzugefügt werden, werden nicht mehr automatisch in Transportknoten konvertiert.

Überlegung für die Erstellung von Transportknotenprofilen:

- Sie können maximal vier N-VDS-Switches für jede Konfiguration hinzufügen: erweitertes N-VDS, das für VLAN-Transportzonen erstellt wurde, Standard-N-VDS, das für Overlay-Transportzonen erstellt wurde, erweitertes N-VDS, das für Overlay-Transportzonen erstellt wurde.
- Es gibt keinen Grenzwert für die Anzahl der standardmäßigen N-VDS-Switches, die für die VLAN-Transportzone erstellt werden.



- In einer einzelnen Host-Cluster-Topologie, in der mehrere Standard-Overlay-N-VDS-Switches und Edge-VM auf demselben Host ausgeführt werden, bietet NSX-T Data Center Datenverkehrsisolierung, sodass Datenverkehr, der über den ersten N-VDS läuft, vom Datenverkehr, der über den zweiten N-VDS läuft, isoliert wird, usw. Die physischen Netzwerkkarten auf jedem N-VDS müssen der Edge-VM auf dem Host zugeordnet werden, sodass die Nord-Süd-Datenverkehrs-Konnektivität mit der Außenwelt ermöglicht wird. Pakete, die aus einer VM auf der ersten Transportzone verschoben werden, müssen über einen externen Router oder eine externe VM zur VM auf der zweiten Transportzone weitergeleitet werden.
- Jeder N-VDS-Switch-Name muss eindeutig sein. NSX-T Data Center lässt nicht die Verwendung von doppelten Switch-Namen zu.
- Jede Transportzonen-ID muss eindeutig sein. NSX-T Data Center lässt nicht die Verwendung von doppelten IDs zu.
- Sie können maximal 1000 Transportzonen zum Transportknotenprofil hinzufügen.
- Um eine Transportzone hinzuzufügen, muss sie von einem beliebigen N-VDS realisiert werden, das im Transportknotenprofil vorhanden ist.

#### Voraussetzungen

- Stellen Sie sicher, dass die Hosts Teil eines vCenter Server-Clusters sind.
- vCenter Server muss mindestens einen Cluster aufweisen.
- Stellen Sie sicher, dass eine Transportzone konfiguriert ist. Siehe [Erstellen von Transportzonen](#).
- Stellen Sie sicher, dass ein Cluster verfügbar ist. Siehe [Bereitstellen von NSX Manager-Knoten zur Bildung eines Clusters über die Benutzeroberfläche](#).
- Stellen Sie sicher, dass ein IP-Pool konfiguriert ist. Andernfalls muss DHCP in der Netzwerkbereitstellung verfügbar sein. Siehe [Erstellen eines IP-Pools für Tunnel-Endpoint-IP-Adressen](#).
- Stellen Sie sicher, dass ein Compute Manager konfiguriert ist. Siehe [Hinzufügen eines Compute Managers](#).

#### Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **System > Fabric > Profile > Transportknotenprofile > Hinzufügen** aus.
- 3 Geben Sie einen Namen für das Transportknotenprofil ein.  
Sie können optional die Beschreibung über das Transportknotenprofil hinzufügen.

- 4 Wählen Sie die verfügbaren Transportzonen aus und klicken Sie auf die Schaltfläche >, um die Transportzonen in das Transportknotenprofil aufzunehmen.

---

**Hinweis** Sie können mehrere Transportzonen hinzufügen.

---

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

Option	Beschreibung
<b>N-VDS-Name</b>	Wenn der Transportknoten an eine Transportzone angehängt ist, dann stellen Sie sicher, dass der eingegebene Name für den N-VDS identisch mit dem N-VDS-Namen ist, der in der Transportzone angegeben ist. Ein Transportknoten kann erstellt werden, ohne ihn zu einer Transportzone anzuhängen.
<b>Zugeordnete Transportzonen</b>	Zeigt die Transportzonen, die durch den zugeordneten Host-Switches realisiert werden. Sie können keine Transportzone hinzufügen, wenn sie nicht von einem beliebigen N-VDS im Transportknotenprofil realisiert wurde.
<b>NIOC-Profil</b>	Wählen Sie das NIOC-Profil im Dropdown-Menü aus. Die Bandbreitenzuteilungen aus dem Profil für die Datenverkehrsressourcen werden erzwungen.
<b>Uplink-Profil</b>	Wählen Sie im Dropdown-Menü ein vorhandenes Profil aus, oder erstellen Sie ein benutzerdefiniertes Uplink-Profil. Sie können auch das standardmäßige Uplink-Profil verwenden.
<b>LLDP-Profil</b>	Standardmäßig empfängt NSX-T nur LLDP-Pakete von einem LLDP-Nachbarn. NSX-T kann jedoch so eingestellt werden, dass LLDP-Pakete an einen LLDP-Nachbarn gesendet und LLDP-Pakete von einem LLDP-Nachbarn empfangen werden.
<b>IP-Zuweisung</b>	Wählen Sie <b>DHCP verwenden</b> , <b>IP-Pool verwenden</b> oder <b>Statische IP-Liste verwenden</b> , um eine IP-Adresse zu virtuellen Tunnel-Endpoints (VTEPs) des Transportknotens zuzuweisen. Wenn Sie <b>Liste statischer IPs verwenden</b> auswählen, müssen Sie eine Liste mit durch Komma getrennten IP-Adressen, ein Gateway und eine Subnetzmaske angeben. Alle VTEPs des Transportknotens müssen sich im selben Subnetz befinden. Andernfalls wird eine Sitzung mit bidirektionalem Flow (BFD) nicht aufgebaut.
<b>IP-Pool</b>	Wenn Sie <b>IP-Pool verwenden</b> für eine IP-Zuweisung ausgewählt haben, geben Sie den Namen des IP-Pools an.

Option	Beschreibung
<b>Physische Netzwerkkarten</b>	<p>Fügen Sie physische Netzwerkkarten zum Transportknoten hinzu. Sie können den standardmäßigen Uplink verwenden oder einen vorhandenen Uplink aus dem Dropdown-Menü zuweisen.</p> <p>Klicken Sie auf <b>PNIC hinzufügen</b>, um zusätzliche physische Netzwerkkarten zum Transportknoten zu konfigurieren.</p> <hr/> <p><b>Hinweis</b> Die Migration der physischen Netzwerkkarten, die Sie in diesem Feld hinzufügen, hängt davon ab, wie Sie <b>Migration nur von PNIC</b>, <b>Netzwerkzuordnungen für die Installation</b> und <b>Netzwerkzuordnungen für die Deinstallation</b> konfigurieren.</p> <hr/> <ul style="list-style-type: none"> <li>■ Um eine verwendete physische Netzwerkkarte (z. B. nach einem standardmäßigen vSwitch oder vSphere-Distributed Switch) ohne eine verbundene VMkernel-Zuordnung zu migrieren, stellen Sie sicher, dass <b>Migration nur von PNIC</b> aktiviert ist. Andernfalls bleibt der Transportknotenstatus <b>Teilweise erfolgreich</b>, und die Fabric-Knoten-LCP-Konnektivität kann nicht hergestellt werden.</li> <li>■ Um eine verwendete physische Netzwerkkarte mit einer verbundenen VMkernel-Netzwerkzuordnung zu migrieren, deaktivieren Sie <b>Migration nur von PNIC</b> und konfigurieren Sie die VMkernel-Netzwerkzuordnung.</li> <li>■ Um eine freie physische Netzwerkkarte zu migrieren, aktivieren Sie <b>Migration nur von PNIC</b>.</li> </ul> <hr/>

Option	Beschreibung
<b>Migration nur von PNIC</b>	<p>Vor dem Festlegen dieses Felds berücksichtigen Sie die folgenden Punkte:</p> <ul style="list-style-type: none"> <li>■ Bringen Sie in Erfahrung, ob die definierte physische Netzwerkkarte eine verwendete oder eine freie Netzwerkkarte ist.</li> <li>■ Bestimmen Sie, ob VMkernel-Schnittstellen eines Hosts zusammen mit physischen Netzwerkkarten migriert werden müssen.</li> </ul> <p>Legen Sie das Feld fest:</p> <ul style="list-style-type: none"> <li>■ Aktivieren Sie <b>Migration nur von PNIC</b>, wenn Sie nur physische Netzwerkkarten von einem VSS- oder DVS-Switch zu einem N-VDS-Switch migrieren möchten.</li> <li>■ Deaktivieren Sie <b>Migration nur von PNIC</b>, wenn Sie eine verwendete physische Netzwerkkarte und dessen zugeordnete VMkernel-Schnittstellenzuordnung migrieren möchten. Eine freie oder physische Netzwerkkarte ist an den N-VDS-Switch angehängt, wenn eine Migrationszuordnung für die VMkernel-Schnittstelle angegeben ist.</li> </ul> <p>Auf einem Host mit mehreren Host-Switches:</p> <ul style="list-style-type: none"> <li>■ Wenn alle Host-Switches nur PNICs migrieren sollen, können Sie PNICs in einem einzigen Vorgang migrieren.</li> <li>■ Wenn einige Hosts-Switches VMkernel-Schnittstellen migrieren sollen und die verbleibenden Host-Switches nur PNICs migrieren sollen: <ol style="list-style-type: none"> <li>1 Migrieren Sie im ersten-Vorgang nur PNICs.</li> <li>2 Migrieren Sie im zweiten Vorgang VMkernel-Schnittstellen. Stellen Sie sicher, dass <b>Migration nur von PNIC</b> deaktiviert ist.</li> </ol> </li> </ul> <p>Sowohl die Migration nur von PNIC als auch die VMkernel-Schnittstellenmigration werden nicht gleichzeitig über mehrere Hosts hinweg unterstützt.</p> <hr/> <p><b>Hinweis</b> Um die Netzwerkkarte eines Verwaltungsnetzwerks zu migrieren, konfigurieren Sie dessen zugeordnete VMkernel-Netzwerk-Zuordnung und lassen Sie <b>Migration nur von PNIC</b> deaktiviert. Wenn Sie nur die Management-Netzwerkkarte migrieren, verliert der Host die Verbindung.</p> <hr/> <p>Weitere Informationen finden Sie unter <a href="#">VMkernel-Migration auf einen N-VDS-Switch</a>.</p>

Option	Beschreibung
<b>Netzwerkzuordnungen für die Installation</b>	<p>Um VMkernels während der Installation zum N-VDS-Switch zu migrieren, ordnen Sie VMkernels einem vorhandenen logischen Switch zu. Der NSX Manager migriert den VMkernel zum zugeordneten logischen Switch auf N-VDS.</p> <p><b>Vorsicht</b> Stellen Sie sicher, dass die Management-Netzwerkkarte und die Verwaltungs-VMkernel-Schnittstelle auf einen logischen Switch migriert werden, der mit demselben VLAN verbunden ist, mit dem die Management-Netzwerkkarte vor der Migration verbunden war. Wenn vmnic &lt;n&gt; und VMkernel &lt;n&gt; auf ein anderes VLAN migriert werden, dann wird die Verbindung zum Host unterbrochen.</p> <p><b>Vorsicht</b> Stellen Sie bei angehefteten physischen Netzwerkkarten sicher, dass die Host-Switch-Zuordnung einer physischen Netzwerkkarte zu einer VMkernel-Schnittstelle mit der Konfiguration aus dem Transportknotenprofil übereinstimmt. Im Rahmen des Validierungsverfahrens überprüft NSX-T Data Center die Zuordnung, und wenn die Validierung bestanden wird, ist die Migration von VMkernel-Schnittstellen zu einem N-VDS-Switch erfolgreich. Es ist auch erforderlich, die Netzwerkzuordnung für Deinstallation zu konfigurieren, da NSX-T Data Center die Zuordnungskonfiguration des Host-Switch nicht speichert, nachdem die VMkernel-Schnittstellen zum N-VDS-Switch migriert wurden. Wenn die Zuordnung nicht konfiguriert ist, kann die Verbindung zu Diensten wie vSAN verloren gehen, nachdem die Migration wieder zurück zum VSS- oder VDS-Switch durchgeführt wurde.</p> <p>Weitere Informationen finden Sie unter <a href="#">VMkernel-Migration auf einen N-VDS-Switch</a>.</p>
<b>Netzwerkzuordnungen für die Deinstallation</b>	<p>Um die Migration des VMkernels während der Deinstallation wiederherzustellen, ordnen Sie VMkernels zu Portgruppen auf VSS oder DVS zu, sodass NSX Manager weiß, zu welcher Portgruppe der VMkernel auf dem VSS oder DVS wieder zurückmigriert werden muss. Stellen Sie bei einem DVS-Switch sicher, dass die Portgruppe den Typ Flüchtling aufweist.</p> <p><b>Vorsicht</b> Stellen Sie bei angehefteten physischen Netzwerkkarten sicher, dass die Transportknotenprofil-Zuordnung einer physischen Netzwerkkarte zu einer VMkernel-Schnittstelle mit der Konfiguration aus dem Host-Switch übereinstimmt. Es ist erforderlich, die Netzwerkzuordnung für Deinstallation zu konfigurieren, da NSX-T Data Center die Zuordnungskonfiguration des Host-Switch nicht speichert, nachdem die VMkernel-Schnittstellen zum N-VDS-Switch migriert wurden. Wenn die Zuordnung nicht konfiguriert ist, kann die Verbindung zu Diensten wie vSAN verloren gehen, nachdem die Migration wieder zurück zum VSS- oder VDS-Switch durchgeführt wurde.</p> <p>Weitere Informationen finden Sie unter <a href="#">VMkernel-Migration auf einen N-VDS-Switch</a>.</p>

- 6 Wenn Sie mehrere Transportzonen ausgewählt haben, klicken Sie erneut auf **+ N-VDS hinzufügen**, um den Switch für die anderen Transportzonen zu konfigurieren.
- 7 Klicken Sie auf **Fertigstellen**, um die Konfiguration abzuschließen.

## Nächste Schritte

Wenden Sie das Transportknotenprofil auf einen vorhandenen vSphere-Cluster an. Siehe [Konfigurieren eines verwalteten Host-Transportknotens](#).

## VMkernel-Migration auf einen N-VDS-Switch

Um VMkernel-Schnittstellen von einem VSS- oder DVS-Switch zu einem N-VDS-Switch auf Clusterebene zu migrieren, konfigurieren Sie das Transportknotenprofil mit für die Migration erforderlichen Netzwerkzuordnungsdetails (ordnen Sie VMkernel-Schnittstellen logischen Switches zu). Konfigurieren Sie analog die Transportknotenkonfiguration, um VMkernel-Schnittstellen auf einem Hostknoten zu migrieren. Um VMkernel-Schnittstellen wieder zurück zu einem VSS- oder DVS-Switch zu migrieren, konfigurieren Sie die Netzwerkzuordnung für die Deinstallation (Zuordnung von logischen Ports zur VMkernel-Schnittstelle) im Transportknotenprofil, das während der Deinstallation realisiert werden soll.

Während der Migration werden derzeit verwendete physische Netzwerkkarten auf einen N-VDS-Switch migriert, während verfügbare oder freie physische Netzwerkkarten nach der Migration an den N-VDS-Switch angehängt werden.

---

**Hinweis** Transportknotenprofile werden auf alle Hosts angewendet, die Mitglieder im betreffenden Cluster sind. Wenn Sie jedoch die Migration von VMkernel-Schnittstellen auf bestimmten Hosts einschränken möchten, können Sie den Host direkt konfigurieren. Nach der Migration verarbeitet N-VDS Datenverkehr im VLAN und Overlay-Netzwerk für die Schnittstellen, die mit dem N-VDS-Switch verbunden sind.

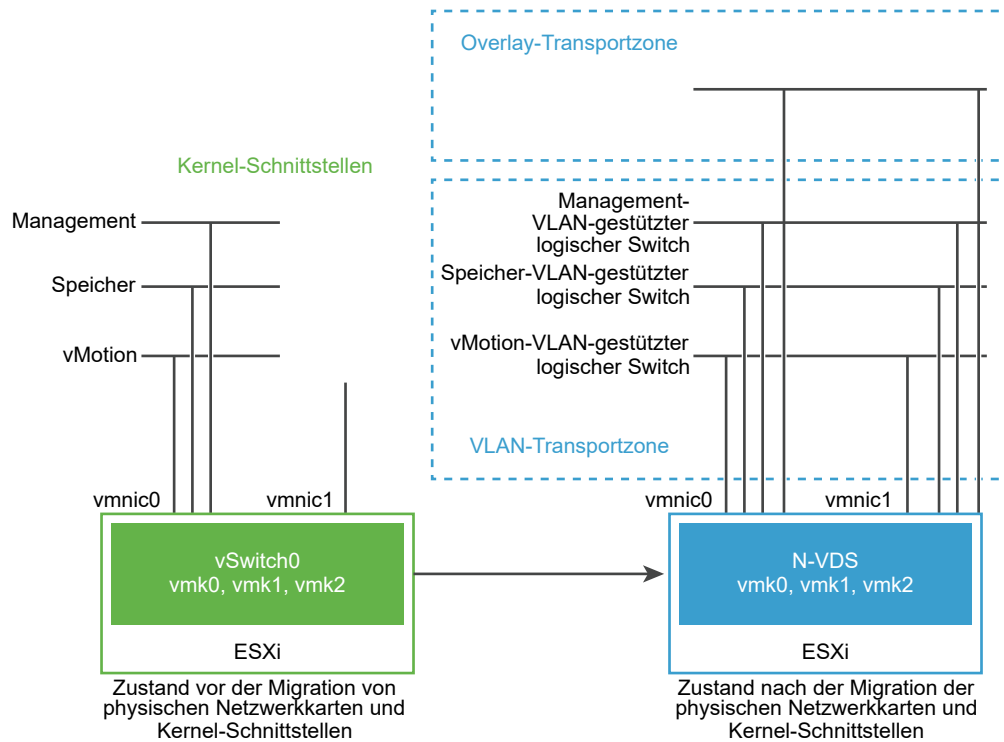
---

**Wichtig** Konfigurationen, die an einzelnen Hosts vorgenommen werden, werden mit dem Flag **Überschrieben** markiert. Weitere Aktualisierungen des Transportknotenprofils werden nicht auf diese überschriebenen Hosts angewendet. Diese Hosts bleiben im überschriebenen Zustand, bis NSX-T Data Center deinstalliert wird.

---

Wenn ein Host nur über zwei physische Netzwerkkarten verfügt, können Sie der Redundanz halber beide Netzwerkkarten dem N-VDS zuweisen, einschließlich der zugehörigen VMkernel-Schnittstellen, damit die Schnittstellen die Verbindung zum Host nicht verlieren. Dies ist in der folgenden Abbildung dargestellt.

Abbildung 10-2. Vor und nach der Migration der Netzwerkschnittstellen zu einem N-VDS



Vor der Migration verfügt der ESXi-Host über zwei Uplinks, die von zwei physischen Ports abgeleitet sind, vmnic0 und vmnic1. Hierbei ist vmnic0 für einen aktiven Zustand konfiguriert und an einen VSS angehängt, während vmnic1 nicht verwendet wird. Darüber hinaus sind drei VMkernel-Schnittstellen vorhanden: vmk0, vmk1 und vmk2.

VMkernel-Schnittstellen können Sie mithilfe der NSX-T Data Center Manager-Benutzeroberfläche oder der NSX-T Data Center-APIs migrieren. Siehe *Handbuch für die NSX-T Data Center-API*.

Nach der Migration werden die vmnic0, vmnic1 und deren VMkernel-Schnittstellen zum N-VDS-Switch migriert. Sowohl vmnic0 als auch vmnic1 sind über VLAN und Overlay-Transportzonen verbunden.

## Überlegungen für die VMkernel-Migration

- **PNIC- und VMkernel-Migration:** Bevor Sie angeheftete physische Netzwerkkarten und zugehörige VMkernel-Schnittstellen zu einem N-VDS-Switch migrieren, notieren Sie sich die Netzwerkzuordnung (Zuordnung physischer Netzwerkkarten zu Portgruppen) auf dem Host-Switch.
- **Migration nur von PNIC:** Wenn Sie nur PNICs migrieren möchten, stellen Sie sicher, dass die mit der VMkernel-Verwaltungsschnittstelle verbundene physische Verwaltungsnetzwerkkarte nicht migriert wird. Andernfalls wäre ein Verlust der Konnektivität mit dem Host die Folge. Weitere Informationen finden Sie im Feld **Migration nur von PNIC** unter [Hinzufügen eines Transportknotenprofils](#).

- Migration wiederherstellen: Bevor Sie die Migration von VMkernel-Schnittstellen zum VSS- oder DVS-Host-Switch für angeheftete physische Netzwerkkarten wiederherstellen möchten, stellen Sie sicher, dass Sie sich die Netzwerkzuordnung (Zuordnung der physischen Netzwerkkarte zur Portgruppe) auf dem Host-Switch notieren. Es ist zwingend erforderlich, das Transportknotenprofil mit der Host-Switch-Zuordnung im Feld **Netzwerkzuordnung für Deinstallation** zu konfigurieren. Ohne diese Zuordnung weiß NSX-T Data Center nicht, zu welchen Portgruppen die VMkernel-Schnittstellen zurückmigriert werden müssen. Diese Situation kann zu einem Verlust der Konnektivität mit dem vSAN-Netzwerk führen.
- vCenter Server-Registrierung vor der Migration: Wenn Sie vorhaben, einen VMkernel oder eine PNIC zu migrieren, die mit einem DVS-Switch verbunden sind, stellen Sie sicher, dass ein vCenter Server beim NSX Manager registriert ist.
- VLAN-ID-Übereinstimmung: Nach der Migration müssen sich die Verwaltungsnetzwerkkarte und die VMkernel-Verwaltungsschnittstelle auf demselben VLAN befinden, mit dem die Verwaltungsnetzwerkkarte vor der Migration verbunden war. Wenn vmnic0 und vmk0 mit dem Verwaltungsnetzwerk verbunden sind und zu einem anderen VLAN migriert werden, geht die Konnektivität mit dem Host verloren.
- Migration zu VSS-Switch: Zwei VMkernel-Schnittstellen können nicht zur gleichen Portgruppe eines VSS-Switch zurückmigriert werden.
- vMotion: Führen Sie vMotion aus, um VM-Arbeitslasten vor einer VMkernel- und/oder PNIC-Migration auf einen anderen Host zu verschieben. Wenn die Migration fehlschlägt, werden die Arbeitslast-VMs nicht beeinträchtigt.
- vSAN: Wenn der vSAN-Datenverkehr auf dem Host ausgeführt wird, versetzen Sie den Host über vCenter Server in den Wartungsmodus und verschieben Sie die VMs vor der VMkernel- und/oder PNIC-Migration mithilfe der vMotion-Funktion vom Host.
- Migration: Wenn ein VMkernel bereits mit einem Ziel-Switch verbunden ist, kann er weiterhin für die Migration zum selben Switch ausgewählt werden. Mit dieser Eigenschaft wird der VMK- und/oder PNIC-Migrationsvorgang idempotent. Dies ist hilfreich, wenn Sie nur PNICs zu einem Ziel-Switch migrieren möchten. Da für die Migration immer mindestens ein VMkernel und eine PNIC erforderlich sind, wählen Sie einen VMkernel aus, der bereits zu einem Ziel-Switch migriert wurde, wenn Sie nur PNICs zu einem Ziel-Switch migrieren. Wenn kein VMkernel migriert werden muss, erstellen Sie entweder auf dem Quell-Switch oder Ziel-Switch über vCenter Server einen temporären VMkernel. Migrieren Sie den temporären VMkernel zusammen mit den PNICs und löschen Sie ihn über vCenter Server, sobald die Migration abgeschlossen ist.
- Gemeinsame MAC-Nutzung: Wenn eine VMkernel-Schnittstelle und eine PNIC dieselbe MAC nutzen und sich auf demselben Switch befinden, müssen sie zusammen zum selben Ziel-Switch migriert werden, wenn sie beide nach der Migration verwendet werden. Behalten Sie vmk0 und vmnic0 immer auf demselben Switch bei.

Überprüfen Sie die MACs, die von allen VMKs und PNICs auf dem Host verwendet werden, indem Sie die folgenden Befehle ausführen:



```
esxcfg-vmknics -l
```

```
esxcfg-nics -l
```

- Nach der Migration erstellte logische VIF-Ports: Nachdem Sie VMkernel von einem VSS- oder DVS-Switch zu einem N-VDS-Switch migriert haben, wird ein logischer Switch Port des Typs VIF auf dem NSX Manager erstellt. Sie dürfen keine Regeln für verteilte Firewalls auf diesen logischen VIF-Switch-Ports erstellen.

## Migrieren von VMkernel-Schnittstellen zu einem N-VDS-Switch

Allgemeiner Workflow zum Migrieren von VMkernel-Schnittstellen zu einem N-VDS-Switch:

- 1 Erstellen Sie bei Bedarf einen logischen Switch.
- 2 Schalten Sie VMs auf dem Host aus, von dem VMkernel-Schnittstellen und PNICs auf einen N-VDS-Switch migriert werden.
- 3 Konfigurieren Sie ein Transportknotenprofil mit einer Netzwerkzuordnung, mit der die VMkernel-Schnittstellen während der Erstellung von Transportknoten migriert werden. Netzwerkzuordnung bedeutet die Zuordnung einer VMkernel-Schnittstelle zu einem logischen Switch.

Weitere Informationen finden Sie unter [Hinzufügen eines Transportknotenprofils](#).

- 4 Stellen Sie sicher, dass die Netzwerkadapterzuordnungen in vCenter Server eine neue Zuordnung des VMkernel-Switches zu einem N-VDS-Switch widerspiegeln. Überprüfen Sie bei angehefteten physischen Netzwerkkarten, ob die Zuordnung in NSX-T Data Center alle VMKernels widerspiegelt, die an eine physische Netzwerkkarte im vCenter Server angeheftet sind.
- 5 Gehen Sie in NSX Manager zu **Netzwerk und Sicherheit – Erweitert > Netzwerke > Switching**. Überprüfen Sie auf der Seite **Switches**, ob die VMkernel-Schnittstelle über einen neu erstellten logischen Port mit dem logischen Switch verbunden ist.
- 6 Wechseln Sie zu **System > Knoten > Host-Transportknoten**. Überprüfen Sie für jeden Transportknoten, ob als Status in der Spalte **Knotenstatus** „Erfolgreich“ angezeigt wird, um zu bestätigen, dass die Transportknotenkonfiguration erfolgreich validiert wurde.
- 7 Überprüfen Sie auf der Seite **Host-Transportknoten** ober als **Konfigurationszustand** „Erfolgreich“ angezeigt wird, um sicher zu sein, dass der Host mit der angegebenen Konfiguration erfolgreich realisiert wurde.

Nach der Migration von VMkernel-Schnittstellen und PNICs von einem VDS- zu einem N-VDS-Switch mithilfe der NSX-T-Benutzeroberfläche oder der Transportknoten-API zeigt vCenter Server Warnungen für den VDS an. Wenn der Host mit dem VDS verbunden werden muss, entfernen Sie den Host vom VDS. vCenter Server zeigt keine Warnung mehr für VDS an.

Weitere Informationen zu Fehlern, die während der Migration auftreten können, finden Sie unter [Fehler bei der VMkernel-Migration](#).

## Wiederherstellen der Migration von VMkernel-Schnittstellen zu einem VSS- oder DVS-Switch

Allgemeiner Workflow zum Wiederherstellen der Migration von VMkernel-Schnittstellen von einem N-VDS-Switch zu einem VSS- oder DVS-Switch während der Deinstallation von NSX-T Data Center:

- 1 Schalten Sie auf dem ESXi-Host VMs aus, die mit den logischen Ports verbunden sind, auf denen die VMkernel-Schnittstelle nach der Migration gehostet wird.
- 2 Konfigurieren Sie das Transportknotenprofil mit einer Netzwerkzuordnung, mit der die VMkernel-Schnittstellen während des Deinstallationsvorgangs migriert werden. Die Netzwerkzuordnung während der Deinstallation ordnet die VMkernel-Schnittstellen einer Portgruppe auf dem VSS- oder DVS-Switch auf dem ESXi-Host zu.

---

**Hinweis** Wenn Sie die Migration eines VMkernel zu einer Portgruppe auf einem DVS-Switch wiederherstellen, müssen Sie darauf achten, dass als Portgruppentyp **Flüchtig** festgelegt ist.

---

Weitere Informationen finden Sie unter [Hinzufügen eines Transportknotenprofils](#).

- 3 Stellen Sie sicher, dass die Netzwerkadapterzuordnungen in vCenter Server eine neue Zuordnung des VMkernel-Switches zu einer Portgruppe des VSS- oder DVS-Switches widerspiegeln.
- 4 Gehen Sie in NSX Manager zu **Netzwerk und Sicherheit – Erweitert > Netzwerke > Switching**. Überprüfen Sie auf der Seite **Switches**, ob der logische Switch, der VMkernel-Schnittstellen enthält, gelöscht wird.

Weitere Informationen zu Fehlern, die während der Migration auftreten können, finden Sie unter [Fehler bei der VMkernel-Migration](#).

## Aktualisieren der Host-Switch-Zuordnung

### Wichtig

- Statusbehaftete-Hosts: Hinzufügen und Aktualisieren werden unterstützt. Um eine vorhandene Zuordnung zu aktualisieren, können Sie der Netzwerkzuordnungskonfiguration einen neuen VMkernel-Schnittstelleneintrag hinzufügen. Wenn Sie die Netzwerkzuordnungskonfiguration einer VMkernel-Schnittstelle aktualisieren, die bereits zum N-VDS-Switch migriert wurde, wird die aktualisierte Netzwerkzuordnung auf dem Host nicht realisiert.
- Statusfreie Hosts: Hinzufügen, Aktualisieren und Entfernen werden unterstützt. Alle Änderungen, die Sie an der Netzwerkzuordnungskonfiguration vornehmen, werden nach dem Neustart des Hosts wirksam.

Um die VMkernel-Schnittstellen auf einen neuen logischen Switch zu aktualisieren, können Sie das Transportknotenprofil so bearbeiten, dass die Netzwerkzuordnungen auf Clusterebene angewendet werden. Wenn die Updates nur auf einen einzelnen Host angewendet werden sollen, konfigurieren Sie den Transportknoten mithilfe von APIs auf Hostebene.

---

**Hinweis** Nachdem Sie die Transportknotenkonfiguration für einen einzelnen Host aktualisiert haben, werden alle neuen Updates, die über das Transportknotenprofil angewendet werden, nicht auf diesen Host angewendet. Der Status dieses Hosts wechselt zu **Überschrieben**.

---

- 1 Um alle Hosts in einem Cluster zu aktualisieren, bearbeiten Sie das Feld **Netzwerkzuordnung während der Installation**, um die VMkernel-Zuordnung zu logischen Switches zu aktualisieren. Weitere Informationen finden Sie unter [Hinzufügen eines Transportknotenprofils](#).
- 2 Speichern Sie die Änderungen. Änderungen an einem Transportknotenprofil werden automatisch auf alle Mitgliedshosts des Clusters angewendet, außer auf Hosts, die mit dem Status **Überschrieben** gekennzeichnet sind.
- 3 Um einen einzelnen Host zu aktualisieren, bearbeiten Sie die VMkernel-Zuordnung in der Transportknotenkonfiguration.

---

**Hinweis** Wenn Sie das Feld **Netzwerkzuordnung während der Installation** mit einer neuen VMkernel-Zuordnung aktualisieren, muss dieselbe VMkernel-Schnittstelle dem Feld **Netzwerkzuordnung während der Deinstallation** hinzugefügt werden.

---

Weitere Informationen zu Fehlern, die während der Migration auftreten können, finden Sie unter [Fehler bei der VMkernel-Migration](#).

## Migrieren von VMkernel-Schnittstellen in einem statusfreien Cluster

- 1 Bereiten Sie einen Host vor und konfigurieren Sie ihn mithilfe von Transportknoten-APIs als Referenzhost.
- 2 Extrahieren Sie ein Hostprofil aus dem Referenzhost.
- 3 Wenden Sie das Hostprofil im vCenter Server auf den statusfreien Cluster an.

- 4 Wenden Sie in das Transportknotenprofil in NSX-T Data Center auf den statusfreien Cluster an.
- 5 Starten Sie jeden Host des Clusters neu.

Es kann einige Minuten dauern, bis die aktualisierten Zustände der Clusterhosts wirksam werden.

## Migrationsfehlerszenarien

- Wenn die Migration aus irgendeinem Grund fehlschlägt, versucht der Host drei Mal, die physischen Netzwerkkarten und VMkernel-Schnittstellen zu migrieren.
- Schlägt die Migration weiterhin fehl, stellt der Host die frühere Konfiguration wieder her, indem die VMkernel-Konnektivität mit der physischen Verwaltungsnetzwerkkarte (vmnic0) beibehalten wird.
- Falls die Wiederherstellung ebenfalls fehlschlägt, sodass der für die physische Verwaltungsnetzwerkkarte konfigurierte VMkernel verloren gegangen ist, müssen Sie den Host zurücksetzen.

## Nicht unterstützte Migrationsszenarien

Die folgenden Szenarien werden nicht unterstützt:

- VMkernel-Schnittstellen von zwei verschiedenen VSS- oder DVS-Switches werden gleichzeitig migriert.
- Auf statusbehafteten Hosts wird die Netzwerkzuordnung aktualisiert, um die VMkernel-Schnittstelle einem anderen logischen Switch zuzuordnen. Beispielsweise wird der VMkernel vor der Migration dem logischen Switch 1 zugeordnet und die VMkernel-Schnittstelle dem logischen Switch 2.

## Fehler bei der VMkernel-Migration

Beim Migrieren von VMkernel-Schnittstellen und physischen Netzwerkkarten von einem VSS- oder DVS-Switch auf einen N-VDS-Switch oder beim Rückmigrieren von Schnittstellen zu einem VSS- oder DVS-Host-Switch können Fehler auftreten.

Tabelle 10-1. Fehler bei der VMkernel-Migration

Fehlercode	Problem	Ursache	Lösung
8224	Der in der Konfiguration des Transportknotens angegebene Host-Switch kann nicht gefunden werden.	Die Host-Switch-ID kann nicht gefunden werden.	<ul style="list-style-type: none"> <li>■ Stellen Sie sicher, dass die Transportzone mit dem Host-Switch-Namen erstellt wurde, und erstellen Sie dann den Transportknoten.</li> <li>■ Stellen Sie sicher, dass ein gültiger Host-Switch in der Konfiguration des Transportknotens verwendet wird.</li> </ul>
8225	VMkernel-Migration wird durchgeführt.	Migration wird durchgeführt.	Warten Sie, bis die Migration abgeschlossen ist, bevor Sie eine andere Aktion durchführen.
8226	VMkernel-Migration wird nur auf einem ESXi-Host unterstützt.	Migration ist nur für ESXi-Hosts gültig.	Stellen Sie vor dem Starten der Migration sicher, dass es sich bei dem Host um einen ESXi-Host handelt.
8227	Der Host-Switch-Name wurde nicht an die VMkernel-Schnittstelle angehängt.	Auf einem Host mit mehreren Host-Switches kann NSX-T Data Center die Verknüpfung zwischen den VMkernel-Schnittstellen und den zugehörigen Host-Switches nicht erkennen.	<p>Wenn der Host mehrere N-VDS-Host-Switches aufweist, stellen Sie sicher, dass der Host-Switch-Name des N-VDS, mit dem der Host verbunden ist, an die VMkernel-Schnittstelle angehängt wird.</p> <p>Beispiel: Die Netzwerkzuordnung für die Deinstallation eines Hosts mit dem N-VDS-Host-Switch-Namen „nsxvswitch1“ und „VMkernel1“ und einem anderen N-VDS-Host-Switch-Namen „nsxvswitch2“ und „VMkernel2“ muss folgendermaßen definiert werden: <code>device_name: VMkernel1@nsxvswitch1</code>, <code>destination_network: DPortGroup</code>.</p>
8228	Im Feld <code>device_name</code> verwendeter Host-Switch wurde auf dem Host nicht gefunden.	Falscher Host-Switch-Name	Geben Sie den korrekten Host-Switch-Namen an.
8229	Die Transportzone des logischen Switches wurde im Transportknoten nicht angegeben.	Transportzone wurde nicht hinzugefügt.	Fügen Sie der Konfiguration des Transportknotens die Transportzone hinzu.

Tabelle 10-1. Fehler bei der VMkernel-Migration (Fortsetzung)

Fehlercode	Problem	Ursache	Lösung
8230	Keine physische Netzwerkkarte auf dem Host-Switch.	Mindestens eine physische Netzwerkkarte muss auf dem Host-Switch vorhanden sein.	Geben Sie mindestens eine physische Netzwerkkarte ein, um ein Uplink-Profil und die Konfiguration der VMkernel-Zuordnung mit einem logischen Switch zu verbinden.
8231	Host-Switch-Name stimmt nicht überein.	Der in vmk1@host_switch verwendete Host-Switch-Name stimmt nicht mit dem vom logischen Ziel-Switch der Schnittstelle verwendeten Host-Switch-Namen überein.	Stellen Sie sicher, dass der in der Konfiguration der Netzwerkzuordnung angegebene Host-Switch-Name mit dem vom logischen Switch der Schnittstelle verwendeten Namen übereinstimmt.
8232	Logischer Switch auf dem Host konnte nicht dargestellt werden.	Die Darstellung des logischen Switches auf dem Host war nicht erfolgreich.	Synchronisieren Sie den Host mit dem NSX Manager.
8233	Unerwarteter logischer Switch in der Netzwerkzuordnung der Schnittstelle.	In der Netzwerkzuordnung der Schnittstelle werden für die Installation und Deinstallation sowohl logische Switches als auch Portgruppen aufgelistet.	Die Netzwerkzuordnung für die Installation darf nur logische Switches als Ziele enthalten. Ebenso darf die Netzwerkzuordnung für die Deinstallation nur Portgruppen als Ziele enthalten.
8294	Logischer Switch ist in der Netzwerkzuordnung der Schnittstelle nicht vorhanden.	Es wurden keine logischen Switches angegeben.	Stellen Sie sicher, dass die logischen Switches in der Konfiguration für die Netzwerkzuordnung der Schnittstelle angegeben werden.
8296	Host-Switch stimmt nicht überein.	Die Netzwerkzuordnung der Schnittstelle für die Deinstallation ist mit dem falschen Host-Switch-Namen konfiguriert.	Stellen Sie sicher, dass der in der Zuordnungskonfiguration verwendete Host-Switch-Name dem Namen entspricht, der auf dem Host-Switch, auf dem sich die VMkernel-Schnittstellen befinden, eingegeben wurde.
8297	Doppelter VMkernel.	Doppelte VMkernel sind für die Migration angegeben.	Stellen Sie sicher, dass keine doppelten VMkernel-Schnittstellen in der Zuordnungskonfiguration der Installation oder Deinstallation angegeben wurden.
8298	Nichtübereinstimmung bei der Anzahl der VMkernel-Schnittstellen und -Ziele.	Falsche Konfiguration.	Stellen Sie sicher, dass für jede VMkernel-Schnittstelle ein entsprechendes Ziel in der Konfiguration angegeben wurde.

Tabelle 10-1. Fehler bei der VMkernel-Migration (Fortsetzung)

Fehlercode	Problem	Ursache	Lösung
8299	Transportknoten kann nicht gelöscht werden, da die VMkernel-Schnittstelle Ports auf dem N-VDS verwendet.	VMkernel-Schnittstellen verwenden Ports aus dem N-VDS-Switch.	Führen Sie eine Rückmigration aller VMkernel-Schnittstellen vom N-VDS-Switch zu einem VSS-/DVS-Switch durch. Versuchen Sie dann, den Transportknoten zu löschen.
9412	VMkernel kann nicht von einem N-VDS auf einen anderen N-VDS migriert werden.	Nicht unterstützte Aktion.	Führen Sie eine Rückmigration der VMkernel-Schnittstelle auf einen VSS- oder DVS-Switch durch. Anschließend können Sie die VMkernel-Schnittstelle auf einen anderen N-VDS-Switch migrieren.
9413	VMkernel-Schnittstellen können nicht auf einen anderen logischen Switch migriert werden.	Auf statusbehafteten Hosts kann ein mit einem logischen Switch verbundener VMkernel nicht auf einen anderen logischen Switch migriert werden.	Führen Sie eine Rückmigration des VMkernels vom logischen Switch zu einem VSS-/DVS-Switch durch. Migrieren Sie den VMkernel anschließend auf einen anderen logischen Switch auf dem N-VDS.
9414	Duplizieren der VMkernel-Schnittstellen.	Duplizieren Sie VMkernel-Schnittstellen, die in der Zuordnungskonfiguration der Installation und Deinstallation zugeordnet sind.	Stellen Sie sicher, dass jede VMkernel-Schnittstelle in den Installations- und Deinstallationszuordnungen eindeutig ist.
9415	Eingeschaltete VMs auf dem Host.	Bei eingeschalteten VMs wird die Migration nicht fortgesetzt.	Schalten Sie die VMs auf dem Host aus, bevor Sie mit der Migration von VMkernel-Schnittstellen beginnen.
9416	VMkernel kann auf dem Host nicht gefunden werden.	In der Konfiguration der Netzwerkzuordnung wurde kein VMkernel angegeben, der auf dem Host vorhanden ist.	Geben Sie einen vorhandenen VMkernel in der Konfiguration der Netzwerkzuordnung an.
9417	Portgruppe nicht gefunden.	Es wurde keine Portgruppe angegeben, die in der Konfiguration der Netzwerkzuordnung auf dem Host vorhanden ist.	Geben Sie eine vorhandene Portgruppe in der Konfiguration der Netzwerkzuordnung an.
9419	Logischer Switch während der Migration nicht gefunden.	Der in der Konfiguration der Netzwerkschnittstellenzuordnung definierte logische Switch wurde nicht gefunden.	Geben Sie einen vorhandenen logischen Switch in der Konfiguration der Netzwerkschnittstellenzuordnung an.
9420	Logischer Port während der Migration nicht gefunden.	Während der Migration findet NSX-T Data Center die auf dem logischen Switch erstellten Ports nicht.	Stellen Sie für eine erfolgreiche Migration sicher, dass keine logischen Ports vom logischen Switch gelöscht werden.

Tabelle 10-1. Fehler bei der VMkernel-Migration (Fortsetzung)

Fehlercode	Problem	Ursache	Lösung
9421	Zum Validieren der Migration fehlen Hostinformationen.	Informationen konnten nicht aus der Bestandsliste abgerufen werden.	Wiederholen Sie den Migrationsvorgang.
9423	An eine VMkernel-Schnittstelle angeheftete physische Netzwerkkarten werden nicht mit dem richtigen Host-Switch migriert.	Eine angeheftete physische Netzwerkkarte wurde in der Umgebung gefunden, aber der VMkernel und die physische Netzwerkkarte werden nicht auf denselben Host-Switch migriert.	Eine einer VMkernel-Schnittstelle zugewiesene physische Netzwerkkarte muss eine Transportknotenkonfiguration aufweisen, die dem VMkernel die physische Netzwerkkarte auf demselben Host-Switch zuordnet.
600	Objekt nicht gefunden.	Die vom logischen Switch verwendete angegebene Transportzone ist nicht vorhanden. Der im VMK-Zuordnungsziel enthaltene logische Switch kann nicht gefunden werden.	<ul style="list-style-type: none"> <li>■ Geben Sie eine Transportzone an, die in der Umgebung vorhanden ist.</li> <li>■ Erstellen Sie den gewünschten logischen Switch oder verwenden Sie einen vorhandenen logischen VLAN-Switch.</li> </ul>
8310	Der Typ des logischen Switches ist falsch.	Der Typ des logischen Switch lautet „Overlay“.	Erstellen Sie einen logischen VLAN-Switch.
9424	Kann nicht migriert werden, wenn die Einstellung „Nur PNIC-Migration“ und die Einstellung „Netzwerkzuordnung für Installation und Deinstallation“ gleichzeitig konfiguriert sind.	Migration wird nur fortgesetzt, wenn eine dieser Einstellungen konfiguriert wurde.	Stellen Sie sicher, dass entweder die Einstellung „Nur PNIC-Migration“ oder die Einstellung „Netzwerkzuordnung für Installation und Deinstallation“ konfiguriert ist.

## Erstellen eines eigenständigen Hosts oder Bare-Metal-Server-Transportknotens

Sie müssen zuerst Ihren ESXi-Host, KVM-Host oder Bare-Metal-Server zur NSX-T Data Center-Fabric hinzufügen und dann den Transportknoten konfigurieren.

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

Ein Transportknoten ist ein Knoten, der an einem NSX-T Data Center-Overlay oder NSX-T Data Center-VLAN-Networking teilnimmt.



Bei einem KVM-Host oder Bare-Metal-Server können Sie den N-VDS im Voraus konfigurieren oder die Konfiguration von NSX Manager durchführen lassen. Bei einem ESXi-Host wird der N-VDS immer von NSX Manager konfiguriert.

---

**Hinweis** Wenn Sie Transportknoten aus einer Vorlagen-VM erstellen möchten, achten Sie darauf, dass keine Zertifikate für den Host in `/etc/vmware/nsx/` vorhanden sind. Der netcpa-Agent erstellt kein Zertifikat, wenn ein Zertifikat vorhanden ist.

---

Der Bare-Metal-Server unterstützt ein Overlay- und VLAN-Transportzone. Sie können die Management-Schnittstelle verwenden, um den Bare-Metal-Server zu verwalten. Mit der Anwendungsschnittstelle können Sie auf die Anwendungen auf dem Bare-Metal-Server zugreifen.

Einzelne physische Netzwerkkarten bieten eine IP-Adresse für die Verwaltungs- und Anwendungs-IP-Schnittstellen.

Zwei physische Netzwerkkarten bieten eine physische Netzwerkkarte und eine eindeutige IP-Adresse für die Verwaltungsschnittstelle. Zwei physische Netzwerkkarten bieten auch eine physische Netzwerkkarte und eine eindeutige IP-Adresse für die Anwendungsschnittstelle.

Mehrere physische Netzwerkkarten in einer verbundenen Konfiguration bieten zwei physische Netzwerkkarten und eine eindeutige IP-Adresse für die Verwaltungsschnittstelle. Mehrere physische Netzwerkkarten in einer verbundenen Konfiguration bieten auch zwei physische Netzwerkkarten und eine eindeutige IP-Adresse für die Anwendungsschnittstelle.

Sie können maximal vier N-VDS-Switches für jede Konfiguration hinzufügen: Standard-N-VDS, das für VLAN-Transportzonen erstellt wurde, erweitertes N-VDS, das für VLAN-Transportzonen erstellt wurde, Standard-N-VDS, das für Overlay-Transportzonen erstellt wurde, erweitertes N-VDS, das für Overlay-Transportzonen erstellt wurde.

In einer einzelnen Host-Cluster-Topologie, in der mehrere Standard-Overlay-N-VDS-Switches und Edge-VM auf demselben Host ausgeführt werden, bietet NSX-T Data Center Datenverkehrsisolierung, sodass Datenverkehr, der über den ersten N-VDS läuft, vom Datenverkehr, der über den zweiten N-VDS läuft, isoliert wird, usw. Die physischen Netzwerkkarten auf jedem N-VDS müssen der Edge-VM auf dem Host zugeordnet werden, sodass die Nord-Süd-Datenverkehrs-Konnektivität mit der Außenwelt ermöglicht wird. Pakete, die aus einer VM auf der ersten Transportzone verschoben werden, müssen über einen externen Router oder eine externe VM zur VM auf der zweiten Transportzone weitergeleitet werden.

