

# Administratorhandbuch für NSX-T Data Center

Geändert am 19. MÄRZ 2021  
VMware NSX-T Data Center 2.4

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

Grundlegende Informationen zur Verwaltung von VMware NSX-T Data Center  
11

## 1 Übersicht über NSX Manager 12

## 2 Tier-0-Gateways 16

- Hinzufügen eines Tier-0-Gateways 16
- Erstellen einer IP-Präfix-Liste 18
- Erstellen einer Community-Liste 20
- Konfigurieren einer statischen Route 20
- Erstellen einer Route Map 21
- Konfigurieren des BGP-Protokolls 23

## 3 Tier-1-Gateway 26

- Tier-1-Gateway hinzufügen 26

## 4 Segmente 29

- Segmentprofile 29
  - Grundlegendes zum QoS-Segmentprofil 30
  - Grundlegendes zum Segmentprofil für die IP Discovery 33
  - Grundlegendes zum Spoofguard-Segmentprofil 35
  - Grundlegendes zu Segmentprofilen für die Segmentsicherheit 37
  - Grundlegendes zum Segmentprofil für die MAC Discovery 39
- Hinzufügen eines Segments 41

## 5 Virtual Private Network (VPN) 43

- Grundlegendes zu IPSec-VPNs 44
  - Verwendung von richtlinienbasiertem IPSec-VPN 45
  - Verwenden von routenbasiertem IPSec-VPN 45
- Grundlegendes zu Layer 2-VPN 47
- Hinzufügen von VPN-Diensten 48
  - Hinzufügen eines IPSec-VPN-Dienstes 50
  - Hinzufügen eines L2-VPN-Diensts 52
- Hinzufügen von IPSec-VPN-Sitzungen 55
  - Hinzufügen einer richtlinienbasierten IPSec-Sitzung 55
  - Hinzufügen einer routenbasierten IPSec-Sitzung 59
- Hinzufügen von L2-VPN-Sitzungen 62
  - Hinzufügen einer L2-VPN-Server-Sitzung 63

Hinzufügen einer L2-VPN-Clientsitzung	65
Herunterladen der L2-VPN-Konfiguration der Remote-Site	67
Hinzufügen von lokalen Endpoints	68
Hinzufügen von Profilen	69
Hinzufügen von IKE-Profilen	69
Hinzufügen von IPSec-Profilen	72
Hinzufügen von DPD-Profilen	74
Überprüfen des realisierten Zustands einer IPSec-VPN-Sitzung	75
Überwachung und Fehlerbehebung von VPN-Sitzungen	78
<b>6 Netzwerkadressübersetzung (NAT)</b>	<b>80</b>
Konfigurieren von NAT auf einem Gateway	80
<b>7 Lastausgleich</b>	<b>82</b>
Wichtige Load Balancer-Konzepte	83
Skalieren von Load Balancer-Ressourcen	83
Unterstützte Load Balancer-Funktionen	84
Load Balancer-Topologien	85
Einrichten von Load Balancer-Komponenten	87
Hinzufügen von Load Balancers	88
Hinzufügen einer aktiven Überwachung	89
Hinzufügen einer passiven Überwachung	93
Hinzufügen eines Serverpools	95
Einrichten von Komponenten des virtuellen Servers	100
<b>8 Weiterleitungsrichtlinien</b>	<b>125</b>
Hinzufügen oder Bearbeiten von Weiterleitungsrichtlinien	126
<b>9 IP-Adressverwaltung (IPAM)</b>	<b>128</b>
Hinzufügen einer DNS-Zone	128
Hinzufügen eines DNS-Weiterleitungsdiensts	129
Hinzufügen eines DHCP-Servers	130
Konfigurieren eines DHCP-Relay-Servers für ein Tier-0- oder Tier-1-Gateway	131
Hinzufügen eines IP-Adressenpools	132
Hinzufügen eines IP-Adressblocks	133
<b>10 Sicherheit</b>	<b>134</b>
Überblick über die Sicherheitskonfiguration	134
Sicherheit – Terminologie	135
Identitätsbasierte Firewall	135
Workflow für die identitätsbasierte Firewall	137

Kontextprofil der Schicht 7	139
Layer 7-Workflow für Regeln für verteilte Firewall	140
Anwendungsidentifikations-GUIDs	141
Verteilte Firewall	146
Hinzufügen einer verteilten Firewall	146
Hinzufügen einer Firewallregel für die Aufnahme von FQDN/URLs in die Whitelist	150
Protokolle des verteilten Firewallpakets	152
Auswählen einer Standard-Konnektivitätsstrategie	154
Konfigurieren einer Gateway-Firewall	155
Hinzufügen von Regeln und Richtlinien für eine Gateway-Firewall	155
Konfigurieren der Netzwerk-Introspektion (Ost-West)	159
Allgemeine Aufgaben für die Ost-West-Netzwerksicherheit	159
Wichtige Konzepte des Netzwerkschutzes (Ost-West)	159
Bereitstellen eines Diensts für die Selbstprüfung von Ost-West-Datenverkehr	160
Hinzufügen eines Dienstprofils	162
Hinzufügen einer Dienstkette	162
Hinzufügen von Umleitungsregeln für Ost-West-Datenverkehr	164
Konfigurieren der Netzwerk-Introspektion (Nord-Süd)	166
Allgemeine Aufgaben für die Nord-Süd-Netzwerksicherheit	166
Bereitstellen eines Diensts für die Selbstprüfung von Nord-Süd-Datenverkehr	166
Konfigurieren der Umleitung des Datenverkehrs	168
Hinzufügen von Umleitungsregeln für Nord-Süd-Datenverkehr	170
Überwachung der Umleitung des Datenverkehrs	171
Konfigurieren von Endpoint-Schutz	172
Grundlegendes zum Endpoint-Schutz	172
Workflow für Endpoint-Schutz	180
Hinzufügen von Domänen und VM-Gruppen	197

## 11 Bestand 211

Hinzufügen einer Domäne	211
Hinzufügen eines Diensts	212
Hinzufügen einer Gruppe	213
Hinzufügen eines Kontextprofils	214

## 12 Überwachung 216

Hinzufügen eines Firewall-IPFIX-Profiles	216
Hinzufügen eines Switch-IPFIX-Profiles	217
Hinzufügen eines IPFIX-Collectors	218
Hinzufügen eines Port-Mirroring-Profiles	218
Erweiterte Überwachungstools	219
Anzeigen der Portverbindungsinformationen	219