### Voraussetzungen

- Der Host muss mit der Management Plane verbunden sein, und die Konnektivität muss auf Aktiv stehen.
- Eine Transportzone muss konfiguriert sein.
- Es muss entweder ein Uplink-Profil konfiguriert werden, oder Sie können das standardmäßige Uplink-Profil verwenden.
- Ein IP-Pool muss konfiguriert sein, oder DHCP muss in der Netzwerkbereitstellung verfügbar sein.

- Mindestens eine nicht verwendete physische Netzwerkkarte (NIC) muss auf dem Hostknoten verfügbar sein.
- Hostname
- Verwaltungs-IP-Adresse
- Benutzername
- Kennwort
- Optional: (KVM) SHA-256-SSL-Fingerabdruck
- Optional: (ESXi) SHA-256-SSL-Fingerabdruck
- Stellen Sie sicher, dass die erforderlichen Drittanbieterpakete installiert sind. Siehe [Installieren von Drittanbieterpaketen auf einem KVM-Host](#).

## Verfahren

- 1 (Optional) Rufen Sie den Hypervisor-Fingerabdruck ab, damit Sie diesen beim Hinzufügen des Hosts zur Fabric angeben können.
  - a Sammeln Sie die Informationen zum Hypervisor-Fingerabdruck.

Verwenden Sie eine Linux-Shell.

```
# echo -n | openssl s_client -connect <esxi-ip-address>:443 2>/dev/null | openssl x509 -noout -fingerprint -sha256
```

Verwenden Sie die ESXi-CLI auf dem Host.

```
[root@host:~] openssl x509 -in /etc/vmware/ssl/rui.crt -fingerprint -sha256 -noout
SHA256
Fingerprint=49:73:F9:A6:0B:EA:51:2A:15:57:90:DE:C0:89:CA:7F:46:8E:30:15:CA:4D:5C:95:28:0A:9E:A
2:4E:3C:C4:F4
```

- b Um den SHA-256-Fingerabdruck von einem KVM-Hypervisor abzurufen, führen Sie den Befehl auf dem KVM-Host aus.

```
# awk '{print $2}' /etc/ssh/ssh_host_rsa_key.pub | base64 -d | sha256sum -b | sed 's/ .*$//' | xxd -r -p | base64
```

- 2 Wählen Sie **System > Fabric > Knoten > Host-Transportknoten** aus.
- 3 Wählen über das Feld „Veraltet von“ **Eigenständige Hosts** aus und klicken Sie auf **+ Hinzufügen**.

- 4 Geben Sie Details für den eigenständigen Host oder den Bare-Metal-Server ein, die zur Fabric hinzugefügt werden sollen.

Option	Beschreibung
<b>Name und Beschreibung</b>	Geben Sie den Namen ein, um den eigenständigen Host oder Bare-Metal-Server zu identifizieren.  Sie können optional die Beschreibung des Betriebssystems hinzufügen, die für den Host oder den Bare-Metal-Server verwendet werden.
<b>IP-Adressen</b>	Geben Sie die IP-Adresse des Hosts oder Bare-Metal-Servers ein.
<b>Betriebssystem</b>	Wählen Sie im Dropdown-Menü das Betriebssystem aus. In Abhängigkeit von Ihrem Host oder Bare-Metal-Server können Sie ein beliebiges unterstütztes Betriebssystem auswählen. Siehe <a href="#">Systemvoraussetzungen</a> .  <b>Wichtig</b> Bei all den verschiedenen unterstützten Linux-Typen müssen Sie den Unterschied zwischen einem Bare Metal-Server, der eine Linux-Distribution ausführt, und der Verwendung einer Linux-Distribution als Hypervisor-Host kennen. Wenn Sie z. B. Ubuntu Server als Betriebssystem auswählen, richten Sie einen Bare Metal-Server ein, auf dem ein Linux-Server ausgeführt wird. Wenn Sie jedoch Ubuntu KVM auswählen, lautet der bereitgestellte Linux-Hypervisor Ubuntu.
<b>Benutzername und Kennwort</b>	Geben Sie den Benutzernamen und das Kennwort für den Hostbenutzer ein.
<b>SHA-256-Fingerabdruck</b>	Geben Sie den Host-Fingerabdruck-Wert für die Authentifizierung ein. Wenn Sie den Fingerabdruckwert leer lassen, werden Sie aufgefordert, den vom Server bereitgestellten Wert zu akzeptieren. Es dauert einige Sekunden, bis NSX-T Data Center den Host erkennt und authentifiziert.

- 5 (Erforderlich) Wählen Sie für einen KVM-Host oder Bare-Metal-Server den N-VDS-Typ aus.

Option	Beschreibung
<b>NSX erstellt</b>	NSX Manager erstellt den N-VDS.  Diese Option ist standardmäßig ausgewählt.
<b>Vorkonfiguriert</b>	Der N-VDS ist bereits konfiguriert.

Bei einem ESXi-Host ist der N-VDS-Typ immer auf **NSX erstellt** festgelegt.

- 6 Geben Sie die Standard-N-VDS-Details ein. Mehrere N-VDS-Switches können auf einem einzelnen Host konfiguriert werden.

Option	Beschreibung
<b>Transportzone</b>	Wählen Sie aus dem Dropdown-Menü die Transportzone aus, zu der dieser Transportknoten gehört.
<b>N-VDS-Name</b>	Muss mit dem N-VDS-Namen der Transportzone identisch sein, zu der dieser Knoten gehört.
<b>NIOC-Profil</b>	Wählen Sie für einen ESXi-Host das NIOC-Profil im Dropdown-Menü aus.

Option	Beschreibung
<b>Uplink-Profil</b>	<p>Wählen Sie im Dropdown-Menü ein vorhandenes Profil aus, oder erstellen Sie ein benutzerdefiniertes Uplink-Profil.</p> <p>Sie können auch das standardmäßige Uplink-Profil verwenden.</p>
<b>LLDP-Profil</b>	<p>Standardmäßig empfängt NSX-T nur LLDP-Pakete von einem LLDP-Nachbarn.</p> <p>NSX-T kann jedoch so konfiguriert werden, dass LLDP-Pakete an einen LLDP-Nachbarn gesendet und LLDP-Pakete von einem LLDP-Nachbarn empfangen werden.</p>
<b>IP-Zuweisung</b>	<p>Wählen Sie <b>DHCP verwenden</b>, <b>IP-Pool verwenden</b> oder <b>Liste statischer IPs verwenden</b>.</p> <p>Wenn Sie <b>Liste statischer IPs verwenden</b> auswählen, müssen Sie eine Liste mit durch Komma getrennten IP-Adressen, ein Gateway und eine Subnetzmaske angeben.</p>
<b>IP-Pool</b>	<p>Wenn Sie <b>IP-Pool verwenden</b> für die IP-Zuweisung ausgewählt haben, geben Sie den Namen des IP-Pools an.</p>
<b>Physische Netzwerkkarten</b>	<p>Fügen Sie physische Netzwerkkarten zum Transportknoten hinzu. Sie können den standardmäßigen Uplink verwenden oder einen vorhandenen Uplink aus dem Dropdown-Menü zuweisen.</p> <p>Klicken Sie auf <b>PNIC hinzufügen</b>, um zusätzliche physische Netzwerkkarten zum Transportknoten zu konfigurieren.</p> <p><b>Hinweis</b> Die Migration der physischen Netzwerkkarten, die Sie in diesem Feld hinzufügen, hängt davon ab, wie Sie <b>Migration nur von PNIC</b>, <b>Netzwerkzuordnungen für die Installation</b> und <b>Netzwerkzuordnungen für die Deinstallation</b> konfigurieren.</p> <ul style="list-style-type: none"> <li>■ Um eine verwendete physische Netzwerkkarte (z. B. nach einem standardmäßigen vSwitch oder vSphere-Distributed Switch) ohne eine verbundene VMkernel-Zuordnung zu migrieren, stellen Sie sicher, dass <b>Migration nur von PNIC</b> aktiviert ist. Andernfalls bleibt der Transportknotenstatus <b>Teilweise erfolgreich</b>, und die Fabric-Knoten-LCP-Konnektivität kann nicht hergestellt werden.</li> <li>■ Um eine verwendete physische Netzwerkkarte mit einer verbundenen VMkernel-Netzwerkzuordnung zu migrieren, deaktivieren Sie <b>Migration nur von PNIC</b> und konfigurieren Sie die VMkernel-Netzwerkzuordnung.</li> <li>■ Um eine freie physische Netzwerkkarte zu migrieren, aktivieren Sie <b>Migration nur von PNIC</b>.</li> </ul>

Option	Beschreibung
<b>Migration nur von PNIC</b>	<p>Vor dem Festlegen dieses Felds berücksichtigen Sie die folgenden Punkte:</p> <ul style="list-style-type: none"> <li>■ Bringen Sie in Erfahrung, ob die definierte physische Netzwerkkarte eine verwendete oder eine freie Netzwerkkarte ist.</li> <li>■ Bestimmen Sie, ob VMkernel-Schnittstellen eines Hosts zusammen mit physischen Netzwerkkarten migriert werden müssen.</li> </ul> <p>Legen Sie das Feld fest:</p> <ul style="list-style-type: none"> <li>■ Aktivieren Sie <b>Migration nur von PNIC</b>, wenn Sie nur physische Netzwerkkarten von einem VSS- oder DVS-Switch zu einem N-VDS-Switch migrieren möchten.</li> <li>■ Deaktivieren Sie <b>Migration nur von PNIC</b>, wenn Sie eine verwendete physische Netzwerkkarte und dessen zugeordnete VMkernel-Schnittstellenzuordnung migrieren möchten. Eine freie oder physische Netzwerkkarte ist an den N-VDS-Switch angehängt, wenn eine Migrationszuordnung für die VMkernel-Schnittstelle angegeben ist.</li> </ul> <p>Auf einem Host mit mehreren Host-Switches:</p> <ul style="list-style-type: none"> <li>■ Wenn alle Host-Switches nur PNICs migrieren sollen, können Sie PNICs in einem einzigen Vorgang migrieren.</li> <li>■ Wenn einige Hosts-Switches VMkernel-Schnittstellen migrieren sollen und die verbleibenden Host-Switches nur PNICs migrieren sollen: <ol style="list-style-type: none"> <li>1 Migrieren Sie im ersten-Vorgang nur PNICs.</li> <li>2 Migrieren Sie im zweiten Vorgang VMkernel-Schnittstellen. Stellen Sie sicher, dass <b>Migration nur von PNIC</b> deaktiviert ist.</li> </ol> </li> </ul> <p>Sowohl die Migration nur von PNIC als auch die VMkernel-Schnittstellenmigration werden nicht gleichzeitig über mehrere Hosts hinweg unterstützt.</p> <hr/> <p><b>Hinweis</b> Um die Netzwerkkarte eines Verwaltungsnetzwerks zu migrieren, konfigurieren Sie dessen zugeordnete VMkernel-Netzwerk-Zuordnung und lassen Sie <b>Migration nur von PNIC</b> deaktiviert. Wenn Sie nur die Management-Netzwerkkarte migrieren, verliert der Host die Verbindung.</p> <hr/> <p>Weitere Informationen finden Sie unter <a href="#">VMkernel-Migration auf einen N-VDS-Switch</a>.</p>

Option	Beschreibung
<b>Netzwerkzuordnungen für die Installation</b>	<p>Um VMkernels während der Installation zum N-VDS-Switch zu migrieren, ordnen Sie VMkernels einem vorhandenen logischen Switch zu. Der NSX Manager migriert den VMkernel zum zugeordneten logischen Switch auf N-VDS.</p> <p><b>Vorsicht</b> Stellen Sie sicher, dass die Management-Netzwerkkarte und die Verwaltungs-VMkernel-Schnittstelle auf einen logischen Switch migriert werden, der mit demselben VLAN verbunden ist, mit dem die Management-Netzwerkkarte vor der Migration verbunden war. Wenn vmnic &lt;n&gt; und VMkernel &lt;n&gt; auf ein anderes VLAN migriert werden, dann wird die Verbindung zum Host unterbrochen.</p> <p><b>Vorsicht</b> Stellen Sie bei angehefteten physischen Netzwerkkarten sicher, dass die Host-Switch-Zuordnung einer physischen Netzwerkkarte zu einer VMkernel-Schnittstelle mit der Konfiguration aus dem Transportknotenprofil übereinstimmt. Im Rahmen des Validierungsverfahrens überprüft NSX-T Data Center die Zuordnung, und wenn die Validierung bestanden wird, ist die Migration von VMkernel-Schnittstellen zu einem N-VDS-Switch erfolgreich. Gleichzeitig ist es erforderlich, die Netzwerkzuordnung für Deinstallation zu konfigurieren, da NSX-T Data Center die Zuordnungskonfiguration des Host-Switch nicht speichert, nachdem die VMkernel-Schnittstellen zum N-VDS-Switch migriert wurden. Wenn die Zuordnung nicht konfiguriert ist, kann die Verbindung zu Diensten wie vSAN verloren gehen, nachdem die Migration wieder zurück zum VSS- oder VDS-Switch durchgeführt wurde.</p> <p>Weitere Informationen finden Sie unter <a href="#">VMkernel-Migration auf einen N-VDS-Switch</a>.</p>
<b>Netzwerkzuordnungen für die Deinstallation</b>	<p>Um die Migration des VMkernels während der Deinstallation wiederherzustellen, ordnen Sie VMkernels zu Portgruppen auf VSS oder DVS zu, sodass NSX Manager weiß, zu welcher Portgruppe der VMkernel auf dem VSS oder DVS wieder zurückmigriert werden muss. Stellen Sie bei einem DVS-Switch sicher, dass die Portgruppe den Typ Flüchtig aufweist.</p> <p><b>Vorsicht</b> Stellen Sie bei angehefteten physischen Netzwerkkarten sicher, dass die Transportknotenprofil-Zuordnung einer physischen Netzwerkkarte zu einer VMkernel-Schnittstelle mit der Konfiguration aus dem Host-Switch übereinstimmt. Es ist erforderlich, die Netzwerkzuordnung für Deinstallation zu konfigurieren, da NSX-T Data Center die Zuordnungskonfiguration des Host-Switch nicht speichert, nachdem die VMkernel-Schnittstellen zum N-VDS-Switch migriert wurden. Wenn die Zuordnung nicht konfiguriert ist, kann die Verbindung zu Diensten wie vSAN verloren gehen, nachdem die Migration wieder zurück zum VSS- oder VDS-Switch durchgeführt wurde.</p> <p>Weitere Informationen finden Sie unter <a href="#">VMkernel-Migration auf einen N-VDS-Switch</a>.</p>

- 7 Geben Sie die N-VDS-Details für den erweiterten Datenpfad ein. Mehrere N-VDS-Switches können auf einem einzelnen Host konfiguriert werden.

Option	Beschreibung
<b>N-VDS-Name</b>	Muss mit dem N-VDS-Namen der Transportzone identisch sein, zu der dieser Knoten gehört.
<b>IP-Zuweisung</b>	<p>Wählen Sie <b>DHCP verwenden</b>, <b>IP-Pool verwenden</b> oder <b>Liste statischer IPs verwenden</b>.</p> <p>Wenn Sie <b>Liste statischer IPs verwenden</b> auswählen, müssen Sie eine Liste mit durch Komma getrennten IP-Adressen, ein Gateway und eine Subnetzmaske angeben.</p>
<b>IP-Pool</b>	Wenn Sie <b>IP-Pool verwenden</b> für eine IP-Zuweisung ausgewählt haben, geben Sie den Namen des IP-Pools an.
<b>Physische Netzwerkkarten</b>	<p>Fügen Sie physische Netzwerkkarten zum Transportknoten hinzu. Sie können den standardmäßigen Uplink verwenden oder einen vorhandenen Uplink aus dem Dropdown-Menü zuweisen.</p> <p>Klicken Sie auf <b>PNIC hinzufügen</b>, um zusätzliche physische Netzwerkkarten zum Transportknoten zu konfigurieren.</p> <p><b>Hinweis</b> Die Migration der physischen Netzwerkkarten, die Sie in diesem Feld hinzufügen, hängt davon ab, wie Sie <b>Migration nur von PNIC</b>, <b>Netzwerkzuordnungen für die Installation</b> und <b>Netzwerkzuordnungen für die Deinstallation</b> konfigurieren.</p> <ul style="list-style-type: none"> <li>■ Um eine verwendete physische Netzwerkkarte (z. B. nach einem standardmäßigen vSwitch oder vSphere-Distributed Switch) ohne eine verbundene VMkernel-Zuordnung zu migrieren, stellen Sie sicher, dass <b>Migration nur von PNIC</b> aktiviert ist. Andernfalls bleibt der Transportknotenstatus <b>Teilweise erfolgreich</b>, und die Fabric-Knoten-LCP-Konnektivität kann nicht hergestellt werden.</li> <li>■ Um eine verwendete physische Netzwerkkarte mit einer verbundenen VMkernel-Netzwerkzuordnung zu migrieren, deaktivieren Sie <b>Migration nur von PNIC</b> und konfigurieren Sie die VMkernel-Netzwerkzuordnung.</li> <li>■ Um eine freie physische Netzwerkkarte zu migrieren, aktivieren Sie <b>Migration nur von PNIC</b>.</li> </ul>
<b>Uplink</b>	Wählen Sie ein Uplink-Profil im Dropdown-Menü aus.

Option	Beschreibung
<b>CPU-Konfiguration</b>	<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> <hr/> <p><b>Hinweis</b> 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> <hr/> <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 get</code> ermitteln.</p> <hr/> <p><b>Hinweis</b> 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> <hr/>

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

Option	Beschreibung
<b>Externe N-VDS-ID</b>	Muss mit dem N-VDS-Namen der Transportzone identisch sein, zu der dieser Knoten gehört.
<b>VTEP</b>	Name des virtuellen Tunnel-Endpoints.

**9** Überprüfen Sie den Verbindungsstatus auf der Seite **Host-Transportknoten**.

Nach dem Hinzufügen des Hosts oder Bare-Metal-Servers als Transportknoten ändert sich die Verbindung zu NSX Manager nach 3-4 Minuten „Aktiv“.

**Hinweis** Wenn die Hostvorbereitung aufgrund einer Nichtübereinstimmung des Konfigurations-Hashs fehlschlägt, was zu einer Ermittlungsschleife führt, versuchen Sie eine der folgenden Optionen:

- Legen Sie FQDN auf „false“ fest und starten Sie nsx-proxy auf dem Host neu. Dadurch wird erzwungen, dass der Host und NSX Manager keinen FQDN verwenden.

■ ODER

Wenn Sie den FQDN-Modus verwenden möchten, stellen Sie sicher, dass Sie die NSX Manager-Appliance mit einem FQDN als Hostnamen bereitstellen, und vergewissern Sie sich, dass die Groß-/Kleinschreibung sowohl mit dem Forward- als auch mit dem Reverse-DNS-Lookup für die NSX Manager-IP-Adresse übereinstimmt. Diese Einstellung muss über alle NSX Manager-Knoten hinweg konsistent sein.



**10** Alternativ können Sie den Verbindungsstatus mit CLI-Befehlen anzeigen.

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

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

- ◆ Geben Sie für KVM den Befehl `netstat -anp --tcp | grep 1234` ein.

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

**11** Stellen Sie sicher, dass die NSX-T Data Center-Module auf Ihrem Host oder dem Bare-Metal-Server installiert sind.

Nachdem ein Host oder Bare-Metal-Server zur NSX-T Data Center-Fabric hinzugefügt wurde, wird eine Sammlung von NSX-T Data Center-Modulen auf dem Host oder Bare-Metal-Server installiert.

Die Module auf unterschiedlichen Hosts werden wie folgt zu Paketen zusammengestellt:

- KVM unter RHEL oder CentOS – RPM-Dateien
- KVM unter Ubuntu – DEB-Dateien
- Geben Sie unter ESXi den Befehl `esxcli software vib list | grep nsx` ein.

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

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

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

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

- Kopieren Sie mit dem NSX-T Data Center-CLI-Befehl `copy file` oder der API POST `/api/v1/node/file-store/<file-name>?action=copy_to_remote_file` das Skript `aggsvc_change_intervals.py` auf einen Host.
- Führen Sie das Skript aus, das sich im Dateispeicher von NSX-T Data Center befindet.

```
python aggsvc_change_intervals.py -m '<NSX ManagerIPAddress>' -u 'admin' -p '<password>' -i 900
```

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

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

## Ergebnisse

**Hinweis** Wenn Sie für einen durch NSX-T Data Center erstellten N-VDS nach dem Erstellen des Transportknotens die Konfiguration (z. B. die IP-Zuweisung zum Tunnel-Endpoint) ändern möchten, müssen Sie diese Änderung über die NSX Manager-GUI vornehmen, und nicht über die Befehlszeilenschnittstelle (CLI) auf dem Host.

## Nächste Schritte

Migrieren Sie Netzwerkschnittstellen von einem vSphere-Standard-Switch zu einem N-VDS. Siehe [VMkernel-Migration auf einen N-VDS-Switch](#).

## Konfigurieren eines verwalteten Host-Transportknotens

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

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

## Voraussetzungen

- Stellen Sie sicher, dass alle Hosts auf dem vCenter Server eingeschaltet sind.
- Stellen Sie sicher, dass die Systemanforderungen erfüllt sind. Siehe [Systemvoraussetzungen](#).
- Stellen Sie sicher, dass eine Transportzone verfügbar ist. Siehe [Erstellen von Transportzonen](#).
- Stellen Sie sicher, dass ein Transportknotenprofil konfiguriert ist. Siehe [Hinzufügen eines Transportknotenprofils](#).
- Die NSX-T Data Center-Installation auf vSphere schlägt fehl, wenn Ihre Ausnahmeliste für den vSphere-Sperrmodus abgelaufene Benutzerkonten enthält. Stellen Sie sicher, dass Sie alle abgelaufenen Benutzerkonten gelöscht haben, bevor Sie mit der Installation beginnen. Weitere Informationen zu Konten mit Zugriffsrechten im Sperrmodus finden Sie unter *Angeben von Konten mit Zugriffsrechten im Sperrmodus* im Sicherheitshandbuch von vSphere.

## Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **System > Fabric > Knoten > Host-Transportknoten** aus.
- 3 Wählen Sie im Dropdown-Menü „Veraltet von“ einen vorhandenen vCenter Server aus.  
Auf der Seite sind die verfügbaren vSphere-Cluster bzw. ESXi-Hosts aus dem ausgewählten vCenter Server aufgeführt. Möglicherweise müssen Sie einen Cluster erweitern, um die ESXi-Hosts anzuzeigen.

- 4 Wählen Sie einen einzelnen Host in der Liste aus und klicken Sie auf **NSX konfigurieren**.

Das Dialogfeld „NSX konfigurieren“ wird geöffnet.

- a Überprüfen Sie den Hostnamen im Bereich „Hostdetails“. Optional können Sie eine Beschreibung hinzufügen.
  - b Klicken Sie auf **Weiter**, um zum Bereich **NSX konfigurieren** zu wechseln.
  - c Wählen Sie die verfügbaren Transportzonen aus und klicken Sie auf die Schaltfläche **>**, um die Transportzonen in das Transportknotenprofil aufzunehmen.
- 5 Überprüfen Sie den Hostnamen im Bereich „Hostdetails“ und klicken Sie auf **Weiter**.  
Optional können Sie eine Beschreibung hinzufügen.
- 6 Wählen Sie im Bereich **NSX konfigurieren** die gewünschten Transportzonen aus.  
Sie können mehr als eine Transportzone auswählen.
- 7 Klicken Sie auf die Registerkarte **N-VDS** und geben Sie die Switch-Informationen ein.

Option	Beschreibung
<b>N-VDS-Name</b>	Wenn der Transportknoten an eine Transportzone angehängt ist, dann stellen Sie sicher, dass der eingegebene Name für den N-VDS identisch mit dem N-VDS-Namen ist, der in der Transportzone angegeben ist. Ein Transportknoten kann erstellt werden, ohne ihn zu einer Transportzone anzuhängen.
<b>Zugeordnete Transportzonen</b>	Zeigt die Transportzonen, die durch den zugeordneten Host-Switches realisiert werden. Sie können keine Transportzone hinzufügen, wenn sie nicht von einem beliebigen N-VDS im Transportknotenprofil realisiert wurde.
<b>NIOC-Profil</b>	Wählen Sie das NIOC-Profil im Dropdown-Menü aus. Die Bandbreitenzuteilungen aus dem Profil für die Datenverkehrsressourcen werden erzwungen.
<b>Uplink-Profil</b>	Wählen Sie im Dropdown-Menü ein vorhandenes Profil aus, oder erstellen Sie ein benutzerdefiniertes Uplink-Profil. Sie können auch das standardmäßige Uplink-Profil verwenden.
<b>LLDP-Profil</b>	Standardmäßig empfängt NSX-T nur LLDP-Pakete von einem LLDP-Nachbarn. NSX-T kann jedoch so eingestellt werden, dass LLDP-Pakete an einen LLDP-Nachbarn gesendet und LLDP-Pakete von einem LLDP-Nachbarn empfangen werden.
<b>IP-Zuweisung</b>	Wählen Sie <b>DHCP verwenden</b> , <b>IP-Pool verwenden</b> oder <b>Statische IP-Liste verwenden</b> , um eine IP-Adresse zu virtuellen Tunnel-Endpoints (VTEPs) des Transportknotens zuzuweisen. Wenn Sie <b>Liste statischer IPs verwenden</b> auswählen, müssen Sie eine Liste mit durch Komma getrennten IP-Adressen, ein Gateway und eine Subnetzmaske angeben. Alle VTEPs des Transportknotens müssen sich im selben Subnetz befinden. Andernfalls wird eine Sitzung mit bidirektionalem Flow (BFD) nicht aufgebaut.
<b>IP-Pool</b>	Wenn Sie <b>IP-Pool verwenden</b> für eine IP-Zuweisung ausgewählt haben, geben Sie den Namen des IP-Pools an.

Option	Beschreibung
<b>Physische Netzwerkkarten</b>	<p>Fügen Sie physische Netzwerkkarten zum Transportknoten hinzu. Sie können den standardmäßigen Uplink verwenden oder einen vorhandenen Uplink aus dem Dropdown-Menü zuweisen.</p> <p>Klicken Sie auf <b>PNIC hinzufügen</b>, um zusätzliche physische Netzwerkkarten zum Transportknoten zu konfigurieren.</p> <hr/> <p><b>Hinweis</b> Die Migration der physischen Netzwerkkarten, die Sie in diesem Feld hinzufügen, hängt davon ab, wie Sie <b>Migration nur von PNIC</b>, <b>Netzwerkzuordnungen für die Installation</b> und <b>Netzwerkzuordnungen für die Deinstallation</b> konfigurieren.</p> <hr/> <ul style="list-style-type: none"> <li>■ Um eine verwendete physische Netzwerkkarte (z. B. nach einem standardmäßigen vSwitch oder vSphere-Distributed Switch) ohne eine verbundene VMkernel-Zuordnung zu migrieren, stellen Sie sicher, dass <b>Migration nur von PNIC</b> aktiviert ist. Andernfalls bleibt der Transportknotenstatus <b>Teilweise erfolgreich</b>, und die Fabric-Knoten-LCP-Konnektivität kann nicht hergestellt werden.</li> <li>■ Um eine verwendete physische Netzwerkkarte mit einer verbundenen VMkernel-Netzwerkzuordnung zu migrieren, deaktivieren Sie <b>Migration nur von PNIC</b> und konfigurieren Sie die VMkernel-Netzwerkzuordnung.</li> <li>■ Um eine freie physische Netzwerkkarte zu migrieren, aktivieren Sie <b>Migration nur von PNIC</b>.</li> </ul> <hr/>

Option	Beschreibung
<b>Migration nur von PNIC</b>	<p>Vor dem Festlegen dieses Felds berücksichtigen Sie die folgenden Punkte:</p> <ul style="list-style-type: none"> <li>■ Bringen Sie in Erfahrung, ob die definierte physische Netzwerkkarte eine verwendete oder eine freie Netzwerkkarte ist.</li> <li>■ Bestimmen Sie, ob VMkernel-Schnittstellen eines Hosts zusammen mit physischen Netzwerkkarten migriert werden müssen.</li> </ul> <p>Legen Sie das Feld fest:</p> <ul style="list-style-type: none"> <li>■ Aktivieren Sie <b>Migration nur von PNIC</b>, wenn Sie nur physische Netzwerkkarten von einem VSS- oder DVS-Switch zu einem N-VDS-Switch migrieren möchten.</li> <li>■ Deaktivieren Sie <b>Migration nur von PNIC</b>, wenn Sie eine verwendete physische Netzwerkkarte und dessen zugeordnete VMkernel-Schnittstellenzuordnung migrieren möchten. Eine freie oder physische Netzwerkkarte ist an den N-VDS-Switch angehängt, wenn eine Migrationszuordnung für die VMkernel-Schnittstelle angegeben ist.</li> </ul> <p>Auf einem Host mit mehreren Host-Switches:</p> <ul style="list-style-type: none"> <li>■ Wenn alle Host-Switches nur PNICs migrieren sollen, können Sie PNICs in einem einzigen Vorgang migrieren.</li> <li>■ Wenn einige Hosts-Switches VMkernel-Schnittstellen migrieren sollen und die verbleibenden Host-Switches nur PNICs migrieren sollen: <ol style="list-style-type: none"> <li>1 Migrieren Sie im ersten-Vorgang nur PNICs.</li> <li>2 Migrieren Sie im zweiten Vorgang VMkernel-Schnittstellen. Stellen Sie sicher, dass <b>Migration nur von PNIC</b> deaktiviert ist.</li> </ol> </li> </ul> <p>Sowohl die Migration nur von PNIC als auch die VMkernel-Schnittstellenmigration werden nicht gleichzeitig über mehrere Hosts hinweg unterstützt.</p> <hr/> <p><b>Hinweis</b> Um die Netzwerkkarte eines Verwaltungsnetzwerks zu migrieren, konfigurieren Sie dessen zugeordnete VMkernel-Netzwerk-Zuordnung und lassen Sie <b>Migration nur von PNIC</b> deaktiviert. Wenn Sie nur die Management-Netzwerkkarte migrieren, verliert der Host die Verbindung.</p> <hr/> <p>Weitere Informationen finden Sie unter <a href="#">VMkernel-Migration auf einen N-VDS-Switch</a>.</p>

Option	Beschreibung
<b>Netzwerkzuordnungen für die Installation</b>	<p>Um VMkernels während der Installation zum N-VDS-Switch zu migrieren, ordnen Sie VMkernels einem vorhandenen logischen Switch zu. Der NSX Manager migriert den VMkernel zum zugeordneten logischen Switch auf N-VDS.</p> <p><b>Vorsicht</b> Stellen Sie sicher, dass die Management-Netzwerkkarte und die Verwaltungs-VMkernel-Schnittstelle auf einen logischen Switch migriert werden, der mit demselben VLAN verbunden ist, mit dem die Management-Netzwerkkarte vor der Migration verbunden war. Wenn vmnic &lt;n&gt; und VMkernel &lt;n&gt; auf ein anderes VLAN migriert werden, dann wird die Verbindung zum Host unterbrochen.</p> <p><b>Vorsicht</b> Stellen Sie bei angehefteten physischen Netzwerkkarten sicher, dass die Host-Switch-Zuordnung einer physischen Netzwerkkarte zu einer VMkernel-Schnittstelle mit der Konfiguration aus dem Transportknotenprofil übereinstimmt. Im Rahmen des Validierungsverfahrens überprüft NSX-T Data Center die Zuordnung, und wenn die Validierung bestanden wird, ist die Migration von VMkernel-Schnittstellen zu einem N-VDS-Switch erfolgreich. Es ist auch erforderlich, die Netzwerkzuordnung für Deinstallation zu konfigurieren, da NSX-T Data Center die Zuordnungskonfiguration des Host-Switch nicht speichert, nachdem die VMkernel-Schnittstellen zum N-VDS-Switch migriert wurden. Wenn die Zuordnung nicht konfiguriert ist, kann die Verbindung zu Diensten wie vSAN verloren gehen, nachdem die Migration wieder zurück zum VSS- oder VDS-Switch durchgeführt wurde.</p> <p>Weitere Informationen finden Sie unter <a href="#">VMkernel-Migration auf einen N-VDS-Switch</a>.</p>
<b>Netzwerkzuordnungen für die Deinstallation</b>	<p>Um die Migration des VMkernels während der Deinstallation wiederherzustellen, ordnen Sie VMkernels zu Portgruppen auf VSS oder DVS zu, sodass NSX Manager weiß, zu welcher Portgruppe der VMkernel auf dem VSS oder DVS wieder zurückmigriert werden muss. Stellen Sie bei einem DVS-Switch sicher, dass die Portgruppe den Typ Flüchtling aufweist.</p> <p><b>Vorsicht</b> Stellen Sie bei angehefteten physischen Netzwerkkarten sicher, dass die Transportknotenprofil-Zuordnung einer physischen Netzwerkkarte zu einer VMkernel-Schnittstelle mit der Konfiguration aus dem Host-Switch übereinstimmt. Es ist erforderlich, die Netzwerkzuordnung für Deinstallation zu konfigurieren, da NSX-T Data Center die Zuordnungskonfiguration des Host-Switch nicht speichert, nachdem die VMkernel-Schnittstellen zum N-VDS-Switch migriert wurden. Wenn die Zuordnung nicht konfiguriert ist, kann die Verbindung zu Diensten wie vSAN verloren gehen, nachdem die Migration wieder zurück zum VSS- oder VDS-Switch durchgeführt wurde.</p> <p>Weitere Informationen finden Sie unter <a href="#">VMkernel-Migration auf einen N-VDS-Switch</a>.</p>

- 8 Wenn Sie mehrere Transportzonen ausgewählt haben, klicken Sie erneut auf **+ N-VDS hinzufügen**, um den Switch für die anderen Transportzonen zu konfigurieren.
- 9 Klicken Sie auf **Fertigstellen**, um die Konfiguration abzuschließen.

**10** (Optional) Zeigen Sie den ESXi-Verbindungsstatus an.

```
# esxcli network ip connection list | grep 1235
tcp    0    0  192.168.210.53:20514  192.168.110.34:1234  ESTABLISHED  1000144459  newreno  netcpa
```

**11** Stellen Sie auf der Seite mit Host-Transportknoten sicher, dass der NSX Manager-Konnektivitätsstatus von Hosts im Cluster „Aktiv“ ist und der Konfigurationszustand von NSX-T Data Center „Erfolgreich“ ist.

Sie können auch sehen, dass die Transportzone auf die Hosts im Cluster angewendet wird.

**12** (Optional) Entfernen Sie eine NSX-T Data Center-Installation und einen Transportknoten von einem Host in der Transportzone.

- a Wählen Sie einen oder mehrere Hosts aus und klicken Sie auf **Aktionen > NSX entfernen**.

Die Deinstallation dauert bis zu drei Minuten. Durch die Deinstallation von NSX-T Data Center wird die Transportknotenkonfiguration für Hosts getrennt und der Host wird von der/den Transportzone(n) und vom N-VDS-Switch getrennt. Jeder neue Host, der dem vCenter Server-Cluster hinzugefügt wird, wird erst dann automatisch konfiguriert, wenn das Transportknotenprofil erneut auf den Cluster angewendet wird.

**13** (Optional) Entfernen Sie einen Transportknoten aus der Transportzone.

- a Wählen Sie einen einzelnen Transportknoten aus und klicken Sie auf **Aktionen > Aus Transportzone entfernen**.

**Nächste Schritte**

Erstellen Sie einen logischen Switch und weisen Sie ihm logische Ports zu. Informationen finden Sie im Abschnitt „Erweiterte Switching“ in *Administratorhandbuch für NSX-T Data Center*.

## Konfigurieren von ESXi-Hosttransportknoten mit Linkaggregation (LAG)

Dieses Verfahren beschreibt, wie Sie ein Uplink-Profil mit Konfiguration einer Linkaggregationsgruppe erstellen, und wie Sie einen ESXi-Hosttransportknoten für die Verwendung dieses Uplink-Profiles konfigurieren.

**Voraussetzungen**

- Machen Sie sich mit den Schritten zum Erstellen eines Uplink-Profiles vertraut. Siehe [Erstellen eines Uplink-Profiles](#).
- Machen Sie sich mit den Schritten zum Erstellen eines Hosttransportknotens vertraut. Siehe [Erstellen eines eigenständigen Hosts oder Bare-Metal-Server-Transportknotens](#).

**Verfahren**

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

- 3** Geben Sie einen Namen und optional eine Beschreibung ein.  
Geben Sie z. B. den Namen **Uplink-Profil1** ein.
- 4** Klicken Sie unter **LAG** auf **Hinzufügen**, um eine Linkaggregationsgruppe hinzufügen.  
Beispielsweise fügen Sie eine **lag1** genannte LAG mit 2 Uplinks hinzu.
- 5** Wählen Sie unter **Teamings** die Option **Standard-Teaming** aus.
- 6** Geben Sie im Feld **Aktive Uplinks** den Namen der in Schritt 4 hinzugefügten LAG ein. In diesem Beispiel ist der Name **lag1**.
- 7** Geben Sie einen Wert für den **Transport-VLAN** und die **MTU** ein.
- 8** Klicken Sie unten im Dialogfeld auf **Hinzufügen**.
- 9** Klicken Sie unter **Teamings** auf **Hinzufügen**, um einen Eintrag für die Linkaggregation hinzuzufügen.
- 10** Wählen Sie **Fabric > Knoten > Host-Transportknoten > Hinzufügen** aus.
- 11** Geben Sie auf der Registerkarte **Hostdetails** die IP-Adresse, den Betriebssystemnamen, die Administratoranmeldedaten und den SHA-256-Fingerabdruck des Hosts ein.
- 12** Wählen Sie auf der Registerkarte **N-VDS** das in Schritt 3 erstellte Uplink-Profil **uplink-profile1** aus.
- 13** Im Feld **Physische Netzwerkkarten** spiegelt die Dropdown-Liste der physischen Netzwerkkarten und Uplinks die neuen Netzwerkkarten und das Uplink-Profil wider. Insbesondere werden die Uplinks **lag1-0** und **lag1-1** in Übereinstimmung mit der in Schritt 4 erstellten LAG **lag1** angezeigt. Wählen Sie eine physische Netzwerkkarte für **lag1-0** und eine physische Netzwerkkarte für **lag1-1** aus.
- 14** Geben Sie die Daten in die übrigen Felder ein.

## Überprüfen des Transportknotenstatus

Stellen Sie sicher, dass die Transportknotenerstellung ordnungsgemäß funktioniert.

Nach dem Erstellen eines Hosttransportknotens wird der N-VDS auf dem Host installiert.

### Verfahren

- 1** Melden Sie sich beim NSX-T Data Center an.
- 2** Navigieren Sie zur Seite „Transportknoten“ und zeigen Sie den N-VDS-Status an.



- 3 Alternativ können Sie zum Anzeigen des N-VDS unter ESXi den Befehl `esxcli network ip interface list` ausführen.

Unter ESXi sollte die Befehlsausgabe eine vmk-Schnittstelle (z. B. vmk10) mit einem VDS-Namen enthalten, der mit dem Namen übereinstimmt, den Sie beim Konfigurieren der Transportzone und des Transportknotens verwendet haben.

```
# esxcli network ip interface list
...

vmk10
  Name: vmk10
  MAC Address: 00:50:56:64:63:4c
  Enabled: true
  Portset: DvsPortset-1
  Portgroup: N/A
  Netstack Instance: vxlan
  VDS Name: overlay-hostswitch
  VDS UUID: 18 ae 54 04 2c 6f 46 21-b8 ae ef ff 01 0c aa c2
  VDS Port: 10
  VDS Connection: 10
  Opaque Network ID: N/A
  Opaque Network Type: N/A
  External ID: N/A
  MTU: 1600
  TSO MSS: 65535
  Port ID: 67108895
...
```

Wenn Sie den vSphere Client verwenden, können Sie den installierten N-VDS auf der Benutzeroberfläche anzeigen, indem Sie **Konfiguration > Netzwerkadapter** für den Host auswählen.

Der KVM-Befehl zum Prüfen der N-VDS-Installation lautet `ovs-vsctl show`. Beachten Sie, dass bei KVM der N-VDS-Name `nsx-switch.0` lautet. Dieser stimmt nicht mit dem Namen in der Transportknotenkonfiguration überein. Dies ist so vorgesehen.

```
# ovs-vsctl show
...
  Bridge "nsx-switch.0"
    Port "nsx-uplink.0"
      Interface "em2"
    Port "nsx-vtep0.0"
      tag: 0
      Interface "nsx-vtep0.0"
        type: internal
    Port "nsx-switch.0"
```

```
Interface "nsx-switch.0"
  type: internal
  ovs_version: "2.4.1.3340774"
```

#### 4 Prüfen Sie die zugewiesene Tunnel-Endpoint-Adresse des Transportknotens.

Die Schnittstelle vmk10 erhält eine IP-Adresse vom NSX-T Data Center-IP-Pool oder von DHCP (wie hier gezeigt):

```
# esxcli network ip interface ipv4 get
Name    IPv4 Address    IPv4 Netmask    IPv4 Broadcast    Address Type    DHCP DNS
-----
vmk0    192.168.210.53  255.255.255.0   192.168.210.255   STATIC          false
vmk1    10.20.20.53     255.255.255.0   10.20.20.255     STATIC          false
vmk10  192.168.250.3  255.255.255.0   192.168.250.255   STATIC          false
```

In KVM können Sie den Tunnel-Endpoint und die IP-Zuteilung mit dem Befehl `ifconfig` prüfen.

```
# ifconfig
...
nsx-vtep0.0 Link encap:Ethernet HWaddr ba:30:ae:aa:26:53
    inet addr:192.168.250.4 Bcast:192.168.250.255 Mask:255.255.255.0
    ...
```

#### 5 Überprüfen Sie die API auf die Statusinformationen des Transportknotens.

Verwenden Sie den API-Aufruf GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/state`. Beispiel:

```
{
  "state": "success",
  "host_switch_states": [
    {
      "endpoints": [
        {
          "default_gateway": "192.168.250.1",
          "device_name": "vmk10",
          "ip": "192.168.250.104",
          "subnet_mask": "255.255.255.0",
          "label": 69633
        }
      ],
      "transport_zone_ids": [
        "efd7f38f-c5da-437d-af03-ac598f82a9ec"
      ],
      "host_switch_name": "overlay-hostswitch",
      "host_switch_id": "18 ae 54 04 2c 6f 46 21-b8 ae ef ff 01 0c aa c2"
    }
  ]
}
```

```

    }
  ],
  "transport_node_id": "2d030569-5769-4a13-8918-0c309c63fdb9"
}

```

## Migrieren von ESXi-VMkernel- und physischen Adaptern

Nach der Vorbereitung eines Hosts als Transportknoten können Sie Änderungen an der aktuellen Migrationskonfiguration von VMkernel-Adaptern und physischen Adaptern vornehmen.

### Voraussetzungen

- Stellen Sie sicher, dass der Host über mindestens einen freien physischen Adapter verfügt.
- Stellen Sie sicher, dass auf dem Host VMkernel-Adapter und Portgruppen vorhanden sind.

### Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Navigieren Sie zu **System > Fabric > Host-Transportknoten**.
- 3 Wählen Sie einen Transportknoten aus und klicken Sie auf **Aktionen -> ESX-VMkernel und physische Adapter migrieren**.
- 4 Geben Sie unter „ESX-VMkernel und physische Adapter migrieren“ die folgenden Details ein.

Feld	Beschreibung
Richtung	<p>Treffen Sie eine Auswahl:</p> <ul style="list-style-type: none"> <li>■ <b>Auf logische Switches migrieren:</b> zum Migrieren von VMkernel-Adaptern von einem VSS- oder VDS-Switch zu einem N-VDS-Switch in NSX-T Data Center.</li> <li>■ <b>Auf Portgruppen migrieren:</b> zum Migrieren von VMkernel-Adaptern von einem N-VDS-Switch zu einem VSS- oder VDS-Switch.</li> </ul>
Switch auswählen	Wählen Sie den Switch aus, von dem Sie die VMkernel-Adapter und die physischen Adapter migrieren möchten. Sie können aus den verfügbaren Switches auswählen.
Zu migrierende VMkernel-Adapter auswählen	Klicken Sie auf <b>Hinzufügen</b> , um den Namen des VMkernel-Adapters einzugeben, und wählen Sie für das Ziel einen logischen Switch oder eine Portgruppe aus – je nachdem, wohin Sie migrieren möchten.
Physische Adapter in N-VDS bearbeiten	Klicken Sie auf <b>Hinzufügen</b> , um den Namen des physischen Adapters einzugeben, und ordnen Sie ihn einem Uplink auf dem Host-Switch zu.

- 5 Klicken Sie auf **Speichern**, um die Migration von VMkernel-Adaptern und physischen Adaptern zu starten.

## Ergebnisse

Die aktualisierten VMkernel-Adapter und die physischen Adapter werden zum N-VDS-Switch migriert oder zum VSS- oder VDS-Switch im ESXi-Host zurück migriert.

## NSX-Wartungsmodus

Wenn Sie Verlagerungen von VMs per vMotion auf einen nicht funktionsfähigen Transportknoten vermeiden möchten, versetzen Sie diesen Transportknoten in den NSX-Wartungsmodus.

Um einen Transportknoten in den NSX-Wartungsmodus zu versetzen, wählen Sie den Knoten aus und klicken Sie auf „Aktionen → NSX-Wartungsmodus“.

Wenn Sie einen Host in den NSX-Wartungsmodus versetzen, kann der Transportknoten nicht zum Netzwerk gehören. Darüber hinaus können VMs, die auf anderen Transportknoten mit N-VDS oder vSphere Distributed Switch als Host-Switch ausgeführt werden, nicht mit vMotion auf diesen Transportknoten verlagert werden. Zudem kann ein logisches Netzwerk nicht auf ESXi- oder KVM-Hosts konfiguriert werden.

Szenarien zum Versetzen des Transportknotens in den NSX-Wartungsmodus:

- Ein Transportknoten ist nicht funktionsfähig.
- Wenn auf einem Host Hardware- oder Softwareprobleme vorliegen, die nicht mit NSX-T zusammenhängen, Sie jedoch den Knoten und die zugehörigen Konfigurationen in NSX-T beibehalten möchten, versetzen Sie den Host in den NSX-Wartungsmodus.
- Ein Transportknoten wird automatisch in den NSX-Wartungsmodus versetzt, wenn ein Upgrade auf diesem Transportknoten fehlschlägt.

In den NSX-Wartungsmodus versetzte Transportknoten werden nicht aktualisiert.