Traceflow	220
Überwachen von Port-Mirroring-Sitzungen	223
Konfigurieren von Filtern für eine Port-Mirroring-Sitzung	226
Konfigurieren von IPFIX	228
Überwachen einer Logischer Switch Port-Aktivität	398
Überwachen von Fabric-Knoten	398

## 13 Logische Switches 400

Grundlegendes zu den BUM-Frame-Replizierungsmodi	401
Erstellen eines logischen Switches	403
Verbinden einer VM mit einem logischen Switch	404
Anfügen einer auf vCenter Server gehosteten VM an einen logischen NSX-T Data Center-Switch	405
Verknüpfen einer auf eigenständigem ESXi gehosteten VM mit einem logischen NSX-T Data Center-Switch	406
Anfügen einer auf KVM-Hosts gehosteten VM an einen logischen NSX-T Data Center-Switch	412
Erstellen eines logischen Switch Ports	413
Testen der Schicht-2-Konnektivität	414
Erstellen eines logischen VLAN-Switch für den NSX Edge-Uplink	417
Switching-Profil für logische Switches und logische Ports	419
Grundlegendes zum QoS-Switching-Profil	421
Grundlegendes zum Switching-Profil für Port-Mirroring	424
Grundlegendes zum Switching-Profil für die IP Discovery	427
Grundlegendes zu SpoofGuard	429
Grundlegendes zum Switching-Profil für die Switch-Sicherheit	432
Grundlegendes zum Switching-Profil für die MAC-Verwaltung	434
Zuordnen eines benutzerdefinierten Profils zu einem logischen Switch	436
Zuordnen eines benutzerdefinierten Profils zu einem logischen Port	437
Schicht 2-Bridging	438
Erstellen eines ESXi-Bridge-Clusters	439
Erstellen eines Edge-Bridge-Profiles	440
Konfigurieren von Edge-basiertem Bridging	440
Erstellen eines Bridge-gestützten logischen Schicht-2-Switches	443

## 14 Logische Router 446

Logischer Tier-1-Router	446
Erstellen eines logischen Tier-1-Routers	448
Hinzufügen eines Downlink-Ports auf einem logischen Tier-1-Router	450
Hinzufügen eines VLAN-Ports auf einem logischen Tier-0- oder Tier-1-Router	451
Konfigurieren von Routen-Advertisement auf einem logischen Tier-1 Router	451
Konfigurieren einer statischen Route auf einem logischen Tier-1-Router	453

Erstellen eines eigenständigen logischen Tier-1-Routers	455
Logischer Tier-0 Router	457
Erstellen eines logischen Tier-0-Routers	458
Anfügen von Tier-0 und Tier-1	460
Verbinden eines logischen Tier-0 Routers mit einem logischen VLAN-Switch für den NSX Edge-Uplink	462
Hinzufügen eines Loopback-Router-Ports	466
Hinzufügen eines VLAN-Ports auf einem logischen Tier-0- oder Tier-1-Router	466
Konfigurieren einer statischen Route	467
BGP-Konfigurationsoptionen	471
Konfigurieren von BFD auf einem logischen Tier-0 Router	479
Aktivieren von Route Redistribution auf dem logischen Tier-0 Router	479
Grundlegendes zum ECMP-Routing	483
Erstellen einer IP-Präfix-Liste	487
Erstellen einer Community-Liste	488
Erstellen einer Route Map	489
Konfigurieren des Timers für die Weiterleitung der Aktiv-Benachrichtigung	490
<b>15 Erweitertes NAT</b>	<b>492</b>
Netzwerkadressübersetzung (NAT)	492
Tier-1-NAT	493
Tier-0-NAT	500
Reflexive NAT	501
<b>16 Erweiterte Gruppierungsobjekte</b>	<b>505</b>
Erstellen eines IP Sets	505
Erstellen eines IP-Pools	506
Erstellen eines MAC Set	506
Erstellen einer NS-Gruppe	507
Konfigurieren von Diensten und Dienstgruppen	509
Erstellen eines NS-Dienstes	510
Verwalten von Tags für eine virtuelle Maschine	510
<b>17 Erweitertes DHCP</b>	<b>512</b>
DHCP	512
Erstellen eines DHCP-Serverprofils	513
Erstellen eines DHCP-Servers	513
Anfügen eines DHCP-Servers an einen logischen Switch	514
Trennen eines DHCP-Servers von einem logischen Switch	514
Erstellen eines DHCP-Relay-Profils	515
Erstellen eines DHCP-Relay-Dienstes	515
Hinzufügen eines DHCP-Relay-Dienstes zu einem Port für einen logischen Router	515

Löschen einer DHCP-Lease	516
Metadaten-Proxyserver	516
Hinzufügen eines Metadaten-Proxyservers	517
Anfügen eines Metadaten-Proxyserver an einen logischen Switch	518
Trennen eines Metadaten-Proxy-Servers von einem logischen Switch	518
<b>18</b> Erweiterte IP-Adressverwaltung	520
Verwalten von IP-Blöcken	520
Verwalten von Subnetzen für IP-Blöcke	521
<b>19</b> Erweitertes Load Balancing	522
Wichtige Load Balancer-Konzepte	523
Konfigurieren von Load Balancer-Komponenten	524
Erstellen eines Load Balancers	524
Konfigurieren einer aktiven Systemzustandsüberwachung	526
Konfigurieren von passiven Systemzustandsüberwachungen	530
Hinzufügen eines Serverpools für das Load Balancing	531
Konfigurieren der Komponenten des virtuellen Servers	535
<b>20</b> Erweiterte Firewall	560
Firewallabschnitte und Firewallregeln	560
Hinzufügen eines Firewallregelabschnitts	561
Löschen eines Firewallregelabschnitts	562
Aktivieren und Deaktivieren von Abschnittsregeln	562
Aktivieren und Deaktivieren von Abschnittsprotokollen	563
Informationen über Firewallregeln	563
Hinzufügen einer Firewallregel	565
Löschen einer Firewallregel	568
Bearbeiten der standardmäßigen Regel für die verteilte Firewall	568
Ändern der Reihenfolge von Firewallregeln	569
Filtern der Firewallregeln	570
Konfigurieren der Firewall für den Bridge-Port eines logischen Switches	570
Konfigurieren einer Firewall-Ausschlussliste	571
Aktivieren und Deaktivieren einer verteilten Firewall	571
Hinzufügen oder Löschen einer Firewallregel zu bzw. von einem logischen Router	571
CPU- und Arbeitsspeicher-Nutzungsschwellenwert mithilfe der API	572
<b>21</b> Vorgänge und Verwaltung	577
Überprüfen des Umsetzungsstatus einer Konfigurationsänderung	578
Suchen nach Objekten	581
Hinzufügen eines Compute Managers	582



Hinzufügen von Active Directory	584
Hinzufügen eines LDAP-Servers	585
Synchronisieren von Active Directory	586
Verwalten von Benutzerkonten und der rollenbasierten Zugriffssteuerung	587
Verwalten eines Benutzerkennworts	587
Zurücksetzen der Kennwörter einer Appliance	588
Authentifizierungsrichtlinien-Einstellungen	592
Abrufen des Certificate Thumbprint von einem vIDM-Host	592
Konfigurieren der Integration von VMware Identity Manager	593
Zeitsynchronisierung zwischen NSX Manager, vIDM und zugehörigen Komponenten	595
Rollenbasierte Zugriffssteuerung	597
Hinzufügen einer Rollenzuweisung oder Prinzipalidentität	604
Sichern und Wiederherstellen von NSX Manager	606
Konfigurieren von Sicherungen	607
Entfernen alter Sicherungen	608
Auflisten der verfügbaren Sicherungen	609
Wiederherstellen einer Sicherung	610
Entfernen der NSX-T Data Center-Erweiterung aus vCenter Server	613
Verwalten des NSX Manager-Clusters	614
Anzeigen der Konfiguration und des Status des NSX Manager-Clusters	614
Neustarten eines NSX Manager	617
Ändern der IP-Adresse eines NSX Manager	617
Ändern der Größe eines NSX Manager-Knotens	619
Bereitstellung von NSX-T Data Center für mehrere Sites	620
Konfigurieren von Appliances	624
Hinzufügen eines Lizenzschlüssels und Generieren eines Lizenznutzungsberichts	625
Einrichten von Zertifikaten	626
Importieren eines Zertifikats	626
Erstellen einer Datei für die Zertifikatsignieranforderung	627
Importieren eines CA-Zertifikats	629
Erstellen eines selbstsignierten Zertifikats	629
Ersetzen des Zertifikats für einen NSX Manager-Knoten oder eine virtuelle NSX Manager-Cluster-IP	630
Importieren einer Zertifikatswiderrufsliste	631
Konfigurieren von NSX Manager zum Abrufen einer Zertifikatswiderrufsliste	632
Importieren eines Zertifikats für eine CSR	633
Speichern von öffentlichen Zertifikaten und privaten Schlüsseln	633
Erfassen von Support-Paketen	633
Protokollmeldungen	635
Konfigurieren der Remoteprotokollierung	636
Protokollmeldungs-IDs	638
Programm zur Verbesserung der Benutzerfreundlichkeit	639

- Bearbeiten der CEIP-Konfiguration (Einstellungen bzgl. der Teilnahme am „Programm zur Verbesserung der Benutzerfreundlichkeit“) 640
- Hinzufügen von Tags zu einem Objekt 640
- Suchen nach dem SSH-Fingerabdruck eines Remote-Servers 641
- Anzeigen von Daten über Anwendungen, die auf virtuellen Maschinen ausgeführt werden 642

## **22 Verwenden von NSX Cloud 643**

- Der Cloud Service Manager 643
  - Clouds 644
  - System 646
- Verwalten der Quarantäne-Richtlinie 649
  - Quarantäne-Richtlinie aktivieren oder deaktivieren 649
  - Quarantäne-Richtlinie-Auswirkungen bei Deaktivierung 651
  - Quarantäne-Richtlinie-Auswirkungen bei Aktivierung 653
  - NSX Cloud-Sicherheitsgruppen für die Public Cloud 654
- Überblick über Onboarding und Verwaltung von Workload-VMs 655
  - Onboarding und Verwaltung von Arbeitslast-VMs 656
- Onboarden von Workload-VMs 657
  - Unterstützte Betriebssysteme 657
  - Taggen von virtuellen Maschinen in der Public Cloud 657
  - Installieren von NSX Agent 658
  - Automatische Installation von NSX Agent 661
- Verwalten von Workload-VMs 662
  - DFW-Regeln für NSX-verwaltete Arbeitslast-VMs 663
  - Gruppen-VMs mit NSX-T Data Center und Public-Cloud-Tags 663
  - Einrichten von Mikro-Segmentierung für Workload-VMs 667
  - Verwendung von NSX-T Data Center-Funktionen mit der Public Cloud 667
- Verwenden von erweiterten NSX Cloud-Funktionen 669
  - Überprüfen von NSX Cloud-Komponenten 670
  - Aktivieren von NAT auf NSX-verwalteten VMs 670
  - Erzeugen replizierbarer Images 671
  - Diensteinfügung für Ihre Public Cloud 672
  - Aktivieren von Syslog-Weiterleitung 679
- FAQ 679
  - Ich habe meine VM korrekt gekennzeichnet und den Agenten installiert, aber meine VM steht unter Quarantäne. Was soll ich tun? 679
  - Was soll ich tun, wenn ich nicht auf meine Arbeitslast-VM zugreifen kann? 680

# Grundlegende Informationen zur Verwaltung von VMware NSX-T Data Center

Im *Administratorhandbuch für NSX-T Data Center* erhalten Sie Informationen zum Konfigurieren und Verwalten der Netzwerke für VMware NSX-T™ Data Center. Dabei wird unter anderem behandelt, wie Sie logische Switches und Ports erstellen und wie Sie Netzwerke für logische Router mit Ebenen einrichten, wie Sie NAT, Firewalls, SpoofGuard, die Gruppierung und DHCP einrichten. Außerdem wird beschrieben, wie Sie NSX Cloud konfigurieren.

## Zielgruppe

Die vorliegenden Informationen richten sich an Benutzer, die NSX-T Data Center konfigurieren möchten. Die Informationen sind für erfahrene Windows- oder Linux-Systemadministratoren bestimmt, die mit VM-Technologie, Netzwerken und Sicherheitsoperationen vertraut sind.