## Optische Darstellung eines N-VDS

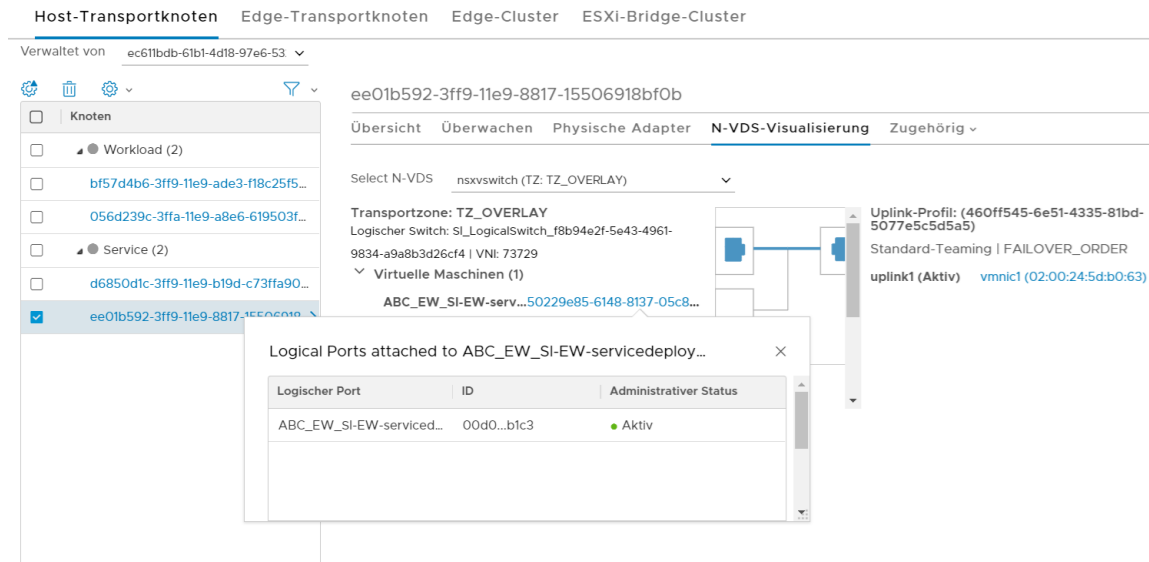
Sie erhalten eine detaillierte Ansicht eines N-VDS auf einer einzelnen Hostebene. NSX-T Data Center stellt eine optische Darstellung des Konnektivitätsstatus zwischen dem Uplink des N-VDS und den VMs bereit, die einer Transportzone zugeordnet sind. Zu den optisch dargestellten Objekten gehören die Teaming-Richtlinie - Uplink und physische Netzwerkkarte, die Konnektivität für VMs bereitstellen. Bei dem anderen optisch dargestellten Satz von Objekten handelt es sich um VMs, zugeordnete logische Ports und Switches und den Status der VMs. Die optische Darstellung erleichtert die Verwaltung des N-VDS.

---

**Hinweis** Nur ESXi-Hosts unterstützen die Darstellung von N-VDS-Objekten.

---

Abbildung 10-3. N-VDS-Visualisierung



## Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **System > Fabric > Knoten > Host-Transportknoten** aus.
- 3 Wählen Sie im Feld „Verwaltet von“ die Option **Eigenständiger Host** oder *Compute Manager* aus.
- 4 Wählen Sie den Host aus.
- 5 Klicken Sie auf die Registerkarte **Darstellung des N-VDS**.
- 6 Wählen Sie einen N-VDS aus.

NSX-T stellt mit VMs verbundene Uplink-Profile, virtuellen Maschinen zugeordnete logische Ports und mit einer Transportzone verknüpfte logische Switches optisch dar.

- 7 Wählen Sie eine VM aus, um die mit einer VM verbundenen Uplink-Profile und den logischen Port anzuzeigen, mit denen eine VM verknüpft ist.

NSX-T stellt die Konnektivität zwischen einer VM und einem Uplink-Profil optisch dar.

- 8 Wählen Sie das Uplink-Profil aus, um die VMs anzuzeigen, die mit einem Uplink-Profil verknüpft sind.
- 9 Zum Anzeigen logischer Ports, die mit einer VM verknüpft sind, erweitern Sie den logischen Switch und klicken auf die VM.

Die Details des logischen Ports werden in einem separaten Dialogfeld angezeigt.

**Hinweis** Der Administratorstatus eines logischen Ports wird im Dialogfeld angezeigt. Wenn der Betriebsstatus nicht verfügbar ist, wird er im Dialogfeld nicht angezeigt.

## Integritätsprüfung für VLAN-ID-Bereiche und MTU-Einstellungen

Führen Sie Integritätsprüfungs-APIs aus, um die Kompatibilität zwischen den von Ihnen angegebenen VLAN-ID-Bereichen und den MTU-Einstellungen auf einem Transportknoten mit den entsprechenden Einstellungen auf einem physischen Switch zu überprüfen.

Die fehlerhafte Zuordnung der VLAN- oder MTU-Konfiguration ist ein allgemeiner Konfigurationsfehler, der zu einem Ausfall der Konnektivität führen kann.

### Hinweis

- Die Ergebnisse der Integritätsprüfung sind lediglich Indikatoren für mögliche Netzwerkkonfigurationsfehler. Beispielsweise führt die Integritätsprüfung auf Hosts aus unterschiedlichen L2-Domänen zu nicht abgeschnittenen VLAN-IDs. Dieses Ergebnis kann nicht als Konfigurationsfehler betrachtet werden, da sich die Hosts in derselben L2-Domäne befinden müssen, damit das Tool für die Integritätsprüfung korrekte Ergebnisse liefert.
- Es können jeweils nur 50-Integritätsprüfungsvorgänge ausgeführt werden.
- Nach Abschluss einer Integritätsprüfung behält NSX-T Data Center die Ergebnisse des Systems nur 24 Stunden lang bei.

Bei einem Integritätsprüfungsvorgang sendet der NSX-T Data Center-opsAgent Prüfpakete von einem Transportknoten an einen anderen Knoten, um die Kompatibilität zwischen dem von Ihnen angegebenen VLAN-ID-Bereich und dem MTU-Wert auf dem Transportknoten mit den entsprechenden Einstellungen auf dem physischen Switch zu überprüfen.

Wenn die Anzahl der zu überprüfenden VLAN-ID-Bereiche zunimmt, steigt die Wartezeit.

Anzahl der VLANs	Wartezeit (Sek.)
[3073, 4095]	150
[1025, 3072]	120
[513, 1024]	80
[128, 512]	60
[64, 127]	30
[1, 63]	20

### Voraussetzungen

- Mindestens zwei für N-VDS konfigurierte Uplinks, damit die VLAN- und MTU-Prüfung funktioniert.
- Transportknoten in derselben L2-Domäne.
- Die Integritätsprüfung wird auf ESX-Hosts mit v6.7U2 oder unterstützt.

## Verfahren

### 1 Erstellen Sie eine manuelle Integritätsprüfung.

POST [https://<NSXManager\\_IP>/api/v1/manual-health-checks](https://<NSXManager_IP>/api/v1/manual-health-checks)

Example Request:

POST <https://<nsx-mgr>/api/v1/manual-health-checks>

```
{
  "resource_type": "ManualHealthCheck",
  "display_name": "Manual HealthCheck 002",
  "transport_zone_id": "7754341c-8f3c-443f-9c1a-2d635d5b0d1c",
  "vlangs": {
    "vlan_ranges": [{
      "start": 0,
      "end": 6
    }],
  },
}
```

Example Response:

```
{
  "operation_status": "FINISHED",
  "transport_zone_id": "7754341c-8f3c-443f-9c1a-2d635d5b0d1c",
  "vlangs": {
    "vlan_ranges": [
      {
        "start": 0,
        "end": 6
      }
    ]
  },
  "result": {
    "vlan_mtu_status": "UNTRUNKED",
    "results_per_transport_node": [
      {
        "transport_node_id": "dfcabffa-8839-11e9-b30e-6f45344d8a04",
        "result_on_host_switch": {
          "host_switch_name": "nsxvswitch",
          "results_per_uplink": [
            {
              "uplink_name": "uplink1",
              "vlan_and_mtu_allowed": [
                {
                  "start": 0,
                  "end": 0
                }
              ],
              "mtu_disallowed": [],
              "vlan_disallowed": [
                {
                  "start": 1,
                  "end": 6
                }
              ]
            }
          ]
        }
      }
    ]
  }
}
```

```

    ]
  },
  {
    "transport_node_id": "a300ea62-8839-11e9-a94e-31732bb71949",
    "result_on_host_switch": {
      "host_switch_name": "nsxvswitch",
      "results_per_uplink": [
        {
          "uplink_name": "uplink1",
          "vlan_and_mtu_allowed": [
            {
              "start": 0,
              "end": 0
            }
          ],
          "mtu_disallowed": [],
          "vlan_disallowed": [
            {
              "start": 1,
              "end": 6
            }
          ]
        }
      ]
    }
  ]
}
],
"resource_type": "ManualHealthCheck",
"id": "8a56ed9e-a31b-479e-987b-2dbfbde07c38",
"display_name": "mc1",
"_create_user": "admin",
"_create_time": 1560149933059,
"_last_modified_user": "system",
"_last_modified_time": 1560149971220,
"_system_owned": false,
"_protection": "NOT_PROTECTED",
"_revision": 0
}

```

Ein neues Integritätsprüfungsobjekt wird mit der ID 8a56ed9e-a31b-479e-987b-2dbfbde07c38 erstellt.

- 2 Um eine Liste aller initiierten manuellen Integritätsprüfungsvorgänge abzurufen, führen Sie den API-Aufruf aus.

GET https://<NSXManager\_IP>/api/v1/manual-health-checks

- 3 Um eine manuelle Integritätsprüfung zu löschen, führen Sie den API-Aufruf aus.

DELETE https://<NSXManager\_IP>/api/v1/manual-health-checks/<Health-check-ID>

- 4 Um eine einzelne Integritätsprüfung manuell zu initiieren, führen Sie den API-Aufruf aus.

GET https://<NSXManager\_IP>/api/v1/manual-health-checks/< Health-check-ID>



## Ergebnisse

Der Abschnitt für die API-Antwort enthält die Ergebnisse der Integritätsprüfung. Der NSX Ops-Agent wartet auf ein Bestätigungspaket vom Zieltransportknoten, um auf dem physischen Switch unterstützte VLAN-ID-Bereiche abzurufen.

- **Ungebündelt:** Listet die VLAN-ID-Bereiche auf, die nicht mit einem physischen Switch kompatibel sind. Die VLAN-ID-Bereiche, die mit dem physischen Switch kompatibel sind, werden ebenfalls aufgelistet.
- **Gebündelt:** Listet die VLAN-ID-Bereiche auf, die mit einem physischen Switch kompatibel sind.
- **Unbekannt:** Es gibt kein gültiges Ergebnis für einige oder alle Uplinks aufgrund von Infrastrukturproblemen oder nicht unterstützten Plattformtypen wie KVM und Edge.

Parameter im API-Antwort-Abschnitt:

- **vlan\_and\_mtu\_allowed:** Listet die kompatiblen VLAN-ID-Bereiche auf.
- **mtu\_disallowed:** Listet die VLAN-ID-Bereiche auf, für die der MTU-Wert nicht mit einem physischen Switch kompatibel ist.
- **vlan\_disallowed:** Listet die VLAN-ID-Bereiche auf, die nicht mit einem physischen Switch kompatibel sind.

## Nächste Schritte

- Aktualisieren Sie in einer Overlay-basierten Transportzone sowohl die VLAN-ID als auch die MTU-Konfiguration im Uplink-Profil auf N-VDS. Aktualisieren Sie ebenfalls VLAN oder MTU auf dem physischen Switch.
- Aktualisieren Sie in einer VLAN-basierten Transportzone die MTU-Konfiguration im Uplink-Profil. Aktualisieren Sie zudem die VLAN-Konfiguration auf logischen Switches dieser Transportzone. Aktualisieren Sie gleichermaßen VLAN oder MTU auf dem physischen Switch.

## Anzeigen des Erkennungsstatus für die bidirektionale Weiterleitung

Zeigen Sie den BFD-Status zwischen Transportknoten an. Jeder Transportknoten erkennt den Verbindungsstatus mit einem anderen Remote-Transportknoten über einen Tunnelstatus, der den BFD-Status zusätzlich zu anderen Details im Zusammenhang mit dem Knoten anzeigt.

Sowohl Hosttransportknoten (eigenständige und in vCenter registrierte Hosts) als auch Edge-Knoten zeigen den Tunnelstatus an. BFD-Pakete unterstützen sowohl die GENEVE- als auch die STT-Kapselung. GENEVE ist die Standardkapselung.

## Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Navigieren Sie zu **System > Fabric > Knoten > Host-Transportknoten**.

- 3 Klicken Sie in der Spalte „Tunnel“ auf die angezeigte Tunnelnummer.

Auf der Seite „Überwachen“ werden der Status des Tunnels, der BFD-Diagnosecode, die Remote-Knoten-UUID, die Kapselung in BFD-Paketen und der Tunnelname angezeigt.

Der Tunnel-BFD-Diagnosecode gibt den Grund für die Änderung des Sitzungsstatus an.

Code	Beschreibung
0	Keine Diagnose
1	Zeit zur Erkennung der Kontrolle abgelaufen
2	Echo-Funktion fehlgeschlagen
3	Nachbar hat inaktive Sitzung signalisiert
4	Zurücksetzen der Weiterleitungsebene
5	Pfad inaktiv
6	Verketteter Pfad inaktiv
7	Administrativ inaktiv
8	Verketteter Umkehrpfad inaktiv

## Ergebnisse

Wenn der BFD-Status inaktiv ist, verwenden Sie den Diagnosecode, um die Konnektivität zwischen den Transportknoten herzustellen.

## 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-Hypervisors

Um Hosts auf die Teilnahme an NSX-T Data Center vorzubereiten, müssen Sie NSX-T Data Center-Kernel-Module auf ESXi-Hosts installieren. So können Sie die NSX-T Data Center-Steuerungskomponenten- und Managementebenen-Fabric erstellen. In VIB-Dateien gepackte NSX-T Data Center-Kernel-Module werden im Hypervisor-Kernel ausgeführt und stellen Dienste wie Distributed Routing, verteilte Firewall und Bridging-Funktionen bereit.

Sie können die NSX-T Data Center-VIBs manuell herunterladen und zum Host-Image hinzufügen. Die Download-Pfade für jede Version von NSX-T Data Center variieren. Rufen Sie die jeweiligen VIBs stets über die NSX-T Data Center-Download-Seite ab.

## Verfahren

- 1 Melden Sie sich als Root oder als Benutzer mit Administratorrechten beim Host an.
- 2 Gehen Sie zum Verzeichnis /tmp.

```
[root@host:~]: cd /tmp
```

- 3 Laden Sie die Datei nsx-lcp herunter und kopieren Sie sie in das Verzeichnis /tmp.
- 4 Führen Sie den Installationsbefehl aus.

```
[root@host:/tmp]: esxcli software vib install -d /tmp/nsx-lcp-<release>.zip
Installation Result
  Message: Operation finished successfully.
  Reboot Required: false
  VIBs Installed: VMware_bootbank_nsx-aggsservice-<release>, VMware_bootbank_nsx-
da-<release>, VMware_bootbank_nsx-esx-datapath-<release>, VMware_bootbank_nsx-exporter-<release>,
VMware_bootbank_nsx-host-<release>, VMware_bootbank_nsx-lldp-<release>, VMware_bootbank_nsx-
mpa-<release>, VMware_bootbank_nsx-netcpa-<release>, VMware_bootbank_nsx-python-
protobuf-<release>, VMware_bootbank_nsx-sfhc-<release>, VMware_bootbank_nsx-<release>,
VMware_bootbank_nsxcli-<release>
  VIBs Removed:
  VIBs Skipped:
```

Je nachdem, was bereits auf dem Host installiert wurde, können einige VIBs installiert, andere entfernt und wieder andere übersprungen werden. Ein Neustart ist nur erforderlich, wenn in der Befehlsausgabe `Reboot Required: true` steht.

## Ergebnisse

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

### nsx-adf

(Automatisiertes Diagnose-Framework) Erfasst und analysiert Leistungsdaten, um sowohl lokale (auf dem Host) als auch zentrale (datencenterübergreifende) Diagnosen zu Leistungsproblemen zu erstellen.

### nsx-aggsservice

Stellt hostseitige Bibliotheken für den NSX-T Data Center-Zusammenfassungsdienst bereit. Der NSX-T Data Center-Zusammenfassungsdienst wird auf den Managementebenenknoten ausgeführt und ruft Laufzeitstatistiken von NSX-T Data Center-Komponenten ab.

### nsx-cli-libs

Stellt die NSX-T Data Center-CLI auf Hypervisor-Hosts bereit.

#### **nsx-common-libs**

Stellen einige Hilfsklassen bereit, unter anderem AES, SHA-1, UUID und Bitmap.

#### **nsx-context-mux**

Bietet NSX Guest Introspektion-Relaisfunktionalität. Ermöglicht VMware Tools Guest-Agents das Weiterleiten von Gastkontext an interne und registrierte Partner-Appliances von Drittanbietern.

#### **nsx-esx-datapath**

Bietet NSX-T Data Center-Paket-Verarbeitungsfunktionalität auf der Data Plane.

#### **nsx-exporter**

Stellt Hostagents bereit, die Laufzeitstatistiken an den Zusammenfassungsdienst melden, der auf der Management Plane ausgeführt wird.

#### **nsx-host**

Liefert Metadaten für das VIB-Paket, das auf dem Host installiert ist.

#### **nsx-metrics-libs**

Stellt Metrik-Hilfsklassen für das Erfassen von Daemon-Metriken bereit.

#### **nsx-mpa**

Stellt Kommunikation zwischen NSX Manager und Hypervisor-Hosts bereit.

#### **nsx-nestdb-libs**

NestDB ist eine Datenbank, in der NSX-Konfigurationen im Zusammenhang mit dem Host gespeichert werden (gewünschter/Laufzeitstatus usw.).

#### **nsx-netcpa**

Stellt Kommunikation zwischen der zentralen Control Plane und Hypervisors bereit. Erhält den logischen Netzwerkzustand von der zentralen Control Plane und programmiert diesen Zustand auf der Data Plane.

#### **nsx-opsagent**

Gibt Operations Agent-Ausführungen (Transportknoten-Realisation, Link-Layer-Discovery-Protokoll-LLDP, Traceflow, Paketerfassung usw.) an die Management Plane weiter.

#### **nsx-platform-client**

Stellt einen allgemeinen CLI-Ausführungs-Agent für die zentrale CLI und die Erfassung von Überwachungsprotokollen bereit.

#### **nsx-profiling-libs**

Bietet die Funktionalität der Profilerstellung basierend auf gpeftool, welches auch für die Daemon-Prozess-Profilerstellung verwendet wird.

### **nsx-proxy**

Stellt den einzigen Northbound-Kontaktpunkt-Agent bereit, der mit der zentralen Control Plane und der Management Plane kommuniziert.

### **nsx-python-gevent**

Enthält Python Gevent

### **nsx-python-greenlet**

Enthält die Python Greenlet-Bibliothek (Drittanbieterbibliotheken).

### **nsx-python-logging**

Enthält die Python-Protokolle.

### **nsx-python-protobuf**

Bietet Python-Bindungen für Protokollpuffer.

### **nsx-rpc-libs**

Diese Bibliothek bietet NSX-RPC-Funktionalität.

### **nsx-sfhc**

Dienst-Fabric-Hostkomponente (Service Fabric Host Component; SFHC). Liefert einen Hostagenten für die Verwaltung des Lebenszyklus des Hypervisors als Fabric-Host im Bestand der Managementebene. Darüber erhalten Sie einen Kanal für Vorgänge wie NSX-T Data Center-Upgrade sowie Deinstallation und Überwachung von NSX-T Data Center-Modulen auf Hypervisors.

### **nsx-shared-libs**

Enthält die gemeinsam genutzten NSX-Bibliotheken.

### **nsx-upm-libs**

Bietet einheitliche Profil-Verwaltungsfunktionen für eine verminderte clientseitige Konfiguration und das Vermeiden einer doppelten Datenübertragung.

### **nsx-vdpi**

Bietet Deep Packet Inspection-Funktionen für die verteilte Firewall für NSX-T Data Center.

### **nsxcli**

Stellt die NSX-T Data Center-CLI auf Hypervisor-Hosts bereit.

### **vsipfwlib**

Bietet verteilte Firewall-Funktionalität.

Zur Überprüfung können Sie die Befehle `esxcli software vib list | grep nsx` und `esxcli software vib list | grep vsipfwlib` auf dem ESXi-Host ausführen. Alternativ können Sie den Befehl `esxcli software vib list | grep <yyyy-mm-dd>` ausführen, wobei es sich beim Datum um das Installationsdatum handelt.

### Nächste Schritte

Fügen Sie den Host der NSX-T Data Center-Management Plane hinzu. Siehe [Bereitstellen von NSX Manager-Knoten zur Bildung eines Cluster mithilfe der CLI](#).

## Manuelles Installieren von NSX-T Data Center-Softwarepaketen 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-Control Plane- und Management Plane-Fabric erstellen. In DEB-Dateien gepackte NSX-T Data Center-Kernel-Module werden im Hypervisor-Kernel ausgeführt und stellen Dienste wie Distributed Routing, verteilte Firewall und Bridging-Funktionen bereit.

Sie können die NSX-T Data Center-DEBs manuell herunterladen und zum Host-Image hinzufügen. Beachten Sie, dass die Download-Pfade von Version zu Version von NSX-T Data Center variieren können. Rufen Sie die jeweiligen DEBs stets über die NSX-T Data Center-Download-Seite ab.

### Voraussetzungen

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

### Verfahren

- 1 Melden Sie sich als Benutzer mit Administratorrechten beim Host an.
- 2 (Optional) Gehen Sie zum Verzeichnis /tmp.

```
cd /tmp
```

- 3 Laden Sie die Datei nsx-lcp herunter und kopieren Sie sie in das Verzeichnis /tmp.
- 4 Dekomprimieren Sie das Paket.

```
tar -xvf nsx-lcp-<release>-ubuntu-trusty-amd64.tar.gz
```

- 5 Gehen Sie zum Paketverzeichnis.

```
cd nsx-lcp-trusty-amd64/
```

- 6 Installieren Sie die Pakete.

```
sudo dpkg -i *.deb
```

- 7 Laden Sie das OVS-Kernel-Modul erneut.

```
/etc/init.d/openvswitch-switch force-reload-kmod
```

Wenn der Hypervisor DHCP auf OVS-Schnittstellen verwendet, starten Sie die Netzwerkschnittstelle, auf der DHCP konfiguriert ist, neu. Sie können den alten Dhclient-Prozess auf der Netzwerkschnittstelle manuell anhalten und einen neuen Dhclient-Prozess auf dieser Schnittstelle starten.

- 8 Zur Überprüfung können Sie den Befehl `dpkg -l | egrep 'nsx|openvswitch'` ausführen.

Die installierten Pakete in der Ausgabe müssen mit den Paketen im Verzeichnis `nsx-lcp-trusty_amd64` übereinstimmen.

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-Management Plane hinzu. Siehe [Bereitstellen von NSX Manager-Knoten zur Bildung eines Cluster mithilfe der CLI](#).

## Manuelles Installieren von NSX-T Data Center-Softwarepaketen 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-Control Plane- und Management Plane-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 Repositories zugreifen können.

**6** Laden Sie das OVS-Kernel-Modul erneut.

```
/usr/share/openvswitch/scripts/ovs-systemd-reload 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'` 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-Management Plane hinzu. Siehe [Bereitstellen von NSX Manager-Knoten zur Bildung eines Cluster mithilfe der CLI](#).

## Manuelles Installieren von NSX-T Data Center-Softwarepaketen auf SUSE-KVM-Hypervisoren

Um Hosts auf die Teilnahme an NSX-T Data Center vorzubereiten, können Sie NSX-T Data Center-Kernel-Module manuell auf SUSE-KVM-Hosts installieren.

So können Sie die NSX-T Data Center-Control Plane- und Management Plane-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 SUSE-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-3.0.0.0.14335404-linux64-sles12sp3.tar.gz
```

- 4 Gehen Sie zum Paketverzeichnis.

```
cd nsx-lcp-linux64-sles12sp3
```

- 5 Installieren Sie die Pakete.

```
sudo zypper --no-gpg-checks install -y *.rpm
```

Beim Ausführen des Zypper-Installationsbefehls werden sämtliche NSX-T Data Center-Abhängigkeiten aufgelöst, vorausgesetzt, dass die SUSE-Hosts auf ihre jeweiligen Repositories zugreifen können.

- 6 Laden Sie das OVS-Kernel-Modul erneut.

```
/usr/share/openvswitch/scripts/ovs-systemd-reload 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 `zypper packages --installed-only | grep System | egrep 'openvswitch|nsx'` ausführen.

Die installierten Pakete in der Ausgabe müssen mit den Paketen im Verzeichnis nsx-lcp-linux64-sles12sp3 übereinstimmen.

## Nächste Schritte

Fügen Sie den Host der NSX-T Data Center-Management Plane hinzu. Siehe [Bereitstellen von NSX Manager-Knoten zur Bildung eines Cluster mithilfe der CLI](#).

## Bereitstellung eines vollständig reduzierten vSphere-Clusters NSX-T

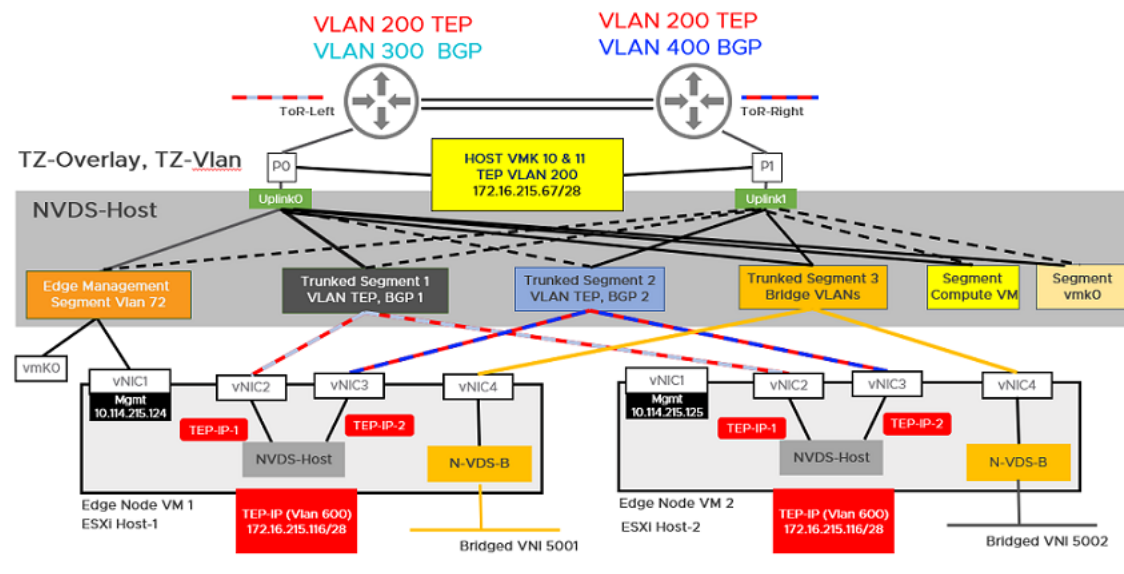
Sie können NSX Manager, Host-Transportknoten und NSX Edge-VMs in einem einzelnen Cluster konfigurieren. Jeder Host im Cluster stellt zwei physische NICs bereit, die für NSX-T konfiguriert sind.

**Wichtig** Stellen Sie ab NSX-T-Version 2.4.2 oder 2.5 die vollständig reduzierte vSphere-Einzel-Cluster-Topologie bereit.

Die bei dieser Vorgehensweise referenzierte Topologie verwendet Folgendes:

- Mit den Hosts im Cluster konfiguriertes vSAN.
- Mindestens zwei physische Netzwerkkarten pro Host.
- vMotion- und Management-VMkernel-Schnittstellen.

Abbildung 10-4. Topologie: einzelner N-VDS-Switch, der die Host-Kommunikation mit NSX Edge und Gast-VMs verwaltet

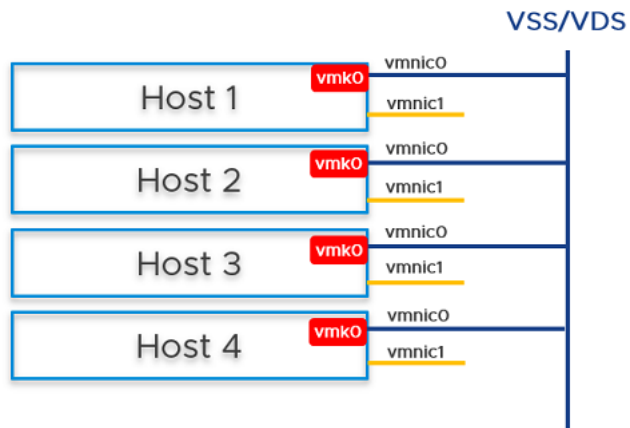


### Voraussetzungen

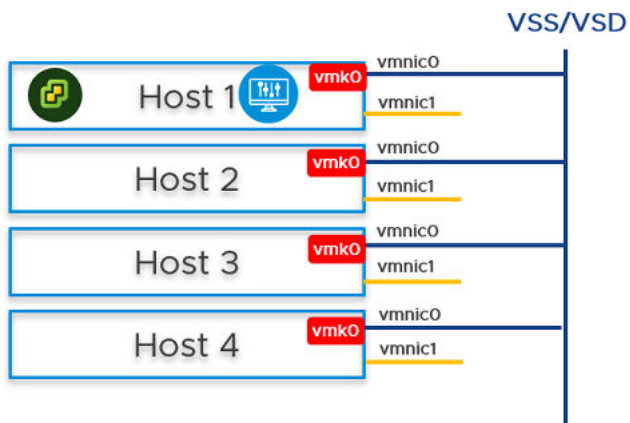
- Alle Hosts müssen Teil eines vSphere-Clusters sein.
- Auf jedem Host sind zwei physische Netzwerkkarten aktiviert.
- Registrieren Sie alle Hosts bei einem vCenter Server.
- Überprüfen Sie auf dem vCenter Server, ob freigegebener Speicher für die Verwendung durch die Hosts verfügbar ist.
- Die IP des Hosts und die TEP IP von NSX Edge müssen sich in einem anderen VLAN befinden. Der vertikale Datenverkehr von Host-Arbeitslasten wird in GENEVE eingekapselt und an einen NSX Edge-Knoten mit der Quell-IP-Adresse als Host und der Ziel-IP als NSX Edge-TEP gesendet. Da sich diese TEPs in verschiedenen VLAN/Subnetzen befinden müssen, muss dieser Datenverkehr über die Top-of-Rack (Tor)-Switches geleitet werden. Die für den Host verwendete Transport-VLAN ist VLAN 200 und die für NSX Edge verwendete Transport-VLAN ist VLAN 600.

## Verfahren

- 1 Bereiten Sie vier ESXi-Hosts mit vmnic0 auf vSS oder vDS vor, vmnic1 ist frei.



- 2 Installieren Sie vCenter Server auf Host 1, konfigurieren Sie eine vSS/vDS-Portgruppe und installieren Sie NSX Manager auf der Portgruppe, die auf dem Host erstellt wurde.

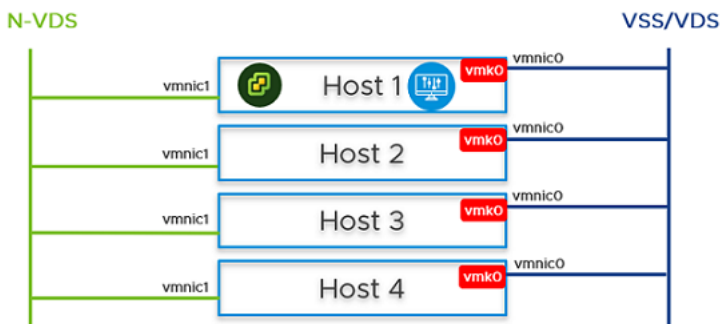


- 3 Bereiten Sie ESXi-Hosts 1, 2, 3 und 4 als Transportknoten vor.
  - a Erstellen Sie eine VLAN-Transportzone und eine Overlay-Transportzone mit einer benannten Teaming-Richtlinie. Siehe [Erstellen von Transportzonen](#).
  - b Erstellen Sie einen IP-Pool oder DHCP für Tunnel-Endpoint-IP-Adressen für die Hosts. Siehe [Erstellen eines IP-Pools für Tunnel-Endpoint-IP-Adressen](#).
  - c Erstellen Sie einen IP-Pool oder DHCP für Tunnel-Endpoint-IP-Adressen für den Edge-Knoten. Siehe [Erstellen eines IP-Pools für Tunnel-Endpoint-IP-Adressen](#).
  - d Erstellen Sie ein Uplink-Profil mit einer benannten Teaming-Richtlinie. Siehe [Erstellen eines Uplink-Profiles](#).

- e Konfigurieren Sie Hosts als Transportknoten, indem Sie ein Transportknotenprofil anwenden. In diesem Schritt migriert das Transportknotenprofil nur vmnic1 (die nicht verwendete physische NIC) zum N-VDS-Switch. Nachdem das Transportknotenprofil auf die Cluster-Hosts angewendet wurde, wird der N-VDS-Switch erstellt und vmnic1 ist mit dem N-VDS-Switch verbunden. Siehe [Hinzufügen eines Transportknotenprofils](#).

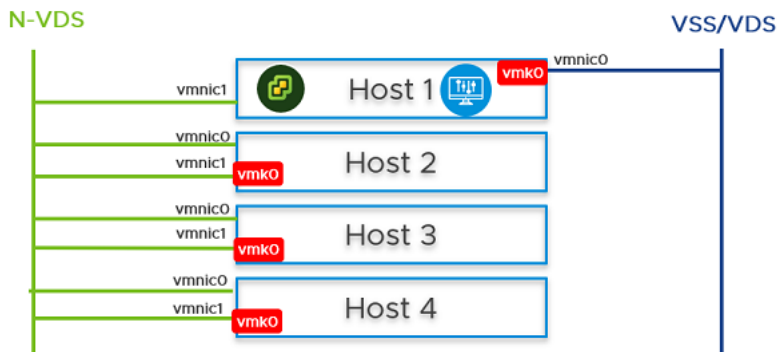
## Transportknotenprofil bearbeiten – TNP-host ?

N-VDS-Name *	vds-1	▼
Zugeordnete Transportzonen	tz	
NIOC-Profil *	nsx-default-nioc-hostswitch-profile	▼
	<a href="#">ODER Neues NIOC-Profil erstellen</a>	
Uplink-Profil *	hostnodeprofile	▼
	<a href="#">ODER Neues Uplink-Profil erstellen</a>	
LLDP-Profil *	LLDP [Send Packet Enabled]	▼
IP-Zuweisung *	IP-Pool verwenden	▼
IP-Pool *	ippoolhostnode	▼
	<a href="#">ODER Neuen IP-Pool erstellen und verwenden</a>	
Physische Netzwerkkarten	vmnic1	activeuplinkhost ▼
		<a href="#">PNIC hinzufügen</a>
Migration nur von PNIC	<input checked="" type="checkbox"/> Ja	
Aktivieren Sie diese Option, wenn auf dem für die Migration ausgewählten PNIC keine VMKs existieren		
Netzwerkzuordnungen für die Installation	<a href="#">Zuordnung hinzufügen</a>	
Netzwerkzuordnungen für die Deinstallation	<a href="#">Zuordnung hinzufügen</a>	

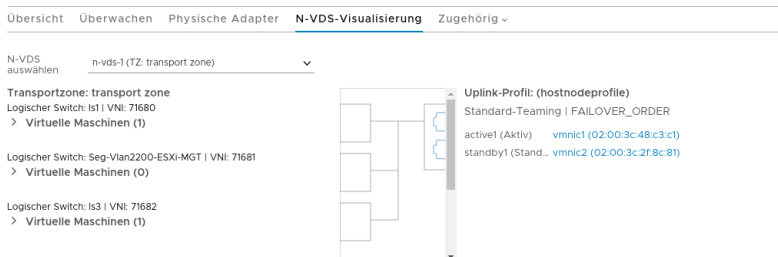


vmnic1 auf allen Hosts werden dem N-VDS-Switch hinzugefügt. Von den beiden physischen Netzwerkkarten wird also eine auf den N-VDS-Switch migriert. Die vmnic0-Schnittstelle ist weiterhin mit dem vSS- oder vDS-Switch verbunden, wodurch sichergestellt wird, dass die Konnektivität mit dem Host verfügbar ist.

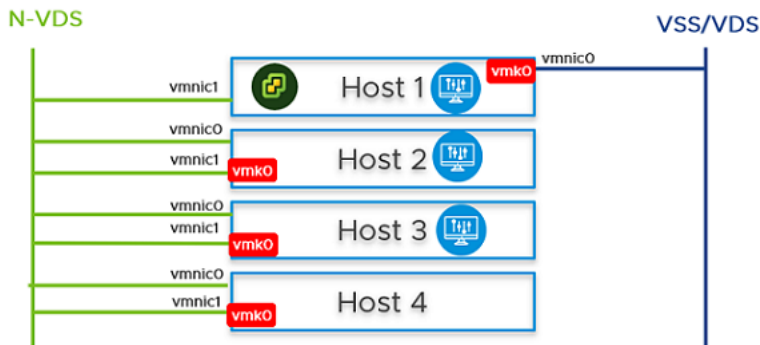
- 4 Erstellen Sie auf der NSX Manager-Benutzeroberfläche VLAN-gestützte Segmente für NSX Manager, vCenter Server und NSX Edge. Stellen Sie sicher, dass für jedes der VLAN-gestützten Segmente die richtige Teaming-Richtlinie ausgewählt ist. Verwenden Sie keinen logischen VLAN-Trunk-Switch als Ziel. Geben Sie beim Erstellen von Zielsegmenten auf der NSX Manager-Benutzeroberfläche im Feld **VLAN-Liste eingeben** nur einen VLAN-Wert ein.
- 5 Auf Host 2, Host 3 und Host 4 müssen Sie den vmkO-Adapter und vmnic0 zusammen von VSS/VDS auf den N-VDS-Switch migrieren. Aktualisieren Sie die NSX-T-Konfiguration auf jedem Host. Stellen Sie beim Migrieren Folgendes sicher:
  - vmkO ist dem **Edge-Verwaltungssegment** zugeordnet.
  - vmnic0 ist einem aktiven Uplink (**uplink-1**) zugeordnet.



- 6 Wechseln Sie in vCenter Server zu Host 2, Host 3 und Host 4. Stellen Sie sicher, dass der vmkO-Adapter mit der physischen vmnic0-NIC auf dem N-VDS verbunden und erreichbar ist.
- 7 Wechseln Sie in der NSX Manager-Benutzeroberfläche zu Host 2, Host 3 und Host 4. Überprüfen Sie, ob sich beide pNICs auf dem N-VDS-Switch befinden.

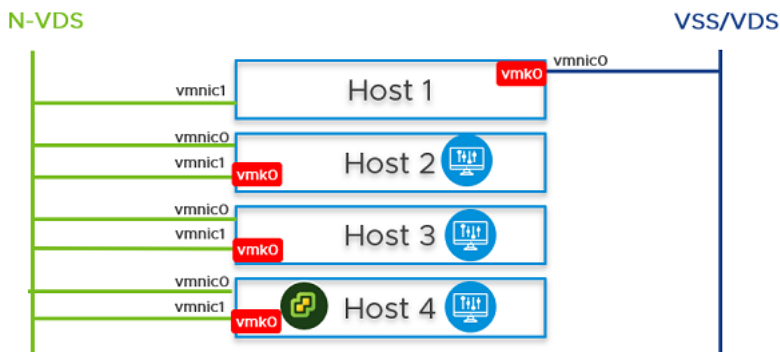


- 8 Installieren Sie über die NSX Manager-Benutzeroberfläche NSX Manager auf Host 2 und Host 3 und hängen Sie NSX Manager an das Segment an. Warten Sie etwa 10 Minuten, bis sich der Cluster formiert hat, und stellen Sie sicher, dass dies richtig durchgeführt wurde.



- 9 Schalten Sie den ersten NSX Manager-Knoten aus. Warten Sie etwa 10 Minuten.
- 10 Verbinden Sie NSX Manager und vCenter Server erneut mit dem zuvor erstellten logischen Switch. Schalten Sie NSX Manager auf Host 4 ein. Warten Sie etwa 10 Minuten, um sicherzustellen, dass sich der Cluster in einem stabilen Zustand befindet. Wenn der erste NSX Manager ausgeschaltet ist, führen Sie eine kalte vMotion aus, um NSX Manager und vCenter Server von Host 1 auf Host 4 zu migrieren.

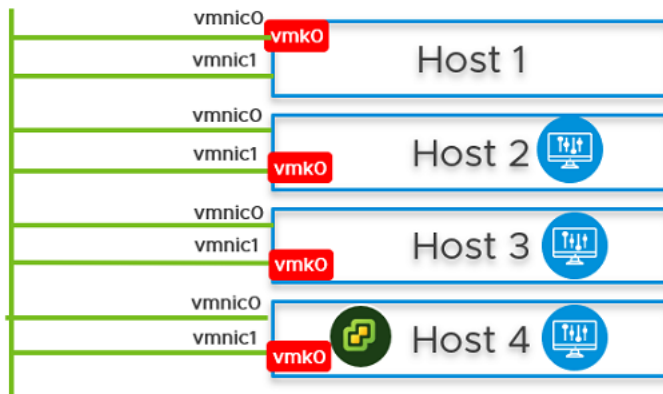
Informationen zu vMotion-Einschränkungen finden Sie unter <https://kb.vmware.com/s/article/56991>.



- 11 Wechseln Sie auf der NSX Manager-Benutzeroberfläche zu Host 1, migrieren Sie vmk0 und vmnic0 zusammen von VSS zum N-VDS-Switch.

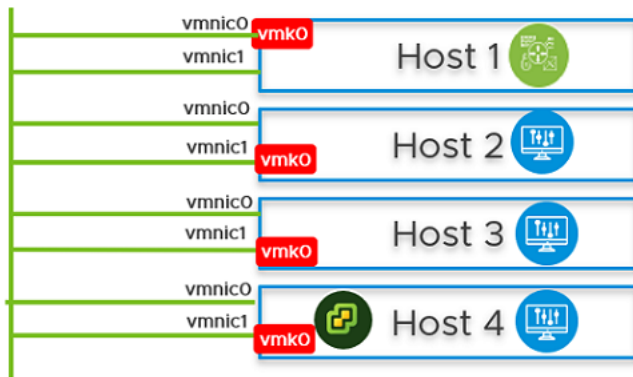
- 12** Stellen Sie im Feld **Netzwerkzuordnung für Installation** sicher, dass der vmk0-Adapter dem **Edge-Verwaltungssegment** auf dem N-VDS-Switch zugeordnet ist.

## N-VDS



- 13** Installieren Sie auf Host 1 die NSX Edge-VM über die Benutzeroberfläche von NSX Manager.  
Siehe [Erstellen eines NSX Edge-Transportknotens](#).

## N-VDS



- 14 Verbinden Sie die NSX Edge-VM mit der Management Plane.

Siehe [Verbinden von NSX Edge mit der Management Plane](#).

- 15 Um die Konnektivität für den Nord-Süd-Datenverkehr einzurichten, konfigurieren Sie die NSX Edge-VM mit einem externen Router.
- 16 Stellen Sie sicher, dass die Nord-Süd-Datenverkehrskonnektivität zwischen der NSX Edge-VM und dem externen Router besteht.
- 17 Im Falle eines Stromausfalls, bei dem der gesamte Cluster neu gestartet wird, kann die NSX-T-Verwaltungskomponente möglicherweise nicht mehr mit dem N-VDS kommunizieren. Um dieses Szenario zu vermeiden, führen Sie die folgenden Schritte aus:

---

**Vorsicht** Jeder API-Befehl, der falsch ausgeführt wird, führt zu einem Verlust der Konnektivität mit NSX Manager.

---

**Hinweis** In einer einzelnen Clusterkonfiguration werden Verwaltungskomponenten auf einem N-VDS-Switch als VMs gehostet. Der N-VDS-Port, mit dem die Verwaltungskomponente standardmäßig eine Verbindung herstellt, wird aus Sicherheitsgründen als blockierter Port initialisiert. Im Falle eines Stromausfalls, bei dem alle vier Hosts neu gestartet werden müssen, wird der Verwaltungs-VM-Port in einem blockierten Zustand initialisiert. Um zirkuläre Abhängigkeiten zu vermeiden, wird empfohlen, einen Port auf dem N-VDS im Zustand „nicht blockiert“ zu erstellen. Ein nicht blockierter Port stellt sicher, dass die NSX-T-Verwaltungskomponente bei einem Neustart des Clusters mit dem N-VDS kommunizieren kann, um wieder eine normale Funktion zu gewährleisten.

---

Am Ende der Teilaufgabe übernimmt der Migrationsbefehl Folgendes:

- UUID des Host-Knotens, auf dem sich der NSX Manager befindet.
- UUID der NSX Manager-VM und migriert sie auf den statischen logischen Port, der sich in einem nicht blockierten Zustand befindet.



Wenn alle Hosts aus- oder eingeschaltet sind oder eine NSX Manager-VM auf einen anderen Host verschoben wird, wird sie, nachdem NSX Manager wiederhergestellt wurde, an einen nicht blockierten Port angehängt. Dadurch wird der Verlust der Konnektivität mit der Verwaltungskomponente von NSX-T verhindert.

- a Gehen Sie in der NSX Manager-Benutzeroberfläche zur Registerkarte **Netzwerk und Sicherheit – Erweitert** (2.5.1 und Vorgängerversionen). Suchen Sie nach dem Segment **Segment-Computing-VM**. Wählen Sie die UUID auf der Registerkarte **Übersicht** aus und kopieren Sie sie. Die in diesem Beispiel verwendete UUID ist `c3fd8e1b-5b89-478e-abb5-d55603f04452`.
- b Erstellen Sie eine JSON-Nutzlast für jeden NSX Manager.
  - Erstellen Sie in der JSON-Nutzlast logische Ports mit dem Initialisierungsstatus **UNBLOCKED\_VLAN**, indem Sie den Wert für `logical_switch_id` mit der UUID des zuvor erstellten **Edge-Verwaltungssegments** ersetzen.
  - In der Nutzlast für jeden NSX Manager sind die Werte `attachment_type_id` und `display_name` unterschiedlich.

---

**Wichtig** Wiederholen Sie diesen Schritt, um insgesamt vier JSON-Dateien zu erstellen: drei für NSX Manager und eine für vCenter Server Appliance (VCSA).

```
port1.json
{
  "admin_state": "UP",
  "attachment": {
    "attachment_type": "VIF",
    "id": "nsxmgr-port-147"
  },
  "display_name": "NSX Manager Node 147 Port",
  "init_state": "UNBLOCKED_VLAN",
  "logical_switch_id": "c3fd8e1b-5b89-478e-abb5-d55603f04452"
}
```

Dabei gilt Folgendes:

- `admin_state`: Dies ist der Status des Ports. Er muss „AKTIV“ sein.
- `attachment_type`: Muss auf VIF festgelegt sein. Alle VMs werden mithilfe einer VIF-ID mit NSX-T Switch-Ports verbunden.
- `id`: Dies ist die VIF-ID. Sie muss für jeden NSX Manager eindeutig sein. Wenn Sie über drei NSX Manager verfügen, gibt es drei Nutzlasten, für die jeweils eine andere VIF-ID vorhanden sein muss. Um eine eindeutige UUID zu generieren, müssen Sie sich bei der Root-Shell von NSX Manager an und führen Sie `/usr/bin/uuidgen` aus, damit eine eindeutige UUID generiert wird.
- `display_name`: Er muss eindeutig sein, damit ein NSX-Administrator ihn unter den anderen NSX Manager-Anzeigenamen identifizieren kann.

- `init_state`: Wenn der Wert auf `UNBLOCKED_VLAN` festgelegt ist, hebt NSX die Blockierung des Ports für NSX Manager auf, auch wenn der NSX Manager nicht verfügbar ist.
- `logical_switch_id`: Dies ist die ID des logischen Switches für das **Edge-Verwaltungssegment**.

- c Wenn drei NSX Manager bereitgestellt sind, müssen Sie drei Nutzlasten erstellen – eine für jeden logischen Port eines NSX Managers. Beispiel: port1.json, port2.json, port3.json.

Führen Sie die folgenden Befehle aus, um Nutzlasten zu erstellen.