## VMware Technical Publications – 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 Manager

# 1

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 Richtlinienschnittstelle: 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

Verwendenden 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>■ Layer 3-Weiterleitung für IPv4 und IPv6</li> <li>■ Timer für die Weiterleitung der Aktiv-Benachrichtigung</li> <li>■ Ändern der IP des internen Transitnetzwerks</li> <li>■ Unterstützung von VIP HA auf Tier-0</li> <li>■ Standby-Verlagerung</li> <li>■ Routen-Advertisement basierend auf der Auswahl der Tier-1-Präfixe</li> <li>■ Loopback-Erstellung</li> <li>■ BGP-Multihop</li> <li>■ BGP-Quelladressen</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 Dienstregele</li> </ul> </li> </ul>	<p>Sicherheitsfunktionen, die nur in der erweiterten Schnittstelle verfügbar sind:</p> <ul style="list-style-type: none"> <li>■ Möglichkeit zur Aktivierung oder Deaktivierung der verteilten Firewall, identitätsbasierten Firewall und Gateway-Firewall</li> <li>■ Sitzungs-Timer für verteilte Firewall</li> <li>■ Ausschlusslisten</li> <li>■ Schwellenwerte von CPU und Arbeitsspeicher</li> <li>■ Abschnitte für statusfreie Regeln</li> <li>■ Bridge-Firewall</li> <li>■ Abschnittssperrung</li> <li>■ Regel-IDs für verteilte Firewalls</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 Richtlinienchnittstellen und erweiterten Schnittstellen finden

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

Tabelle 1-2. 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 /policy/api beginnen	API-URLs, die mit /api 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

Tabelle 1-3. Objektnamen (Fortsetzung)

Mit der Richtlinienchnittstelle erstellte Objekte	Mit der erweiterten Schnittstelle erstellte Objekte
Sicherheitsrichtlinie	Firewallabschnitt
Regel	Firewallregel
Gateway-Firewall	Edge-Firewall

# Tier-O-Gateways

# 2

Ein Tier-O Gateway führt die Funktionen eines logischen Tier-O Routers aus. Es verarbeitet Datenverkehr zwischen den logischen und physischen Netzwerken.

---

**NSX Cloud-Hinweis** Wenn Sie NSX Cloud verwenden, finden Sie unter [Verwendung von NSX-T Data Center-Funktionen mit der Public Cloud](#) eine Liste der automatisch generierten logischen Einheiten, unterstützten Funktionen und Konfigurationen, die für NSX Cloud erforderlich sind.

---

Ein Edge-Knoten kann nur ein Tier-O-Gateway oder einen logischen Router unterstützen. Wenn Sie ein Tier-O-Gateway oder einen logischen Router erstellen, stellen Sie sicher, dass Sie nicht mehr Tier-O-Gateways oder logische Router als die Anzahl der Edge-Knoten im NSX Edge-Cluster anlegen.

---

**Hinweis** Der Begriff „Logischer Tier-O Router“ wird auf der Registerkarte **Netzwerk und Sicherheit – Erweitert** verwendet, um auf ein Tier-O-Gateway zu verweisen.

---

Dieses Kapitel enthält die folgenden Themen:

- [Hinzufügen eines Tier-O-Gateways](#)
- [Erstellen einer IP-Präfix-Liste](#)
- [Erstellen einer Community-Liste](#)
- [Konfigurieren einer statischen Route](#)
- [Erstellen einer Route Map](#)
- [Konfigurieren des BGP-Protokolls](#)

## Hinzufügen eines Tier-O-Gateways

Ein Tier-O-Gateway besitzt Downlink-Verbindungen zu Tier-1-Gateways und Uplink-Verbindungen zu physischen Netzwerken.



Sie können den Hochverfügbarkeitsmodus (HA) eines Tier-0-Gateways als „Aktiv-Aktiv“ oder „Aktiv-Standby“ konfigurieren. Die folgenden Dienste werden nur im „Aktiv-Standby“-Modus unterstützt:

- NAT
- Load Balancing
- Statusbehaftete Firewall
- VPN

Tier-0- und Tier-1-Gateways unterstützen die folgenden Adressierungskonfigurationen für alle Schnittstellen (Uplinks, Dienstports und Downlinks) sowohl in Single- als auch in Multi-Tier-Topologien:

- Nur IPv4
- Nur IPv6
- Dual-Stack – IPv4 und IPv6

Aktivieren Sie für die Verwendung von IPv6 oder der Dual-Stack-Adressierung **IPv4 und IPv6** als Layer-3-Weiterleitungsmodus unter **Netzwerk > Netzwerkeinstellungen > Globale Netzwerkkonfiguration**.

#### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk > Tier-0-Gateways**.
- 3 Klicken Sie auf **Tier-0-Gateway hinzufügen**.
- 4 Geben Sie einen Namen für das Gateway ein.
- 5 (Erforderlich) Wählen Sie einen Modus für die Hochverfügbarkeit aus.

Die Standardeinstellung lautet „Aktiv-Aktiv“. Im Aktiv/Aktiv-Modus findet für den Datenverkehr bezüglich aller Mitglieder ein Load Balancing statt. Im Aktiv/Standby-Modus wird der gesamte Datenverkehr von einem ausgewählten aktiven Mitglied abgewickelt. Wenn das aktive Mitglied ausfällt, wird ein anderes Mitglied als aktiv ausgewählt.

---

**Wichtig** Nachdem Sie das Gateway erstellt haben, kann der HA-Modus nicht geändert werden.

---

- 6 Wenn der HA-Modus Aktiv/Standby lautet, wählen Sie einen Failover-Modus aus.

Option	Beschreibung
Vorbeugend	Wenn der bevorzugte Knoten fehlschlägt und wiederhergestellt wird, hat er Vorrang vor seinem Peer und wird zum aktiven Knoten. Der Peer ändert seinen Zustand in Standby.
Nicht vorbeugend	Wenn der bevorzugte Knoten fehlschlägt und wiederhergestellt wird, erfolgt eine Überprüfung, ob der zugehörige Peer der aktive Knoten ist. Ist dies der Fall, hat der bevorzugte Knoten keinen Vorrang vor seinem Peer, und er ist der Standby-Knoten.

- 7 Wählen Sie einen NSX Edge-Cluster aus.

- 8 Klicken Sie auf **Speichern**.

- 9 Um Route Redistribution zu konfigurieren, klicken Sie auf **Route Redistribution** und **Festlegen**.

Wählen Sie mindestens eine der Quellen aus:

- Tier-0-Subnetze: **Statische Routen, NAT, Lokale IPSec-IP, DNS-Weiterleitungs-IP, Dienstschnittstellen-Subnetz, Externes Schnittstellen-Subnetz, Verbundenes Segment.**
- Angekündigte Tier-1-Subnetze: **DNS-Weiterleitungs-IP, Statische Routen, LB VIP, Verbundene Subnetze, NAT, LB SNAT.**

- 10 Um Schnittstellen zu konfigurieren, klicken Sie auf **Schnittstellen** und **Festlegen**.

- a Klicken Sie auf **Schnittstelle hinzufügen**.
- b Geben Sie einen Namen und eine IP-Adresse im CIDR-Format ein.
- c Wählen Sie ein Segment aus.
- d Wählen Sie einen NSX Edge-Knoten aus.
- e (Optional) Ändern Sie den MTU-Wert und fügen Sie Tags hinzu.

- 11 Klicken Sie auf **Routing**, um IP-Präfix-Listen, Community-Listen, statische Routen und Route Maps hinzuzufügen.

- 12 Klicken Sie auf **BGP**, um BGP zu konfigurieren.

- 13 (Optional) Klicken Sie auf **Erweiterte Konfiguration**, um zur Seite **Netzwerk und Sicherheit – Erweitert > Router** zu wechseln und zusätzliche Konfigurationen vorzunehmen.

## Erstellen einer IP-Präfix-Liste

Eine IP-Präfix-Liste enthält einzelne oder mehrere IP-Adressen, denen Zugriffsberechtigungen für Routen-Advertisement zugewiesen werden. Die IP-Adressen in dieser Liste werden nacheinander verarbeitet. Auf IP-Präfix-Listen wird mit BGP-Nachbarschaftsfiltern oder Route Maps mit ein- oder ausgehender Richtung verwiesen.

So können Sie beispielsweise der IP-Präfix-Liste die IP-Adresse 192.168.100.3/27 hinzufügen und damit verhindern, dass die Route zum vertikalen Router neu verteilt wird. Sie haben auch die Möglichkeit, eine IP-Adresse mit den Modifizierern „kleiner oder gleich“ (le) bzw. „größer oder gleich“ (ge) anzufügen, um die Route Redistribution zu ermöglichen oder zu beschränken. Beispielsweise entspricht 192.168.100.3/27 mit den Modifizierern ge 24 le 30 Subnetzmasken größer oder gleich 24 Bit oder kleiner oder gleich 30 Bit in der Länge.

---

**Hinweis** Die Standardaktion für eine Route ist **Verweigern**. Wenn Sie eine Präfixliste zum Ablehnen oder Erlauben spezifischer Routen erstellen, stellen Sie sicher, dass Sie ein IP-Präfix ohne bestimmte Netzwerkadresse erstellen (wählen Sie in der Dropdown-Liste die Option **Beliebige** aus) und die Aktion **Zulassen**, wenn Sie alle anderen Routen zulassen möchten.

---

### Voraussetzungen

Stellen Sie sicher, dass ein Tier-0-Gateway konfiguriert ist. Siehe [Erstellen eines logischen Tier-0-Routers](#).

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk > Tier-0-Gateways**.
- 3 Um ein Tier-0-Gateway zu bearbeiten, klicken Sie auf das Menüsymbol (drei Punkte) und wählen Sie **Bearbeiten**.
- 4 Klicken Sie auf **Routing**.
- 5 Klicken Sie neben **IP-Präfix-Liste** auf **Festlegen**.
- 6 Klicken Sie auf **IP-Präfix-Liste hinzufügen**.
- 7 Geben Sie einen Namen für die IP-Präfix-Liste ein.
- 8 Klicken Sie auf **Festlegen**, um IP-Präfixe hinzuzufügen.
- 9 Klicken Sie auf **Präfix hinzufügen**.
  - a Geben Sie eine IP-Adresse im CIDR-Format ein.  
Beispiel: 192.168.100.3/27.
  - b (Optional) Legen Sie einen Bereich von IP-Adressnummern in den **le**- oder **ge**-Modifizierern fest.  
Setzen Sie beispielsweise **le** auf 30 und **ge** auf 24.
  - c Wählen Sie **Verweigern** oder **Zulassen** im Dropdown-Menü aus.
  - d Klicken Sie auf **Hinzufügen**.
- 10 Wiederholen Sie den vorherigen Schritt, um zusätzliche Präfixe anzugeben.
- 11 Klicken Sie auf **Speichern**.

## Erstellen einer Community-Liste

Sie können BGP-Community-Listen erstellen, um das Konfigurieren von Routenzuordnungen anhand von Community-Listen zu ermöglichen.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk > Tier-0-Gateways**.
- 3 Um ein Tier-0-Gateway zu bearbeiten, klicken Sie auf das Menüsymbol (drei Punkte) und wählen Sie **Bearbeiten**.
- 4 Klicken Sie auf **Routing**.
- 5 Klicken Sie auf **Festlegen** neben **Community-Liste**.
- 6 Klicken Sie auf **Community-Liste hinzufügen**.
- 7 Geben Sie einen Namen für die Community-Liste ein.
- 8 Geben Sie eine Community im Format „aa:nn“ an, z. B. 300:500 und drücken Sie die Eingabetaste. Wiederholen Sie diese Schritte, wenn Sie weitere Communitys hinzufügen möchten.

Darüber hinaus können Sie eine oder mehrere der folgenden Optionen auswählen:

- NO\_EXPORT\_SUBCONFED – Keine Ankündigung für EBG-Peers.
- NO\_ADVERTISE – Keine Ankündigung für alle Peers.
- NO\_EXPORT – Keine Ankündigung außerhalb der BGP-Konföderation.

- 9 Klicken Sie auf **Speichern**.

## Konfigurieren einer statischen Route

Sie können auf dem Tier-0-Gateway eine statische Route zu externen Netzwerken konfigurieren. Nach der Konfiguration einer statischen Route müssen Sie die Route nicht von Tier-0 zu Tier-1 ankündigen, da Tier-1-Gateways automatisch über eine statische Standardroute zum verbundenen Tier-0-Gateway verfügen.

Rekursive statische Routen werden unterstützt.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk > Tier-0-Gateways**.
- 3 Um ein Tier-0-Gateway zu bearbeiten, klicken Sie auf das Menüsymbol (drei Punkte) und wählen Sie **Bearbeiten**.

- 4 Klicken Sie auf **Routing**.
- 5 Klicken Sie neben **Statische Routen** auf **Festlegen**.
- 6 Klicken Sie auf **Statische Route hinzufügen**.
- 7 Geben Sie einen Namen und eine Netzwerkadresse im CIDR-Format ein. Auf IPv6 basierende statische Routen werden unterstützt. IPv6-Präfixe können nur einen nächsten IPv6-Hop aufweisen.
- 8 Klicken Sie auf **Nächste Hops festlegen**, um Informationen über den nächsten Hop hinzuzufügen.
- 9 Klicken Sie auf **Nächsten Hop hinzufügen**.
- 10 Geben Sie eine IP-Adresse ein.
- 11 Geben Sie die administrative Distanz an.
- 12 Wählen Sie eine Schnittstelle im Dropdown-Menü aus.
- 13 Klicken Sie auf die Schaltfläche **Hinzufügen**.