```
curl -X POST -k -u '<username>:<password>' -H 'Content-Type:application/json' -d @port1.json https://nsxmgr/api/v1/logical-ports
```

```
curl -X POST -k -u '<username>:<password>' -H 'Content-Type:application/json' -d @port2.json https://nsxmgr/api/v1/logical-ports
```

```
curl -X POST -k -u '<username>:<password>' -H 'Content-Type:application/json' -d @port3.json https://nsxmgr/api/v1/logical-ports
```

Ein Beispiel für die API-Ausführung zum Erstellen eines logischen Ports.

```
root@nsx-mgr-147:/var/CollapsedCluster# curl -X POST -k -u
'<username>:<password>' -H 'Content-Type:application/json' -d @port1.json https://
localhost/api/v1/logical-ports
{
  "logical_switch_id" : "c3fd8e1b-5b89-478e-abb5-d55603f04452",
  "attachment" : {
    "attachment_type" : "VIF",
    "id" : "nsxmgr-port-147"
  },
  "admin_state" : "UP",
  "address_bindings" : [ ],
  "switching_profile_ids" : [ {
    "key" : "SwitchSecuritySwitchingProfile",
    "value" : "fbc4fb17-83d9-4b53-a286-ccdf04301888"
  }, {
    "key" : "SpoofGuardSwitchingProfile",
    "value" : "fad98876-d7ff-11e4-b9d6-1681e6b88ec1"
  }, {
    "key" : "IpDiscoverySwitchingProfile",
    "value" : "0c403bc9-7773-4680-a5cc-847ed0f9f52e"
  }, {
    "key" : "MacManagementSwitchingProfile",
    "value" : "1e7101c8-cfef-415a-9c8c-ce3d8dd078fb"
  }, {
    "key" : "PortMirroringSwitchingProfile",
    "value" : "93b4b7e8-f116-415d-a50c-3364611b5d09"
  }, {
    "key" : "QosSwitchingProfile",
    "value" : "f313290b-eba8-4262-bd93-fab5026e9495"
  } ],
  "init_state" : "UNBLOCKED_VLAN",
  "ignore_address_bindings" : [ ],
  "resource_type" : "LogicalPort",
  "id" : "02e0d76f-83fa-4839-a525-855b47ecb647",
  "display_name" : "NSX Manager Node 147 Port",
  "_create_user" : "admin",
  "_create_time" : 1574716624192,
  "_last_modified_user" : "admin",
```

```
"_last_modified_time" : 1574716624192,
"_system_owned" : false,
"_protection" : "NOT_PROTECTED",
"_revision" : 0
```

- d Stellen Sie sicher, dass der logische Port erstellt wurde.

Switches <b>Ports</b> Switching-Profile						
<div> + HINZUFÜGEN BEARBEITEN LÖSCHEN AKTIONEN </div> <div>Suchen</div>						
<input type="checkbox"/>	Logischer Port	ID	Administrativer	Betriebsstatus	Switching-Profile	Anhang
<input type="checkbox"/>	1356a49d-dc33-42be-9e83-4c6...	1356...d0ee	Aktiv	Aktiv	nsx-default-switch-security-non...	LR:80fb...2662
<input type="checkbox"/>	61d5708b-a4ff-4954-b217-8338...	61d5...b43a	Aktiv	Aktiv	nsx-default-switch-security-non...	LR:42ac...ad24
<input type="checkbox"/>	NSX Manager Node 147 Port	58ad...a1cb	Aktiv	Inaktiv	nsx-default-switch-security-vif...	VM.nsx-mgr-147
<input type="checkbox"/>	ubuntu12.04.1-2G-LAMP/ubuntu1...	3fb2...f698	Aktiv	Aktiv	nsx-default-switch-security-vif...	VM.vm1
<input type="checkbox"/>	vmnic@n-vds-1@94b323e6-1ee...	2021...4d76	Aktiv	Aktiv	nsx-default-switch-security-vif...	VIF:abf2...0495
<input type="checkbox"/>	worker/worker.vmx@94b323e6-...	50b7...9b4c	Aktiv	Aktiv	nsx-default-switch-security-vif...	VM.vm3

- e Suchen Sie die VM-Instanz-ID für jeden NSX Manager. Wechseln Sie zum Abrufen der Instanz-ID zu **Bestand** → **Virtuelle Maschinen**, wählen Sie die NSX Manager-VM und dann die Registerkarte **Übersicht** aus und kopieren Sie die Instanz-ID. Alternativ können Sie die Instanz-ID im Browser für verwaltete Objekte (Managed Object Browser, MOB) von vCenter Server durchsuchen. Fügen Sie der ID **:4000** hinzu, um den VNIC-Hardwareindex einer NSX Manager-VM abzurufen.

Wenn die Instanz-UUID der VM beispielsweise 503c9e2b-0abf-a91c-319c-1d2487245c08 ist, lautet deren VNIC-Index 503c9e2b-0abf-a91c-319c-1d2487245c08:4000. Die drei NSX Manager-VNIC-Indizes lauten:

mgr1 vnic: 503c9e2b-0abf-a91c-319c-1d2487245c08:4000

mgr2 vnic: 503c76d4-3f7f-ed5e-2878-cffc24df5a88:4000

mgr3 vnic: 503cafd5-692e-d054-6463-230662590758:4000

- f Suchen Sie die Transportknoten-ID, die NSX Manager hostet. Wenn Sie über drei NSX Manager verfügen, die in unterschiedlichen Transportknoten gehostet werden, notieren Sie die Transportknoten-IDs. Die drei Transportknoten-IDs lauten beispielsweise:

tn1: 12d19875-90ed-4c78-a6bb-a3b1dfe0d5ea

tn2: 4b6e182e-0ee3-403f-926a-fb7c8408a9b7

tn3: d7cec2c9-b776-4829-beea-1258d8b8d59b

- g Rufen Sie die Transportknotenkonfiguration ab, die beim Migrieren der NSX Manager zum neu erstellten Port als Nutzlast verwendet werden soll.

Beispiel:

```
curl -k -u '<user>:<password>' https://nsxmgr/api/v1/transport-nodes/
12d19875-90ed-4c78-a6bb-a3b1dfe0d5ea > tn1.json
```

```
curl -k -u '<user>:<password>' https://nsxmgr/api/v1/transport-nodes/
4b6e182e-0ee3-403f-926a-fb7c8408a9b7 > tn2.json
```

```
curl -k -u '<user>:<password>' https://nsxmgr/api/v1/transport-nodes/d7cec2c9-
b776-4829-beea-1258d8b8d59b > tn3.json
```

- h Migrieren Sie den NSX Manager vom vorherigen Port zum neu erstellten nicht blockierten logischen Port im **Edge-Verwaltungssegment**. Der Wert der VIF-ID ist die Anhang-ID des Ports, der zuvor für NSX Manager erstellt wurde.

Die folgenden Parameter werden zum Migrieren von NSX Manager benötigt:

- Transportknoten-ID
- Transportknotenkonfiguration
- NSX Manager-VNIC-Hardwareindex
- NSX Manager-VIF-ID

Der API-Befehl zum Migrieren von NSX Manager zum neu erstellten nicht blockierten Port lautet:

```
/api/v1/transport-nodes/<TN-ID>?vnic=<VNIC-ID>&vif=<VIF-ID>
```

Beispiel:

```
root@nsx-mgr-147:/var/CollapsedCluster# curl -k -X PUT -u 'admin:VMware1!VMware1!' -H 'Content-Type:application/json' -d @mgr.json 'https://localhost/api/v1/transport-nodes/11161331-11f8-45c7-8747-34e7218b687f?vnic=5028d756-d36f-719e-3db5-7ae24aa1d6f3:4000&vif=nsxmgr-port-147'
```

- i Stellen Sie sicher, dass die statisch erstellte logische Portgruppe aktiv (Up) ist.

Switches <b>Ports</b> Switching-Profile						
+ HINZUFÜGEN    ✎ BEARBEITEN    🗑 LÖSCHEN    ⚙ AKTIONEN <input type="text" value="Suchen"/>						
<input type="checkbox"/>	Logischer Port ↑	ID	Administrativer	Betriebsstatus	Switching-Profil	Logischer Switch
<input type="checkbox"/>	1356a49d-dc33-42be-9e83-4c6...	1356...d0ee	● Aktiv	● Aktiv	nsx-default-switch-security-non...	LR:80fb...2662
<input type="checkbox"/>	61d5708b-a4ff-4954-b217-8338...	61d5...b43a	● Aktiv	● Aktiv	nsx-default-switch-security-non...	LR:42ac...ad24
<input type="checkbox"/>	NSX Manager Node 147 Port	58ad...a1cb	● Aktiv	● Aktiv	nsx-default-switch-security-vif...	VM nsx-mgr-147
<input type="checkbox"/>	ubuntu12.04.1-2G-LAMP/ubuntu1...	3fb2...f698	● Aktiv	● Aktiv	nsx-default-switch-security-vif...	VM:vm1
<input type="checkbox"/>	vmnic@n-vds-1@94b323e6-1ee...	2021...4d76	● Aktiv	● Aktiv	nsx-default-switch-security-vif...	VIF:abf2...0495
<input type="checkbox"/>	worker/worker.vmx@94b323e6-...	50b7...9b4c	● Aktiv	● Aktiv	nsx-default-switch-security-vif...	VM:vm3

- j Wiederholen Sie die vorherigen Schritte für jeden NSX Manager im Cluster.

# Integration des Hostprofils in NSX-T

# 11

Integrieren Sie Hostprofile, die von einem ESXi-Host mit NSX-T extrahiert wurden, um ESXi- und NSX-T-VIBs auf statusorientiert und statusfreien Servern bereitzustellen.

Dieses Kapitel enthält die folgenden Themen:

- [Automatische Bereitstellung statusfreier Cluster](#)
- [Statusorientierte Server](#)

## Automatische Bereitstellung statusfreier Cluster

Statusfreie Hosts behalten die Konfiguration nicht bei, daher benötigen sie einen Server für die automatische Bereitstellung, um die erforderlichen Startdateien bereitzustellen, wenn die Hosts eingeschaltet werden.

In diesem Abschnitt finden Sie Informationen zum Einrichten eines statusfreien Clusters mithilfe von vSphere Auto Deploy und dem NSX-T-Transportknotenprofil, um einen Host mit einem neuen Image-Profil erneut bereitzustellen, das eine andere Version von ESXi und NSX-T enthält. Hosts, die für die automatische Bereitstellung von vSphere eingerichtet sind, verwenden einen Server mit automatischer Bereitstellung und vSphere-Hostprofile, um Hosts anzupassen. Diese Hosts können auch für das NSX-T-Transportknotenprofil eingerichtet werden, um NSX-T auf den Hosts zu konfigurieren.

Daher kann ein statusfreier Host für die automatische Bereitstellung von vSphere und des NSX-T-Transportknotenprofils eingerichtet werden, um einen Host mit einer benutzerdefinierten ESXi- und NSX-T-Version erneut bereitzustellen.

## Allgemeine Aufgaben zum automatischen Bereitstellen statusfreier Cluster

Allgemeine Aufgaben zum automatischen Bereitstellen eines statusfreien Clusters.

Die allgemeinen Aufgaben zum Einrichten eines statusfreien Clusters mit automatischer Bereitstellung lauten wie folgt:

- 1 Voraussetzungen und unterstützte Versionen. Siehe [Voraussetzungen und unterstützte Versionen](#).

- 2 (Referenzhost) Erstellen Sie ein benutzerdefiniertes Image-Profil. Siehe [Erstellen eines benutzerdefinierten Image-Profiles für statusfreie Hosts](#).
- 3 (Referenz- und Zielhosts) Ordnen Sie das benutzerdefinierte Image-Profil zu. Siehe [Zuordnen des benutzerdefinierten Images zu den Referenz- und Zielhosts](#).
- 4 (Referenzhost) Richten Sie die Netzwerkkonfiguration in ESXi ein. Siehe [Einrichten der Netzwerkkonfiguration auf dem Referenzhost](#).
- 5 (Referenzhost) Konfigurieren Sie diesen als Transportknoten in NSX. Siehe [Konfigurieren des Referenzhosts als Transportknoten in NSX-T](#).
- 6 (Referenzhost) Extrahieren und überprüfen Sie das Hostprofil. Siehe [Extrahieren und Überprüfen des Hostprofils](#).
- 7 (Referenz- und Zielhosts) Überprüfen Sie die Hostprofilzuordnung mit dem statusfreien Cluster. Siehe [Überprüfen der Hostprofilzuordnung mit dem statusfreien Cluster](#).
- 8 (Referenzhost) Aktualisieren Sie die Hostanpassung. Siehe [Aktualisieren der Hostanpassung](#).
- 9 (Zielhosts) Lösen Sie die automatische Bereitstellung aus. Siehe [Auslösen der automatischen Bereitstellung auf Zielhosts](#).
  - a Vor dem Anwenden des Transportknotenprofils. Siehe [Neustarten von Hosts vor der TNP-Anwendung](#).
  - b Wenden Sie das Transportknotenprofil an. Siehe [Anwenden von TNP auf einem statusfreien Cluster](#).
  - c Nach dem Anwenden des Transportknotenprofils. Siehe [Neustarten von Hosts nach der TNP-Anwendung](#).
- 10 Beheben Sie Probleme mit dem Hostprofil und Transportknotenprofil. Siehe [Fehlerbehebung für das Host- und Transportknotenprofil](#).

## Voraussetzungen und unterstützte Versionen

Voraussetzungen und unterstützte Versionen von ESXi und NSX-T.

### Unterstützte Workflows

- Mit Image-Profil und Hostprofil

### Voraussetzungen

- Nur homogene Cluster (alle Hosts innerhalb eines Clusters müssen entweder statusfrei oder statusbehaftet sein) werden unterstützt.
- Der Image Builder-Dienst muss aktiviert sein.
- Der automatische Bereitstellungsdienst muss aktiviert sein.

## Unterstützte NSX-und ESXi-Versionen

Unterstützte ESXi-Version	ESXi 67ep6	ESXi 67u2	ESXi 67u3	ESXi 67ep7	ESXi 67ep15	ESXi 67ep17
NSX-T Data Center 2.4	Ja	Ja	Nein	Nein	Nein	Nein
NSX-T Data Center 2.4.1	Ja	Ja	Nein	Nein	Nein	Nein
NSX-T Data Center 2.4.2	Ja	Ja	Nein	Nein	Nein	Nein
NSX-T Data Center 2.4.3	Ja	Ja	Nein	Nein	Nein	Nein
NSX-T Data Center 2.5	Ja	Ja	Ja	Ja	Nein	Nein
NSX-T Data Center 2.5.1	Ja	Ja	Ja	Ja	Ja	Ja

## Erstellen eines benutzerdefinierten Image-Profiles für statusfreie Hosts

Identifizieren Sie in Ihrem Datacenter einen Host, der als Referenzhost vorbereitet werden soll.

Wenn der Referenz Host zum ersten Mal gestartet wird, ordnet ESXi die Standardregel dem Referenzhost zu. In diesem Verfahren fügen wir ein benutzerdefiniertes Image-Profil ( ESXi und NSX VIBs) hinzu und verknüpfen den Referenzhost mit dem neuen benutzerdefinierten Image. Ein Image-Profil mit dem NSX-T-Image reduziert die Installationszeit erheblich. Dasselbe benutzerdefinierte Image ist mit den Zielhosts im statusfreien Cluster verknüpft.

---

**Hinweis** Alternativ können Sie dem Referenzcluster und statusfreien Zielcluster nur ein ESXi-Image-Profil hinzufügen. Die NSX-T-VIBs werden heruntergeladen, wenn Sie das Transportknotenprofil auf dem statusfreien Cluster anwenden. Siehe [Hinzufügen eines Softwaredepots](#).

---

### Voraussetzungen

Stellen Sie sicher, dass der automatische Bereitstellungsdienst und der Image-Erstellungsdienst aktiviert sind. Siehe [Verwenden von vSphere Auto Deploy zum erneuten Bereitstellen von Hosts](#).

### Verfahren

- 1 Erstellen Sie zum Importieren von NSX-T-Paketen ein Softwaredepot.
- 2 Laden Sie die nsx-lcp-Pakete herunter.
  - a Melden Sie sich bei <https://my.vmware.com> an.
  - b Wählen Sie auf der Seite „VMware NSX-T Data Center herunterladen“ die NSX-T-Version aus.
  - c Suchen Sie auf der Seite „Produkt-Downloads“ die NSX-T-Kernel-Module für eine bestimmte VMware ESXi-Version.
  - d Klicken Sie auf **Jetzt herunterladen**, um mit dem Herunterladen des nsx-lcp-Pakets zu beginnen.



- e Importieren Sie nsx-lcp-Pakete in das Softwaredepot.

**NSX Kernel Module for VMware ESXi 6.7**  
 Dateigröße: 37,64 MB  
 Dateityp: zip

Jetzt herunterladen

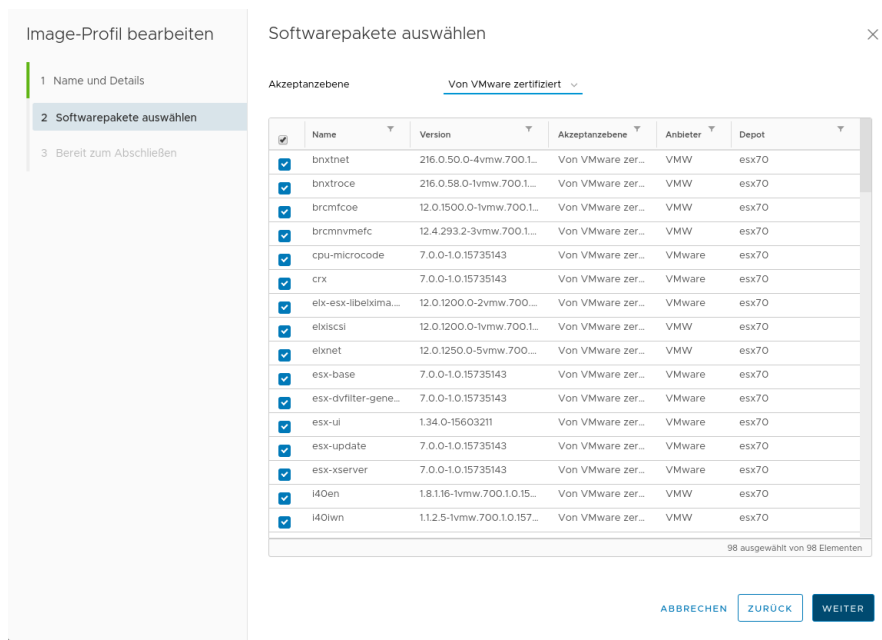
**Name:** nsx-lcp-2.5.0.0.0.14663975-esx67.zip  
**Release-Datum:** 2019-09-19  
**Build-Nummer:** 14663974

NSX Kernel Module for VMware ESXi 6.7  
 This package includes the required kernel modules to enable NSX on ESXi 6.7 if needed for a manual installation. Use esxcli to install manually or include as part of an automated deployment system of the ESXi hosts.  
**MD5SUM:** f224a0e12fc1722ae5b5259d279bfa1  
**SHA1SUM:** a97d3125a26a47b94ec8408acd369d42681d3027  
**SHA256SUM:**  
 1ed76de6a7f22d227eb4be30a2e0aa91492a876b7b164814198de3  
 1eec77bc44

- 3 Erstellen Sie ein weiteres Softwaredepot zum Importieren von ESXi-Paketen.

Der vSphere Web Client zeigt zwei Depots an, die auf dem Referenzhost erstellt wurden.

- 4 Erstellen Sie ein benutzerdefiniertes Softwaredepot, um zuvor importierte ESXi-Images und nsx-lcp-Pakete zu klonen.
- Wählen Sie das ESXi-Image-Profil aus dem ESXi-Softwaredepot aus, das im vorherigen Schritt erstellt wurde.
  - Klicken Sie auf **Klonen**.
  - Geben Sie im Assistenten zum Klonen von Image-Profilen einen Namen für das benutzerdefinierte Image ein, das erstellt werden soll.
  - Wählen Sie das benutzerdefinierte Softwaredepot aus, in dem das geklonte Image ( ESXi) verfügbar sein muss.
  - Wählen Sie im Fenster „Softwarepakete auswählen“ die Akzeptanzstufe für **VMware Certified** aus. Die ESXi-VIBs sind vorausgewählt.
  - Identifizieren und wählen Sie die NSX-T-Pakete manuell in der Liste der Pakete aus und klicken Sie auf **Weiter**.
  - Überprüfen Sie im Bildschirm „Bereit zum Abschließen“ die Details und klicken Sie auf **Fertigstellen**, um das geklonte Image mit den ESXi- und NSX-T-Paketen in dem benutzerdefinierten Softwaredepot zu erstellen.



## Nächste Schritte

Verknüpfen Sie das benutzerdefinierte Image mit den Referenz- und Zielhosts. Siehe [Zuordnen des benutzerdefinierten Images zu den Referenz- und Zielhosts](#).

## Zuordnen des benutzerdefinierten Images zu den Referenz- und Zielhosts

Wenn Sie den Referenzhost und die Zielhosts mit dem neuen benutzerdefinierten Image starten, das ESXi und NSX-Pakete enthält, ordnen Sie das benutzerdefinierte Image-Profil zu.

Zu diesem Zeitpunkt wird das benutzerdefinierte Image nur den Referenz- und Zielhosts zugeordnet, aber die NSX-Installation erfolgt nicht.

**Wichtig** Führen Sie dieses Verfahren für die benutzerdefinierte Image-Zuordnung auf Referenz- und Zielhosts durch.

## Voraussetzungen

### Verfahren

- 1 Navigieren Sie auf dem ESXi-Host zu **Menü > Automatische Bereitstellung > Bereitgestellte Hosts**.
- 2 Wenn Sie das benutzerdefinierte Image-Profil einem Host zuordnen möchten, wählen Sie das benutzerdefinierte Image aus.
- 3 Klicken Sie auf **Image-Profilzuordnung bearbeiten**.
- 4 Klicken Sie im Assistenten „Image-Profilzuordnung bearbeiten“ auf **Durchsuchen** und wählen Sie das benutzerdefinierte Depot sowie das benutzerdefinierte Image-Profil aus.

- 5 Aktivieren Sie die Option **Signaturprüfung für Image-Profil überspringen**.
- 6 Klicken Sie auf **OK**.

Software-Depots	Regeln bereitstellen	Bereitgestellte Hosts	Erkannte Hosts	Skriptpakete	Konfigurieren
<p>Das mit der Auto Deploy-Funktion mit den Hosts verknüpfte Image-Profil, Hostprofil und der Speicherort werden unten aufgelistet. Die Verknüpfungen können sich vom tatsächlichen Hostzustand unterscheiden.</p> <p>ÜBEREINSTIMMUNG DER HOSTZUORDNUNGEN ÜBERPRÜFEN... HOSTZUORDNUNGEN STANDARDISIEREN IMAGE-PROFILZUORDNUNG BEARBEITEN</p>					
<input type="checkbox"/>	Host	Verknüpftes Image-Profil	Verknüpftes Hostprofil	Verknüpfter Speicherort	Verknüpftes Skriptpaket
<input type="checkbox"/>	10.144.139.147	CustomDepot(ESXi and NSX)		1-datacenter-1964	
<input type="checkbox"/>	10.144.137.225	CustomDepot(ESXi and NSX)		Statless-Cluster	

## Ergebnisse

### Nächste Schritte

Richten Sie die Netzwerkkonfiguration auf dem Referenzhost ein. Siehe [Einrichten der Netzwerkkonfiguration auf dem Referenzhost](#).

## Einrichten der Netzwerkkonfiguration auf dem Referenzhost

Auf dem Referenzhost wird ein Standard-Switch mit einem VMkernel-Adapter erstellt, um die Netzwerkkonfiguration für ESXi einzurichten.

Diese Netzwerkkonfiguration wird im Hostprofil erfasst, das vom Referenzhost extrahiert wird. Während einer statusfreien Bereitstellung repliziert das Hostprofil diese Netzwerkkonfigurationseinstellung auf jedem Zielhost.

### Verfahren

- 1 Konfigurieren Sie auf dem ESXi-Host einen vSphere Standard Switch (VSS) oder einen verteilten virtuellen Switch (DVS), indem Sie einen VMkernel-Adapter hinzufügen.
- 2 Stellen Sie sicher, dass der neu hinzugefügte VSS/DVS-Switch auf der Seite „VMkernel-Adapter“ angezeigt wird.

Übersicht	Überwachen	Konfigurieren	Berechtigungen	VMs	Datenspeicher	Netzwerke
<b>VMkernel-Adapter</b> Netzwerk hinzufügen... Aktualisieren Bearbeiten... Entfernen						
Gerät	Netzwerkbezeichn...	Switch	IP-Adresse	TCP/IP-Stack	vH	
vmk0	Management N...	vSwitch0	10.192.193.193	Standard	D	
vmk1	VMkernel	vSwitch2	192.163.242.185	Standard	D	

## Nächste Schritte

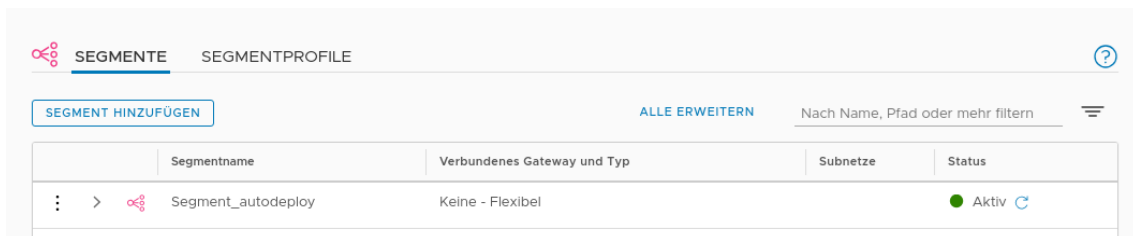
Konfigurieren Sie den Referenzhost als Transportknoten in NSX-T. Siehe [Konfigurieren des Referenzhosts als Transportknoten in NSX-T](#).

## Konfigurieren des Referenzhosts als Transportknoten in NSX-T

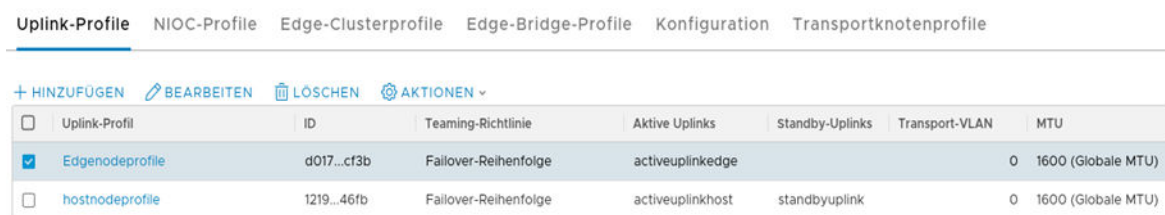
Nachdem der Referenzhost mit dem benutzerdefinierten Image-Profil verknüpft und mit einem VSS-Switch konfiguriert wurde, richten Sie den Referenzhost als Transportknoten in NSX-T ein.

### Verfahren

- 1 Melden Sie sich in einem Browser bei NSX-T unter „https://<NSXManager\_IPAddress>“ an.
- 2 Den Referenzhost finden Sie unter **System -> Knoten -> Host-Transportknoten**.
- 3 Erstellen Sie eine VLAN-Transportzone, um die Spanne des virtuellen Netzwerks zu definieren. Die Spanne wird durch Anhängen von N-VDS-Switches an die Transportzone definiert. Basierend auf diesem Anhang kann N-VDS auf Segmente zugreifen, die innerhalb der Transportzone definiert sind. Siehe [Erstellen einer Transportzone](#).
- 4 Erstellen Sie ein VLAN-Segment in der Transportzone. Das erstellte Segment wird als logischer Switch angezeigt.
  - a Navigieren Sie zu **Netzwerk -> Segmente**.
  - b Wählen Sie die Transportzone aus, an die das Segment angehängt werden soll.
  - c Geben Sie die VLAN-ID ein.
  - d Klicken Sie auf **Speichern**.



- 5 Erstellen Sie ein Uplink-Profil für den Referenzhost, der definiert, wie ein N-VDS eine Verbindung mit dem physischen Netzwerk herstellt. Siehe [Erstellen eines Uplink-Profiles](#).



- 6 Konfigurieren Sie den Referenzhost als Transportknoten. Siehe [Konfigurieren eines verwalteten Hosttransportknotens](#).
  - a Wählen Sie auf der Seite „Host-Transportknoten“ den Referenzhost aus.

- b Klicken Sie auf „NSX konfigurieren“ und wählen Sie die zuvor erstellte Transportzone, N-VDS und das Uplink-Profil aus.

- 7 Klicken Sie im Abschnitt „Zu installierende Netzwerkzuordnungen“ auf **Zuordnung hinzufügen**, um die Zuordnung der VMkernel zum Segment/logischen Switch hinzuzufügen.

## Netzwerkzuordnungen für die Installation



Die Host-Konnektivität geht möglicherweise verloren, wenn vmnic0 und vmk0 migriert werden.

Das Ändern des logischen Switches für den statusbehafteten Host (eigenständig oder geclustert) wirkt sich nicht aus und der Vorgang schlägt fehl.

[+ HINZUFÜGEN](#) [LÖSCHEN](#)

<input checked="" type="checkbox"/> VMkernel-Adapter *	VLAN-Segment/logischer Switch *
<input checked="" type="checkbox"/> vmk0	segment-autodeploy

- 8 Klicken Sie auf **Fertigstellen**, um die Installation von NSX-T auf dem Referenzhost zu starten. Während der Installation werden VMkernel-Adapter und physische Netzwerkkarten (NICs) von einem VSS- oder DVS-Switch zu einem N-VDS-Switch migriert. Nach der Installation wird für den Konfigurationszustand des Referenzhosts Erfolg angezeigt.

**Hinweis** Der Referenzhost wird unter „Weitere Hosts“ aufgeführt.

Host-Transportknoten

Edge-Transportknoten

Edge-Cluster

ESXi-Bridge-Cluster

Verwaltet von

vc

NSX KONFIGURIEREN

NSX ENTFERNEN

AKTIONEN

Anzeiger: Alle

<input type="checkbox"/>	Knoten	ID	IP-Adressen	Betriebssystem	NSX-Konfigurati	Konfigurationszi	Knotenstatus	Tunnel	Transportzonen	NSX-Version	N-VDS
<input type="checkbox"/>	Other Hosts (2)	MoRef-I...	1 Host herabg...								
<input checked="" type="checkbox"/>	hostnode	6d4c...f...	10.160.169.8...	ESXi 6.7.0	Konfiguriert	Erfolgreich	Aktiv ⓘ	↑ 1	tz	2.5.0.0.0.14...	1
<input type="checkbox"/>	10.192.193.193	42ea...8...	10.192.193.1...	ESXi 6.7.0	Konfiguriert	Erfolgreich	Herabgestuft ⓘ	Nicht v...	tz	2.5.0.0.0.14...	1

- 9 Stellen Sie in vCenter Server sicher, dass die PNICs-und VMkernels-Adapter auf dem VSS-Switch migriert und mit dem N-VDS-Switch verbunden sind.

VMkernel-Adapter				
Netzwerk hinzufügen...		Aktualisieren	Bearbeiten...	Entfernen
Gerät	Netzwerkbezeichnung	Switch	IP-Adresse	TCP/IP-Stack
vmk0	Management Network	vSwitch0	10.160.169.87	Standard
vmk1	Segment_autodeploy	vds-1	169.254.171.95	Standard

## Nächste Schritte

Extrahieren und überprüfen Sie das Hostprofil. Siehe [Extrahieren und Überprüfen des Hostprofils](#).

## Extrahieren und Überprüfen des Hostprofils

Nachdem Sie das Hostprofil vom Referenzhost extrahiert haben, überprüfen Sie die NSX-T-Konfiguration, die im Hostprofil extrahiert wurde. Sie besteht aus einer ESXi- und NSX-T-Konfiguration, die auf die Zielhosts angewendet wird.

## Verfahren

- 1 Informationen zum Extrahieren des Hostprofils finden Sie unter [Extrahieren und Konfigurieren des Hostprofils vom Referenzhost](#).

## 2 Überprüfen Sie die NSX-Konfiguration im extrahierten Hostprofil.

FAVORITEN

ALLE

Q Filter

> Allgemeine Systemeinstellungen

> Andere

> Erweiterte Konfigurationseinstellungen

> Netzwerkkonfiguration
 

> Standard-Switch

> VM-Portgruppe

> Hostportgruppe

> Konfiguration der physischen Netzwerkkarte
 

vSphere Distributed Switch

Virtuelle Netzwerkkarte des Hosts

> vNIC des NSX-Hosts:
 

> vNIC des NSX-Hosts : Segment\_autodeploy

> Netstack-Instanz

Netzwerk-Core-Dump-Einstellungen

> Sicherheit und Dienste

> Speicherkonfiguration

vNIC des NSX-Hosts : Segment\_autodeploy

LogicSwitch ermitteln, mit dem diese virtuelle Netzwerkkarte verbunden werden soll

LogicSwitch zum Anschließen auswählen

\*LogicSwitch-Name

Segment\_autodeploy

Festlegen, wann die virtuelle Netzwerkkarte im LogicSwitch erstellt werden soll

Objekt immer erstellen

Eigenschaften für den statusfreien Start von virtuellen Netzwerkkarten im LogicSwitch

Konfigurationsparameter für den statusfreien Start (sehen Sie vor dem Ändern in der Dokumentation nach)

*VLAN (sehen Sie vor dem Ändern in der Dokumentation nach)	0
*Gruppierungsrichtlinien (sehen Sie vor dem Ändern in der Dokumentation nach)	first uplink
Verwendete aktive Uplinks (sehen Sie vor dem Ändern in der Dokumentation nach)	vmnic1
Verwendete Standby-Uplinks (sehen Sie vor dem Ändern in der Dokumentation nach)	--
*Verwendeter OpaqueSwitch-Name (sehen Sie vor dem Ändern in der Dokumentation nach)	vds-1

> Netzwerkkonfiguration
 

> Standard-Switch

> VM-Portgruppe

> Hostportgruppe

> Konfiguration der physischen Netzwerkkarte
 

vSphere Distributed Switch

Virtuelle Netzwerkkarte des Hosts

> vNIC des NSX-Hosts:
 

> vNIC des NSX-Hosts : Segment\_autodeploy

> Netstack-Instanz

Netzwerk-Core-Dump-Einstellungen

> Sicherheit und Dienste

> Speicherkonfiguration

Festlegen, wie die MAC-Adresse für vmknic entschieden werden soll

Benutzer zur Eingabe der MAC-Adresse auffordern, falls keine Standardadresse verfügbar ist

Namensrichtlinie für VMkernel-Netzwerkadapter

Zugewiesener Schnittstellenname

VMkernel-Netzwerkadapter

vmk1

MTU-Richtlinie

Angegebene MTU zuweisen

\*MTU

1500

TCP/IP-Stack:

Netstack-Instanz, mit der vmknic verbunden ist

\*Name

defaultTcpipStack

### Ergebnisse

Das Hostprofil enthält eine Konfiguration, die sich auf ESXi und NSX bezieht, da der Host für beide Umgebungen vorbereitet wurde.

### Nächste Schritte

Überprüfen Sie die Hostprofilzuordnung mit dem statusfreien Cluster. Siehe [Überprüfen der Hostprofilzuordnung mit dem statusfreien Cluster](#).

## Überprüfen der Hostprofilzuordnung mit dem statusfreien Cluster

Um den statusfreien Ziel-Cluster mit der ESXi- und NSX-Konfiguration vorzubereiten, ordnen Sie das vom Referenzhost extrahierte Hostprofil dem statusfreien Ziel-Cluster zu.

Wenn Sie dem statusfreien Cluster kein Hostprofil zuordnen, können neue Knoten, die dem Cluster hinzugefügt werden, nicht automatisch mit ESXi- und NSX-VIBs bereitgestellt werden.

VMware, Inc.

231

## Verfahren

- 1 Hängen Sie das Hostprofil an den statusfreien Cluster an oder trennen Sie es. Siehe [Anhängen von Einheiten an oder Trennen von Einheiten von einem Hostprofil](#).
- 2 Vergewissern Sie sich auf der Registerkarte „Bereitgestellte Hosts“, dass der vorhandene statusfreie Host dem korrekten Image und dem Hostprofil zugeordnet ist.
- 3 Wenn die Hostprofilzuordnung fehlt, wählen Sie den Zielhost aus und klicken Sie auf „Hostzuordnungen standardisieren“, um das Aktualisieren des Images und des Hostprofils auf dem Zielhost zu erzwingen.

Software-Depots	Regeln bereitstellen	Bereitgestellte Hosts	Erkannte Hosts	Skriptpakete	Konfigurieren
<p>① Das mit der Auto Deploy-Funktion mit den Hosts verknüpfte Image-Profil, Hostprofil und der Speicherort werden unten aufgelistet. Die Verknüpfungen können sich vom tatsächlichen Hostzustand unterscheiden.</p> <p>ÜBEREINSTIMMUNG DER HOSTZUORDNUNGEN ÜBERPRÜFEN...    HOSTZUORDNUNGEN STANDARDISIEREN    IMAGE-PROFILZUORDNUNG BEARBEITEN</p>					
<input type="checkbox"/>	Host	Verknüpftes Image-Profil	Verknüpftes Hostprofil	Verknüpfter Speicherort	Verknüpftes Skriptpaket
<input type="checkbox"/>	10.144.139.147	CustomDepot(ESXi and NSX)		1-datacenter-1964	
<input type="checkbox"/>	10.144.137.225	CustomDepot(ESXi and NSX)	Host Profile_ReferenceHost	Statless-Cluster	

## Nächste Schritte

Aktualisieren Sie die Hostanpassung. Siehe [Aktualisieren der Hostanpassung](#).

## Aktualisieren der Hostanpassung

Nach dem Anhängen des Hostprofils an den Zielcluster sind möglicherweise zusätzliche benutzerdefinierte Einträge auf dem Host erforderlich, um die ESXi- und NSX-T-Pakete erfolgreich darauf bereitzustellen.

## Verfahren

- 1 Wenn die Hosts nach dem Anhängen des Hostprofils an den Zielcluster nicht mit benutzerdefinierten Werten aktualisiert werden, wird vom System die folgende Meldung angezeigt.

**Host Profile**

AKTIONEN ▾

Übersicht

Überwachen

Konfigurieren

Hosts

Name: Host Profile  
Beschreibung:  
Erstellt am: 07.11.2019 14:36  
Letzte Änderung: 07.11.2019 14:36  
Version: 6.7.0

⚠ Der Host 10.160.183.211 muss zusätzlich angepasst werden.

⚠ Der Host 10.160.170.243 muss zusätzlich angepasst werden.



- 2 Navigieren Sie zum Aktualisieren der Hostanpassungen zum Hostprofil, klicken Sie auf **Aktionen -> Hostanpassungen bearbeiten**.
- 3 Geben Sie für die ESXi-Versionen 67ep6, 67ep7, 67u2 das MUX-Benutzerkennwort ein.

Customize hosts

Enter host customizations.

IMPORT HOST CUSTOMIZATIONS ⓘ

Required	Property Name	Path	Value
No	MAC Address	Networking configu...	02:00:0c:23:e9:9a
Yes	Adapter MA...	Storage configurati...	02:00:0c:23:e9:9a
Yes	Activate	Storage configurati...	false
Yes	Password	Security and Services > Security Settings > Security > User Configuration > mux_user > Pass	

- 4 Stellen Sie sicher, dass alle erforderlichen Felder mit den entsprechenden Werten aktualisiert wurden.

#### Nächste Schritte

Lösen Sie die automatische Bereitstellung auf Zielhosts aus. Siehe [Auslösen der automatischen Bereitstellung auf Zielhosts](#).

## Auslösen der automatischen Bereitstellung auf Zielhosts

Wenn dem Cluster ein neuer Knoten zum hinzugefügt wird, muss er manuell neu gestartet werden, damit die ESXi- und NSX-T- VIBs konfiguriert werden können.

**Hinweis** Gilt nur für statusfreie Hosts.

Es gibt zwei Möglichkeiten, Hosts für die Auslösung der automatischen Bereitstellung von ESXi- und NSX-T-VIBs vorzubereiten, die konfiguriert werden sollen.

- Starten Sie die Hosts neu, bevor Sie TNP auf den statusfreien Cluster anwenden.
- Starten Sie die Hosts neu, nachdem Sie TNP auf den statusfreien Cluster angewendet haben.

Wenn Sie VMkernel-Adapter bei der Installation von NSX-T auf den Hosts migrieren möchten, finden Sie weitere Informationen unter:

- [Szenarien, in denen sich der statusfreie Host im Zielcluster befindet](#)
- [Szenarien, in denen sich der statusfreie Host außerhalb des Zielclusters befindet](#)

#### Nächste Schritte

Starten Sie die Hosts neu, bevor Sie TNP auf den statusfreien Cluster anwenden. Siehe [Neustarten von Hosts vor der TNP-Anwendung](#).

## Neustarten von Hosts vor der TNP-Anwendung

Gilt nur für statusfreie Hosts. In diesem Szenario wird das Transportknotenprofil nicht auf den statusfreien Cluster angewendet, d. h., dass NSX-T nicht auf dem Zielhost installiert und konfiguriert ist.

### Verfahren

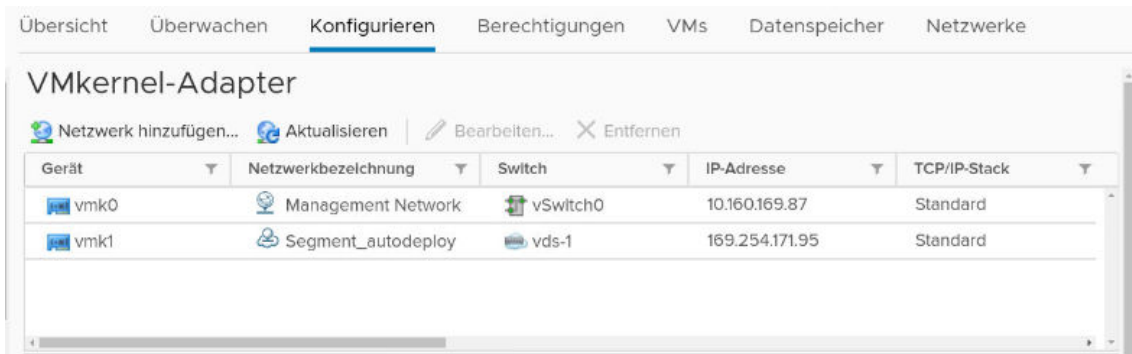
#### 1 Starten Sie Hosts neu.

Der Zielhost beginnt mit dem ESXi-Image. Nach dem Start verbleibt der Zielhost im Wartungsmodus, bis das TNP-Profil auf den Zielhost angewendet wird und die Installation von NSX-T abgeschlossen ist. Profile werden in der folgenden Reihenfolge auf Hosts angewendet:

Profile werden in der folgenden Reihenfolge auf Hosts angewendet.

- Das Image-Profil wird auf den Host angewendet.
- Die Hostprofilkonfiguration wird auf den Host angewendet.
- Die NSX-T-Konfiguration wird auf den Host angewendet.

#### 2 Auf dem ESXi-Host ist der VMkernel-Adapter an ein temporäres Segment mit dem Namen <N-LogicalSegment> angehängt, da der Host noch kein Transportknoten ist. Nach der Installation von NSX-T wird der temporäre Switch durch den tatsächlichen N-VDS-Switch und das logische Segment ersetzt.



Gerät	Netzwerkbezeichnung	Switch	IP-Adresse	TCP/IP-Stack
vmk0	Management Network	vSwitch0	10.160.169.87	Standard
vmk1	Segment_autodeploy	vds-1	169.254.171.95	Standard

ESXi-VIBs werden auf alle neu gestarteten Hosts angewendet. Ein temporärer NSX-Switch auf einem ESXi-Host. Wenn TNP auf die Hosts angewendet wird, wird der temporäre Switch durch den tatsächlichen NSX-T-Switch ersetzt.

### Nächste Schritte

Wenden Sie TNP auf den statusfreien Cluster an. Siehe [Anwenden von TNP auf einem statusfreien Cluster](#).

## Anwenden von TNP auf einem statusfreien Cluster

Die Konfiguration und Installation von NSX-T erfolgt nur dann auf den Ziel-Hosts, wenn TNP auf den Cluster angewendet wird.

## Verfahren

- 1 Notieren Sie die Einstellungen, die im Hostprofil vom Referenzhost extrahiert wurden. Die entsprechenden Entitäten im TNP-Profil müssen denselben Wert haben. Beispielsweise muss der im Hostprofil und TNP verwendete N-VDS-Name identisch sein.

Weitere Informationen zu extrahierten Hostprofil-Einstellungen finden Sie unter [Extrahieren und Überprüfen des Hostprofils](#).

- 2 Fügen Sie ein TNP hinzu. Siehe [Hinzufügen eines Transportknotenprofils](#).
- 3 Stellen Sie sicher, dass die Werte der folgenden Parameter sowohl im neuen TNP-Profil als auch im vorhandenen Hostprofil identisch sind.
  - N-VDS-Name: Stellen Sie sicher, dass der im Hostprofil und TNP referenzierte N-VDS-Name identisch ist.
  - Uplink-Profil: Stellen Sie sicher, dass das im Hostprofil und TNP referenzierte Uplink-Profil identisch ist.
  - PNIC: Wenn Sie eine physische Netzwerkkarte (NIC) einem Uplink-Profil zuordnen, überprüfen Sie zuerst die im Hostprofil verwendete Netzwerkkarte (NIC) und ordnen Sie diese physische Netzwerkkarte (NIC) dem Uplink-Profil zu.
  - Netzwerkzuordnung für Installation: Überprüfen Sie beim Zuordnen des Netzwerks während der Installation zuerst für das Hostprofil die Zuordnung zwischen VMkernel und Segment und fügen Sie dieselbe Zuordnung in TNP hinzu.
  - Netzwerkzuordnung für Deinstallation: Überprüfen Sie beim Zuordnen des Netzwerks während der Deinstallation zuerst für das Hostprofil die Zuordnung zwischen VMkernel und VSS/DVS und fügen Sie dieselbe Zuordnung in TNP hinzu.

- 4 Fügen Sie ein TNP hinzu, indem Sie in allen erforderlichen Feldern Eingaben vornehmen. Siehe [Hinzufügen eines Transportknotenprofils](#).

Stellen Sie sicher, dass die Werte der folgenden Parameter sowohl im neuen TNP-Profil als auch im vorhandenen Hostprofil identisch sind.

- Transportzone: Stellen Sie sicher, dass die im Hostprofil und TNP referenzierte Transportzone identisch ist.
- N-VDS-Name: Stellen Sie sicher, dass der im Hostprofil und TNP referenzierte N-VDS-Name identisch ist.
- Uplink-Profil: Stellen Sie sicher, dass das im Hostprofil und TNP referenzierte Uplink-Profil identisch ist.
- PNIC: Wenn Sie eine physische Netzwerkkarte (NIC) einem Uplink-Profil zuordnen, überprüfen Sie zuerst die im Hostprofil verwendete Netzwerkkarte (NIC) und ordnen Sie diese physische Netzwerkkarte (NIC) dem Uplink-Profil zu.

- Netzwerkzuordnung für Installation: Überprüfen Sie beim Zuordnen des Netzwerks während der Installation zuerst für das Hostprofil die Zuordnung zwischen VMkernel und logischem Switch und fügen Sie dieselbe Zuordnung in TNP hinzu.
- Netzwerkzuordnung für Deinstallation: Überprüfen Sie beim Zuordnen des Netzwerks während der Deinstallation zuerst für das Hostprofil die Zuordnung zwischen VMkernel und VSS/DVS und fügen Sie dieselbe Zuordnung in TNP hinzu.

N-VDS-Name *	vds-tzvian		▼
Zugeordnete Transportzonen	tz-33		
NIOC-Profil *	nsx-default-nioc-hostswitch-profile		▼
	<a href="#">ODER Neues NIOC-Profil erstellen</a>		
Uplink-Profil *	nsx-default-uplink-hostswitch-profile		▼
	<a href="#">ODER Neues Uplink-Profil erstellen</a>		
LLDP-Profil *	LLDP [Send Packet Enabled]		▼
IP-Zuweisung *	▼		
Physische Netzwerkkarten	vmnic1	▼	uplink-1
			▼
			<a href="#">PNIC hinzufügen</a>
Migration nur von PNIC	<input type="checkbox"/> Nein		
Aktivieren Sie diese Option, wenn auf dem für die Migration ausgewählten PNIC keine VMKs existieren			
Netzwerkzuordnungen für die Installation	<a href="#">1 Zuordnung</a>		
Netzwerkzuordnungen für die Deinstallation	<a href="#">Zuordnung hinzufügen</a>		





Wenn die TNP-Konfiguration nach der TNP-Anwendung auf Zielknoten nicht mit der Hostprofil-Konfiguration übereinstimmt, wird der Knoten aufgrund von Konformitätsfehlern möglicherweise nicht angezeigt.

- 5 Stellen Sie sicher, dass das TNP-Profil erfolgreich erstellt wurde.

- 6 Wenden Sie das TNP-Profil auf den Zielcluster an und klicken Sie auf **Speichern**.



- 7 Stellen Sie sicher, dass das TNP-Profil erfolgreich auf den Zielcluster angewendet wird. Das bedeutet, dass NSX erfolgreich auf allen Knoten des Clusters konfiguriert wurde.
- 8 Stellen Sie in vSphere sicher, dass die physischen Netzwerkkarten (NICs) oder VMkernel-Adapter an den N-VDS-Switch angehängt sind.

VMkernel-Adapter				
   				
Gerät	Netzwerkbezeichnung	Switch	IP-Adresse	TCP/IP-Stack
vmk0	Management Network	vSwitch0	10.160.169.87	Standard
vmk1	Segment_autodeploy	vds-1	169.254.171.95	Standard

- 9 Stellen Sie in NSX sicher, dass der ESXi-Host erfolgreich als Transportknoten konfiguriert ist.

### Nächste Schritte

Alternativ können Sie einen Zielhost nach dem Anwenden von TNP auf den Cluster neu starten. Siehe [Neustarten von Hosts nach der TNP-Anwendung](#).

## Neustarten von Hosts nach der TNP-Anwendung

Gilt nur für statusfreie Hosts. Wenn dem Cluster ein neuer Knoten hinzugefügt wird, starten Sie den Knoten manuell neu, damit die ESXi- und NSX-T-Pakete darauf konfiguriert werden.

### Verfahren

- 1 Wenden Sie TNP auf den statusfreien Cluster an, der bereits mit dem Hostprofil vorbereitet wurde. Siehe [Erstellen und Anwenden von TNP auf statusfreie Cluster](#).
- 2 Starten Sie Hosts neu.

Wenn Sie nach dem Anwenden des TNP-Profiles auf den statusfreien Cluster einen neuen Knoten neu starten, der dem Cluster hinzugefügt wird, wird dieser Knoten automatisch mit NSX-T auf dem Host konfiguriert.

## Nächste Schritte

Stellen Sie sicher, dass Sie jeden neuen Knoten neu starten, der dem Cluster hinzugefügt wird, um ESXi und NSX-T automatisch auf dem neu gestarteten Knoten bereitzustellen und zu konfigurieren.

Informationen zur Fehlerbehebung bei Problemen im Zusammenhang mit dem Hostprofil und dem Transportknotenprofil beim Konfigurieren der automatischen Bereitstellung finden Sie unter [Fehlerbehebung für das Host- und Transportknotenprofil](#).

## Szenarien, in denen sich der statusfreie Host im Zielcluster befindet

In diesem Abschnitt werden Anwendungsfälle beschrieben, in denen ein statusfreier Host im Zielcluster vorhanden ist.

---

**Wichtig** Auf einem statusfreien Zielhost:

- Die Migration des vmkO-Adapters von VSS/DVS auf N-VDS wird in NSX-T 2.4 und NSX-T 2.4.1 nicht unterstützt.
  - Die Migration des vmkO-Adapters von VSS/DVS auf N-VDS wird in NSX-T 2.5 unterstützt.
-

Zielhost	Referenzhostkonfiguration	Schritte zum automatischen Bereitstellen von Zielhosts
Auf dem Zielhost ist der vmk0-Adapter konfiguriert.	Für das vom Referenzhost extrahierte Hostprofil ist vmk0 auf einem N-VDS-Switch konfiguriert. In NSX-T ist für TNP nur die vmk0-Migrationszuordnung konfiguriert.	<ol style="list-style-type: none"> <li>1 Hängen Sie das Hostprofil an den Zielhost an. Der vmk0-Adapter ist an einen vSwitch angehängt.</li> <li>2 Aktualisieren Sie bei Bedarf die Hostanpassungen.</li> <li>3 Starten Sie den Host neu. Das Hostprofil wird auf den Host angewendet. vmk0 ist an einen temporären Switch angehängt.</li> <li>4 Wenden Sie TNP an.  Der vmk0-Adapter wird zu N-VDS migriert. Der Zielhost wird erfolgreich mit ESXi- und NSX-T-VIBs bereitgestellt.</li> </ol>
Auf dem Zielhost ist der vmk0-Adapter konfiguriert.	Für das vom Referenzhost extrahierte Hostprofil ist vmk0 auf einem vSwitch und vmk1 auf einem N-VDS-Switch konfiguriert. In NSX-T ist für TNP nur die vmk1-Migrationszuordnung konfiguriert.	<ol style="list-style-type: none"> <li>1 Hängen Sie das Hostprofil an den Zielhost an. Der vmk0-Adapter ist an einen vSwitch angehängt, aber vmk1 wird auf keinem Switch erkannt.</li> <li>2 Aktualisieren Sie bei Bedarf die Hostanpassungen.</li> <li>3 Starten Sie den Host neu.  vmk0 ist an einen vSwitch angehängt und vmk1 ist an einen temporären NSX-Switch angehängt.</li> <li>4 Wenden Sie TNP an.  Der vmk1-Adapter wird zu N-VDS migriert.</li> <li>5 (optional) Wenn der Host nicht mit dem Hostprofil konform bleibt, starten Sie den Host neu, damit der Host übereinstimmt. Der Zielhost wird erfolgreich mit ESXi- und NSX-T-VIBs bereitgestellt.</li> </ol>
Auf dem Zielhost ist der vmk0-Adapter konfiguriert.	Für das vom Referenzhost extrahierte Hostprofil ist vmk0 auf einem vSwitch und vmk1 auf einem N-VDS-Switch konfiguriert. In NSX-T sind für TNP die vmk0- und vmk1-Migrationszuordnungen konfiguriert.	<ol style="list-style-type: none"> <li>1 Hängen Sie das Hostprofil an den Zielhost an. Der vmk0-Adapter ist an einen vSwitch angehängt, aber vmk1 wird auf keinem Switch erkannt.</li> <li>2 Aktualisieren Sie bei Bedarf die Hostanpassungen.</li> <li>3 Starten Sie den Host neu.  Der vmk0-Adapter ist an einen vSwitch angehängt und vmk1 ist an einen temporären NSX-Switch angehängt.</li> <li>4 Wenden Sie TNP an.</li> <li>5 (optional) Wenn der Host nicht mit dem Hostprofil konform bleibt, starten Sie den Host neu, damit der Host übereinstimmt. Der Zielhost wird erfolgreich mit ESXi- und NSX-T-VIBs bereitgestellt.</li> </ol>