#### Nächste Schritte

Prüfen Sie, ob die statische Route korrekt konfiguriert ist. Siehe [Überprüfen der statischen Route](#).

## Erstellen einer Route Map

Eine Route Map besteht aus einer Abfolge von IP-Präfix-Listen, BGP-Pfadattributen und einer zugeordneten Aktion. Der Router prüft die Abfolge auf eine Übereinstimmung mit der IP-Adresse. Ist die Übereinstimmung gegeben, führt der Router die vorgesehene Aktion aus und keine weitere Prüfung mehr durch.

Auf Route Maps kann auf der Ebene der BGP-Nachbarschaft und für die Route Redistribution verwiesen werden.

#### Voraussetzungen

- Stellen Sie sicher, dass eine IP-Präfixliste oder eine Community-Liste konfiguriert ist. Siehe [Erstellen einer IP-Präfix-Liste](#) oder [Erstellen einer Community-Liste](#).

#### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk > Tier-0-Gateways**.
- 3 Um ein Tier-0-Gateway zu bearbeiten, klicken Sie auf das Menüsymbol (drei Punkte) und wählen Sie **Bearbeiten**.
- 4 Klicken Sie auf **Routing**.
- 5 Klicken Sie auf **Festlegen** neben **Route Maps**.

- 6 Klicken Sie auf **Route Maps hinzufügen**.
- 7 Geben Sie einen Namen ein und klicken Sie auf **Festlegen**, um Übereinstimmungskriterien hinzuzufügen.
- 8 Klicken Sie auf **Übereinstimmungskriterien hinzufügen**, um mindestens ein Übereinstimmungskriterium hinzuzufügen.
- 9 Wählen Sie für jedes Kriterium **IP-Präfix** oder **Community-Liste** aus und klicken Sie auf **Festlegen**, um mindestens einen Übereinstimmungsausdruck anzugeben.
  - a Wenn Sie **Community-Liste** ausgewählt haben, geben Sie Übereinstimmungsausdrücke an, die definieren, wie Mitglieder von Community-Listen abgeglichen werden sollen. Für jede Community-Liste sind die folgenden Übereinstimmungsoptionen verfügbar:
    - **BELIEBIGE ÜBEREINSTIMMUNG** – Die festgelegte Aktion in der Route Map wird ausgeführt, wenn eine der Communitys in der Community-Liste übereinstimmt.
    - **ALLE ÜBEREINSTIMMUNGEN** – Die festgelegte Aktion in der Route Map wird ausgeführt, wenn alle Communitys in der Community-Liste unabhängig von der Reihenfolge übereinstimmen.
    - **GENAUE ÜBEREINSTIMMUNG** – Die festgelegte Aktion in der Route Map wird ausgeführt, wenn alle Communitys in der Community-Liste in derselben Reihenfolge übereinstimmen.
    - **REGEX-ÜBEREINSTIMMUNG** – Die festgelegte Aktion in der Route Map wird ausgeführt, wenn alle mit dem NRLI verbundenen Communitys mit dem regulären Ausdruck übereinstimmen.

Für jedes Übereinstimmungskriterium werden die Übereinstimmungsausdrücke in einem UND-Vorgang angewendet, was bedeutet, dass alle Übereinstimmungsausdrücke erfüllt sein müssen, damit eine Übereinstimmung vorliegt. Wenn mehrere Übereinstimmungskriterien vorhanden sind, werden sie in einem ODER-Vorgang angewendet, was bedeutet, dass eine Übereinstimmung vorliegt, wenn ein Übereinstimmungskriterium erfüllt ist.

- 10 Legen Sie BGP-Attribute fest.

BGP-Attribut	Beschreibung
AS für Pfad voranstellen	Stellen Sie einem Pfad eine oder mehrere AS-Nummern des autonomen Systems voran, um den Pfad zu verlängern und damit in der Priorität herabzustufen.
MED	Der Multi-Exit Discriminator zeigt einem externen Peer einen bevorzugten Pfad für ein autonomes System an.
Gewicht	Legen Sie eine Gewichtung für die Pfadauswahl fest. Der Bereich liegt zwischen 0 und 65535.

BGP-Attribut	Beschreibung
Community	<p>Geben Sie eine Community-Liste im Format „aa:nn“ an, z. B. 300:500. Sie können mithilfe des Dropdown-Menüs auch eine der folgenden Optionen auswählen:</p> <ul style="list-style-type: none"> <li>■ NO_EXPORT_SUBCONFED – Keine Ankündigung für EBGPeers.</li> <li>■ NO_ADVERTISE – Keine Ankündigung für alle Peers.</li> <li>■ NO_EXPORT – Keine Ankündigung außerhalb der BGP-Konföderation.</li> </ul>
Lokale Präferenz	Verwenden Sie diesen Wert, um den ausgehenden externen BGP-Pfad auszuwählen. Der Pfad mit dem höchsten Wert wird bevorzugt.

- 11** Wählen Sie in der Spalte „Aktion“ die Option **Zulassen** oder **Verweigern** aus.

Sie können IP-Adressen, die mittels IP-Präfix-Listen oder Community-Listen für die Ankündigung abgeglichen wurden, zulassen oder ablehnen.

- 12** Klicken Sie auf **Speichern**.

## Konfigurieren des BGP-Protokolls

Um den Zugriff zwischen Ihren VMs und der Außenwelt zu ermöglichen, können Sie eine externe BGP-Verbindung (eBGP) zwischen einem Tier-0-Gateway und einem Router in Ihrer physischen Infrastruktur konfigurieren.

Wenn Sie BGP konfigurieren, müssen Sie eine lokale AS-Nummer des autonomen Systems für das Tier-0-Gateway konfigurieren. BGP-Multihop wird unterstützt.

BGPv6 wird für Single-Hop und für Multihop unterstützt. Ein BGPv6-Nachbar unterstützt nur IPv6-Adressen. Redistribution, Präfix-Liste und Routenzuordnungen werden mit IPv6-Präfixen unterstützt.

Ein Tier-0-Gateway im Aktiv/Aktiv-Modus unterstützt Inter-SR-iBGP (Servicerouter). Wenn Gateway 1 nicht mit einem physischen Northbound-Router kommunizieren kann, wird der Datenverkehr zu Gateway 2 im Aktiv/Aktiv-Cluster umgeleitet. Wenn Gateway 2 mit dem physischen Router kommunizieren kann, wird der Datenverkehr zwischen Gateway 1 und dem physische Router nicht beeinflusst.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk > Tier-0-Gateways**.
- 3 Um ein Tier-0-Gateway zu bearbeiten, klicken Sie auf das Menüsymbol (drei Punkte) und wählen Sie **Bearbeiten**.
- 4 Klicken Sie auf **BGP**.
  - a Geben Sie die lokale AS-Nummer ein.
  - b Klicken Sie auf die **BGP-Umschaltfläche**, um BGP zu aktivieren oder zu deaktivieren.

- c Wenn dieses Gateway im Aktiv/Aktiv-Modus ist, klicken Sie auf die Umschaltfläche **Inter-SR-iBGP**, um Inter-SR-iBGP zu aktivieren oder zu deaktivieren.
- d Klicken Sie auf die Umschaltfläche **ECMP**, um ECMP zu aktivieren oder zu deaktivieren.
- e Klicken Sie auf die Umschaltfläche **Multipath Relax**, um Lastverteilung über mehrere Pfade hinweg zu aktivieren oder zu deaktivieren, die sich nur in den AS-Pfad-Attributwerten unterscheiden, aber dieselbe AS-Pfadlänge haben.

---

**Hinweis** **ECMP** muss aktiviert sein, damit **Multipath Relax** funktioniert.

---

- f Klicken Sie auf die Umschaltfläche **Graceful Restart**, um den Graceful Restart zu aktivieren oder zu deaktivieren.

Graceful Restart wird nur unterstützt, wenn der dem Tier-0-Gateway zugeordnete NSX Edge-Cluster nur über einen Edge-Knoten verfügt.

**5 Konfigurieren Sie Routenaggregation durch Hinzufügen von IP-Adresspräfixen.**

- a Klicken Sie auf **Präfix hinzufügen**.
- b Geben Sie ein IP-Adresspräfix im CIDR-Format ein.
- c Wählen Sie für die Option **Nur Zusammenfassung** entweder **Ja** oder **Nein**.

**6 Konfigurieren Sie BGP-Nachbarn.**

- a Geben Sie die IP-Adresse des Nachbarn ein.
- b Aktivieren oder deaktivieren Sie BFD.
- c Geben Sie die Remote-AS-Nummer ein.
- d Konfigurieren Sie den ausgehenden Filter.
- e Konfigurieren Sie den eingehenden Filter.
- f Aktivieren oder deaktivieren Sie die Funktion **Allowas-in**.

Diese ist standardmäßig deaktiviert. Wenn diese Funktion aktiviert ist, können BGP-Nachbarn Routen mit demselben AS empfangen, z. B. wenn Sie zwei Standorte haben, die über denselben Dienstleister miteinander verbunden sind. Diese Funktion gilt für alle Adressfamilien und kann nicht auf bestimmte Adressfamilien angewendet werden.

- g Klicken Sie auf **Timer und Kennwort**.
- h Geben Sie einen Wert für **BFD-Intervall** ein.
- i Geben Sie einen Wert für **BFD-Multiplikator** ein.
- j Geben Sie einen Wert für **Hold Down-Zeit** ein.
- k Geben Sie einen Wert für **Keep Alive-Zeit** ein.
- l Geben Sie ein Kennwort ein.

Dies ist erforderlich, wenn Sie die MD5-Authentifizierung unter BGP-Peers konfigurieren.



**7** Klicken Sie auf **Speichern**.

# Tier-1-Gateway

# 3

Ein Tier-1-Gateway führt die Funktionen eines logischen Tier-1-Routers aus. Es verfügt über Downlink-Verbindungen zu Segmenten und Uplink-Verbindungen zu Tier-0-Gateways.

---

**Hinweis** Auf der Registerkarte **Netzwerk und Sicherheit – Erweitert** bezieht sich der Begriff „logischer Tier-1-Router“ auf ein Tier-1-Gateway.

---

Sie können Routenankündigungen und statische Routen auf einem Tier-1-Gateway konfigurieren. Rekursive statische Routen werden unterstützt.

Dieses Kapitel enthält die folgenden Themen:

- [Tier-1-Gateway hinzufügen](#)

## Tier-1-Gateway hinzufügen

Ein Tier-1-Gateway ist in der Regel mit einem Tier-0-Gateway in Northbound-Richtung oder mit Segmenten in Southbound-Richtung verbunden.

Tier-0- und Tier-1-Gateways unterstützen die folgenden Adressierungskonfigurationen für alle Schnittstellen (Uplinks, Dienstports und Downlinks) sowohl in Single- als auch in Multi-Tier-Topologien:

- Nur IPv4
- Nur IPv6
- Dual-Stack – IPv4 und IPv6

Aktivieren Sie für die Verwendung von IPv6 oder der Dual-Stack-Adressierung **IPv4 und IPv6** als Layer-3-Weiterleitungsmodus unter **Netzwerk > Netzwerkeinstellungen > Globale Netzwerkkonfiguration**.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk > Tier-1-Gateways**.

- 3 Klicken Sie auf **Tier-1-Gateway hinzufügen**.
- 4 Geben Sie einen Namen für das Gateway ein.
- 5 (Optional) Wählen Sie ein Tier-0-Gateway aus, das mit diesem Tier-1-Gateway verbunden wird, um eine Topologie mit mehreren Ebenen zu erstellen.
- 6 Wählen Sie einen Failover-Modus aus.

Option	Beschreibung
Vorbeugend	Wenn der bevorzugte NSX Edge-Knoten fehlschlägt und wiederhergestellt wird, hat er Vorrang vor seinem Peer und wird zum aktiven Knoten. Der Peer ändert seinen Zustand in Standby. Dies ist die Standardoption.
Nicht vorbeugend	Wenn der bevorzugte NSX Edge-Knoten fehlschlägt und wiederhergestellt wird, wird überprüft, ob der zugehörige Peer der aktive Knoten ist. Ist dies der Fall, hat der bevorzugte Knoten keinen Vorrang vor seinem Peer, und er ist der Standby-Knoten.

- 7 (Optional) Wählen Sie einen NSX Edge-Cluster aus, wenn dieses Tier-1-Gateway statusbehaftete Dienste (NAT, LB, FW) hosten soll.