Zielhost	Referenzhostkonfiguration	Schritte zum automatischen Bereitstellen von Zielhosts
Auf dem Zielhost sind vmk0- und vmk1-Adapter konfiguriert.	Für das vom Referenzhost extrahierte Hostprofil ist vmk0 auf einem vSwitch und vmk1 auf einem N-VDS-Switch konfiguriert. In NSX-T ist für TNP eine vmk1-Migrationszuordnung konfiguriert.	<ol style="list-style-type: none"> <li>1 Hängen Sie das Hostprofil an den Zielhost an. Die vmk0- und vmk1-Adapter sind an einen vSwitch angehängt.</li> <li>2 Aktualisieren Sie bei Bedarf die Hostanpassungen.</li> <li>3 Den Host neu starten.</li> <li>4 Wenden Sie TNP an.  Der vmk0-Adapter ist an einen vSwitch angehängt und vmk1 ist an einen N-VDS-Switch angehängt.</li> <li>5 (optional) Wenn der Host nicht mit dem Hostprofil konform bleibt, starten Sie den Host neu, damit der Host übereinstimmt.</li> </ol> Der Zielhost wird erfolgreich mit ESXi- und NSX-T-VIBs bereitgestellt.
Auf dem Zielhost sind vmk0- und vmk1-Adapter konfiguriert.	Für das vom Referenzhost extrahierte Hostprofil sind vmk0 und vmk1 auf einem N-VDS-Switch konfiguriert. In NSX-T sind für TNP die vmk0- und vmk1-Migrationszuordnungen konfiguriert.	<ol style="list-style-type: none"> <li>1 Hängen Sie das Hostprofil an den Zielhost an. Die vmk0- und vmk1-Adapter sind an einen vSwitch angehängt.</li> <li>2 Aktualisieren Sie bei Bedarf die Hostanpassungen.</li> <li>3 Starten Sie den Host neu.</li> <li>4 Wenden Sie TNP an.  vmk0 und vmk1 werden zu einem N-VDS-Switch migriert.</li> </ol> Der Zielhost wird erfolgreich mit ESXi- und NSX-T-VIBs bereitgestellt.

## Szenarien, in denen sich der statusfreie Host außerhalb des Zielclusters befindet

In diesem Abschnitt werden Anwendungsfälle beschrieben, in denen ein statusfreier Host außerhalb des Zielclusters vorhanden ist.

**Wichtig** Auf statusfreien Hosts:

- Die Migration des vmk0-Adapters von VSS/DVS auf N-VDS wird in NSX-T 2.4 und NSX-T 2.4.1 nicht unterstützt.
- Die Migration des vmk0-Adapters von VSS/DVS auf N-VDS wird in NSX-T 2.5 unterstützt.

.



Zielhostzustand	Referenzhostkonfiguration	Schritte zum automatischen Bereitstellen von Zielhosts
<p>Der Host befindet sich im ausgeschalteten Zustand (erster Start). Er wird später dem Cluster hinzugefügt.</p> <p>Die Standardregel für die automatische Bereitstellung wird für den Zielcluster konfiguriert und dem Hostprofil zugeordnet.</p> <p>Das Transportknotenprofil wird auf dem Cluster angewendet.</p>	<p>Für das vom Referenzhost extrahierte Hostprofil sind der VMkernel-Adapter 0 (vmk0) auf einem vSwitch und der VMkernel-Adapter 1 (vmk1) auf einem N-VDS-Switch konfiguriert.</p> <p>In NSX-T ist für TNP nur die vmk1-Migrationszuordnung konfiguriert.</p>	<p>1 Schalten Sie den Host ein.</p> <p>Nach dem Einschalten des Hosts.</p> <ul style="list-style-type: none"> <li>■ Der Host wird dem Cluster hinzugefügt.</li> <li>■ Das Hostprofil wird auf den Zielhost angewendet.</li> <li>■ Der vmk0-Adapter befindet sich auf dem vSwitch und der vmk1-Adapter befindet sich auf einem temporären Switch.</li> <li>■ TNP wird ausgelöst.</li> <li>■ Nachdem TNP auf den Cluster angewendet wurde, befindet sich der vmk0-Adapter auf dem vSwitch und vmk1 wird auf den N-VDS-Switch migriert.</li> </ul> <p>2 (Optional) Wenn der Host nicht mit dem Hostprofil konform bleibt, starten Sie den Host neu, damit der Host übereinstimmt.</p> <p>Der Host wird erfolgreich mit ESXi- und NSX-T-VIBs bereitgestellt.</p>
<p>Der Host befindet sich im ausgeschalteten Zustand (erster Start). Er wird später dem Cluster hinzugefügt.</p> <p>Die Standardregel für die automatische Bereitstellung wird für den Zielcluster konfiguriert und dem Hostprofil zugeordnet.</p> <p>Das Transportknotenprofil wird auf dem Cluster angewendet.</p>	<p>Für das vom Referenzhost extrahierte Hostprofil sind der VMkernel-Adapter 0 (vmk0) und der VMkernel-Adapter 1 (vmk1) auf einem N-VDS-Switch konfiguriert.</p> <p>In NSX-T sind für TNP die vmk0- und vmk1-Migration konfiguriert.</p>	<p>1 Schalten Sie den Host ein.</p> <p>Nach dem Einschalten des Hosts.</p> <ul style="list-style-type: none"> <li>■ Der Host wird dem Cluster hinzugefügt.</li> <li>■ Das Hostprofil wird auf den Zielhost angewendet.</li> <li>■ Die vmk0- und vmk1-Adapter befinden sich auf einem temporären Switch.</li> <li>■ TNP wird ausgelöst.</li> <li>■ Nachdem TNP auf den Cluster angewendet wurde, werden vmk0 und vmk1 auf den N-VDS-Switch migriert.</li> </ul> <p>Der Host wird erfolgreich mit ESXi- und NSX-T-VIBs bereitgestellt.</p>

Zielhostzustand	Referenzhostkonfiguration	Schritte zum automatischen Bereitstellen von Zielhosts
<p>Der Host befindet sich im eingeschalteten Zustand. Er wird später dem Cluster hinzugefügt.</p> <p>Die Standardregel für die automatische Bereitstellung wird für den Zielcluster konfiguriert und dem Hostprofil zugeordnet.</p> <p>Auf dem Zielhost ist nur der vmk0-Adapter konfiguriert.</p>	<p>Für das vom Referenzhost extrahierte Hostprofil sind der VMkernel-Adapter 0 (vmk0) auf einem vSwitch und der VMkernel-Adapter 1 (vmk1) auf einem N-VDS-Switch konfiguriert.</p> <p>In NSX-T ist für TNP eine vmk1-Migrationszuordnung konfiguriert.</p>	<ol style="list-style-type: none"> <li>1 Verschieben Sie den Host, sodass er Teil des Clusters ist.</li> <li>2 Starten Sie den Host neu.</li> </ol> <p>Nachdem der Host neu gestartet wurde, wird das Hostprofil auf den Zielhost angewendet.</p> <ul style="list-style-type: none"> <li>■ Der vmk0-Adapter ist an einen vSwitch angehängt, während der vmk1-Adapter an einen temporären NSX-Switch angehängt ist.</li> <li>■ TNP wird ausgelöst.</li> <li>■ vmk1 wird zum N-VDS-Switch migriert.</li> </ul> <ol style="list-style-type: none"> <li>3 (Optional) Wenn der Host nicht mit dem Hostprofil konform bleibt, starten Sie den Host neu, damit der Host übereinstimmt.</li> </ol> <p>Der Host wird erfolgreich mit ESXi- und NSX-T-VIBs bereitgestellt.</p>
<p>Der Host befindet sich im eingeschalteten Zustand. Er wird später dem Cluster hinzugefügt.</p> <p>Die Standardregel für die automatische Bereitstellung wird für den Zielcluster konfiguriert und dem Hostprofil zugeordnet.</p> <p>Auf dem Zielhost ist nur der vmk0-Adapter konfiguriert.</p>	<p>Für das vom Referenzhost extrahierte Hostprofil sind der VMkernel-Adapter 0 (vmk0) und der VMkernel-Adapter 1 (vmk1) auf N-VDS konfiguriert.</p> <p>In NSX-T sind für TNP die vmk0- und vmk1-Migration konfiguriert.</p>	<ol style="list-style-type: none"> <li>1 Verschieben Sie den Host, sodass er Teil des Clusters ist.</li> <li>2 Starten Sie den Host neu.</li> </ol> <p>Nachdem der Host neu gestartet wurde, wird das Hostprofil auf den Zielhost angewendet.</p> <ul style="list-style-type: none"> <li>■ Die vmk0- und vmk1-Adapter sind an einen temporären NSX-Switch angehängt.</li> <li>■ TNP wird ausgelöst.</li> <li>■ vmk0 und vmk1 sind an einen N-VDS-Switch angehängt.</li> </ul> <p>Der Host wird erfolgreich mit ESXi- und NSX-T-VIBs bereitgestellt.</p>

Zielhostzustand	Referenzhostkonfiguration	Schritte zum automatischen Bereitstellen von Zielhosts
<p>Der Host befindet sich im eingeschalteten Zustand. Er wird später dem Cluster hinzugefügt.</p> <p>Die Standardregel für die automatische Bereitstellung wird für den Zielcluster konfiguriert und dem Hostprofil zugeordnet.</p> <p>Auf dem Zielhost sind die vmk0- und vmk1-Netzwerkzuordnungen konfiguriert.</p>	<p>Für das vom Referenzhost extrahierte Hostprofil sind der VMkernel-Adapter 0 (vmk0) auf einem vSwitch und der VMkernel-Adapter 1 (vmk1) auf einem N-VDS-Switch konfiguriert.</p> <p>In NSX-T ist für TNP eine vmk1-Migration konfiguriert.</p>	<ol style="list-style-type: none"> <li>1 Verschieben Sie den Host, sodass er Teil des Clusters ist.</li> <li>2 Starten Sie den Host neu.</li> </ol> <p>Nachdem der Host neu gestartet wurde, wird das Hostprofil auf den Zielhost angewendet.</p> <ul style="list-style-type: none"> <li>■ Der vmk0-Adapter ist an einen vSwitch angehängt, während der vmk1-Adapter an einen temporären NSX-Switch angehängt ist.</li> <li>■ TNP wird ausgelöst.</li> <li>■ vmk1 wird zum N-VDS-Switch migriert.</li> </ul> <ol style="list-style-type: none"> <li>3 (Optional) Wenn der Host nicht mit dem Hostprofil konform bleibt, starten Sie den Host neu, damit der Host übereinstimmt.</li> </ol> <p>Der Host wird erfolgreich mit ESXi- und NSX-T-VIBs bereitgestellt.</p>
<p>Der Host befindet sich im eingeschalteten Zustand. Er wird später dem Cluster hinzugefügt.</p> <p>Die Standardregel für die automatische Bereitstellung wird für den Zielcluster konfiguriert und dem Hostprofil zugeordnet.</p> <p>Auf dem Host sind die vmk0- und vmk1-Netzwerkzuordnungen konfiguriert.</p>	<p>Auf dem Referenzhost sind für das Hostprofil der VMkernel-Adapter 0 (vmk0) und der VMkernel-Adapter 1 (vmk1) auf einem N-VDS-Switch konfiguriert.</p> <p>In NSX-T sind für TNP die vmk0- und vmk1-Migration konfiguriert.</p>	<ol style="list-style-type: none"> <li>1 Verschieben Sie den Host, sodass er Teil des Clusters ist.</li> <li>2 Starten Sie den Host neu.</li> </ol> <p>Nachdem der Host neu gestartet wurde, wird das Hostprofil auf den Zielhost angewendet.</p> <ul style="list-style-type: none"> <li>■ Die vmk0- und vmk1-Adapter sind an einen temporären NSX-Switch angehängt.</li> <li>■ TNP wird ausgelöst.</li> <li>■ Die vmk0- und vmk1-Adapter werden zum N-VDS-Switch migriert.</li> </ul> <p>Der Host wird erfolgreich mit ESXi- und NSX-T-VIBs bereitgestellt.</p>

## Fehlerbehebung für das Host- und Transportknotenprofil

Beheben Sie Probleme mit Hostprofilen und TNPs, wenn sie für die automatische Bereitstellung von statusfreien Clustern verwendet werden.

Szenario	Beschreibung
Hostprofil ist nicht portabel.	<p>Problem: keiner der vCenter-Server kann das Hostprofil verwenden, das die NSX-T-Konfiguration enthält.</p> <p>Probleumlösung: Keine</p>
Regel-Engine für automatische Bereitstellung	<p>Problem: Das Hostprofil kann nicht in Regeln zum automatischen Bereitstellen verwendet werden, um neue Cluster bereitzustellen. Wenn neue Cluster bereitgestellt werden, werden die Hosts mit Basisnetzwerk bereitgestellt und sie bleiben im Wartungsmodus.</p> <p>Probleumlösung: Bereiten Sie jeden Cluster über die NSX-T-GUI vor. Siehe <a href="#">Anwenden von TNP auf einem statusfreien Cluster</a>.</p>

Szenario	Beschreibung
Prüfung von Konformitätsfehlern.	<p>Problem: Die Hostprofilwartung kann die Konformitätsfehler im Zusammenhang mit der NSX-T-Konfiguration nicht beheben.</p> <ul style="list-style-type: none"> <li>■ Die auf dem Hostprofil und in TNP konfigurierten physischen Netzwerkkarten unterscheiden sich.</li> <li>■ Zuordnung zwischen vNIC-zu-LS-Zuordnung. Hostprofil findet eine Nichtübereinstimmung in der Zuordnung zwischen logischem Switch und vNIC mit dem TNP-Profil.</li> <li>■ Nichtübereinstimmung zwischen VMkernel und verbundenem N-VDS auf Hostprofil und TNP.</li> <li>■ Nichtübereinstimmung des opaken Switches auf Hostprofil und TNP.</li> </ul> <p>Problemumgehung: Stellen Sie sicher, dass die NSX-T-Konfiguration auf dem Hostprofil und TNP übereinstimmt. Starten Sie den Host neu, um die Konfigurationsänderungen umzusetzen. Der Host wird angezeigt.</p>
Wartung	<p>Problem: Wenn NSX-T-spezifische Konformitätsfehler vorliegen, wird die Hostprofilwartung auf diesem Cluster blockiert.</p> <p>Falsche Konfiguration:</p> <ul style="list-style-type: none"> <li>■ Zuordnung zwischen vNIC-zu-LS-Zuordnung</li> <li>■ Zuordnung physischer Netzwerkkarten</li> </ul> <p>Problemumgehung: Stellen Sie sicher, dass die NSX-T-Konfiguration auf dem Hostprofil und TNP übereinstimmt. Starten Sie den Host neu, um die Konfigurationsänderungen umzusetzen. Der Host wird angezeigt.</p>
Anhängen	<p>Problem: In einem mit NSX-T konfigurierten Cluster kann das Hostprofil nicht auf Hostebene angehängt werden.</p> <p>Problemumgehung: Keine</p>
Trennen	<p>Problem: Beim Trennen und Anhängen eines neuen Hostprofils in einem Cluster, der mit NSX-T konfiguriert ist, wird die NSX-T-Konfiguration nicht entfernt. Auch wenn der Cluster mit dem neu angehängten Hostprofil konform ist, weist er weiterhin die NSX-T-Konfiguration aus einem vorherigen Profil auf.</p> <p>Problemumgehung: Keine</p>
Aktualisieren	<p>Problem: Wenn der Benutzer die NSX-T-Konfiguration im Cluster geändert hat, extrahieren Sie ein neues Hostprofil. Aktualisieren Sie das Hostprofil manuell für alle verloren gegangenen Einstellungen.</p> <p>Problemumgehung: Keine</p>
Transportknotenkonfiguration auf Hostebene	<p>Problem: Nachdem der anportsport-Knoten automatisch bereitgestellt wurde, fungiert er als einzelne Einheit. Eine Aktualisierung dieses Transportknotens stimmt möglicherweise nicht mit TNP überein.</p> <p>Problemumgehung: Aktualisieren Sie den Cluster. Eine Aktualisierung in einem eigenständigen Transportknoten kann die zugehörige Migrationsspezifikation nicht beibehalten. Bei der Migration schlägt das Posten des Neustarts möglicherweise fehl.</p>

Szenario	Beschreibung
Das Hostprofil kann nicht angewendet werden, da die mux_user-Kennwortrichtlinie und das Kennwort nicht zurückgesetzt wurden.	<p>Problem: nur auf Hosts, auf denen Versionen vor vSphere 6.7 U3 ausgeführt werden. Die Hostwartung und Hostprofilanwendung auf Hosts schlagen möglicherweise fehl, es sei denn, das Kennwort <b>mux_user</b> wird zurückgesetzt.</p> <p>Problemumgehung: Bearbeiten Sie unter „Richtlinien &amp; Profile“ das Hostprofil, um die Kennwortrichtlinie „mux_user“ zu ändern und setzen Sie das Kennwort <b>mux_user</b> zurück.</p>
Die PeerDNS-Konfiguration wird auf dem VMkernel-Adapter, der für die Migration zum NVDS-Switch ausgewählt wurde, nicht unterstützt.	<p>Problem: Wenn ein für die Migration auf NVDS ausgewählter VMkernel-Adapter Peer-DNS-fähig ist, schlägt die Hostprofilanwendung fehl.</p> <p>Problemumgehung: Bearbeiten Sie das extrahierte Hostprofil, indem Sie die Peer-DNS-Einstellung auf dem VMkernel-Adapter deaktivieren, der auf einen NVDS-Switch migriert werden muss. Stellen Sie alternativ sicher, dass Sie keine Peer-DNS-fähigen VMkernel-Adapter auf einen NVDS-Switch migrieren.</p>
DHCP-Adresse der VMkernel-NIC-Adresse wird nicht beibehalten	<p>Problem: Wenn der Referenzhost statusbehaftet ist, können statusfreie Hosts, für die ein vom statusbehafteten Referenzhost extrahiertes Profil verwendet wird, die zugehörige MAC-Adresse für die VMkernel-Verwaltung nicht beibehalten, die vom per PXE gestarteten MAC abgeleitet wurde. Dies führt zu DHCP-Adressierungsproblemen.</p> <p>Problemumgehung: Bearbeiten des extrahierten Hostprofil des statusbehafteten Hosts und ändern Sie die Einstellung <b>Bestimmung der MAC-Adresse für vmknics festlegen</b> in <b>MAC-Adresse verwenden, von der das System per PXE gestartet wurde</b>.</p>
Ein Fehler bei der Hostprofilanwendung in vCenter kann zu NSX-Konfigurationsfehlern auf dem Host führen.	<p>Problem: Wenn die Hostprofilanwendung in vCenter fehlschlägt, schlägt die NSX-Konfiguration möglicherweise ebenfalls fehl.</p> <p>Problemumgehung: Stellen Sie in vCenter sicher, dass das Hostprofil erfolgreich angewendet wurde. Korrigieren Sie die Fehler und versuchen Sie es erneut.</p>
LAGs werden auf statusfreien ESXi-Hosts nicht unterstützt.	<p>Problem: Das als LAGs in NSX konfigurierte Uplink-Profil wird auf einem statusfreien ESXi-Host, der von einem vCenter Server oder in NSX verwaltet wird, nicht unterstützt.</p> <p>Problemumgehung: Keine</p>

## Statusorientierte Server

Integrieren Sie Hostprofile eines ESXi-Hosts in NSX-T auf statusorientierten Servern.

Ein statusorientierter Host ist ein Host, der alle Konfigurationen und die installierten VIBs auch nach dem Neustart aufrechterhält. Während ein Autobereitstellungsserver für statusorientierte Hosts erforderlich ist, da die Startdateien, die zum Herauffahren eines statusfreien Hosts erforderlich sind, auf dem Autobereitstellungsserver gespeichert werden, benötigt ein statusorientierter Host keine vergleichbare Infrastruktur. Die Startdateien, die zum Öffnen eines statusorientierten Hosts erforderlich sind, werden auf der Festplatte gespeichert.

Bei dieser Vorgehensweise befindet sich der Referenzhost außerhalb des statusorientierten Clusters und die Zielhosts innerhalb des Clusters. Ein Zielhost kann sich innerhalb eines Clusters oder eines eigenständigen Hosts außerhalb des Clusters befinden. Bereiten Sie einen Cluster durch Anwendung des Hostprofils und des Transportknotenprofils (TN-Profil) vor, sodass alle neuen Zielhosts, die dem Cluster hinzugefügt werden, automatisch mit NSX-T-VIBs vorbereitet werden. Konfigurieren Sie den Zielhost als Transportknoten. Auf ähnliche Weise wenden Sie für einen eigenständigen Host das Hostprofil an und konfigurieren NSX-T, um NSX-T-VIBs zu installieren. Wenn die NSX-T-Konfiguration abgeschlossen ist, wird sie zu einem Transportknoten.

**Hinweis** NSX-T-VIBs werden aus dem TN-Profil installiert, und ESXi-Hostkonfigurationen werden von den Hostprofilen angewendet.

Während der Konfiguration eines Zielhosts in einem Transportknoten können VMkernel-Adapter und vmnics oder physische Netzwerkschnittstellen, die an den VSS- oder VDS-Switch angehängt sind, migriert und mit dem NSX-T Virtual Distributed Switch, dem N-VDS-Switch, verbunden werden.

## Unterstützte NSX-T- und ESXi-Versionen

Unterstützte NSX-T- und ESXi-Versionen auf statusorientierten Servern.

Versionsname	67ep6	67U2	67U3	67ep7	67U2C	6.5U3	6.5p03
NSX-T 2.4	Ja	Nein	Nein	Nein	Nein	Nein	Ja
NSX-T 2.4.1	Ja	Ja	Nein	Nein	Nein	Nein	Ja
NSX-T 2.4.2	Ja	Ja	Nein	Nein	Nein	Nein	Ja
NSX-T 2.4.3	Ja	Ja	Nein	Nein	Nein	Nein	Ja
NSX-T 2.5	Ja	Ja	Ja	Ja	Ja	Ja	Ja
NSX-T 2.5.1	Ja	Ja	Ja	Ja	Ja	Ja	Ja

## Vorbereiten eines statusorientierten Zielclusters

Bereiten Sie einen statusorientierten Zielcluster vor, sodass jeder neue Host, der dem Cluster hinzugefügt wird, automatisch mit ESXi- und NSX-T-VIBs bereitgestellt wird.

Sie können einen Host entweder innerhalb des Clusters oder außerhalb des Clusters als Referenzhost auswählen. Sie müssen einen Referenzhost erstellen, da das Hostprofil vom Referenzhost extrahiert und auf einen Zielhost angewendet wird. In dieser Vorgehensweise sind die Anweisungen, vmk0 (Verwaltungsdatenverkehr) und vmk1 (vMotion-Datenverkehr) zu einem N-VDS-Switch zu migrieren.

### Voraussetzungen

## Verfahren

- 1 Stellen Sie auf dem Referenzhost einen unterstützten ESXi-Build bereit.
    - a Fügen Sie in vSphere vmk1-Adapter hinzu. vmk0 ist bereits vorhanden, um den Verwaltungsdatenverkehr zu bedienen.
  - 2 Konfigurieren Sie den Referenzknoten als Transportknoten.
    - a Stellen Sie mithilfe von vSphere Web Client vor der Migration von vmk0 und vmk1 sicher, dass ein logischer Switch in NSX-T erstellt wird.
    - b (Optional) Konfigurieren Sie mithilfe der NSX-T-Manager-Benutzeroberfläche NSX so, dass der vmk1-Adapter, der einem logischen Switch zugeordnet ist, nach der Installation von NSX-T zum N-VDS-Switch migriert wird.
    - c (Optional) Konfigurieren Sie mithilfe der NSX-T-Manager-Benutzeroberfläche NSX-T so, dass der vmk0-Adapter, der einem logischen Switch zugeordnet ist, nach der Installation von NSX-T zum N-VDS-Switch migriert wird.
- 
- Hinweis** vmk0 und vmk1 können sich auf unterschiedlichen VSS- oder DVS-Switches befinden.
- 
- d Stellen Sie mithilfe von vSphere Web Client sicher, dass vmk0 und vmk1 mit einem logischen Switch auf einem N-VDS-Switch verbunden sind.
- 3 Extrahieren Sie ein Hostprofil aus dem Referenzhost.
  - 4 In Ihrer Umgebung kann es eine Reihe von VMkernel-Adaptoren geben, die zum N-VDS-Switch migriert werden müssen. Bevor Sie jedoch VMK-Adapter von VSS/DVS zu einem N-VDS-Switch migrieren, müssen Sie sicherstellen, dass die Konfigurationsparameter auf dem Zielhost mit denen auf dem Referenzhost übereinstimmen.
  - 5 Auf einem Zielhost, bei dem es sich um einen eigenständigen Host handelt:
    - a Hängen Sie das Hostprofil an den Zielhost an.
    - b Konfigurieren Sie NSX-T auf dem Host manuell. Wenn Sie den Host als Transportknoten konfigurieren, da das Hostprofil auf ESXi, stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind.
    - c Der Host muss zur gleichen Transportzone gehören.
    - d Der vmk1-Adapter muss mit demselben logischen Switch verbunden sein, der vom Referenzhost verwendet wird.
    - e Der Zielhost muss denselben IP-Pool verwenden, der vom Referenzhost verwendet wird.
    - f Uplink-Profil, LLDP, NIOC, Netzwerkzuordnung für die Installation, N-VDS, der auf dem Zielhost konfiguriert ist – diese müssen mit den auf dem Referenzhost konfigurierten Instanzen identisch sein.

- g Fügen Sie VMkernel-Adapter, vmk1 und vmnic1 manuell hinzu, damit sie vom VSS-/DVS-Switch zum N-VDS-Switch migriert werden. Weitere Informationen finden Sie in den vmk1-Migrationsszenarien.
  - h Fügen Sie den Verwaltungsadapter, vmk0 und/oder vmnic0 manuell hinzu.
- 6** Auf einem Zielhost, der Teil eines Clusters ist:
- a Hängen Sie das Hostprofil an den statusorientierten Zielcluster an.
  - b Erstellen Sie das TN-Profil auf dem Cluster und wenden Sie es an.
  - c Informationen zum Konfigurieren von vmk1 und vmnic1, die migriert werden sollen, finden Sie in den vmk1-Migrationsszenarien.
  - d Informationen zum Konfigurieren von vmk0 und vmnic0, die migriert werden sollen, finden Sie in den vmk0-Migrationsszenarien.
  - e So wenden Sie ein TN-Profil auf den Cluster an.

#### Nächste Schritte

Szenarien, in denen VMkernel-Adapter mit und ohne auf NSX-T angewendete Hostprofile migriert werden.

## VMkernel-Migration mit angewendetem Hostprofil

In dem in diesem Abschnitt dargestellten Szenario wird der VMkernel 1(vmk1)-Adapter zum N-VDS-Switch migriert, wobei das Hostprofil in NSX-T angewendet wird. Der vmk1-Adapter unterstützt den Infrastrukturdatenverkehr für vMotion, Fault Tolerance und andere Infrastrukturdienste.



Szenario	Fehler	Problemumgehung
<p>vmk1-Migration auf einem eigenständigen Zielhost durch Anwendung des Referenzhostprofils.</p>	<p>Der Zielhost wird nicht als Transportknoten konfiguriert. Da der Zielhost keine NSX-T-Objekte kennt, schlägt die Hostprofilanwendung fehl. Die Standardisierung des Hostprofils auf dem Zielhost schlägt fehl.</p> <div data-bbox="496 436 1037 499"> <p><b>Error: Received SOAP response fault : generate HostConfigTask Spec..</b></p> </div>	<p>1 Bevor Sie das Referenzhostprofil anwenden, um vmk1 zum logischen Switch auf dem Zielhost zu migrieren, konfigurieren Sie den Zielhost als Transportknoten, der NSX-T-VIBs installiert, einen N-VDS-Switch erstellt und den vmk1-Adapter vom VSS-Switch zum N-VDS-Switch migriert.</p> <p>Wenn Sie den Host als Transportknoten konfigurieren, da das hostprofil auf dem ESXi, stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind.</p> <ul style="list-style-type: none"> <li>■ Der Host muss zur gleichen Transportzone gehören.</li> <li>■ Der vmk1-Adapter muss mit demselben logischen Switch verbunden sein, der vom Referenzhost verwendet wird.</li> <li>■ Der Zielhost muss denselben IP-Pool verwenden, der vom Referenzhost verwendet wird.</li> <li>■ Uplink-Profil, LLDP, NIOC, Netzwerkzuordnung für die Installation, N-VDS, der auf dem Zielhost konfiguriert ist – diese müssen mit den auf dem Referenzhost konfigurierten Instanzen identisch sein.</li> </ul>

Szenario	Fehler	Problemumgehung
		Die Hostprofilstandardisierung ist erfolgreich, wenn der Zielhost mit demselben logischen Switch-Namen konfiguriert ist, der im Hostprofil vorhanden ist.
vmk1-Migration auf Zielhosts in einem statusorientierten Cluster.	<p>Bevor Sie das Hostprofil auf den Zielhost anwenden, schlägt die vmk1-Migration fehl, wenn Sie den Cluster durch Anwenden des TN-Profiles vorbereiten, das mit dem logischen Switch zugeordneten vmk1 konfiguriert ist.</p> <p><b>Error: vmk1 missing on the host.</b></p>	<ol style="list-style-type: none"> <li>1 Wenden Sie das Referenzhostprofil auf den Zielhost an, der dem Cluster beigetreten ist.</li> <li>2 Standardisieren Sie das Hostprofil auf dem Zielhost, um den vmk1-Adapter auf dem Zielhost zu erstellen.</li> <li>3 Wenden Sie das TN-Profil erneut auf den Cluster an, um vmk1 auf den Zielcluster zu migrieren.</li> </ol>
vmk0- und vmk1-Migration auf einem eigenständigen Host.	Wenn beim Konfigurieren von NSX-T auf dem eigenständigen Host das Feld „Netzwerkzuordnung für Installation“ keine vmk0- oder vmk1-Zuordnungen angibt, schlägt die Migration fehl.	Stellen Sie beim Konfigurieren von NSX-T auf dem Zielhost sicher, dass das Feld „Netzwerkzuordnung für Installation“ mit vmk0 und vmk1 angegeben ist, die demselben logischen Switch auf dem N-VDS zugeordnet sind.
vmk0- und vmk1-Migration auf einem Clusterhost.	Wenn das TN-Profil auf einen Cluster angewendet wird, schlägt die Migration fehl, wenn das Feld „Netzwerkzuordnung für Installation“ keine vmk0- oder vmk1-Zuordnungen enthält.	Wenden Sie das TN-Profil auf den Cluster an. Stellen Sie beim Konfigurieren des TN-Profiles für den Cluster sicher, dass das Feld „Netzwerkzuordnung für Installation“ mit vmk0 und vmk1 angegeben ist, die einem logischen Switch auf dem N-VDS zugeordnet sind.

## VMkernel-Migration ohne angewendetes Hostprofil

In dem in diesem Abschnitt dargestellten Szenario wird der VMkernel O(vmk0)-Adapter auf den N-VDS-Switch migriert, ohne dass das Hostprofil in NSX-T angewendet wird. Der vmk0-Adapter unterstützt den Verwaltungsdatenverkehr für NSX-T.

Sie müssen kein Hostprofil auf den Zielhost anwenden, da vmk0 bereits darauf vorhanden ist. Der vmk0-Adapter unterstützt den Verwaltungsdatenverkehr auf einem ESXi-Host.

Szenario	Vorgehensweise	Ergebnis
vmkO-Migration zu einem eigenständigen Host.	Stellen Sie beim Konfigurieren von NSX-T auf dem Zielhost sicher, dass das Feld <b>Netzwerkzuordnung für Installation</b> mit vmkO angegeben ist, das einem logischen Switch auf dem N-VDS zugeordnet ist.	vmkO wird auf den logischen Switch auf dem Zielhost migriert.
vmkO-Migration zu einem Clusterhost.	Wenden Sie das TN-Profil auf den Cluster an. Stellen Sie beim Konfigurieren des TN-Profiles auf dem Cluster sicher, dass das Feld <b>Netzwerkzuordnung für Installation</b> mit vmkO angegeben ist, das einem logischen Switch auf dem N-VDS zugeordnet ist.	vmkO wird auf den logischen Switch auf dem Zielhost migriert.

# Deinstallieren von NSX-T Data Center von einem Host-Transportknoten

# 12

Die Schritte zum Deinstallieren von NSX-T Data Center von einem Host-Transportknoten variieren je nach Host-Typ und dessen Konfiguration.

- **Überprüfen der Host-Netzwerkzuordnungen für die Deinstallation**

Bevor Sie NSX-T Data Center von einem ESXi-Host deinstallieren, stellen Sie sicher, dass Sie die entsprechenden Netzwerkzuordnungen für die Deinstallation konfiguriert haben. Die Zuordnungen sind erforderlich, wenn der ESXi-Host über VMkernel-Schnittstellen verfügt, die mit N-VDS verbunden sind.

- **Deinstallieren von NSX-T Data Center von einem vSphere-Cluster**

Wenn Sie NSX-T Data Center auf einem vSphere-Cluster mithilfe von Transportknotenprofilen installiert haben, können Sie diese Anweisungen befolgen, um NSX-T Data Center von allen Hosts im Cluster zu deinstallieren.

- **Deinstallieren von NSX-T Data Center von einem Host in einem vSphere-Cluster**

Sie können NSX-T Data Center von einem einzelnen Host deinstallieren, der von vCenter Server verwaltet wird. Die anderen Hosts im Cluster sind davon nicht betroffen.

- **Deinstallieren von NSX-T Data Center von einem eigenständigen Host**

Sie können NSX-T Data Center von einem eigenständigen Host deinstallieren. Eigenständige Hosts können ESXi oder KVM sein.

## Überprüfen der Host-Netzwerkzuordnungen für die Deinstallation

Bevor Sie NSX-T Data Center von einem ESXi-Host deinstallieren, stellen Sie sicher, dass Sie die entsprechenden Netzwerkzuordnungen für die Deinstallation konfiguriert haben. Die Zuordnungen sind erforderlich, wenn der ESXi-Host über VMkernel-Schnittstellen verfügt, die mit N-VDS verbunden sind.

Die Deinstallationszuordnung legt fest, wo die Schnittstellen nach der Deinstallation verbunden sind. Es sind Deinstallationszuordnungen für physische Schnittstellen (vmnicX) und VMkernel-Schnittstellen (vmkX) vorhanden. Beim Deinstallieren werden VMkernel-Schnittstellen von ihren aktuellen Verbindungen zu den Portgruppen verschoben, die in der Deinstallationszuordnung

angegeben sind. Wenn eine physische Schnittstelle in der Deinstallationszuordnung enthalten ist, wird die physische Schnittstelle mit dem entsprechenden vSphere Distributed Switch oder vSphere Standard Switch verbunden, der auf der Zielportgruppe der VMkernel-Schnittstellen basiert.

**Vorsicht** Die Deinstallation von NSX-T Data Center von einem ESXi-Host ist störend, wenn die physischen Schnittstellen oder VMkernel-Schnittstellen mit N-VDS verbunden sind. Wenn der Host oder Cluster an anderen Anwendungen wie z. B. vSAN teilnimmt, sind diese Anwendungen möglicherweise von der Deinstallation betroffen.







Es gibt zwei Möglichkeiten, die Netzwerkzuordnungen für die Deinstallation zu konfigurieren.

- In der Transportknotenkonfiguration, die für den jeweiligen Host gilt.
- In einer Transportknoten-Profilkonfiguration, die dann auf einen Cluster angewendet werden kann.

**Hinweis** Sie müssen über einen Compute Manager verfügen, der so konfiguriert ist, dass ein Transportknotenprofil auf einen Cluster angewendet wird.

Wenn ein Compute Manager konfiguriert ist, kann ein Host sowohl über eine Transportknotenkonfiguration als auch über eine Transportknotenprofilkonfiguration verfügen. Die zuletzt angewendete Konfiguration ist aktiv. Stellen Sie sicher, dass die Netzwerkzuordnungen für die Deinstallation für die aktive Konfiguration ordnungsgemäß konfiguriert sind.

In diesem Beispiel wird für das Cluster Cluster-1 das Transportknotenprofil TNP-1 angewendet. Der Host tn-1 zeigt „Nichtübereinstimmung bei Konfiguration“ an. Diese Nichtübereinstimmungsmeldung deutet darauf hin, dass nach dem Anwenden des Transportknotenprofils eine andere Konfiguration auf tn-1 angewendet wurde. Der Transportknoten tn-2 verwendet die Netzwerkzuordnungen aus dem Transportknotenprofil und der Transportknoten tn-1 verwendet seine eigene Konfiguration.

 NSX KONFIGURIEREN  NSX ENTFERNEN  AKTIONEN ▾					
<input type="checkbox"/>	Knoten	ID	IP-Adres	Betriebssy	NSX-Konfiguration
<input type="checkbox"/>	 New Cluster (2)	MoR...			 TNP-1
<input type="checkbox"/>	tn-1	926...	10....	ESXi ...	 Nichtübereinstimmung bei Konfiguration
<input type="checkbox"/>	tn-2	901f....	10....	ESXi ...	Konfiguriert

### Voraussetzungen

- Stellen Sie sicher, dass die entsprechenden Portgruppen für die Verwendung in der Deinstallationszuordnung konfiguriert sind. Sie müssen flüchtige vSphere Distributed Switch-Portgruppen oder vSphere Standard Switch-Portgruppen verwenden.

- Konfigurieren Sie einen Compute Manager, wenn Sie eine vSphere Distributed-Switch-Portgruppe in den Deinstallationszuordnungen für einen eigenständigen ESXi-Host verwenden möchten. Siehe [Hinzufügen eines Compute Managers](#). Wenn kein Compute Manager konfiguriert ist, müssen Sie eine vSphere Standard Switch-Portgruppe verwenden.

#### Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **System > Fabric > Knoten > Host-Transportknoten** aus.
- 3 Stellen Sie für jeden Host, den Sie deinstallieren möchten, sicher, dass die Netzwerkzuordnung für die Deinstallation eine Portgruppe für jede VMkernel-Schnittstelle enthält, die sich auf N-VDS befindet. Fügen Sie fehlende Zuordnungen hinzu.

---

**Wichtig** Bei der Portgruppe in der Netzwerkzuordnung für die Deinstallation muss es sich um eine flüchtige vSphere Distributed Switch-Portgruppe oder um eine vSphere Standard Switch-Portgruppe handeln.

---

- a Wenn Sie VMkernel-Schnittstellen anzeigen möchten, melden Sie sich bei vCenter Server an, wählen Sie den Host aus und klicken Sie auf **Konfigurieren > VMkernel-Adapter**.
- b Wenn die Konfiguration des Transportknotens die aktive Konfiguration ist, wählen Sie den Host aus und klicken Sie auf **Bearbeiten** (bei eigenständigen Hosts) oder auf **NSX konfigurieren** (bei verwalteten Hosts). Klicken Sie auf **Weiter** und anschließend auf **Netzwerkzuordnungen für die Deinstallation**. Zeigen Sie die Zuordnungen auf den Registerkarten **VMKNic-Zuordnungen** und **Physische Netzwerkkartenzuordnungen** an.
- c Wenn das Transportknotenprofil die aktive Konfiguration ist, klicken Sie in der Spalte **NSX-Konfiguration** auf den Namen des Transportknotenprofils für den Cluster und klicken Sie dann auf **Bearbeiten**. Klicken Sie auf der Registerkarte **N-VDS** auf **Netzwerkzuordnungen für die Deinstallation**. Zeigen Sie die Zuordnungen auf den Registerkarten **VMKNic-Zuordnungen** und **Physische Netzwerkkartenzuordnungen** an.

## Deinstallieren von NSX-T Data Center von einem vSphere-Cluster

Wenn Sie NSX-T Data Center auf einem vSphere-Cluster mithilfe von Transportknotenprofilen installiert haben, können Sie diese Anweisungen befolgen, um NSX-T Data Center von allen Hosts im Cluster zu deinstallieren.

Weitere Informationen zu Transportknotenprofilen finden Sie unter [Hinzufügen eines Transportknotenprofils](#).

**Vorsicht** Die Deinstallation von NSX-T Data Center von einem ESXi-Host ist störend, wenn die physischen Schnittstellen oder VMkernel-Schnittstellen mit N-VDS verbunden sind. Wenn der Host oder Cluster an anderen Anwendungen wie z. B. vSAN teilnimmt, sind diese Anwendungen möglicherweise von der Deinstallation betroffen.

Wenn Sie kein Transportknotenprofil zum Installieren von NSX-T Data Center verwendet haben oder wenn Sie NSX-T Data Center aus einer Teilmenge der Hosts im Cluster entfernen möchten, finden Sie weitere Informationen unter [Deinstallieren von NSX-T Data Center von einem Host in einem vSphere-Cluster](#).

**Hinweis** Durch das Entfernen eines Hosts von einem Cluster wird NSX-T Data Center nicht deinstalliert. Befolgen Sie diese Anweisungen, um NSX-T Data Center von einem Host in einem Cluster zu deinstallieren: [Deinstallieren von NSX-T Data Center von einem Host in einem vSphere-Cluster](#).

#### Voraussetzungen

- Stellen Sie sicher, dass für die Hosts, die Sie deinstallieren möchten, Netzwerk-Deinstallationszuordnungen konfiguriert sind. Siehe [Überprüfen der Host-Netzwerkzuordnungen für die Deinstallation](#).
- Stellen Sie sicher, dass sich die Hosts, die Sie deinstallieren möchten, in vSphere im Wartungsmodus befinden.

#### Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **System > Fabric > Knoten > Host-Transportknoten** aus.
- 3 Wählen Sie im Dropdown-Menü **Verwaltet von** den vCenter Server aus.
- 4 Wählen Sie den Cluster aus, den Sie deinstallieren möchten, und klicken Sie auf **NSX entfernen**.
- 5 Stellen Sie sicher, dass die NSX-T Data Center-Software vom Host entfernt wurde.
  - a Melden Sie sich als Root bei der Befehlszeilenschnittstelle des Hosts an.
  - b Führen Sie diesen Befehl aus, um nach NSX-T Data Center-VIBs zu suchen

```
esxcli software vib list | grep -E 'nsx|vsipfwlib'
```

Wenn die NSX-T Data Center-Software erfolgreich entfernt wurde, werden keine VIBs aufgeführt. Wenn NSX-VIBs auf dem Host verbleiben, wenden Sie sich an den VMware Support.

- 6 Wenn NSX Intelligence auch auf dem Host bereitgestellt wird, schlägt die Deinstallation von NSX-T Data Center fehl, weil alle Transportknoten Teil einer Standardnetzwerksicherheitsgruppe werden. So deinstallieren Sie:
  - a Wählen Sie den Cluster aus und klicken Sie auf **NSX entfernen**.
  - b Wählen Sie im Bestätigungs-Popup-Fenster **Löschen erzwingen** aus.

NSX-T wird von allen Hosts im Cluster deinstalliert.

## Deinstallieren von NSX-T Data Center von einem Host in einem vSphere-Cluster

Sie können NSX-T Data Center von einem einzelnen Host deinstallieren, der von vCenter Server verwaltet wird. Die anderen Hosts im Cluster sind davon nicht betroffen.

---

**Vorsicht** Die Deinstallation von NSX-T Data Center von einem ESXi-Host ist störend, wenn die physischen Schnittstellen oder VMkernel-Schnittstellen mit N-VDS verbunden sind. Wenn der Host oder Cluster an anderen Anwendungen wie z. B. vSAN teilnimmt, sind diese Anwendungen möglicherweise von der Deinstallation betroffen.

---

### Voraussetzungen

- Stellen Sie sicher, dass für die Hosts, die Sie deinstallieren möchten, Netzwerk-Deinstallationszuordnungen konfiguriert sind. Siehe [Überprüfen der Host-Netzwerkzuordnungen für die Deinstallation](#).
- Stellen Sie sicher, dass sich die Hosts, die Sie deinstallieren möchten, in vSphere im Wartungsmodus befinden.

### Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **System > Fabric > Knoten > Host-Transportknoten** aus.
- 3 Wählen Sie im Dropdown-Menü **Verwaltet von** den vCenter Server aus.
- 4 Wenn auf den Cluster ein Transportknotenprofil angewendet wurde, wählen Sie den Cluster aus und klicken Sie auf **Aktionen > TN-Profil trennen**.

Wenn auf dem Cluster ein Transportknotenprofil angewendet wurde, wird in der Spalte **NSX-Konfiguration** für den Cluster der Profilname angezeigt.

- 5 Wählen Sie den Host aus und klicken Sie auf **NSX entfernen**.



- 6 Stellen Sie sicher, dass die NSX-T Data Center-Software vom Host entfernt wurde.
  - a Melden Sie sich als Root bei der Befehlszeilenschnittstelle des Hosts an.
  - b Führen Sie diesen Befehl aus, um nach NSX-T Data Center-VIBs zu suchen

```
esxcli software vib list | grep -E 'nsx|vsipfwlib'
```

Wenn die NSX-T Data Center-Software erfolgreich entfernt wurde, werden keine VIBs aufgeführt. Wenn NSX-VIBs auf dem Host verbleiben, wenden Sie sich an den VMware Support.

- 7 Wenn auf dem Cluster ein Transportknotenprofil angewendet wurde und Sie es erneut anwenden möchten, wählen Sie den Cluster aus, klicken Sie auf **NSX konfigurieren** und wählen Sie das Profil im Dropdown-Menü **Bereitstellungsprofil auswählen** aus.

## Deinstallieren von NSX-T Data Center von einem eigenständigen Host

Sie können NSX-T Data Center von einem eigenständigen Host deinstallieren. Eigenständige Hosts können ESXi oder KVM sein.

---

**Vorsicht** Die Deinstallation von NSX-T Data Center von einem ESXi-Host ist störend, wenn die physischen Schnittstellen oder VMkernel-Schnittstellen mit N-VDS verbunden sind. Wenn der Host oder Cluster an anderen Anwendungen wie z. B. vSAN teilnimmt, sind diese Anwendungen möglicherweise von der Deinstallation betroffen.

---

### Voraussetzungen

Wenn Sie NSX-T Data Center von einem eigenständigen ESXi-Host deinstallieren, überprüfen Sie die folgenden Einstellungen:

- Stellen Sie sicher, dass für die Hosts, die Sie deinstallieren möchten, Netzwerk-Deinstallationszuordnungen konfiguriert sind. Siehe [Überprüfen der Host-Netzwerkzuordnungen für die Deinstallation](#).
- Stellen Sie sicher, dass sich die Hosts, die Sie deinstallieren möchten, in vSphere im Wartungsmodus befinden.

### Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **System > Fabric > Knoten > Host-Transportknoten** aus.
- 3 Wählen Sie im Dropdown-Menü **Verwaltet von** den Eintrag **Keine: Eigenständige Hosts** aus.

- 4 Wählen Sie den Host aus und klicken Sie auf **Löschen**. Stellen Sie im angezeigten Bestätigungsdialogfeld sicher, dass **NSX-Komponenten deinstallieren** ausgewählt und **Löschen erzwingen** deaktiviert ist. Klicken Sie auf **Löschen**.

Die NSX-T Data Center-Software wurde vom Host entfernt. Es kann bis zu 5 Minuten dauern, bis die gesamte NSX-T Data Center-Software entfernt wurde.

- 5 Wenn die Deinstallation fehlschlägt, wählen Sie den Host aus und klicken Sie erneut auf **Löschen**. Deaktivieren Sie im Bestätigungsdialogfeld **NSX-Komponenten deinstallieren** und wählen Sie **Löschen erzwingen** aus.

Der Host-Transportknoten wird aus der Management Plane gelöscht, aber auf dem Host ist möglicherweise noch NSX-T Data Center-Software installiert.

- 6 Stellen Sie sicher, dass die NSX-T Data Center-Software vom Host entfernt wurde.
- Melden Sie sich als Root bei der Befehlszeilenschnittstelle des Hosts an.
  - Führen Sie den entsprechenden Befehl aus, um nach NSX-T Data Center-Softwarepaketen zu suchen.

Tabelle 12-1. Paketlistenbefehle

Hostbetriebssystem	Befehl
ESXi	<code>esxcli software vib list   grep -E 'nsx vsipfwlib'</code>
Red Hat Enterprise Linux und CentOS Linux	<code>rpm -qa   grep -E 'nsx vsipfwlib'</code>
Ubuntu	<code>dpkg -l   grep -E 'nsx vsipfwlib'</code>
SUSE Linux Enterprise Server	<code>zypper packages --installed-only   grep -E 'nsx vsipfwlib'</code>

Wenn die NSX-T Data Center-Software erfolgreich entfernt wurde, werden keine Pakete aufgeführt. Wenn noch NSX-Softwarepakete auf dem Host verbleiben, wenden Sie sich an den VMware Support.

# Installieren von NSX Cloud-Komponenten

# 13

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.

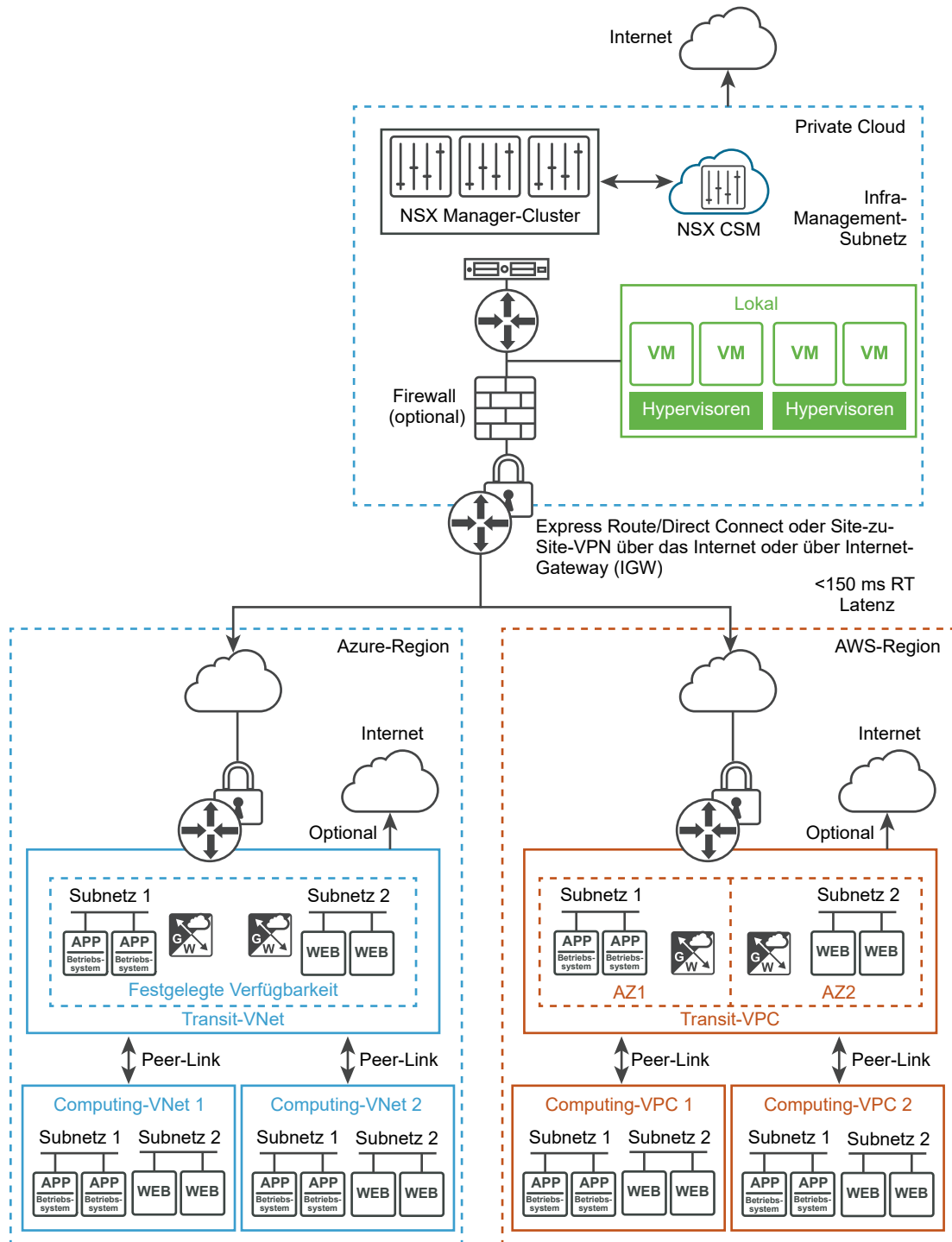
Dieses Kapitel enthält die folgenden Themen:

- [Architektur und Komponenten von NSX Cloud](#)
- [Übersicht über das Bereitstellen von NSX Cloud](#)
- [Bereitstellen lokaler Komponenten von NSX-T Data Center](#)
- [Ihr Public Cloud-Konto hinzufügen](#)
- [Bereitstellen des NSX Public Cloud Gateway](#)
- [\(Optional\) Installieren von NSX Tools auf Ihren Arbeitslast-VMs](#)
- [Aufheben der Bereitstellung oder Entfernen der Verknüpfung von PCGs](#)

## Architektur und Komponenten von NSX Cloud

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

Abbildung 13-1. Die Architektur von NSX Cloud



## Hauptkomponenten

Die Hauptkomponenten von NSX Cloud sind:

- **NSX Manager** für die Management Plane mit richtlinienbasiertem Routing, rollenbasierter Zugriffssteuerung (RBAC), Control Plane und definiertem Laufzeitstatus.

- **Cloud Service Manager (CSM)** für die Integration in NSX Manager, um Public-Cloud-spezifische Informationen für die Management Plane bereitzustellen.
- **Public Cloud-Gateway (PCG)** für Konnektivität zu den NSX-Management und -Control Planes, für NSX Edge-Gateway-Dienste und für die API-basierte Kommunikation mit den Public-Cloud-Entitäten.
- **NSX Tools**-Funktionalität, die einen NSX-verwalteten Datenpfad für Workload-VMs bereitstellt.

## Übersicht über das Bereitstellen von NSX Cloud

Anhand dieser Übersicht können Sie den allgemeinen Prozess der Installation und Konfiguration von NSX Cloud-Komponenten verstehen, um die Verwaltung Ihrer Public Cloud-Arbeitslast-VMs mit NSX-T Data Center zu ermöglichen.



**Hinweis** Stellen Sie bei der Planung Ihrer Bereitstellung sicher, dass die lokalen NSX-T Data Center-Appliances über eine gute Konnektivität mit der PCG-Bereitstellung in der Public Cloud verfügen und dass sich Transit-VPCs/VNets in derselben Region befinden wie die Computing-VPCs/VNets.

Tabelle 13-1. Workflow für die Bereitstellung von NSX Cloud

Aufgabe	Anweisungen
<input type="checkbox"/> Installieren Sie CSM und stellen Sie eine Verbindung zu NSX Manager her.	Siehe <a href="#">Bereitstellen lokaler Komponenten von NSX-T Data Center</a> .
<input type="checkbox"/> Fügen Sie eines oder mehrere Ihrer Public-Cloud-Konten zu CSM hinzu.	Siehe <a href="#">Ihr Public Cloud-Konto hinzufügen</a> .
<input type="checkbox"/> Stellen Sie PCG in Ihren Transit-VPCs oder VNets bereit und verknüpfen Sie sich mit Ihren Rechen-VPCs oder VNets.	Siehe <a href="#">Bereitstellen des NSX Public Cloud Gateway</a> .
Nächste Schritte	Befolgen Sie die Anweisungen unter <a href="#">Verwenden von NSX Cloud</a> im <i>Administratorhandbuch für NSX-T Data Center</i> .

## Bereitstellen lokaler Komponenten von NSX-T Data Center

Sie müssen NSX Manager bereits installiert haben, um mit der Installation von CSM fortfahren zu können.

## Installieren von CSM

Cloud Service Manager (CSM) ist eine Hauptkomponente von NSX Cloud.

Installieren Sie nach der Installation von NSX Manager CSM, indem Sie die folgenden Schritte ausführen, um NSX Manager zu installieren und **nsx-cloud-service-manager** als die Rolle „VM“ auszuwählen. Weitere Anweisungen finden Sie unter [Installieren Sie NSX Manager und die verfügbaren Appliances](#).

Je nach Bedarf können Sie CSM in der besonders kleinen VM-Größe oder höher bereitstellen. Einzelheiten dazu finden Sie unter [Systemanforderungen für NSX Manager-VM und -Host-Transportknoten](#).

## Verbinden von CSM mit NSX Manager

Sie müssen die CSM-Appliance mit NSX Manager verbinden, damit diese Komponenten miteinander kommunizieren können.

### Voraussetzungen

- NSX Manager muss installiert sein und Sie benötigen den Benutzernamen und das Kennwort für das Administratorkonto, um sich bei NSX Manager anzumelden.
- CSM muss installiert sein, und Ihnen muss in CSM die Rolle „Enterprise-Administrator“ zugewiesen sein.

### Verfahren

- 1 Melden Sie sich über einem Webbrowser bei CSM an.
- 2 Wenn Sie im Setup-Assistenten dazu aufgefordert werden, klicken Sie auf **Mit Setup beginnen**.
- 3 Geben Sie im Bildschirm „NSX Manager-Anmeldedaten“ die folgenden Details ein:

Option	Beschreibung
<b>NSX Manager-Hostname</b>	Geben Sie den vollqualifizierten Domännennamen (FQDN) von NSX Manager ein, falls dieser verfügbar ist. Sie können auch die IP-Adresse von NSX Manager eingeben.
<b>Administratoren-Anmeldedaten</b>	Geben Sie den Benutzernamen und das Kennwort eines Enterprise-Administrators für NSX Manager ein.
<b>Manager-Fingerabdruck</b>	Geben Sie optional den Fingerabdruckwert des NSX Manager ein. Wenn Sie dieses Feld leer lassen, wird der Fingerabdruck vom System erkannt und im nächsten Bildschirm angezeigt.

- 4 (Optional) Wenn Sie keinen Fingerabdruckwert für NSX Manager bereitgestellt haben oder der Wert falsch war, wird der Bildschirm **Fingerabdruck überprüfen** angezeigt. Aktivieren Sie das Kontrollkästchen, um den vom System erkannten Fingerabdruck zu akzeptieren.

## 5 Klicken Sie auf **Verbinden**.

**Hinweis** Wenn Sie diese Einstellung im Setup-Assistenten ausgelassen haben oder den zugehörigen NSX Manager ändern möchten, melden Sie sich bei CSM an und klicken Sie auf **System > Einstellungen** und dann auf **Konfigurieren** im Fenster **Zugeordneter NSX-Knoten**.

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

## 6 (Optional) Richten Sie den Proxy-Server ein. Weitere Anweisungen finden Sie unter [\(Optional\) Proxy-Server konfigurieren](#).

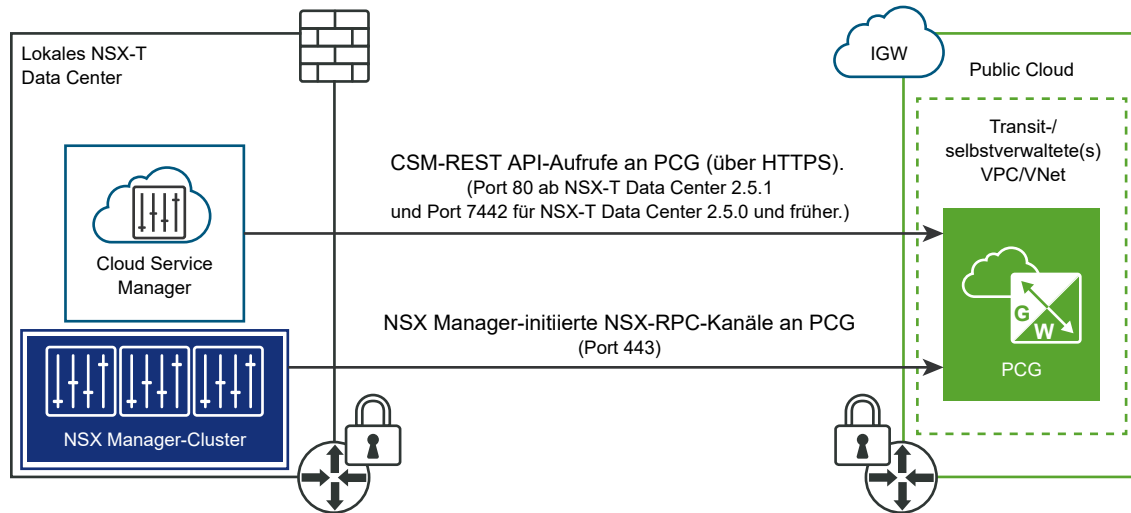
## Aktivieren des Zugriffs auf Ports und Protokolle

Zum Aktivieren der Public Cloud-Konnektivität müssen in Ihrer lokalen Bereitstellung von NSX-T Data Center keine eingehenden Ports geöffnet sein.

Die folgenden ausgehenden Ports sind erforderlich:

**Tabelle 13-2. Ports und Protokolle, die für die Public Cloud-Konnektivität mit NSX-T Data Center erforderlich sind**

Von	An	Port	Protokoll	Erforderlich für:
CSM	PCG	80  <b>Hinweis</b> Wenn Sie NSX-T Data Center-Version 2.5.0 verwenden, müssen Sie stattdessen den nicht standardmäßigen Port 7442 öffnen und sicherstellen, dass Ihre Firewall SSL-Datenverkehr darüber zulässt.	TCP	CSM-Konfiguration, z. B. Upgrade-Workflow, über HTTPS.
NSX Manager	PCG	443	TCP	NSX-RPC-Kanal/-Kanäle.
CSM	NSX Manager	443	TCP	CSM für den Zugriff auf NSX Manager. Einzelheiten zu der lokalen Bereitstellung finden Sie unter <a href="#">Ports und Protokolle</a> .



## (Optional) Proxy-Server konfigurieren

Wenn Sie den gesamten internetgebundenen HTTP/HTTPS-Verkehr über einen zuverlässigen HTTP-Proxy routen und überwachen möchten, können Sie in CSM bis zu fünf Proxyserver konfigurieren.

Die gesamte Public Cloud-Kommunikation von PCG und CSM wird über den ausgewählten Proxyserver geleitet.

Proxysteinstellungen für PCG sind unabhängig von Proxysteinstellungen für CSM. Sie haben die Auswahl zwischen keinem oder einem anderen Proxyserver für PCG.

Sie können die folgenden Authentifizierungsebenen auswählen:

- Auf Anmeldedaten basierende Authentifizierung.
- Zertifikatsbasierte Authentifizierung zum Abfangen von HTTPS.
- Keine Authentifizierung.

### Verfahren

- 1 Klicken Sie auf **System > Einstellungen**. Klicken Sie dann im Bereich mit dem Titel **Proxyserver** auf **Konfigurieren**.

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

- 2 Geben Sie auf dem Bildschirm „Proxy-Server konfigurieren“ die folgenden Details ein:

Option	Beschreibung
<b>Standard</b>	Verwenden Sie dieses Optionsfeld, um den Standard-Proxyserver anzugeben.
<b>Profilname</b>	Geben Sie einen Namen für das Proxyserverprofil an. Dies ist ein Pflichtfeld.



Option	Beschreibung
<b>Proxyserver</b>	Geben Sie die IP-Adresse des Proxyservers ein. Dies ist ein Pflichtfeld.
<b>Port</b>	Geben Sie den Port des Proxiservers ein. Dies ist ein Pflichtfeld.
<b>Authentifizierung</b>	Optional Wenn Sie eine zusätzliche Authentifizierung einrichten möchten, aktivieren Sie dieses Kontrollkästchen und geben Sie einen gültigen Benutzernamen und das Kennwort ein.
<b>Benutzername</b>	Dies ist erforderlich, wenn Sie das Kontrollkästchen „Authentifizierung“ aktivieren.
<b>Kennwort</b>	Dies ist erforderlich, wenn Sie das Kontrollkästchen „Authentifizierung“ aktivieren.
<b>Zertifikat</b>	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.
<b>Kein Proxy</b>	Wählen Sie diese Option, wenn Sie keinen der konfigurierten Proxyserver verwenden möchten.

## (Optional) Einrichten von vIDM für Cloud Service Manager

Wenn Sie VMware Identity Manager verwenden, können Sie diesen so einrichten, dass innerhalb von NSX Manager auf CSM zugegriffen werden kann.

### Verfahren

- 1 Konfigurieren Sie vIDM für NSX Manager und CSM. Weitere Informationen finden Sie unter [Konfigurieren der Integration von VMware Identity Manager](#) im *Administratorhandbuch für NSX-T Data Center*.
- 2 Weisen Sie dem vIDM-Benutzer dieselbe Rolle für NSX Manager und CSM zu. Weisen Sie beispielsweise die Rolle **Unternehmensadministrator** dem Benutzer mit dem Namen **vIDM\_admin** zu. Sie müssen sich sowohl bei NSX Manager als auch bei CSM anmelden und demselben Benutzernamen dieselbe Rolle zuweisen. Detaillierte Anweisungen finden Sie unter [Hinzufügen einer Rollenzuweisung oder Prinzipalidentität](#) im *Administratorhandbuch für NSX-T Data Center*.
- 3 Melden Sie sich bei NSX Manager an. Sie werden zur vIDM-Anmeldung umgeleitet.
- 4 Geben Sie die Anmeldedaten des vIDM-Benutzers ein. Nachdem Sie sich angemeldet haben, können Sie zwischen NSX Manager und CSM wechseln, indem Sie auf das Anwendungssymbol klicken.



## Ihr Public Cloud-Konto hinzufügen

Zum Hinzufügen Ihres Public-Cloud-Bestands müssen Sie Ihr Public Cloud-Konto mit der lokalen Bereitstellung von NSX-T Data Center verbinden, erforderliche Subnetze in der VPC/im VNet erstellen und Rollen in Ihrer Public Cloud erstellen, um den Zugriff auf NSX Cloud zuzulassen.

Diese Schritte unterliegen keiner bestimmten Reihenfolge und können unabhängig voneinander ausgeführt werden.

---

### Hinweis

- Verbinden Sie VPCs/VNets lokal. Verwenden Sie dazu geeignete Methoden, z. B. Direct Connect für AWS oder Express Route für Microsoft Azure oder Site-to-Site-VPN, wobei ein beliebiger VPN-Endpunkt lokal und PCG als VPN-Endpunkt in Ihrer Public Cloud fungieren.
- Wenn Sie sich für eine Transit-/Computing-Topologie entscheiden, stellen Sie sicher, dass zwischen den Transit- und Computing-VPCs/VNets Peer-Verbindungen vorhanden sind. Sie können über einen einzelnen PCG mehrere Computing-VPCs/VNets verwalten. Sie haben auch die Möglichkeit, eine flache Computing-VPC/VNet-Architektur mit einem PCG-Paar zu verwenden, das in jeder VPC/jedem VNet installiert ist.

---

## Ihr Microsoft Azure-Netzwerk mit Ihrer lokalen NSX-T Data Center-Bereitstellung verbinden

Zwischen Ihrem Microsoft Azure-Netzwerk und Ihren lokalen NSX-T Data Center-Appliances muss eine Verbindung eingerichtet sein.

---

**Hinweis** Sie müssen bereits NSX Manager installiert und eine Verbindung zu CSM in Ihrer lokalen Bereitstellung hergestellt haben.

---

### Übersicht

- Verbinden Sie Ihr Microsoft Azure-Abonnement mit dem lokalen NSX-T Data Center.
- Konfigurieren Sie Ihre VNets mit den notwendigen CIDR-Blöcken und Subnetzen, die für NSX Cloud erforderlich sind.
- Synchronisieren Sie die Uhrzeit auf der CSM-Apliance mit dem Microsoft Azure Storage-Server oder NTP.

## Verbinden Sie Ihr Microsoft Azure-Abonnement mit dem lokalen NSX-T Data Center

Jede Public Cloud bietet Optionen für die Verbindung mit einer lokalen Bereitstellung. Sie können eine der verfügbaren Konnektivitätsoptionen, die Ihren Anforderungen genügt, auswählen. Einzelheiten finden Sie in der Microsoft Azure-Referenzdokumentation.

---

**Hinweis** Sie müssen die anwendbaren Sicherheitsüberlegungen und Best Practices von Microsoft Azure überprüfen und implementieren. Zum Beispiel sollte für alle privilegierten Benutzerkonten, die auf das Microsoft Azure-Portal oder die Azure-API zugreifen, Multi-Faktor-Authentifizierung (MFA) aktiviert sein. MFA stellt sicher, dass nur ein autorisierter Benutzer auf das Portal zugreifen kann und reduziert die Wahrscheinlichkeit eines Zugriffs, selbst wenn Anmeldeinformationen gestohlen oder weitergegeben werden. Weitere Informationen und Empfehlungen hierzu finden Sie in der Microsoft 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.

Details zur Verwendung dieser Subnetze finden Sie unter [Bereitstellen des NSX Public Cloud Gateway](#).

## Einrichten eines sicheren Zugriffs auf Ihre Microsoft Azure-Bestandsliste

Damit NSX Cloud im Rahmen Ihres Abonnements funktioniert, richten Sie einen Service Principal ein, welcher die erforderlichen Berechtigungen gewährt, sowie Rollen für CSM und PCG basierend auf der Microsoft Azure-Funktion für die Verwaltung von Identitäten für Azure-Ressourcen.

### Übersicht:

- Ihr Microsoft Azure-Abonnement enthält ein oder mehrere VNets, die unter NSX-T Data Center-Verwaltung gestellt werden sollen. Das VNet befindet sich möglicherweise im Übergangsmodus (Transit) oder im Computing-Modus. Im Transit-VNet stellen Sie das PCG bereit. Sie können andere VNets mit dem Transit-VNet verknüpfen und das Onboarding für die darin gehosteten Workload-VMs vornehmen. Die mit dem Transit-VNet verknüpften VNets werden als Computing-VNets bezeichnet.

- NSX Cloud bietet ein PowerShell-Skript, um den Service Principal zu generieren, sowie Rollen, welche die Funktion der verwalteten Identität von Microsoft Azure verwenden, um die Authentifizierung zu verwalten, während Ihre Microsoft Azure-Anmeldedaten gut geschützt sind. Sie können mit diesem Skript auch mehrere Abonnements unter einem Service Principal aufnehmen.
- Sie haben die Möglichkeit, den Service Principal für all Ihre Abonnements wiederzuverwenden oder nach Bedarf neue Service Principals zu erstellen. Es gibt ein zusätzliches Skript für den Fall, dass Sie separate Service Principals für weitere Abonnements erstellen möchten.
- Für mehrere Abonnements müssen Sie, ganz gleich, ob Sie einen einzelnen Service Principal für alle oder mehrere Service Principals verwenden, die JSON-Dateien für die Rollen CSM und PCG aktualisieren, um jeden zusätzlichen Abonnementnamen unter dem Abschnitt *AssignableScopes* hinzuzufügen.
- Wenn Sie bereits über einen NSX Cloud Service Principal in Ihrem VNet verfügen, können Sie ihn aktualisieren, indem die Skripte erneut ausführen und dabei den Service Principal-Namen in den Parametern auslassen.
- Der Service Principal-Name muss für Ihr Microsoft Azure Active Directory eindeutig sein. Sie können den gleichen Service Principal in verschiedenen Abonnements unter der gleichen Active Directory-Domäne oder unterschiedliche Service Principals pro Abonnement verwenden. Sie können jedoch nicht zwei Service Principals mit demselben Namen erstellen.
- Sie müssen der Eigentümer sein oder über Berechtigungen zum Erstellen und Zuweisen von Rollen in allen Microsoft Azure-Abonnements verfügen.
- Die folgenden Szenarien werden unterstützt:
  - **Szenario 1:** Sie verfügen über ein einzelnes Microsoft Azure-Abonnement, das Sie mit NSX Cloud aktivieren möchten.
  - **Szenario 2:** Sie verfügen über mehrere Microsoft Azure-Abonnements unter demselben Microsoft Azure-Verzeichnis, die Sie mit NSX Cloud aktivieren möchten, Sie möchten jedoch für all Ihre Abonnements nur einen einzigen NSX Cloud Service Principal verwenden.
  - **Szenario 3:** Sie verfügen über mehrere Microsoft Azure-Abonnements unter demselben Microsoft Azure-Verzeichnis, die Sie mit NSX Cloud aktivieren möchten, Sie möchten jedoch unterschiedliche NSX Cloud Service Principal-Namen für unterschiedliche Abonnements verwenden.

Es folgt eine Übersicht des Prozesses:

- 1 Verwenden Sie das NSX Cloud PowerShell-Skript:
  - Erstellen Sie ein Service Principal-Konto für NSX Cloud.
  - Eine Rolle für CSM erstellen.
  - Eine Rolle für PCG erstellen.

- 2 (Optional) Erstellen Sie Service Principals für andere Abonnements, die Sie verknüpfen möchten.
- 3 Fügen Sie das Microsoft Azure-Abonnement zu CSM hinzu.

---

**Hinweis** Wenn Sie mehrere Abonnements verwenden, müssen Sie, egal ob Sie denselben oder unterschiedliche Service Principals verwenden, jedes Abonnement separat in CSM hinzufügen.

---

## Generieren des Service Principal und von Rollen

NSX Cloud bietet PowerShell-Skripte, mit denen Sie den erforderlichen Dienstprinzipal und die Rollen für ein oder mehrere Abonnements generieren können.

### Voraussetzungen

- Sie müssen PowerShell 5.0+ mit dem AzureRM-Modul installiert haben.
- Sie müssen der Eigentümer sein oder über Berechtigungen zum Erstellen und Zuweisen von Rollen in allen Microsoft Azure-Abonnements verfügen.

---

**Hinweis** Die Antwortzeiten von Microsoft Azure können dazu führen, dass das Skript beim ersten Ausführen fehlschlägt. Wenn das Skript fehlschlägt, versuchen Sie es erneut auszuführen.

---

### Verfahren

- 1 Laden Sie auf einem Windows-Desktop oder -Server die ZIP-Datei `CreateNSXCloudCredentials.zip` von der NSX-T Data Center-**Download-Seite > Treiber & Tools > NSX-Cloud-Skripte > Microsoft Azure** herunter.
- 2 Entpacken Sie den folgenden Inhalt der ZIP-Datei in Ihr Windows-System:

Skript/Datei	Beschreibung
<b>CreateNSXRoles.ps1</b>	<p>Das PowerShell-Skript zum Generieren des NSX Cloud Dienstprinzipals und der verwalteten Identitätsrollen für CSM und PCG. Dieses Skript verwendet die folgenden Parameter:</p> <ul style="list-style-type: none"> <li>■ <code>-subscriptionId &lt;the Transit_VNet's_Azure_subscription_ID&gt;</code></li> <li>■ (optional) <code>-servicePrincipalName &lt;Service_Principal_Name&gt;</code></li> <li>■ (optional) <code>-useOneServicePrincipal</code></li> </ul>
<b>AddServicePrincipal.ps1</b>	<p>Ein optionales Skript, das erforderlich ist, wenn Sie jedem Abonnement mehrere Abonnements hinzufügen und verschiedene Dienstprinzipale zuweisen möchten. Weitere Informationen finden Sie unter <b>Szenario 3</b> in den folgenden Schritten. Dieses Skript verwendet die folgenden Parameter:</p> <ul style="list-style-type: none"> <li>■ <code>-computeSubscriptionId &lt;the_Compute_VNet's_Azure_subscription_ID&gt;</code></li> <li>■ <code>-transitSubscriptionId &lt;the Transit_VNet's_Azure_Subscription_ID&gt;</code></li> <li>■ <code>-csmRoleName &lt;CSM_Role_Name&gt;</code></li> <li>■ <code>-servicePrincipalName &lt;Service_Principal_Name&gt;</code></li> </ul>

Skript/Datei	Beschreibung
<b>nsx_csm_role.JSON</b>	Eine JSON-Vorlage für den Namen und die Berechtigungen der CSM-Rolle. Diese Datei ist als Eingabe in das PowerShell-Skript erforderlich und muss sich im selben Ordner wie das Skript befinden.
<b>nsx_pcg_role.JSON</b>	Eine JSON-Vorlage für den Namen und die Berechtigungen der PCG-Rolle. Diese Datei ist als Eingabe in das PowerShell-Skript erforderlich und muss sich im selben Ordner wie das Skript befinden.  <b>Hinweis</b> Der PCG-(Gateway-)Rollenname ist standardmäßig <code>nsx-pcg-role</code> . Sie müssen diesen Wert beim Hinzufügen Ihres Abonnements in CSM angeben.

**3 Szenario 1:** Sie verfügen über ein einzelnes Microsoft Azure-Abonnement, das Sie mit NSX Cloud aktivieren möchten.

- Wechseln Sie aus einer PowerShell-Instanz in das Verzeichnis, in das Sie die Microsoft Azure-Skripte und die JSON-Dateien heruntergeladen haben.
- Führen Sie das Skript mit dem Namen „CreateNSXRoles.ps1“ mit dem Parameter `-SubscriptionId` wie folgt aus:

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

**Hinweis** Wenn Sie den Service Principal-Standardnamen `nsx-service-admin` überschreiben möchten, können Sie auch den Parameter `-servicePrincipalName` verwenden. Der SPN muss in Ihrem Microsoft Azure Active Directory eindeutig sein.

- 4 Szenario 2:** Sie verfügen über mehrere Microsoft Azure-Abonnements unter demselben Microsoft Azure-Verzeichnis, die Sie mit NSX Cloud aktivieren möchten, Sie möchten jedoch für all Ihre Abonnements nur einen einzigen NSX Cloud Service Principal verwenden.

- a Wechseln Sie aus einer PowerShell-Instanz in das Verzeichnis, in das Sie die Microsoft Azure-Skripte und die JSON-Dateien heruntergeladen haben.
- b Bearbeiten Sie jede der JSON-Dateien, um eine Liste anderer Abonnement-IDs unter dem Abschnitt mit dem Titel „*AssignableScopes*“ hinzuzufügen, beispielsweise:

```
"AssignableScopes": [
  "/subscriptions/aaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee",
  "/subscriptions/aaaaaaa-bbbb-cccc-dddd-ffffffffffff",
  "/subscriptions/aaaaaaa-bbbb-cccc-dddd-000000000000"
```

**Hinweis** Sie müssen das im Beispiel gezeigte Format verwenden, um Abonnement-IDs hinzuzufügen: `"/subscriptions/<Subscription_ID>"`

- c Führen Sie das Skript mit dem Namen `CreateNSXRoles.ps1` mit den Parametern `-subscriptionID` und `-useOneServicePrincipal` aus:

```
.\CreateNSXRoles.ps1 -subscriptionId <the_Transit_VNet's_Azure_subscription_ID>
-useOneServicePrincipal
```

**Hinweis** Lassen Sie den Dienstprinzipalnamen hier weg, wenn Sie den Standardnamen verwenden möchten: `nsx-service-admin`. Wenn dieser Dienstprinzipalname bereits in Ihrem Microsoft Azure Active Directory vorhanden ist, führt die Ausführung dieses Skripts ohne Dienstprinzipalnamen dazu, dass der Dienstprinzipal aktualisiert wird.

- 5 Szenario 3:** Sie verfügen über mehrere Microsoft Azure-Abonnements unter demselben Microsoft Azure-Verzeichnis, die Sie mit NSX Cloud aktivieren möchten, Sie möchten jedoch unterschiedliche NSX Cloud Service Principal-Namen für unterschiedliche Abonnements verwenden.

- a Wechseln Sie aus einer PowerShell-Instanz in das Verzeichnis, in das Sie die Microsoft Azure-Skripte und die JSON-Dateien heruntergeladen haben.
- b Führen Sie die Schritte **b** und **c** aus dem zweiten Szenario aus, um in jeder der JSON-Dateien mehrere Abonnements zum Abschnitt „*AssignableScopes*“ hinzuzufügen.

- c Führen Sie das Skript mit dem Namen `CreateNSXRoles.ps1` mit dem Parameter `-subscriptionID` aus:

```
.\CreateNSXRoles.ps1 -subscriptionId <One of the subscription_IDs>
```

**Hinweis** Lassen Sie den Dienstprinzipalnamen hier weg, wenn Sie den Standardnamen verwenden möchten: `nsx-service-admin`. Wenn dieser Dienstprinzipalname in Ihrem Microsoft Azure Active Directory vorhanden ist, führt die Ausführung dieses Skripts ohne Dienstprinzipalnamen dazu, dass der Dienstprinzipal aktualisiert wird.

- d Führen Sie das Skript mit dem Namen `AddServicePrincipal.ps1` mit den folgenden Parametern aus:

Parameter	Wert
<code>-computeSubscriptionId</code>	Die Azure-Abonnement-ID von Compute_VNet
<code>-transitSubscriptionId</code>	Die Azure-Abonnement-ID des Transit-VNet
<code>-csmRoleName</code>	Sie können diesen Wert aus der Datei <code>nsx_csm_role.JSON</code> beziehen.
<code>-servicePrincipalName</code>	Neuer Dienstprinzipalname

```
./AddServicePrincipal.ps1 -computeSubscriptionId <the_Compute_VNet's_Azure_subscription_ID>
-transitSubscriptionId <the_Transit_VNet's_Azure_Subscription_ID>
-csmRoleName <CSM_Role_Name>
-servicePrincipalName <new_Service_Principal_Name>
```

- 6 Suchen Sie nach einer Datei im selben Verzeichnis, in dem Sie das PowerShell-Skript ausgeführt haben. Sie heißt in etwa: `NSXCloud_ServicePrincipal_<your_subscription_ID>_<NSX_Cloud_Service_Principal_name>`. Diese Datei enthält Informationen, die Sie benötigen, um Ihr Microsoft Azure-Abonnement in CSM hinzuzufügen.

- Client-ID
- Client-Schlüssel
- Mandanten-ID
- Abonnement-ID

## Ergebnisse

Es werden die folgenden Konstrukte erstellt:

- eine Azure-AD-Anwendung für NSX Cloud.
- einen Azure Resource Manager Service Principal für die NSX Cloud-Anwendung.
- eine Rolle für CSM, die dem Service-Principal-Konto zugeordnet ist.
- eine Rolle für PCG, um die Arbeit an Ihrem Public-Cloud-Bestand zu ermöglichen.



- Eine Datei mit einem Namen wie `NSXCloud_ServicePrincipal_<your_subscription_ID>_<NSX_Cloud_Service_Principal_name>` wird in demselben Verzeichnis erstellt, in dem Sie das PowerShell-Skript ausgeführt haben. Diese Datei enthält Informationen, die Sie benötigen, um Ihr Microsoft Azure-Abonnement in CSM hinzuzufügen.

---

**Hinweis** In den JSON-Dateien, die zum Erstellen der Rollen CSM und PCG verwendet werden, finden Sie eine Liste der Berechtigungen, die Ihnen nach dem Erstellen der Rollen zur Verfügung stehen.

---

## Nächste Schritte

### Ihr Microsoft-Azure-Abonnement in CSM hinzufügen

---

**Hinweis** Beim Aktivieren von NSX Cloud für mehrere Abonnements müssen Sie jedes separate Abonnement einzeln dem CSM hinzufügen. Wenn Sie beispielsweise insgesamt über fünf Abonnements verfügen, müssen Sie fünf Microsoft Azure-Konten in CSM hinzufügen, wobei alle anderen Werte gleich, die Abonnement-IDs jedoch unterschiedlich sind.

---

### Ihr Microsoft-Azure-Abonnement in CSM hinzufügen

Nachdem Sie über die Details des NSX Cloud Service Principal und der CSM- und PCG-Rollen verfügen, können Sie Ihr Microsoft Azure-Abonnement in CSM hinzufügen.

## Voraussetzungen

- Sie müssen in NSX-T Data Center über die Rolle „Enterprise-Administrator“ verfügen.
- Sie müssen über die Ausgabe des PowerShell-Skripts mit Details zum NSX Cloud Service Principal verfügen.
- Sie müssen den Wert der PCG-Rolle kennen, den Sie beim Ausführen des PowerShell-Skripts angegeben haben, um die Rollen und den Service Principal zu erstellen. Der Standardwert ist `nsx-pcg-role`.

## Verfahren

- 1 Melden Sie sich unter Verwendung eines Kontos mit der Rolle „Enterprise-Administrator“ bei CSM an.
- 2 Wechseln Sie zu **CSM > Clouds > Azure**.

- 3 Klicken Sie auf **+ Hinzufügen** und geben Sie die folgenden Details an:

Option	Beschreibung
<b>Name</b>	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.
<b>Client-ID</b>	Kopieren Sie diesen Wert und fügen Sie ihn aus der Ausgabe des PowerShell-Skripts ein.
<b>Schlüssel</b>	Kopieren Sie diesen Wert und fügen Sie ihn aus der Ausgabe des PowerShell-Skripts ein.
<b>Abonnement-ID</b>	Kopieren Sie diesen Wert und fügen Sie ihn aus der Ausgabe des PowerShell-Skripts ein.
<b>Mandanten-ID</b>	Kopieren Sie diesen Wert und fügen Sie ihn aus der Ausgabe des PowerShell-Skripts ein.
<b>Gateway-Rollenname</b>	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.
<b>Cloud-Tags</b>	Standardmäßig ist diese Option aktiviert und erlaubt es, dass Ihre Microsoft Azure-Tags in NSX Manager angezeigt werden

- 4 Klicken Sie auf **Speichern**.

CSM fügt das Konto hinzu, und nach drei Minuten können Sie es im Bereich **Konten** sehen.

- 5 Verschieben Sie alle VMs in dem VNet, in denen VMs verwaltet werden sollen, in die Whitelist. Dies ist zwar nicht erforderlich, wird jedoch aufgrund der Auswirkungen auf die Quarantäne-Richtlinie beim Ändern vom deaktivierten in den aktivierten Zustand für Brownfield-Bereitstellungen dringend empfohlen.

#### Nächste Schritte

[Bereitstellen von PCG in einem VNet](#)

## 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 relevanten Sicherheitsaspekte und Best Practices von AWS überprüfen und implementieren. Einzelheiten 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.

---

Weitere Informationen finden Sie unter [Bereitstellen des NSX Public Cloud Gateway](#) .

---

- 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.

## Einrichten eines sicheren Zugriffs auf Ihre Microsoft Azure-Bestandsliste

Möglicherweise verfügen Sie über ein oder mehrere AWS-Konten mit VPCs und Workload-VMs, die Sie unter NSX-T Data Center-Verwaltung möchten.

### Übersicht:

- Sie können die Transit-/Computing-VPC-Topologie, bei der Sie das PCG in einer VPC bereitstellen, nutzen, wodurch Sie sie zur Transit-VPC machen und andere VPCs, so genannte Computing-VPCs, damit verknüpfen.
- NSX Cloud liefert ein Shell-Skript, das Sie von der AWS-CLI Ihres AWS-Kontos ausführen können, um das IAM-Profil und die Rolle anzulegen und um eine vertrauenswürdige Beziehung für Transit- und Computing-VPCs erstellen zu können.
- Die folgenden Szenarien werden unterstützt:
  - **Szenario 1:** Sie möchten ein einzelnes AWS-Konto mit NSX Cloud verwenden.
  - **Szenario 2:** Sie möchten mehrere Unterkonten auf dem AWS nutzen, die von einem AWS-Hauptkonto verwaltet werden.
  - **Szenario 3:** Sie möchten mehrere AWS-Konten mit der NSX Cloud verwenden.

Es folgt eine Übersicht des Prozesses:

- 1 Verwenden Sie das NSX Cloud-Shell-Skript, das die AWS-CLI erfordert, für folgende Aufgaben:
  - Ein Uplink-Profil erstellen.
  - Eine Rolle für PCG erstellen.
  - (Optional) Eine vertrauenswürdige Beziehung zwischen dem AWS-Konto, das die Transit-VPC hostet, und dem AWS-Konto, das die Computing-VPC hostet, erstellen.
- 2 Das AWS-Konto in CSM hinzufügen.

### Generieren des IAM-Profiles und der PCG-Rolle

NSX Cloud enthält ein SHELL-Skript, um die Einrichtung von einem oder mehreren Ihrer AWS-Konten durch das Anlegen eines IAM-Profiles und einer Rolle für das PCG zu vereinfachen. Letztere ist an das Profil angehängt, welches die erforderlichen Berechtigungen für Ihr AWS-Konto liefert.

Wenn Sie vorhaben, eine Transit-VPC mit mehreren Computing-VPCs in zwei verschiedenen AWS-Konten zu verknüpfen, können Sie das Skript zum Erstellen einer vertrauenswürdigen Beziehung zwischen diesen Konten verwenden.

---

**Hinweis** Der PCG-(Gateway-)Rollenname ist standardmäßig `nsx_pcg_service`. Wenn Sie einen anderen Wert für den Gateway-Rollenname möchten, können Sie ihn im Skript ändern, notieren Sie sich diesen Wert jedoch, da er für das Hinzufügen des AWS-Kontos zur CSM erforderlich ist.

---

### Voraussetzungen

Bevor Sie das Skript ausführen, müssen Sie auf Ihrem Linux-System oder einem kompatiblen System Folgendes installiert und konfiguriert haben:

- AWS-CLI
- jq (ein JSON-Parser)
- openssl

---

**Hinweis** Wenn Sie mehrere AWS-Konten verwenden, müssen die Konten mit einer geeigneten Methode mittels Peering verbunden werden.

---

### Verfahren

- 1 Laden Sie auf einem Linux- oder kompatiblen Desktop oder Server das SHELL-Skript mit dem Namen `nsx_csm_iam_script.sh` von der NSX-T Data Center-**Download-Seite > Treiber & Tools > NSX Cloud-Skripte > AWS** herunter.

- 2 **Szenario 1:** Sie möchten ein einzelnes AWS-Konto mit NSX Cloud verwenden.

- a Führen Sie das Skript aus, beispielsweise:

```
bash nsx_csm_iam_script.sh
```

- b Geben Sie bei entsprechender Aufforderung mit der Frage `Do you want to create an IAM user for CSM and an IAM role for PCG? [yes/no]` `yes` ein.
- c Geben Sie bei der Frage `What do you want to name the IAM User?` einen Namen für den IAM-Benutzer ein.

---

**Hinweis** Der IAM-Benutzername muss in Ihrem AWS-Konto eindeutig sein.

---

- d Geben Sie bei der Frage `Do you want to add trust relationship for any Transit VPC account? [yes/no]` `no` ein.

Wenn das Skript erfolgreich ausgeführt wird, werden das IAM-Profil und eine Rolle für PCG in Ihrem AWS-Konto erstellt. Die Werte werden in der Ausgabedatei `aws_details.txt` in demselben Verzeichnis gespeichert, in dem Sie das Skript ausgeführt haben. Im nächsten Schritt führen Sie die Anweisungen unter [Ihr AWS-Konto zu CSM hinzufügen](#) und dann [Bereitstellen von PCG in einer VPC](#) aus, um die Einrichtung einer Transit-VPC oder selbstverwalteten VPC abzuschließen.

### 3 **Szenario 2:** Sie möchten mehrere Unterkonten auf dem AWS nutzen, die von einem AWS-Hauptkonto verwaltet werden.

- a Führen Sie das Skript über Ihr AWS-Hauptkonto aus.

```
bash nsx_csm_iam_script.sh
```

- b Geben Sie bei entsprechender Aufforderung mit der Frage `Do you want to create an IAM user for CSM and an IAM role for PCG?` `[yes/no]` `yes` ein.
- c Geben Sie bei der Frage `What do you want to name the IAM User?` einen Namen für den IAM-Benutzer ein.

---

**Hinweis** Der IAM-Benutzername muss in Ihrem AWS-Konto eindeutig sein.

---

- d Geben Sie bei der Frage `Do you want to add trust relationship for any Transit VPC account?` `[yes/no]` `no` ein.

---

**Hinweis** Mit einem AWS-Hauptkonto müssen Sie, wenn Ihre Transit-VPC die Berechtigung zum Anzeigen von Computing-VPCs in den Unterkonten hat, keine vertrauenswürdige Beziehung zu Ihren Unterkonten mehr herstellen. Befolgen Sie andernfalls die Schritte für **Szenario 3**, um mehrere Konten einzurichten.

---

Wenn das Skript erfolgreich ausgeführt wird, werden das IAM-Profil und eine Rolle für das PCG in Ihrem AWS-Hauptkonto erstellt. Die Werte werden in der Ausgabedatei im selben Verzeichnis gespeichert, in dem Sie das Skript ausgeführt haben. Der Dateiname lautet `aws_details.txt`. Im nächsten Schritt führen Sie die Anweisungen unter [Ihr AWS-Konto zu CSM hinzufügen](#) und dann [Bereitstellen von PCG in einer VPC](#) aus, um die Einrichtung einer Transit-VPC oder selbstverwalteten VPC abzuschließen.

### 4 **Szenario 3:** Sie möchten mehrere AWS-Konten mit der NSX Cloud verwenden.

---

**Hinweis** Stellen Sie sicher, dass die AWS-Konten mittels Peering verbunden sind, bevor Sie fortfahren.

---

- a Notieren Sie sich die 12-stellige AWS-Kontonummer für das Konto, auf dem Sie die Transit-VPC hosten möchten.
- b Richten Sie die Transit-VPC im AWS-Konto ein, indem Sie die Schritte *a* bis *d* für *Szenario 1* befolgen. Schließen Sie das Verfahren zum Hinzufügen des Kontos in CSM ab.
- c Laden Sie das Skript NSX Cloud von einem Linux-System oder einem kompatiblen System in Ihrem anderen AWS-Konto, auf dem Sie die Computing-VPCs hosten möchten, herunter und führen Sie es aus.

---

**Hinweis** Alternativ können Sie die AWS-Profile mit anderen Konto-Anmeldedaten nutzen, um so das Skript für Ihr anderes AWS-Konto wieder unter Verwendung desselben Systems auszuführen.

---

- d Geben Sie bei der Frage `Do you want to create an IAM user for CSM and an IAM role for PCG?` `[yes/no]` `yes` ein.

---

**Hinweis** Wenn Sie dieses AWS-Konto bereits im CSM hinzugefügt haben und das Skript für die Verbindung mit einem anderen AWS-Konto wiederverwenden möchten, können Sie `no` eingeben und das Anlegen des IAM-Benutzers überspringen.

---

- e Geben Sie bei der Frage `What do you want to name the IAM User?` einen Namen für den IAM-Benutzer ein.

---

**Hinweis** Der IAM-Benutzername muss in Ihrem AWS-Konto eindeutig sein.

---

- f Geben Sie bei der Frage `Do you want to add trust relationship for any Transit VPC account?` `[yes/no]` `yes` ein.

- g Geben Sie die 12-stellige AWS-Kontonummer, die Sie sich bei der Frage `What is the Transit VPC account number?` in Schritt 1 notiert haben, ein bzw. kopieren und fügen Sie sie ein.

Eine vertrauenswürdige IAM-Beziehung wird zwischen den beiden AWS-Konten eingerichtet, und es wird eine externe ID (ExternalID) vom Skript generiert.

Wenn das Skript erfolgreich ausgeführt wird, werden das IAM-Profil und eine Rolle für das PCG in Ihrem AWS-Hauptkonto erstellt. Die Werte werden in der Ausgabedatei im selben Verzeichnis gespeichert, in dem Sie das Skript ausgeführt haben. Der Dateiname lautet `aws_details.txt`. Im nächsten Schritt führen Sie die Anweisungen unter [Ihr AWS-Konto zu CSM hinzufügen](#) und dann unter [Verknüpfung mit einer Transit-VPC oder einem Transit-VNet](#) aus, um die Verknüpfung mit einer Transit-VPC abzuschließen.

### Ihr AWS-Konto zu CSM hinzufügen

Fügen Sie Ihr AWS-Konto mithilfe der vom Skript generierten Werte hinzu.

#### Verfahren

- 1 Melden Sie sich bei CSM mit der Rolle „Enterprise-Administrator“ an.
- 2 Navigieren Sie zu **CSM > Clouds > AWS**.
- 3 Klicken Sie auf **+Hinzufügen** und geben Sie mit Hilfe der Ausgabedatei `aws_details.txt`, die aus dem Skript NSX Cloud generiert wurde, die folgenden Details ein:

Option	Beschreibung
<b>Name</b>	Geben Sie einen aussagekräftigen Namen für dieses AWS-Konto ein
<b>Zugriffsschlüssel</b>	Geben Sie den Zugriffsschlüssel Ihres Kontos ein
<b>Geheimer Schlüssel</b>	Geben Sie den geheimen Schlüssel Ihres Kontos ein

Option	Beschreibung
<b>Cloud-Tags erkennen</b>	Standardmäßig ist diese Option aktiviert und ermöglicht es, dass Ihre AWS-Tags in NSX Manager angezeigt werden
<b>Gateway-Rollenname</b>	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.

- 4 Verschieben Sie alle VMs in der VPC, in denen VMs verwaltet werden sollen, in die Whitelist. Dies ist zwar nicht erforderlich, wird jedoch aufgrund der Auswirkungen auf die Quarantäne-Richtlinie beim Ändern vom deaktivierten in den aktivierten Zustand für Brownfield-Bereitstellungen dringend empfohlen.

#### Nächste Schritte

[Bereitstellen von PCG in einer VPC](#)

## Bereitstellen des NSX Public Cloud Gateway

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

Machen Sie sich mit der folgenden Terminologie vertraut, in der die Architektur und die Bereitstellungsmodi von PCG für die Arbeitslast-VM-Verwaltung erläutert werden.

**Hinweis** PCG wird für jede unterstützte Public Cloud in einer einzelnen Standardgröße bereitgestellt:

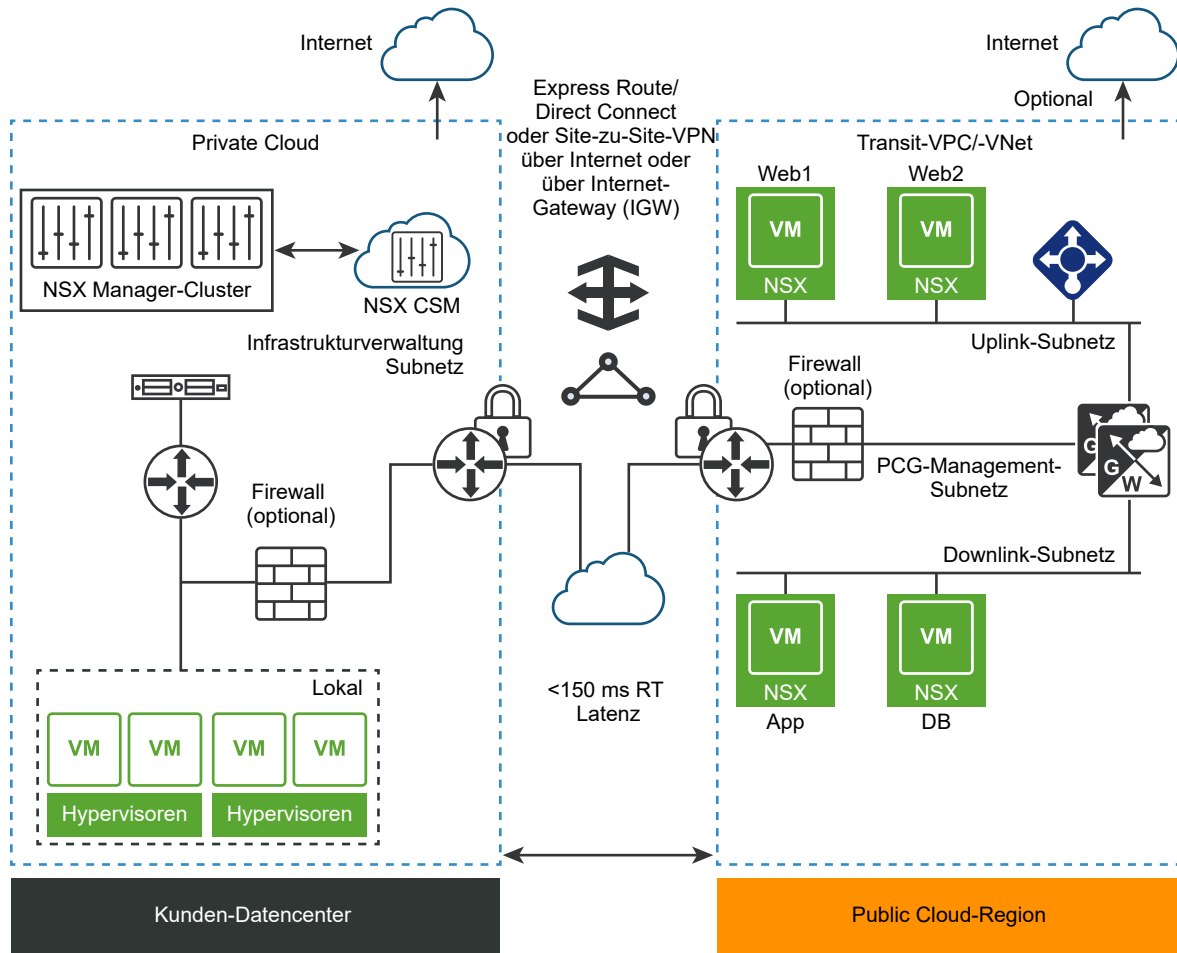
Public Cloud	PCG-Instanztyp
AWS	C4.xlarge
	<b>Hinweis</b> Einige Regionen unterstützen den Typ der C4.xlarge-Instanz möglicherweise nicht. Einzelheiten finden Sie in der AWS-Dokumentation.
Microsoft Azure	Standard-DS3 Version 2

## Architektur

Das PCG kann entweder eine eigenständige-Gateway-Appliance sein oder von Ihren Public Cloud-VPCs oder -VNETs gemeinsam genutzt werden, um eine Hub-and-Spoke-Topologie zu erhalten.



Abbildung 13-2. Die Architektur von NSX Public Cloud Gateway



## Bereitstellungsmodi

**Selbstverwaltete(s) VPC/VNet:** Wenn Sie das PCG in einer VPC oder einem VNet bereitstellen, wird die VPC oder das VNet als *selbstverwaltet* qualifiziert, d. h. Sie können VMs, die in dieser VPC oder diesem VNet gehostet werden, unter NSX-Verwaltung stellen.

**Transit-VPC/VNet :** Eine selbst verwaltete VPC/ein selbst verwaltetes VNet wird zu einer bzw. einem *Transit-VPC/VNet*, wenn Sie Computing-VPCs/VNets damit verknüpfen.

**Computing-VPC/VNet:** VPCs/VNets, auf denen das PCG nicht bereitgestellt ist, die jedoch über eine Verknüpfung zu einer Transit-VPC/einem Transit-VNet verfügen, werden als *Computing-VPCs/VNets* bezeichnet.

## In Ihrer VPC/Ihrem VNet erforderliche Subnetze für die Bereitstellung von PCG

Das PCG nutzt die folgenden Subnetze, die Sie in Ihrem VPC/VNet eingerichtet haben. Siehe [Ihr Microsoft Azure-Netzwerk mit Ihrer lokalen NSX-T Data Center-Bereitstellung verbinden](#) oder [Ihr Amazon Web Services-Netzwerk \(AWS-Netzwerk\) mit Ihrer lokalen NSX-T Data Center-Bereitstellung verbinden](#).

- **Management-Subnetz:** Dieses Subnetz wird für das Management des Datenverkehrs zwischen lokalen NSX-T Data Center und PCG verwendet. Der empfohlene Bereich ist /28.
- **Uplink-Subnetz:** Dieses Subnetz wird für den Nord-Süd-Internetverkehr genutzt. Der empfohlene Bereich ist /24.
- **Downlink-Subnetz:** Dieses Subnetz umfasst den IP-Adressbereich der Workload-VMs und sollte entsprechend dimensioniert werden. Beachten Sie, dass Sie für das Debugging eventuell zusätzliche Schnittstellen auf den Arbeitslast-VMs einbinden müssen.

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.

---

## Modi der VM-Verwaltung

NSX-erzwungener Modus: In diesem Modus werden Arbeitslast-VMs mithilfe von NSX Tools unter NSX-Verwaltung gestellt, die auf jeder Arbeitslast-VM installiert werden müssen, nachdem das Tag „nsx.network=default“ auf sie in AWS oder Microsoft Azure angewendet wurde.

Native Cloud-erzwungener Modus : In diesem Modus können Ihre Arbeitslast-VMs ohne Verwendung von NSX Tools unter NSX-Verwaltung gestellt werden.

## Quarantäne-Richtlinie

Quarantäne-Richtlinie: Dies ist die Bedrohungserkennungsfunktion von NSX Cloud, die mit Ihren Public Cloud-Sicherheitsgruppen funktioniert.

- Im NSX-erzwungener Modus können Sie die Quarantäne-Richtlinie aktivieren oder deaktivieren. Es wird empfohlen, die Quarantäne-Richtlinie zu deaktivieren und alle VMs beim Onboarding von Arbeitslast-VMs in die Whitelist zu verschieben.
- Im Native Cloud-erzwungener Modus ist die Quarantäne-Richtlinie immer aktiviert und kann nicht deaktiviert werden.

## Mögliche Designoptionen

Unabhängig vom Modus, in dem Sie PCG bereitstellen, können Sie eine bzw. ein Computing-VPC/VNet in einem der beiden Modi damit verknüpfen.

Tabelle 13-3. Mögliche Designoptionen für PCG-Bereitstellungsmodi

PCG-Bereitstellungsmodus bei Transit-VPC/VNet	Mögliche Modi beim Verknüpfen von Computing-VPCs/VNets mit dieser bzw. diesem Transit-VPC/VNet
NSX-erzwungener Modus	<ul style="list-style-type: none"> <li>■ NSX-erzwungener Modus</li> <li>■ Native Cloud-erzwungener Modus</li> </ul>
Native Cloud-erzwungener Modus	<ul style="list-style-type: none"> <li>■ NSX-erzwungener Modus</li> <li>■ Native Cloud-erzwungener Modus</li> </ul>

**Hinweis** Sobald ein Modus für eine bzw. ein Transit- oder Computing-VPC/VNet ausgewählt wurde, können Sie den Modus nicht ändern. Wenn Sie den Modus wechseln möchten, müssen Sie die Bereitstellung von PCG aufheben und im gewünschten Modus eine erneute Bereitstellung durchführen.

## Bereitstellen von PCG in einem VNet

Folgen Sie diesen Anweisungen, um PCG in Ihrem Microsoft Azure-VNet bereitzustellen.

Das VNet, in dem Sie PCG bereitstellen, kann als ein Transit-VNet fungieren, mit dem sich andere VNets (so genannte Computing-VNets) verbinden können. Dieses VNet kann auch VMs verwalten und als ein selbstverwaltetes VNet fungieren.

Folgen Sie diesen Anweisungen, um PCG bereitzustellen. Wenn Sie eine Verknüpfung mit einem vorhandenen Transit-VNet herstellen möchten, finden Sie weitere Informationen dazu unter [Verknüpfung mit einer Transit-VPC oder einem Transit-VNet](#).

### Voraussetzungen

- Ihre Public Cloud-Konten müssen bereits in CSM hinzugefügt worden sein.
- In dem VNet, in dem Sie PCG bereitstellen, müssen die erforderlichen Subnetze für die Hochverfügbarkeit angepasst sein: *Uplink*, *Downlink* und *Verwaltung*.

### Verfahren

- 1 Melden Sie sich unter Verwendung eines Kontos mit der Rolle „Enterprise-Administrator“ bei CSM an.
- 2 Klicken Sie auf **Clouds > Azure** und navigieren Sie zur Registerkarte **VNets**.
- 3 Klicken Sie auf ein VNet, in dem Sie das PCG bereitstellen möchten.
- 4 Klicken Sie auf **Gateways bereitstellen**. Der Assistent **Gateway bereitstellen** wird geöffnet.

## 5 Verwenden Sie für allgemeine Eigenschaften die folgenden Richtlinien:

Option	Beschreibung
<b>Öffentlicher SSH-Schlüssel</b>	Geben Sie einen öffentlichen SSH-Schlüssel an, der während der Bereitstellung des PCGs validiert werden kann. Dies ist für jede PCG-Bereitstellung erforderlich.
<b>Quarantäne-Richtlinie für das zugehörige VNet</b>	<p>Sie können die Einstellung für die Quarantäne-Richtlinie nur dann ändern, wenn Sie Arbeitslast-VMs mit NSX Tools (NSX-erzwungener Modus) verwalten. Quarantäne-Richtlinie ist im Native Cloud-erzwungener Modus immer aktiviert.</p> <p>Belassen Sie dies im Standardmodus <b>deaktiviert</b>, wenn Sie das PCG erstmalig bereitstellen. Sie können diesen Wert nach Onboarding von VMs ändern. Weitere Informationen finden Sie unter <b>Verwalten der Quarantäne-Richtlinie</b> im <i>Administratorhandbuch für NSX-T Data Center</i>.</p>
<b>Mit NSX Tools verwalten</b>	Behalten Sie den standardmäßigen deaktivierten Status für das Onboarding von Arbeitslast-VMs im Native Cloud-erzwungener Modus bei. Wenn Sie NSX Tools auf Ihren Arbeitslast-VMs installieren möchten, um den NSX-erzwungener Modus zu verwenden, aktivieren Sie diese Option.
<b>Automatische Installation von NSX Tools</b>	Dies ist nur verfügbar, wenn Sie „Mit NSX Tools verwalten“ aktivieren. Wenn diese Option ausgewählt ist, werden NSX Tools automatisch auf allen Arbeitslast-VMs im Transit-/selbstverwalteten/Linked Computing-VNet installiert, wenn das Tag <code>nsx.network=default</code> auf sie angewendet wird.
<b>Lokales Speicherkonto</b>	<p>Wenn Sie CSM ein Microsoft Azure-Abonnement hinzufügen, steht CSM eine Liste Ihrer Microsoft Azure-Speicherkonten zur Verfügung. Wählen Sie im Dropdown-Menü das Speicherkonto aus. Wenn Sie mit der Bereitstellung des PCGs fortfahren, kopiert CSM die öffentlich verfügbare VHD des PCGs in dieses Speicherkonto der ausgewählten Region.</p> <p><b>Hinweis</b> Wenn das VHD-Image bereits für eine frühere PCG-Bereitstellung in dieses Speicherkonto in der Region kopiert wurde, wird das Image von diesem Speicherort aus für nachfolgende Bereitstellungen verwendet, um die gesamte Bereitstellungszeit zu verkürzen.</p>
<b>VHD-URL</b>	<p>Wenn Sie ein anderes PCG-Image verwenden möchten, das im öffentlichen VMware-Repository nicht verfügbar ist, können Sie die URL der PCG-VHD hier eingeben. Die VHD-Datei muss im selben Konto und derselben Region, in dem/der dieses VNet erstellt wird, vorhanden sein.</p> <p><b>Hinweis</b> Die VHD muss das richtige URL-Format aufweisen. Es wird empfohlen, die Option <b>Zum Kopieren klicken</b> in Microsoft Azure zu verwenden.</p>
<b>Proxyserver</b>	<p>Wählen Sie einen Proxy-Server aus, der für den internetgebundenen Datenverkehr von diesem PCG verwendet werden soll. Die Proxy-Server werden in CSM konfiguriert. Sie können denselben Proxy-Server auswählen wie CSM, falls vorhanden, einen anderen Proxy-Server aus CSM auswählen oder <b>Kein Proxy-Server</b> wählen.</p> <p>Weitere Informationen zur Konfiguration von Proxy-Servern in CSM finden Sie unter <a href="#">(Optional) Proxy-Server konfigurieren</a>.</p>
<b>Erweitert</b>	Die erweiterten DNS-Einstellungen bieten Flexibilität bei der Auswahl der DNS-Server zum Auflösen von NSX-T Data Center-Verwaltungskomponenten.

Option	Beschreibung
<b>Über DHCP des Public-Cloud-Anbieters beziehen</b>	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.
<b>DNS-Server des Public-Cloud-Anbieters überschreiben</b>	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.
<b>DNS-Server des Public-Cloud-Anbieters nur für NSX-T Data Center-Appliances verwenden</b>	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
<b>HA für NSX Cloud-Gateway aktivieren</b>	Wählen Sie diese Option, um Hochverfügbarkeit zu ermöglichen.
<b>Subnetze</b>	Wählen Sie diese Option, um Hochverfügbarkeit zu ermöglichen.
<b>Öffentliche IP für Management-Netzwerkkarte (Mgmt NIC)</b>	Wählen Sie <b>Neue IP-Adresse zuteilen</b> , um der Management-Netzwerkkarte eine öffentliche IP-Adresse bereitzustellen. Sie können die öffentliche IP-Adresse manuell bereitstellen, wenn Sie eine freie öffentliche IP-Adresse wiederverwenden möchten.
<b>Öffentliche IP für Uplink-Netzwerkkarte (NIC)</b>	Wählen Sie <b>Neue IP-Adresse zuteilen</b> , um der Uplink-Netzwerkkarte (NIC) eine öffentliche IP-Adresse bereitzustellen. Sie können die öffentliche IP-Adresse manuell bereitstellen, wenn Sie eine freie öffentliche IP-Adresse wiederverwenden möchten.

### Nächste Schritte

Befolgen Sie die Anweisungen unter [Verwenden von NSX Cloud](#) im *Administratorhandbuch für NSX-T Data Center*.

## Bereitstellen von PCG in einer VPC

Befolgen Sie die Anweisungen zur Bereitstellung von PCG in Ihrer AWS-VPC.

Die VPC, in der Sie eine PCG bereitstellen, kann als Transit-VPC fungieren, mit der sich andere VPCs (so genannte Computing-VPCs) verbinden können. Diese VPC kann auch VMs verwalten und als eine selbstverwaltete VPC fungieren.

Folgen Sie diesen Anweisungen, um PCG bereitzustellen. Wenn Sie eine Verknüpfung mit einer vorhandenen Transit-VPC herstellen möchten, finden Sie weitere Informationen dazu unter [Verknüpfung mit einer Transit-VPC oder einem Transit-VNet](#).

## Voraussetzungen

- Ihre Public Cloud-Konten müssen bereits in CSM hinzugefügt worden sein.
- Auf der VPC, auf der Sie PCG bereitstellen, müssen die erforderlichen Subnetze für die Hochverfügbarkeit angepasst sein: *Uplink*, *Downlink* und *Verwaltung*.
- Die Konfiguration für die Netzwerkzugriffskontrollliste Ihrer VPC muss eine Regel zum ZULASSEN des eingehenden Datenverkehrs enthalten.

## Verfahren

- 1 Melden Sie sich unter Verwendung eines Kontos mit der Rolle „Enterprise-Administrator“ bei CSM an.
- 2 Klicken Sie auf **Clouds > AWS > <AWS\_account\_name>** und öffnen Sie die Registerkarte **VPCs**.
- 3 Wählen Sie auf der Registerkarte **VPCs** einen AWS-Regionsnamen, z. B. us-west. Die AWS-Region muss identisch sein mit der, in der Sie die Computing-VPC erstellt haben.
- 4 Wählen Sie eine für NSX Cloud konfigurierte Computing-VPC aus.
- 5 Klicken Sie auf Gateways bereitstellen.
- 6 Vervollständigen Sie die allgemeinen Gateway-Details:

Option	Beschreibung
<b>PEM-Datei</b>	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.
<b>Quarantäne-Richtlinie für die zugehörige VPC</b>	Sie können die Einstellung für die Quarantäne-Richtlinie nur dann ändern, wenn Sie Arbeitslast-VMs mit NSX Tools (NSX-erzwungener Modus) verwalten. Quarantäne-Richtlinie ist im Native Cloud-erzwungener Modus immer aktiviert  Belassen Sie dies im Standardmodus <b>deaktiviert</b> , wenn Sie das PCG erstmalig bereitstellen. Sie können diesen Wert nach Onboarding von VMs ändern. Weitere Informationen finden Sie unter <b>Verwalten der Quarantäne-Richtlinie</b> im <i>Administratorhandbuch für NSX-T Data Center</i> .
<b>Mit NSX Tools verwalten</b>	Behalten Sie den standardmäßigen deaktivierten Status für das Onboarding von Arbeitslast-VMs im Native Cloud-erzwungener Modus bei. Wenn Sie NSX Tools auf Ihren Arbeitslast-VMs installieren möchten, um den NSX-erzwungener Modus zu verwenden, aktivieren Sie diese Option.
<b>Proxyserver</b>	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 <b>Kein Proxy-Server</b> wählen.  Weitere Informationen zur Konfiguration von Proxy-Servern in CSM finden Sie unter <a href="#">(Optional) Proxy-Server konfigurieren</a> .
<b>Erweitert</b>	Die erweiterten Einstellungen bieten zusätzliche Optionen, falls erforderlich.

Option	Beschreibung
<b>AMI-ID aufheben</b>	Benutzen Sie diese erweiterte Funktion, um eine andere AMI-ID für das PCG zu vergeben als die, die in Ihrem AWS-Konto verfügbar ist.
<b>Über DHCP des Public-Cloud-Anbieters beziehen</b>	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.
<b>DNS-Server des Public-Cloud-Anbieters überschreiben</b>	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.
<b>DNS-Server des Public-Cloud-Anbieters nur für NSX-T Data Center-Appliances verwenden</b>	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
<b>HA für Public Cloud-Gateway aktivieren</b>	Die empfohlene Einstellung ist „Aktivieren“, wodurch ein hochverfügbares Aktiv/Standby-Paar eingerichtet wird, um ungeplante Ausfallzeiten zu vermeiden.
<b>Primäre Gateway-Einstellungen</b>	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.
<b>Sekundäre Gateway-Einstellungen</b>	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.
<b>Öffentliche IP für Management-Netzwerkkarte (Mgmt NIC)</b>	Wählen Sie <b>Neue IP-Adresse zuteilen</b> , um der Management-Netzwerkkarte eine öffentliche IP-Adresse bereitzustellen. Sie können die öffentliche IP-Adresse manuell bereitstellen, wenn Sie eine freie öffentliche IP-Adresse wiederverwenden möchten.
<b>Öffentliche IP für Uplink-Netzwerkkarte (NIC)</b>	Wählen Sie <b>Neue IP-Adresse zuteilen</b> , um der Uplink-Netzwerkkarte (NIC) eine öffentliche IP-Adresse bereitzustellen. Sie können die öffentliche IP-Adresse manuell bereitstellen, wenn Sie eine freie öffentliche IP-Adresse wiederverwenden möchten.

Klicken Sie auf Bereitstellen.

9 Überwachen Sie den Status der primären (und sekundären, falls Sie diese ausgewählt haben) PCG-Bereitstellung. Dieser Vorgang kann 10–12 Minuten dauern.

10 Klicken Sie auf Fertig stellen, wenn PCG erfolgreich bereitgestellt wurde.

## Nächste Schritte

Befolgen Sie die Anweisungen unter [Verwenden von NSX Cloud](#) im *Administratorhandbuch für NSX-T Data Center*.

## Verknüpfung mit einer Transit-VPC oder einem Transit-VNet

Sie können eine oder mehrere Computing-VPCs oder -VNet mit einer Transit-VPC oder -VNet verknüpfen.

### Voraussetzungen

- Stellen Sie sicher, dass Sie über eine Transit-VPC oder ein VNet mit PCG verfügen.
- Stellen Sie sicher, dass die VPC bzw. das VNet, die/das Sie verknüpfen möchten, über VPN oder Peering mit der Transit-VPC oder dem Transit-VNet verbunden ist.
- Stellen Sie sicher, dass sich die Computing-VPC/das Computing-VNet in derselben Region befindet wie die Transit-VPC bzw. das Transit-VNet.

---

**Hinweis** In der routenbasierten IPSec-VPN-Konfiguration müssen Sie die IP-Adresse für den VTI-Port (Virtual Tunnel Interface) angeben. Diese IP muss sich in einem anderen Subnetz als die Arbeitslast-VMs befinden. Dadurch wird verhindert, dass der eingehende Datenverkehr der Arbeitslast-VM an den VTI-Port geleitet wird, von dem er gelöscht wird.

---



---

**Hinweis** In der Public Cloud ist die Anzahl der Regeln für den eingehenden/ausgehenden Datenverkehr durch einen Standardgrenzwert pro Sicherheitsgruppe beschränkt und NSX Cloud erstellt Standardsicherheitsgruppen. Dies wirkt sich darauf aus, wie viele Computing-VPCs/-VNet mit einer Transit-VPC oder einem Transit-VNet verknüpft werden können. Wenn ein CIDR-Block pro VPC/VNet angenommen wird, unterstützt NSX Cloud 10 Computing-VPCs/-VNet pro Transit-VPC/-VNet. Wenn Sie über mehr als einen CIDR-Block in einer Computing-VPC bzw. einem Computing-VNet verfügen, wird die Anzahl der unterstützten Computing-VPCs/-VNet pro Transit-VPC/-VNet reduziert. Sie können die Standardgrenzwerte anpassen, indem Sie sich an Ihren Public-Cloud-Anbieter wenden.

---

### Verfahren

- 1 Melden Sie sich unter Verwendung eines Kontos mit der Rolle „Enterprise-Administrator“ bei CSM an.
- 2 Klicken Sie auf **Clouds > AWS/Azure > <public cloud\_account\_name>** und gehen Sie zur Registerkarte **VPCs/VNets**.
- 3 Wählen Sie auf der Registerkarte **VPCs** oder **VNets** den Namen einer Region aus, in der Sie einen oder mehrere Computing-VPCs oder -VNet hosten.
- 4 Wählen Sie eine Computing-VPC/ein Computing-VNet aus, die bzw. das für NSX Cloud konfiguriert ist.
- 5 Klicken Sie auf **MIT TRANSIT-VPC VERKNÜPFEN** oder auf **MIT TRANSIT-VNET VERKNÜPFEN**.



## 6 Füllen Sie die Optionen im Fenster **Mit Transit-VPC oder -VNet verknüpfen** aus:

Option	Beschreibung
<b>Transit-VPC oder -VNet</b>	<p>Wählen Sie aus dem Dropdown-Menü eine Transit-VPC oder ein Transit-VNet aus. Die Transit-VPC oder das Transit-VNet, die bzw. das Sie auswählen, muss bereits per VPN oder Peering mit dieser VPC verknüpft sein.</p> <p><b>Hinweis</b> Wenn Sie eine Verbindung mit einem Transit-VNet herstellen, muss in diesem eine DNS-Weiterleitungskonfiguration eingestellt und das Tag <code>nsx.dnsserver=&lt;IP address of the DNS forwarder&gt;</code> muss auf die Transit-VNet angewendet sein. Informationen zum Einrichten der DNS-Weiterleitungen finden Sie in der Microsoft Azure-Dokumentation.</p>
<b>Quarantäne-Standardrichtlinie</b>	<p>Belassen Sie dies im Standardmodus <b>deaktiviert</b>, wenn Sie das PCG erstmalig bereitstellen. Sie können diesen Wert nach Onboarding von VMs ändern. Weitere Informationen finden Sie unter <b>Verwalten der Quarantäne-Richtlinie</b> im <i>Administratorhandbuch für NSX-T Data Center</i>.</p>
<b>Mit NSX Tools verwalten</b>	<p>Behalten Sie den standardmäßigen deaktivierten Status für das Onboarding von Arbeitslast-VMs im Native Cloud-erzwungener Modus bei. Wenn Sie NSX Tools auf Ihren Arbeitslast-VMs installieren möchten, um den NSX-erzwungener Modus zu verwenden, aktivieren Sie diese Option.</p>
<b>Automatische Installation von NSX Tools</b>	<p>Diese Option ist nur verfügbar, wenn die Verwaltung mit NSX Tools und nur für Microsoft Azure VNets erfolgen soll. Wenn diese Option ausgewählt ist, werden NSX Tools automatisch auf allen Arbeitslast-VMs im Transit-/selbstverwalteten/Linked Computing-VNet installiert, wenn das Tag <code>nsx.network=default</code> auf sie angewendet wird.</p>

### Nächste Schritte

Befolgen Sie die Anweisungen unter [Verwenden von NSX Cloud](#) im *Administratorhandbuch für NSX-T Data Center*.

## Automatisch erstellte logische Entitäten und Cloud-native Sicherheitsgruppen

Die Bereitstellung von PCG in einem Transit-VPC/-VNet und die Verknüpfung eines Computing-VPC/-VNet damit löst notwendige Konfigurationen in NSX-T Data Center und in der Public Cloud aus.

### Automatisch erstellte logische NSX-T-Elemente

Eine Reihe logischer Entitäten wird automatisch in NSX Manager erstellt.

Melden Sie sich bei NSX Manager an, um die automatisch erstellten logischen Entitäten anzuzeigen.

**Wichtig** Löschen Sie keine dieser automatischen erstellten Entitäten, es sei denn, Sie heben die Bereitstellung von PCG manuell auf. Einzelheiten dazu finden Sie unter [Beheben von Fehlern bei der Aufhebung der PCG-Bereitstellung](#).

## Systementitäten

Auf der Registerkarte **System** werden die folgenden Entitäten angezeigt:

Tabelle 13-4. Automatisch erstellte Systementitäten

Logische Systementität	Wie viele werden erstellt?	Nomenklatur	Geltungsbereich
<b>Transportzonen</b>	Es werden zwei Transportzonen für jede Transit-VPC/jedes Transit-VNet erstellt.	<ul style="list-style-type: none"> <li>■ TZ-&lt;VPC/VNet-ID&gt;-OVERLAY</li> <li>■ TZ-&lt;VPC/VNet-ID&gt;-VLAN</li> </ul>	Geltungsbereich: global
<b>Edge-Transportknoten</b>	Für jedes bereitgestellte PCG wird ein Edge-Transportknoten angelegt, zwei, wenn die Bereitstellung im Hochverfügbarkeitsmodus erfolgt.	<ul style="list-style-type: none"> <li>■ PublicCloudGateway TN-&lt;VPC/VNET-ID&gt;</li> <li>■ PublicCloudGateway TN-&lt;VPC/VNET-ID&gt;-preferred</li> </ul>	Geltungsbereich: global
<b>Edge-Cluster</b>	Für jedes bereitgestellte PCG wird ein Edge-Cluster angelegt, entweder einzeln oder als Bestandteil eines Hochverfügbarkeitspaares.	PCG-cluster-<VPC/VNet-ID>	Geltungsbereich: global

## Bestandslisten-Entitäten

Die folgenden Entitäten sind auf der Registerkarte **Bestand** verfügbar:

Tabelle 13-5. Gruppen

Gruppen	Geltungsbereich
Zwei Gruppen mit dem Namen: <ul style="list-style-type: none"> <li>■ cloud-default-route</li> <li>■ cloud-metadata services</li> </ul>	Geltungsbereich: Freigabe über alle PCGs hinweg
Eine Gruppe, die auf Transit VPC/VNet-Ebene als übergeordnete Gruppe für einzelne Segmente generiert wurde, die auf der Compute-VPC-/VNet-Ebene erstellt wurden. cloud-<Transit VPC/VNet ID>-all-segments	Geltungsbereich: für alle Computing-VPCs/-VNets freigegeben

Tabelle 13-5. Gruppen (Fortsetzung)

Gruppen	Geltungsbereich
<p>Zwei Gruppen für alle Compute-VPCs/VNets:</p> <ul style="list-style-type: none"> <li>■ Netzwerk-CIDR-Gruppe für alle CIDRs von Compute-VPC/VNet: <code>cloud-&lt;Compute VPC/VNet ID&gt;-cidr</code></li> <li>■ Gruppe lokaler Segmente für alle verwalteten Segmente in Compute-VPC/VNet: <code>cloud-&lt;Compute VPC/VNet ID&gt;-local-segments</code></li> </ul>	Geltungsbereich: für alle Computing-VPC/-VNets freigegeben
<p>Die folgenden Gruppen werden für die aktuell unterstützten Public Cloud-Dienste erstellt:</p> <ul style="list-style-type: none"> <li>■ <code>aws-dynamo-db-service-endpoint</code></li> <li>■ <code>aws-elb-service-endpoint</code></li> <li>■ <code>aws-rds-service-endpoint</code></li> <li>■ <code>aws-s3-service-endpoint</code></li> <li>■ <code>azure-cosmos-db-service-endpoint</code></li> <li>■ <code>azure-load-balancer-service-endpoint</code></li> <li>■ <code>azure-sql-service-endpoint</code></li> <li>■ <code>azure-storage-service-endpoint</code></li> </ul>	Geltungsbereich: Freigabe über alle PCGs hinweg

**Hinweis** Für PCGs, die im Native Cloud-erzwungener Modus bereitgestellt oder verknüpft sind, werden alle Arbeitslast-VMs in der VPC/im VNet unter „Virtuelle Maschinen“ in NSX Manager verfügbar.

## Sicherheitsentitäten

Die folgenden Entitäten sind auf der Registerkarte **Sicherheit** verfügbar:

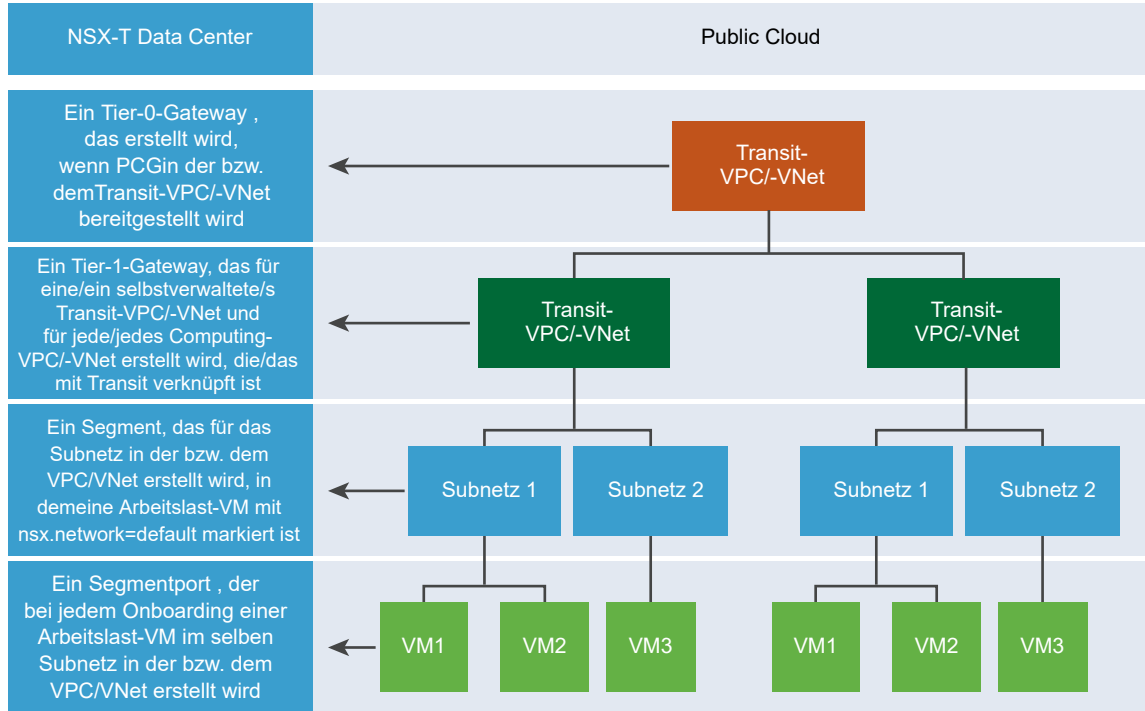
Tabelle 13-6. Automatisch erstellte Sicherheitsentitäten

Logische Sicherheitsentität	Wie viele werden erstellt?	Nomenklatur	Geltungsbereich
Verteilte Firewall (Ost-West)	<p>Zwei pro Transit-VPC/-VNet:</p> <ul style="list-style-type: none"> <li>■ Statusfrei</li> <li>■ Statusbehaftet</li> </ul>	<ul style="list-style-type: none"> <li>■ <code>cloud-stateless-&lt;VPC/VNet ID&gt;</code></li> <li>■ <code>cloud-stateful-&lt;VPC/VNet ID&gt;</code></li> </ul>	<ul style="list-style-type: none"> <li>■ Statusbehaftete Regel, um Datenverkehr innerhalb lokal verwalteter Segmente zuzulassen</li> <li>■ Statusbehaftete Regel, um Datenverkehr von nicht verwalteten VMs abzuweisen</li> </ul>
Gateway-Firewall (Nord-Süd)	Eine pro Transit-VPC/-VNet	<code>cloud-&lt;Transit VPC/VNet ID&gt;</code>	

## Netzwerkentitäten

Die folgenden Entitäten werden in verschiedenen Onboarding-Phasen erstellt und befinden sich auf der Registerkarte **Netzwerk**:

**Abbildung 13-3. Automatisch erstellte Netzwerkentitäten von NSX-T Data Center nach der Bereitstellung von PCG**



**Tabelle 13-7. Automatisch erstellte Netzwerkentitäten**

Onboarding-Aufgabe	Logische Entitäten, im NSX-T Data Center erstellt
PCG, auf Transit-VPC/-VNet bereitgestellt	<ul style="list-style-type: none"> <li>■ Tier-0-Gateway</li> <li>■ Infrasegment (Standard-VLAN-Switch)</li> <li>■ Tier-1-Router</li> </ul>
Computing-VPC oder -VNet, die bzw. das mit dem Transit-VPC/-VNet verknüpft ist	<ul style="list-style-type: none"> <li>■ Tier-1-Router</li> </ul>

Tabelle 13-7. Automatisch erstellte Netzwerkentitäten (Fortsetzung)

Onboarding-Aufgabe	Logische Entitäten, im NSX-T Data Center erstellt
Eine Workload-VM mit darauf installiertem NSX-Agent ist mit dem „nsx.network:default“-Schlüssel:Wert in einem Subnetz einer Computing-VPC/eines Computing VNet oder einer selbstverwalteten VPC/eines selbstverwalteten VNet getaggt.	<ul style="list-style-type: none"> <li>■ Für dieses spezielle Subnetz der Computing-VPC oder des Computing-VNet oder der selbstverwalteten VPC oder des selbstverwalteten VNet wird ein Segment angelegt.</li> <li>■ Hybrid-Ports werden für jede getaggte Workload-VM erstellt, auf der der NSX-Agent installiert ist</li> </ul>
Weitere Workload-VMs werden im selben Subnetz der Computing-VPC/des Computing-VNet oder der selbstverwalteten VPC/des selbstverwalteten VNet getaggt.	<ul style="list-style-type: none"> <li>■ Hybrid-Ports werden für jede getaggte Workload-VM erstellt, auf der der NSX-Agent installiert ist</li> </ul>

## Weiterleitungsrichtlinien

Die folgenden drei Weiterleitungsregeln werden für eine Computing-VPC/ein Computing-VNet, einschließlich einer selbstverwalteten Transit-VPC/eines selbstverwalteten Transit-VNet eingerichtet:

- Zugriff auf alle CIDR von derselben Computing-VPC über das Public Cloud-Netzwerk (Underlay)
- Leiten von Datenverkehr über Public Cloud-Netzwerk an die Public Cloud-Metadatendienste (Underlay)
- Leiten Sie alles, was nicht in den CIDR-Block des Computing-VPC/VNet oder einen bekannten Dienst gehört, über das Netzwerk NSX-T Data Center (Overlay)

## Automatisch erstellte Public Cloud-Konfigurationen

In ihren öffentlichen Clouds werden einige Konfigurationen automatisch eingerichtet, nachdem Sie PCG bereitgestellt haben.

## Public Cloud-Konfigurationen in beiden Modi: NSX-erzwungener Modus und Native Cloud-erzwungener Modus

### In AWS:

- In der AWS VPC wird ein neuer Typ A-Datensatz mit dem Namen `nsx-gw.vmware.local` in eine private gehostete Zone in Amazon Route 53 hinzugefügt. Die diesem Datensatz zugeordnete IP-Adresse entspricht der Management-IP-Adresse von PCG, die vom AWS unter Verwendung von DHCP zugewiesen wird und für jede VPC unterschiedlich ist. Dieser DNS-Eintrag in der privat gehosteten Zone in Amazon Route 53 wird von NSX Cloud zur Auflösung der IP-Adresse von PCG verwendet.

---

**Hinweis** Wenn Sie benutzerdefinierte DNS-Domännennamen nutzen, die in einer privat gehosteten Zone in Amazon Route 53 definiert sind, müssen die **DNS-Auflösung**- und die **DNS-Hostnamen**-Attribute für Ihre VPC-Einstellungen im AWS auf **Ja** festgelegt sein.

---

- Eine sekundäre IP-Adresse für die Uplink-Schnittstelle für PCG wird erstellt. Dieser sekundären IP-Adresse ist eine elastische AWS-IP-Adresse zugeordnet. Diese Konfiguration gilt für SNAT.

### Im Native Cloud-erzwungener Modus :

Die folgenden Sicherheitsgruppen werden bei der PCG-Bereitstellung erstellt.

Nachdem Arbeitslast-VMs mit Gruppen und entsprechenden Sicherheitsrichtlinien in NSX Manager abgeglichen wurden, werden in der Public Cloud Sicherheitsgruppen wie `nsx-<GUID>` für jede übereinstimmende Sicherheitsrichtlinie erstellt.

---

**Hinweis** In AWS werden Sicherheitsgruppen erstellt. In Microsoft Azure werden Anwendungssicherheitsgruppen erstellt, die den Gruppen in NSX Manager entsprechen. Zudem werden Netzwerksicherheitsgruppen erstellt, die den Sicherheitsrichtlinien in NSX Manager entsprechen.

---

Name der Sicherheitsgruppe	Verfügbar in Microsoft Azure?	Verfügbar in AWS?	Beschreibung
vm-quarantine-sg	Ja	Nein	Eine von NSX Cloud erstellte Sicherheitsgruppe in Microsoft Azure für die Zuweisung zu VMs, die nicht mit einer Sicherheitsrichtlinie in NSX-T übereinstimmen.
default	Nein	Ja	Eine bereits vorhandene Sicherheitsgruppe in AWS, die von NSX Cloud für die Zuweisung zu VMs verwendet wird, die nicht mit einer Sicherheitsrichtlinie in NSX-T übereinstimmen.
vm-overlay-sg	Ja	Ja	Overlay-VM-Sicherheitsgruppe (diese wird in der aktuellen Version nicht verwendet)

Von NSX Cloud für PCG-Schnittstellen erstellte Public Cloud-Sicherheitsgruppen, wenn der NSX-erzwungener Modus verwendet wird

Die Sicherheitsgruppen **gw** werden auf die entsprechenden PCG-Schnittstellen angewendet.

Tabelle 13-8. Von NSX Cloud für PCG-Schnittstellen erstellte Public-Cloud-Sicherheitsgruppen

Name der Sicherheitsgruppe	Verfügbar in Microsoft Azure?	Verfügbar in AWS?	Beschreibung
gw-mgmt-sg	Ja	Ja	Gateway-Management-Sicherheitsgruppe
gw-uplink-sg	Ja	Ja	Gateway-Uplink-Sicherheitsgruppe
gw-vtep-sg	Ja	Ja	Gateway-Downlink-Sicherheitsgruppe

Die folgenden Sicherheitsgruppen werden für Arbeitslast-VMs erstellt.

Tabelle 13-9. Von NSX Cloud für Arbeitslast-VMs im NSX-erzwungener Modus erstellte Public Cloud-Sicherheitsgruppen

Name der Sicherheitsgruppe	Verfügbar in Microsoft Azure?	Verfügbar in AWS?	Beschreibung
vm-quarantine-sg	Ja	Nein	Von NSX Cloud erstellte Sicherheitsgruppe in Microsoft Azure für Workflows zur Erkennung von Bedrohungen im NSX-erzwungener Modus
default	Nein	Ja	Eine bereits vorhandene Sicherheitsgruppe in AWS, die von NSX Cloud für Workflows zur Erkennung von Bedrohungen im NSX-erzwungener Modus verwendet wird
vm-underlay-sg	Ja	Ja	Nicht-Overlay-VM-Sicherheitsgruppe
vm-overlay-sg	Ja	Ja	Overlay-VM-Sicherheitsgruppe (diese wird in der aktuellen Version nicht verwendet)

## (Optional) Installieren von NSX Tools auf Ihren Arbeitslast-VMs

Wenn Sie den NSX-erzwungener Modus verwenden, fahren Sie mit der Installation von NSX Tools in ihren Workload-VMs fort.

Weitere Informationen finden Sie unter [Onboarding von VMs im erzwungenen NSX-Modus](#) im *Administratorhandbuch für NSX-T Data Center*.

## Aufheben der Bereitstellung oder Entfernen der Verknüpfung von PCGs

In dieser Übersicht finden Sie Informationen zu den Schritten zur Aufhebung der Bereitstellung oder Entfernung der Verknüpfung von PCGs.

### Im NSX-erzwungener Modus

- Entfernen Sie das `nsx.network=default`-Tag von NSX-verwalteten Arbeitslast-VMs.
- Deaktivieren Sie die Quarantäne-Richtlinie, wenn Sie im NSX-erzwungener Modus aktiviert ist.
- Stellen Sie eine Sicherheitsgruppe in Ihrer Public Cloud bereit, die von NSX Cloud als Fallback-Sicherheitsgruppe verwendet werden kann.



- Löschen Sie alle vom Benutzer erstellten logischen Elemente, die mit dem PCG verknüpft sind.

## Im Native Cloud-erzwungener Modus

- Stellen Sie eine Sicherheitsgruppe in Ihrer Public Cloud bereit, die von NSX Cloud als Fallback-Sicherheitsgruppe verwendet werden kann.
- Löschen Sie alle vom Benutzer erstellten logischen Elemente, die mit dem PCG verknüpft sind.

### Verfahren

#### 1 Entfernen des `nsx.network`-Tags in der Public Cloud

Bevor Sie die Bereitstellung von PCG aufheben können, müssen alle VMs nicht verwaltet sein.

#### 2 Deaktivieren der Quarantäne-Richtlinie, Bereitstellen einer Fallback-Sicherheitsgruppe

In den beiden Modi NSX-erzwungener Modus und Native Cloud-erzwungener Modus müssen Sie eine neue oder vorhandene Sicherheitsgruppe in Ihrer Public Cloud vorbereiten und sie als Fallback-Sicherheitsgruppe in CSM bereitstellen, um mit dem Aufheben der PCG-Bereitstellung oder dem Entfernen der VPC/VNet-Verknüpfung fortzufahren.

#### 3 Vom Benutzer erstellte logische Elemente löschen

Alle vom Benutzer erstellten logischen Elemente, die mit PCG verknüpft sind, müssen gelöscht werden.

#### 4 Bereitstellung aufheben oder Verknüpfung entfernen von CSM

Befolgen Sie diese Anweisungen, um die Bereitstellung aufzuheben oder die Verknüpfung von PCG nach Erfüllen der Voraussetzungen aufzuheben.

#### 5 Beheben von Fehlern bei der Aufhebung der PCG-Bereitstellung

Wenn das Aufheben der PCG-Bereitstellung fehlschlägt, müssen Sie alle von NSX Cloud erstellten Entitäten in NSX Manager sowie in der Public Cloud manuell löschen.

## Entfernen des `nsx.network`-Tags in der Public Cloud

Bevor Sie die Bereitstellung von PCG aufheben können, müssen alle VMs nicht verwaltet sein.

---

**Hinweis** Dies gilt nur für den NSX-erzwungener Modus.

---

Wechseln Sie zur VPC oder zum VNet in Ihrer Public Cloud und entfernen Sie das Tag `nsx.network=default` von den verwalteten VMs.

## Deaktivieren der Quarantäne-Richtlinie, Bereitstellen einer Fallback-Sicherheitsgruppe

In den beiden Modi NSX-erzwungener Modus und Native Cloud-erzwungener Modus müssen Sie eine neue oder vorhandene Sicherheitsgruppe in Ihrer Public Cloud vorbereiten und sie als Fallback-Sicherheitsgruppe in CSM bereitstellen, um mit dem Aufheben der PCG-Bereitstellung oder dem Entfernen der VPC/VNet-Verknüpfung fortzufahren.

Wenn Sie den NSX-erzwungener Modus verwenden, müssen Sie die Quarantäne-Richtlinie deaktivieren, wenn sie zuvor aktiviert wurde.

---

**Hinweis** Die Fallback-Sicherheitsgruppe muss eine vorhandene benutzerdefinierte Sicherheitsgruppe in Ihrer Public Cloud sein. Sie können keine der NSX Cloud-Sicherheitsgruppen als Fallback-Sicherheitsgruppe verwenden. Eine Liste der NSX Cloud Sicherheitsgruppen finden Sie unter [Automatisch erstellte logische Entitäten und Cloud-native Sicherheitsgruppen](#).

In AWS können Sie die default-Sicherheitsgruppe als Fallback-Sicherheitsgruppe konfigurieren, da sie nicht von NSX Cloud erstellt wird.

Wenn Sie bereits eine Fallback-Sicherheitsgruppe bereitgestellt, Sie aber die Computing-VPC/VNet-Verknüpfung entfernt und sie später mit einem Transit-VPC/VNet erneut verknüpft haben, müssen Sie eine andere Fallback-Sicherheitsgruppe konfigurieren.

---

## Wenn die Quarantäne-Richtlinie im NSX-erzwungener Modus aktiviert ist

Wenn die Quarantäne-Richtlinie aktiviert ist, werden Ihren VMs Sicherheitsgruppen in der Public Cloud 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.

Deaktivieren Sie die Quarantäne-Richtlinie für die VPC oder das VNet, von der bzw. dem Sie die Bereitstellung von PCG aufheben und stellen Sie die ID der Fallback-Sicherheitsgruppe bereit:

- Navigieren Sie zur VPC oder zum VNet in CSM.
- Deaktivieren Sie unter **Aktionen > Konfigurationen bearbeiten** die Einstellung für die **Standard-Quarantäne**.
- Geben Sie einen Wert für eine Fallback-Sicherheitsgruppe ein, der VMs zugewiesen werden.
- 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=default`-Tag von solchen VMs entfernen, um sie aus der NSX-Verwaltung zu entfernen, wird ihnen ebenfalls die Fallback-Sicherheitsgruppe zugewiesen.

## Bei Verwendung des Native Cloud-erzwungener Modus

Stellen Sie die Fallback-Sicherheitsgruppen-ID bereit:

- Navigieren Sie zur VPC oder zum VNet in CSM.
- Klicken Sie auf **Aktionen > Konfigurationen bearbeiten**

- Geben Sie die Sicherheitsgruppen-ID von AWS oder die Ressourcen-ID der Netzwerksicherheitsgruppe aus Microsoft Azure als Fallback-Sicherheitsgruppe ein, der VMs zugewiesen werden können, nachdem die PCG-Bereitstellung aufgehoben wurde.

---

**Hinweis** Für Whitelist-VMs führt NSX Cloud keine Aktion aus und VMs werden daher nicht in die Fallback-Sicherheitsgruppe verschoben. Wenn eine Whitelist-VM in den NSX Cloud-zugewiesenen Sicherheitsgruppen vorhanden ist, müssen Sie sie manuell in die vorgesehene Fallback-Sicherheitsgruppe verschieben. Unter [Bedrohungserkennung mit der NSX Cloud-Quarantäne-Richtlinie](#) im *Administratorhandbuch für NSX-T Data Center* finden Sie Anweisungen und weitere Informationen zu den Auswirkungen der Aktivierung und Deaktivierung der Quarantäne-Richtlinie.

---

## Vom Benutzer erstellte logische Elemente löschen

Alle vom Benutzer erstellten logischen Elemente, die mit PCG verknüpft sind, müssen gelöscht werden.

Ermitteln Sie Elemente, die dem PCG zugeordnet sind, und löschen Sie sie.

---

**Hinweis** Löschen Sie nicht die automatisch erstellten logischen Elemente. Diese werden automatisch gelöscht, nachdem Sie auf **Bereitstellung aufheben** oder **Verknüpfung von Transit-VPC/VNet entfernen** von CSM geklickt haben. Weitere Informationen finden Sie unter [Automatisch erstellte logische Entitäten und Cloud-native Sicherheitsgruppen](#).

---

## Bereitstellung aufheben oder Verknüpfung entfernen von CSM

Befolgen Sie diese Anweisungen, um die Bereitstellung aufzuheben oder die Verknüpfung von PCG nach Erfüllen der Voraussetzungen aufzuheben.

- 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 aufheben** oder **Verknüpfung von Transit-VPC/VNet entfernen**.

Die standardmäßig von NSX Cloud erstellten Entitäten werden automatisch entfernt, wenn die Bereitstellung oder Verknüpfung von PCG aufgehoben bzw. entfernt wird.

## Beheben von Fehlern bei der Aufhebung der PCG-Bereitstellung

Wenn das Aufheben der PCG-Bereitstellung fehlschlägt, müssen Sie alle von NSX Cloud erstellten Entitäten in NSX Manager sowie in der Public Cloud manuell löschen.

- In Ihrer Public Cloud:
  - Beenden Sie alle PCGs in der bzw. im Transit-VPC/VNet.

- Verschieben Sie alle Arbeitslast-VMs in eine Sicherheitsgruppe, die nicht von NSX Cloud erstellt wurde.
- Löschen Sie die von NSX Cloud erstellten Sicherheitsgruppen in der Public Cloud, wie hier aufgeführt: [Automatisch erstellte Public Cloud-Konfigurationen](#) .
- Löschen Sie im Falle von Microsoft Azure auch die von NSX Cloud erstellte Ressourcengruppe, die nach dem Muster **nsx-gw-<vnet ID>-rg** benannt ist.
- Synchronisieren Sie Ihre Public-Cloud-Bestandsliste in CSM neu.
- Löschen Sie die automatisch erstellten Entitäten mit der VPC/VNet-ID in NSX Manager wie hier aufgeführt: [Automatisch erstellte logische NSX-T-Elemente](#).

---

**Hinweis** Löschen Sie nicht die globalen, automatisch erstellten Elemente. Löschen Sie nur diejenigen, deren Name die VPC/VNet-ID enthält.

---

# Installieren und Konfigurieren von NSX Intelligence

# 14

VMware NSX® Intelligence™ bietet eine grafische Benutzerschnittstelle, um die Sicherheitsposition und den Netzwerk-Datenverkehr in Ihrer lokalen NSX-T Data Center-Umgebung zu visualisieren.

NSX Intelligence ist für ESXi-basierte Hosts ab NSX-T Data Center Version 2.5 verfügbar. Es bietet die folgende Funktionalität.

- Eine grafische Visualisierung der NSX-T-Komponenten, wie z. B. Gruppen, VMs und Netzwerk-Datenverkehr, in Ihrer NSX-T Data Center-Bereitstellung. Die verwendeten Daten basieren auf dem im angegebenen Zeitraum aggregierten Netzwerk-Datenverkehr.
- Empfehlungen für Sicherheitsrichtlinien, Richtliniensicherheitsgruppen und Dienste für Anwendungen. Die Empfehlungen unterstützen Sie bei der Implementierung der Mikro-Segmentierung auf Anwendungsebene. Sie ermöglichen es Ihnen, eine dynamischere Sicherheitsrichtlinie umzusetzen, indem Sie die Datenverkehrsmuster der Kommunikation zwischen den VMs in Ihrer NSX-T-Datencenter-Umgebung korrelieren.

Sie können NSX Intelligence verwenden, wenn Sie über eine Lizenz für NSX-T Data Center Enterprise Plus verfügen. Außerdem können Sie das Produkt während des Testzeitraums verwenden, wenn Sie über eine NSX-T Data Center-Evaluierungslizenz verfügen.

---

**Wichtig** Sie müssen über eine Enterprise-Administratorrolle verfügen, um die Berechtigung zum Installieren, Konfigurieren und Verwenden von NSX Intelligence zu erhalten.

---

Die NSX Intelligence-Appliance ist in zwei unterschiedlichen Bereitstellungsszenarien verfügbar. Eine kleine Appliance ist für eine Labor- oder Proof-of-Concept-Bereitstellung bzw. eine kleine Produktionsumgebung verfügbar. Eine große Appliance kann für große Produktionsumgebungen verwendet werden. Siehe [Systemanforderungen für NSX Intelligence](#).

Um die NSX Intelligence-Funktionalität zu aktivieren, müssen Sie die NSX Intelligence-Appliance installieren, die separat von der NSX-T Data Center-Appliance bereitgestellt wird. Sie verwenden die NSX Manager-Benutzeroberfläche, um die NSX Intelligence-Appliance zu installieren. Siehe [Installieren der NSX Intelligence-Appliance](#).

Nachdem Sie die NSX Intelligence-Appliance erfolgreich installiert und konfiguriert haben, greifen Sie auf die NSX Intelligence-Funktionen über die Registerkarte **Planen und Fehler beheben** > **Erkennen und planen** in der NSX Manager-Benutzeroberfläche zu. Weitere Informationen finden Sie unter „Erste Schritte mit NSX Intelligence“ im *Administratorhandbuch für NSX-T Data Center*.

Dieses Kapitel enthält die folgenden Themen:

- [Workflow zur NSX Intelligence-Installation und -Konfiguration](#)
- [Vorbereitung für die Installation von NSX Intelligence](#)
- [Herunterladen und Entpacken des NSX Intelligence-Installationspakets](#)
- [Installieren der NSX Intelligence-Appliance](#)
- [Fehlerbehebung bei der Installation der NSX Intelligence-Appliance](#)
- [Deinstallieren der NSX Intelligence-Appliance](#)

## Workflow zur NSX Intelligence-Installation und -Konfiguration

Verfolgen Sie den NSX Intelligence-Installationsprozess anhand der folgenden Prüfliste.

Führen Sie die Verfahren in der Reihenfolge aus, in der sie aufgeführt sind.

- 1 Installieren Sie auf ESXi-basierten Hosts NSX-T Data Center 2.5 oder höher. VMware NSX® Intelligence™ wird nur auf ESXi-basierten Hosts unterstützt. Siehe [Kapitel 2 Workflows für die Installation von NSX-T Data Center](#).
- 2 Stellen Sie sicher, dass die Systemanforderungen von NSX Intelligence erfüllt sind. Siehe [Systemanforderungen für NSX Intelligence](#).
- 3 Synchronisieren Sie die Uhrzeit auf der NSX Manager-VM und dem Computing-Cluster, auf dem die NSX Intelligence-Appliance bereitgestellt werden soll.
- 4 Laden Sie die tar-Datei des NSX Intelligence-Installationsprogramms auf einen lokalen Webserver herunter. Diese tar-Datei enthält die NSX Intelligence-OVF-Datei, die Sie zum Installieren der NSX Intelligence-Appliance verwenden. Siehe [Herunterladen und Entpacken des NSX Intelligence-Installationspakets](#).
- 5 Installieren der NSX Intelligence-Appliance. Siehe [Installieren der NSX Intelligence-Appliance](#).
- 6 Um die NSX Intelligence-Benutzeroberfläche in der NSX Manager-Benutzeroberfläche zu aktivieren, aktualisieren Sie den Webbrowser, den Sie für die NSX Manager-Sitzung verwenden.
- 7 Beginnen Sie mit der Verwendung der NSX Intelligence-Funktionen. Weitere Informationen finden Sie unter „Erste Schritte mit NSX Intelligence“ im *Administratorhandbuch für NSX-T Data Center*.

## Vorbereitung für die Installation von NSX Intelligence

Sie müssen die Bereitstellungsumgebung so vorbereiten, dass Sie die Mindestsystemanforderungen erfüllt, die für die Installation von NSX Intelligence erforderlich sind.

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

Anforderungen	Beschreibung
Unterstützte Bereitstellungsmethode	<p>OVF wird mithilfe von NSX Manager auf dem VMware vCenter Server™ bereitgestellt, der als Compute Manager hinzugefügt wurde.</p> <p><b>Wichtig</b> Die NSX Intelligence-Appliance kann nur mithilfe von NSX Manager installiert werden und wird nicht unterstützt, wenn die OVF unabhängig installiert wird.</p>
Unterstützte Plattform	ESXi-Hosts verwaltet von vCenter Server
IP-Adresse	Eine NSX Intelligence-Appliance muss eine statische IP-Adresse aufweisen. Sie können die IP-Adresse nach der Installation nicht mehr ändern.
Kennwort für NSX Intelligence-Appliance	<ul style="list-style-type: none"> <li>■ mindestens 12 Zeichen</li> <li>■ mindestens ein Kleinbuchstabe</li> <li>■ mindestens ein Großbuchstabe</li> <li>■ mindestens eine Zahl</li> <li>■ mindestens ein Sonderzeichen</li> <li>■ mindestens fünf unterschiedliche Zeichen</li> <li>■ keine Wörterbuchwörter</li> <li>■ keine Palindrome</li> <li>■ Mehr als vier monotone Zeichenfolgen sind nicht zulässig.</li> </ul>
VMware Tools	Auf der unter einem ESXi-Host ausgeführten NSX Intelligence-VM sind VMTools installiert. Entfernen Sie VMTools nicht.
System	<ul style="list-style-type: none"> <li>■ Stellen Sie sicher, dass die Systemanforderungen erfüllt sind. Siehe <a href="#">Systemanforderungen für NSX Intelligence</a>.</li> <li>■ Stellen Sie sicher, dass die erforderlichen Ports geöffnet sind. Siehe <a href="#">Von NSX Intelligence verwendete TCP- und UDP-Ports</a>.</li> <li>■ Rufen Sie die Informationen für die IP-Adresse für das Verwaltungs-Subnetz und -Gateway, die IP-Adresse des DNS-Servers und die IP-Adresse des NTP-Servers für die zu verwendende NSX Intelligence-Appliance ab.</li> <li>■ Stellen Sie sicher, dass ein SSD-basierter Datenspeicher konfiguriert wurde und für die NSX Intelligence-Appliance zugänglich ist.</li> </ul>

## Systemanforderungen für NSX Intelligence

Stellen Sie vor der Installation der NSX Intelligence-Appliance sicher, dass Ihre Umgebung die unterstützten Mindestanforderungen für den Server-Host, auf dem Sie die Appliance installieren möchten, sowie für den Client erfüllt, auf dem die VM-Visualisierungen angezeigt werden.

## Ressourcenvoraussetzungen für die NSX Intelligence-Appliance

In der folgenden Tabelle sind die verfügbaren NSX Intelligence-Appliance-Größen und die jeweils erforderlichen VM-Ressourcen aufgeführt. Die kleine NSX Intelligence-VM-Appliance-Größe eignet sich für Test- oder Proof-of-Concept-Bereitstellungen bzw. kleine Produktionsumgebungen. Die große NSX Intelligence-VM-Appliance-Größe ist für Produktionsumgebungen geeignet.

Appliance-Größe	Arbeitsspeicher	vCPU	Festplattenspeicher
NSX Intelligence Klein	64 GB	16	2 TB
NSX Intelligence Groß	128 GB	32	2 TB

**Hinweis** Nur eine NSX Intelligence-Appliance wird pro NSX Manager-Cluster unterstützt.

## Anforderungen des NSX Intelligence-Webclients an den Arbeitsspeicher, die CPU und den Browser

Ihr Clientsystem muss mindestens zwei 1,4-GHz-CPU-Kerne und mindestens 16 GB RAM aufweisen, um optimale Leistung zu erbringen.

In der folgenden Tabelle sind die für NSX Intelligence unterstützten Webbrowser-Versionen aufgeführt. Die für einen Browser unterstützte Mindestauflösung ist 1280 x 800 Pixel.

Browser	Windows 10	Mac OS X 10.14, 10.13	Ubuntu 18.4
Chrome 76	Ja	Ja	Ja
Firefox 68	Ja	Ja	Ja
Microsoft Edge 44	Ja	Nicht verfügbar	Nicht verfügbar

**Hinweis** Bei der Verwendung von Microsoft Edge treten bekannte Leistungsprobleme auf. Weitere Informationen finden Sie unter *Versionshinweise für NSX-T Data Center*.

## Von NSX Intelligence verwendete TCP- und UDP-Ports

NSX Intelligence verwendet bestimmte TCP- und UDP-Ports, um mit anderen Komponenten und Produkten zu kommunizieren. Diese Ports müssen sowohl auf den physischen als auch auf den Host-Hypervisor-Firewalls offen sein.

**Wichtig** Um Remote-Zugriff auf den NSX Intelligence-Knoten zu erhalten, müssen Sie SSH auf diesem Knoten aktivieren.



Tabelle 14-1. Von NSX Intelligence verwendete TCP- und UDP-Ports

Quelle	Ziel	Port	Protokoll	Beschreibung
NSX Intelligence	DNS-Server	53	TCP	DNS
NSX Intelligence	DNS-Server	53	UDP	DNS
NSX Intelligence	Management-SCP-Server	22	TCP	SSH (Hochladen von Support-Paketen, Sicherungen usw.)
NSX Intelligence	NTP-Server	123	UDP	NTP
NSX Intelligence	vCenter Server/NSX Unified Appliance	443	TCP	NSX Intelligence für Compute Manager-Kommunikation (vCenter Server) und NSX Unified Appliance, wenn konfiguriert.
NSX Intelligence	NSX Unified Appliance/NSX-Transportknoten	9092	TCP	NSX Intelligence ausgehende Kommunikation mit NSX Unified Appliance oder Transportknoten
NTP-Server	NSX Intelligence	123	UDP	NTP
Verwaltungsclients	NSX Intelligence	22	TCP	SSH (standardmäßig deaktiviert)
Management-Clients/NSX Unified Appliance	NSX Intelligence	443	TCP	NSX-API-Server
NSX Unified Appliance/Transportknoten	NSX Intelligence	9092	TCP	Eingehende Nachrichten von NSX Unified Appliance oder Transportknoten bei der NSX Intelligence-Appliance

## Herunterladen und Entpacken des NSX Intelligence-Installationspakets

Um die NSX Intelligence-Appliance zu installieren, laden Sie die NSX Intelligence-Installationspaketdatei auf einen lokalen Webserver herunter und entpacken Sie sie. Die Paketdatei enthält die OVF-Datei und andere unterstützende Dateien, die für die Installation der NSX Intelligence-Appliance verwendet werden.

## Voraussetzungen

- Stellen Sie sicher, dass Sie berechtigt sind, NSX Intelligence zu verwenden. Sie können NSX Intelligence verwenden, wenn Sie über eine Lizenz für NSX-T Data Center Enterprise Plus verfügen. Außerdem können Sie das Produkt während des Testzeitraums verwenden, wenn Sie über eine NSX-T Data Center-Evaluierungslizenz verfügen.
- Sie müssen über eine Enterprise-Administratorrolle verfügen, um NSX Intelligence installieren, konfigurieren und verwenden zu können.
- Stellen Sie sicher, dass der Benutzer, der den Download durchführt, über die erforderliche Berechtigung für das Herunterladen und Extrahieren der .tar-Dateiinhalte auf einen lokalen Webserver verfügt.
- Stellen Sie sicher, dass der lokale Webserver, den Sie zum Herunterladen der NSX Intelligence-Installationspaketdatei verwenden möchten, den Standardport 80 für HTTP verwendet.

## Verfahren

- 1 Suchen Sie im VMware-Download-Portal nach der NSX Intelligence-Installations-TAR-Datei.
- 2 Laden Sie die NSX Intelligence-Installationspaketdatei herunter und speichern Sie sie auf einem lokalen Webserver-Speicherort, auf den von der NSX Manager-Benutzeroberfläche aus zugegriffen werden kann.

---

**Hinweis** Der aktuell unterstützte Webserver ist IIS für Windows und Apache für Linux oder Mac OS. Sie können einen anderen Webserver Ihrer Wahl verwenden, aber IIS und Apache sind die Webserver, die für diese Betriebssysteme getestet wurden und unterstützt sind.

---

Der Dateiname des Installationspakets weist das folgende Format auf: VMware-NSX-Intelligence-Appliance-**<Versionsnummer>**.**<Build-Nummer>**.tar. Beispiel: VMware-NSX-Intelligence-appliance-1.0.0.0.0.14303803.tar.

### 3 Entpacken Sie den Inhalt der TAR-Datei am selben Speicherort auf dem lokalen Webserver.

- a Verwenden Sie zum Entpacken des TAR-Dateiinhalts auf einem der unterstützten Webserver die folgenden Informationen.

Betriebssystem	Webserver	Entpacken des zu verwendenden Tools
Windows	IIS	<p>7-Zip-Anwendung</p> <p>Verwenden Sie die Benutzeroberfläche von 7-Zip File Manager oder ein Eingabeaufforderungsfenster. Um beispielsweise ein Eingabeaufforderungsfenster zum Entpacken der Beispiel-TAR-Datei zu verwenden, navigieren Sie zum Speicherort der heruntergeladenen NSX Intelligence-TAR-Datei und geben Sie den folgenden Befehl ein.</p> <pre>7z x VMware-NSX-Intelligence-appliance-1.0.0.0.14303803.tar</pre>
Linux	Apache	<p>tar-Befehlszeilenprogramm</p> <p>Um beispielsweise die Beispiel-TAR-Datei zu entpacken, geben Sie Folgendes an einer Eingabeaufforderung ein.</p> <pre>tar -xvf VMware-NSX-Intelligence-appliance-1.0.0.0.14303803.tar</pre>
Mac OS	Apache	<p>tar-Befehlszeilenprogramm</p> <p>Um beispielsweise die Beispiel-TAR-Datei zu entpacken, geben Sie Folgendes aus einer Terminal-Befehlszeile ein.</p> <pre>tar -xvf VMware-NSX-Intelligence-appliance-1.0.0.0.14303803.tar</pre>

Bei Verwendung des beispielhaften Paketdateinamens aus dem vorherigen Schritt enthalten die entpackten Inhalte die folgenden Dateien:

- nsx-intelligence-appliance-1.0.0.0.14303803.cert
- nsx-intelligence-appliance-1.0.0.0.14303803.mf
- nsx-intelligence-appliance-1.0.0.0.14303803.ovf
- nsx-intelligence-appliance.vmdk

- b Bevor Sie mit der Installation fortfahren, stellen Sie sicher, dass die Prüfsummen der entpackten Dateien mit den Angaben in der Manifestdatei übereinstimmen.

### 4 Verwenden Sie die folgenden Informationen, um zu überprüfen, ob der verwendete Webserver für jeden NSX Intelligence-Installationsdateityp für den MIME-Typ eingerichtet ist. Aktualisieren Sie bei Bedarf Ihren Webserver manuell.

NSX Intelligence-Installationsdateityp	MIME-Typ
.ovf	application/vmware
.vmdk	application/octet-stream
.mf	text/cache-manifest
.cert	application/x-x509-user-cert

- 5 Kopieren Sie den Dateipfad der NSX IntelligenceOVF-Datei. Beispielsweise `http://local-web-server/nsx-intelligence-appliance-1.0.0.0.14303803.ovf`. Diesen Pfad geben Sie während der Installation der NSX Intelligence-Appliance an.

### Nächste Schritte

Setzen Sie die Installation der NSX Intelligence-Appliance fort. Siehe [Installieren der NSX Intelligence-Appliance](#).

## Installieren der NSX Intelligence-Appliance

Sie verwenden die Benutzeroberfläche von NSX Manager, um die NSX Intelligence-Appliance zu installieren und zu konfigurieren.

Bevor Sie mit der Verwendung der NSX Intelligence-Funktionen beginnen können, müssen Sie die NSX Intelligence-Appliance installieren und konfigurieren, um die NSX Intelligence-Dienste und -Plug-ins mit NSX Manager zu integrieren.

### Voraussetzungen

- Stellen Sie sicher, dass NSX-T Data Center 2.5 oder später installiert ist. Siehe [Kapitel 2 Workflows für die Installation von NSX-T Data Center](#).
- Sie müssen über eine Enterprise-Administratorrolle verfügen, um NSX Intelligence installieren, konfigurieren und verwenden zu können.
- Suchen Sie im VMware-Download-Portal die NSX Intelligence-Installationspaketdatei und laden Sie sie auf einen lokalen Webserver herunter. Siehe [Herunterladen und Entpacken des NSX Intelligence-Installationspakets](#).
- Stellen Sie sicher, dass der lokale Webserver, der die NSX Intelligence-Installationspaketdatei enthält, den Standard-Port 80 für HTTP verwendet.
- Bestimmen Sie die Größe der zu konfigurierenden NSX Intelligence-Appliance. Eine kleine Appliance eignet sich für Labor- oder Proof-of-Concept-Bereitstellungen bzw. kleine Produktionsumgebungen. Eine große Appliance eignet sich für eine große Produktionsumgebung.
- Stellen Sie sicher, dass die NSX Intelligence-Systemanforderungen für die zu installierende Appliance-Größe erfüllt sind. Siehe [Systemanforderungen für NSX Intelligence](#).
- Synchronisieren Sie die Uhrzeit auf dem Computing-Cluster, auf dem die NSX Intelligence-Appliance bereitgestellt werden soll, mit dem NSX Manager-Server.
- Rufen Sie die IP-Adressen für das Verwaltungssubnetz, das Gateway, den DNS-Server und den NTP-Server ab, die zum Konfigurieren der NSX Intelligence -Appliance erforderlich sind.

### Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://<nsx-manager-ip-address>` mit Unternehmensadministratorrechten bei einem NSX Manager an.

- 2 In NSX Manager wählen Sie **System > Appliances** aus.
- 3 Scrollen Sie im Übersichtsbereich der Appliances nach unten, um die NSX Intelligence-Appliance-Karte zu suchen, und klicken Sie auf **NSX Intelligence-Appliance hinzufügen**.
- 4 Geben Sie im Assistenten „Appliance hinzufügen“ die Details der NSX Intelligence-Appliance ein.

Detail	Zu ergreifende Maßnahme
<b>OVF-Datei</b>	Geben Sie die URL für die auf Ihren lokalen Webserver heruntergeladene NSX Intelligence-OVF-Datei ein. Beispiel: <code>http://localhost/nsx-intelligence-appliance-1.1.0.0.13912394.ovf</code> .
<b>Name</b>	Geben Sie einen Namen für die NSX Intelligence-Appliance ein. Dieser Wert kann ein vollqualifizierter Domänenname oder ein einfacher Name sein, z. B. <b>mytest-lab</b> .
<b>Verwaltungs-Subnetz</b>	Geben Sie die für die NSX Intelligence-Appliance zu verwendende IP-Adresse einschließlich des Bereichs ein. Beispiel: <code>10.11.22.33/24</code>
<b>Gateway-IP</b>	Geben Sie eine Gateway-IP-Adresse für die zu verwendende NSX Intelligence-Appliance ein.
<b>DNS-Server</b>	Geben Sie mindestens eine IP-Adresse für einen DNS-Server ein.
<b>NTP-Server</b>	Geben Sie mindestens eine IP-Adresse für einen NTP-Server ein.
<b>Knotengröße</b>	Wählen Sie die zu konfigurierende NSX Intelligence-Appliance-Größe aus. Eine kleine Appliance eignet sich für Labor- oder Proof-of-Concept-Umgebungen bzw. kleine Produktionsumgebungen. Eine große Appliance-Größe eignet sich für eine große Produktionsumgebung.

- 5 Klicken Sie auf **Weiter**.
- 6 Geben Sie die Details für die Bereitstellung der NSX Intelligence-Appliance ein.

Detail	Zu ergreifende Maßnahme
<b>Compute Manager</b>	Wählen Sie im Dropdown-Menü den Compute Manager aus, auf dem die NSX Intelligence-Appliance installiert werden soll.
<b>Cluster</b>	Wählen Sie mithilfe des Dropdown-Menü aus, welcher Cluster verwendet werden soll.
<b>Ressourcenpool</b>	(Optional) Wählen Sie im Dropdown-Menü den Ressourcenpool aus.
<b>Host</b>	<p>(Optional) Wählen Sie im Dropdown-Menü den Host aus. Wenn Sie einen Cluster mit mehreren Transportknoten verwenden, entscheiden Sie, welcher Transportknoten verwendet werden soll.</p> <p><b>Hinweis</b> Durch die explizite Auswahl eines Hosts wird die vCPU-Anzahlprüfung überschrieben. Stellen Sie sicher, dass der ausgewählte Host über genügend vCPU-Anzahl für die Größe der NSX Intelligence-Appliance verfügt, die Sie installieren. Wenn dies nicht der Fall ist, weist die resultierende NSX Intelligence-Appliance möglicherweise eine falsche Konfiguration auf. Wenn Sie sich nicht sicher sind, lassen Sie das Textfeld leer. Dann wird der entsprechende Host automatisch ausgewählt.</p>

Detail	Zu ergreifende Maßnahme
<b>Datenspeicher</b>	Wählen Sie im Dropdown-Menü den Datenspeicher aus, in dem die NSX Intelligence-Konfiguration und die Daten gespeichert werden sollen.
<b>Netzwerk</b>	Wählen Sie im Dropdown-Menü das zu verwendende Netzwerk aus.
<b>SSH aktivieren und Root-Zugriff aktivieren</b>	<p>Geben Sie an, ob Sie einen SSH-Zugriff oder einen Root-Zugriff auf die Befehlszeilenschnittstelle (CLI) der NSX Intelligence-Appliance aktivieren möchten.</p> <p>Standardmäßig sind diese Optionen aus Sicherheitsgründen deaktiviert. Sie verwenden die CLI, um einen Sicherungsdateiserver zu konfigurieren, die Konfiguration der NSX Intelligence-Appliance zu sichern und die Sicherung wiederherzustellen.</p>

7 Klicken Sie auf **Weiter**.

8 Konfigurieren Sie die Admin-Anmeldedaten und den Zugriff auf die NSX Intelligence-Appliance.

- Wenn Sie einen Root-Zugriff aktiviert haben, legen Sie das Root-Kennwort fest. Verwenden Sie die in der Benutzeroberfläche angezeigten Kennwortanforderungen.
- Konfigurieren Sie die CLI-Anmeldedaten und die Audit-CLI-Anmeldedaten. Wählen Sie **Identisch mit Root-Kennwort** aus, wenn Sie das Root-Kennwort als CLI-Kennwort oder Audit-CLI-Kennwort verwenden möchten. Geben Sie andernfalls die Kennwörter ein, die Sie als **CLI-Kennwort** und **Audit-CLI-Kennwort** verwenden möchten.

9 Klicken Sie auf **Appliance installieren**.

Der Fortschritt der Installation wird auf der Registerkarte **Planen und Fehler beheben** angezeigt. Die Installation kann zwischen 5 und 30 Minuten dauern, während das Installationsprogramm alle Dienste und Plug-ins erkennt, die von der NSX Intelligence-Appliance benötigt werden.

---

**Hinweis** Wenn ein Fehler gemeldet wird, verwenden Sie die in den Fehlermeldungen angegebenen Informationen, um das gemeldete Problem zu beheben. Nachdem das Problem behoben wurde, müssen Sie zuerst die NSX Intelligence-Appliance deinstallieren und versuchen, sie über die Registerkarte **System > Appliances** erneut zu installieren. Unter [Deinstallieren der NSX Intelligence-Appliance](#) oder auch [Fehlerbehebung bei der Installation der NSX Intelligence-Appliance](#) finden Sie mögliche Hinweise zur Behebung möglicherweise aufgetretener Probleme.

---

10 Nachdem die NSX Intelligence-Appliance erfolgreich installiert wurde, klicken Sie auf **Zum Anzeigen aktualisieren**.

Die NSX Manager-Benutzeroberfläche wird mit aktivierten NSX Intelligence-Funktionen auf der Registerkarte **Planen und Fehler beheben > Erkennen und planen** aktualisiert.

## Nächste Schritte

Beginnen Sie mit der Verwendung der NSX Intelligence-Funktionen. Siehe „Verwenden von NSX Intelligence“ im *Administratorhandbuch für NSX-T Data Center*.

## Fehlerbehebung bei der Installation der NSX Intelligence-Appliance

Dieser Abschnitt enthält Informationen zur Behebung von Problemen, die bei der Installation der NSX Intelligence-Appliance auftreten können.

### Die Anmeldedaten waren falsch oder das angegebene Konto wurde gesperrt

Der Versuch, die NSX Intelligence-Appliance bereitzustellen, führte zu der Fehlermeldung Die Anmeldedaten waren falsch oder das angegebene Konto wurde gesperrt.

#### Problem

Nachdem das Installationsprogramm für die NSX Intelligence-Appliance ausgeführt wurde, wird die Fehlermeldung Die Anmeldedaten waren falsch oder das angegebene Konto wurde gesperrt angezeigt, wenn das Installationsprogramm versucht, den NSX Intelligence-Server bei NSX Manager zu registrieren

#### Ursache

Der Registrierungsschritt ist möglicherweise aus einem der folgenden Gründe fehlgeschlagen.

- Das Management Plane-Token ist möglicherweise abgelaufen. Das Token ist nur 30 Minuten lang gültig.
- Die Systemzeit wird nicht zwischen dem NSX Intelligence-Server-Host und dem NSX Manager-Host synchronisiert.

#### Lösung

- 1 Stellen Sie sicher, dass die Systemzeit zwischen dem NSX Intelligence-Server-Host und dem NSX Manager-Host synchronisiert wird.
- 2 Wenn die Systemzeiten synchronisiert werden, überprüfen Sie, ob eine Netzwerklatenz vorhanden ist.
- 3 Entfernen Sie die NSX Intelligence-Appliance und wiederholen Sie die Installation, nachdem Sie die Systemzeiten synchronisiert haben oder wenn die Netzwerklatenz behoben ist.

### Status „Fehlgeschlagen“ für die Appliance-Bereitstellung wird nicht gelöscht

Die NSX Intelligence-Appliance wurde erfolgreich bereitgestellt, der Status Appliance-Bereitstellung fehlgeschlagen wird jedoch weiterhin angezeigt.

### Problem

Der erste Versuch, die NSX Intelligence-Appliance bereitzustellen, schlägt fehl, z. B. aufgrund von unzureichenden Ressourcen. Danach wird das gemeldete Problem behoben, die Statusmeldung über die fehlgeschlagene Bereitstellung wird jedoch nicht gelöscht.

### Ursache

Die NSX Intelligence-Appliance erkennt nicht, dass die zugrunde liegende Hauptursache des Bereitstellungsproblems behoben wurde, da die Problembehebung außerhalb der NSX Intelligence-Appliance vorgenommen wurde.

### Lösung

- 1 Nachdem Sie das während des früheren Versuchs zur Bereitstellung der Appliance gemeldete Problem behoben haben, deinstallieren Sie die NSX Intelligence-Appliance.
- 2 Versuchen Sie, die NSX Intelligence-Appliance über die Registerkarte **System > Appliances** neu zu installieren.
- 3 (Optional) Um den neuen Bereitstellungsstatus der NSX Intelligence-Appliance zu erhalten, aktualisieren Sie Ihren Webbrowser.

## Deinstallieren der NSX Intelligence-Appliance

Wenn Sie NSX Intelligence vollständig deinstallieren möchten, führen Sie die folgenden Schritte aus.

### Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://<nsx-manager-ip-address>` mit Enterprise-Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie in der NSX Manager-Benutzeroberfläche **System > Appliances** aus.
- 3 Suchen Sie die NSX Intelligence-Appliance-Karte.
- 4 Klicken Sie auf **Löschen**.
- 5 Klicken Sie im Dialogfeld „Löschen der Appliance bestätigen“ auf **Bestätigen**.



# Beheben von Installationsproblemen

# 15

Eine Auflistung von Problemen bezüglich der Installation und Konfiguration von NSX-T Data Center

Problem	Lösung
vCenter Server- und/oder ESXi-Hosts zeigen nach dem Entfernen von NSX-T vom Host oder Cluster verdeckte Netzwerke an	<a href="https://ikb.vmware.com/s/article/75234">https://ikb.vmware.com/s/article/75234</a>
Die Installation schlägt aufgrund unzureichenden Speicherplatzes in Bootbank auf dem ESXi-Host fehl	<a href="https://kb.vmware.com/s/article/74864">https://kb.vmware.com/s/article/74864</a>

Dieses Kapitel enthält die folgenden Themen:

- [Die Installation schlägt aufgrund unzureichenden Speicherplatzes in Bootbank auf dem ESXi-Host fehl](#)

## Die Installation schlägt aufgrund unzureichenden Speicherplatzes in Bootbank auf dem ESXi-Host fehl

Die NSX-T Data Center-Installation schlägt möglicherweise fehl, wenn nicht genügend Speicherplatz in der Bootbank oder in der alt-Bootbank auf einem ESXi-Host vorhanden ist.

### Problem

Auf dem ESXi-Host wird möglicherweise eine ähnliche Protokollmeldung (`esxupdate.log`) angezeigt:

```
20**_**_**T13:37:50Z esxupdate: 5557508: BootBankInstaller.pyc:
ERROR: The pending transaction requires 245 MB free space,
however the maximum supported size is 239 MB.^@
```

### Ursache

Nicht verwendete VIBs auf dem ESXi-Host können relativ groß sein. Diese nicht verwendeten VIBs können bei der Installation der erforderlichen VIBs zu unzureichendem Speicherplatz in der Bootbank oder in der alt-Bootbank führen.

## Lösung

- Deinstallieren Sie die VIBs, die nicht mehr benötigt werden, und geben Sie zusätzlichen Festplattenspeicher frei.

Weitere Informationen zum Löschen nicht verwendeter VIBs finden Sie im VMware Knowledgebase-Artikel unter <https://kb.vmware.com/s/article/74864>.