Wenn ein NSX Edge-Cluster ausgewählt ist, wird immer ein Dienstrouter erstellt (auch wenn Sie keine statusbehafteten Dienste konfigurieren), was sich auf das Muster des vertikalen Datenverkehrs auswirkt.

- 8 (Optional) Wählen Sie einen NSX Edge-Knoten aus.
- 9 Klicken Sie auf **Speichern**.
- 10 (Optional) Klicken Sie auf **Routenankündigung**.

Wählen Sie mindestens eine der folgenden Optionen aus:

- **Alle statischen Routen**
- **Alle NAT-IP-Adressen**
- **Alle DNS-Weiterleitungsrouten**
- **Alle LB-VIP-Routen**
- **Alle verbundenen Segmente und Dienstports**
- **Alle LB SNAT-IP-Routen**

- 11 (Optional) Klicken Sie auf **Dienstschnittstellen** und **Festlegen**, um Verbindungen mit Segmenten zu konfigurieren. In einigen Topologien erforderlich, z. B. in VLAN-gestützten Segmenten oder einem Load Balancing mit einem Arm.
  - a Klicken Sie auf **Schnittstelle hinzufügen**.
  - b Geben Sie einen Namen und eine IP-Adresse im CIDR-Format ein.
  - c Wählen Sie ein Segment aus.
  - d Klicken Sie auf **Speichern**.

- 12** (Optional) Klicken Sie auf **Statische Routen** und **Festlegen**, um statische Routen zu konfigurieren.
- a Klicken Sie auf **Statische Route hinzufügen**.
  - b Geben Sie einen Namen und eine Netzwerkadresse im CIDR- oder IPv6-CIDR-Format ein.
  - c Klicken Sie auf **Nächste Hops festlegen**, um Informationen über den nächsten Hop hinzuzufügen.
  - d Klicken Sie auf **Speichern**.

# Segmente

# 4

Ein Segment führt die Funktionen eines logischen Switches aus.

---

**Hinweis** Auf der Registerkarte **Netzwerk und Sicherheit – Erweitert** bezieht sich der Begriff „logischer Switch“ auf ein Segment.

---

Dieses Kapitel enthält die folgenden Themen:

- [Segmentprofile](#)
- [Hinzufügen eines Segments](#)

## Segmentprofile

Segmentprofile umfassen Konfigurationsdetails des Layer 2-Netzwerks für Segmente und Segmentports. NSX Manager unterstützt verschiedene Typen von Segmentprofilen.

Die folgenden Typen von Segmentprofilen sind verfügbar:

- QoS (Quality of Service; Dienstqualität)
- IP Discovery
- SpoofGuard
- Segmentsicherheit
- MAC-Verwaltung

---

**Hinweis** Die Standard-Segmentprofile können nicht bearbeitet oder gelöscht werden. Wenn Sie alternative Einstellungen aus dem Standard-Segmentprofil benötigen, können Sie ein benutzerdefiniertes Segmentprofil erstellen. Standardmäßig erben mit Ausnahme des Segmentsicherheitsprofils alle benutzerdefinierten Segmentprofile die Einstellungen des entsprechenden Standard-Segmentprofils. Beispielsweise weist ein benutzerdefiniertes IP Discovery-Segmentprofil standardmäßig dieselben Einstellungen wie das IP Discovery-Standard-Segmentprofil auf.

---

Jedes standardmäßige oder benutzerdefinierte Segmentprofil weist einen eindeutigen Bezeichner auf. Anhand dieses Bezeichners können Sie das Segmentprofil einem Segment oder einem Segmentport zuordnen.

Ein Segment oder Segmentport kann mit nur einem Segmentprofil eines beliebigen Typs verknüpft werden. Es ist beispielsweise nicht möglich, zwei QoS-Segmentprofile mit einem Segment oder Segmentport verknüpfen.

Wenn Sie bei der Erstellung eines Segments kein Segmentprofil zuweisen, ordnet der NSX Manager ein entsprechendes systemdefiniertes Standardsegmentprofil zu. Die untergeordneten Segmentports übernehmen das systemdefinierte Standardsegmentprofil vom übergeordneten Segment.

Beim Erstellen oder Aktualisieren eines Segments oder Segmentports können Sie entweder ein standardmäßiges oder ein benutzerdefiniertes Segmentprofil zuordnen. Wenn Sie das Segmentprofil einem Segment zuordnen bzw. diese Zuordnung aufheben, wird das Segmentprofil für die untergeordneten Segmentports basierend auf den folgenden Kriterien angewendet.

- Wenn dem übergeordneten Segment ein Profil zugeordnet ist, übernimmt der untergeordnete Segmentport das Segmentprofil vom übergeordneten Element.
- Wenn dem übergeordneten Segment kein Segmentprofil zugeordnet ist, wird dem Segment ein Standardsegmentprofil zugewiesen, das vom Segmentport übernommen wird.
- Wenn Sie einem Segmentport explizit ein benutzerdefiniertes Profil zuordnen, überschreibt dieses benutzerdefinierte Profil das vorhandene Segmentprofil.

---

**Hinweis** Wenn Sie einem Segment ein benutzerdefiniertes Segmentprofil zugeordnet haben, das Standardsegmentprofil aber für einen der untergeordneten Segmentports beibehalten möchten, müssen Sie eine Kopie des Standardsegmentprofils erstellen und diese dem jeweiligen Segmentport zuordnen.

---

Sie können ein benutzerdefiniertes Segmentprofil nicht löschen, wenn es mit einem Segment oder Segmentport verknüpft ist. Um zu ermitteln, ob Segmente oder Segmentports mit dem benutzerdefinierten Segmentprofil verknüpft sind, navigieren Sie zum Abschnitt „Zugewiesen zu“ der Übersichtsansicht und klicken Sie auf die aufgeführten Segmente und Segmentports.

## Grundlegendes zum QoS-Segmentprofil

QoS stellt eine qualitativ hochstehende und dedizierte Netzwerkleistung für einen bevorzugten Datenverkehr zur Verfügung, der eine hohe Bandbreite erfordert. Der QoS-Mechanismus ermöglicht dies durch Reservierung von ausreichend Bandbreite, Kontrolle von Latenz und Jitter sowie Reduzierung des Datenverlustes für bevorzugte Pakete, auch bei Netzwerküberlastung. Dieses Netzwerkdienstniveau wird durch eine effiziente Nutzung der Netzwerkressourcen erreicht.

In dieser Version werden CoS (Class of Service, Dienstklasse) und DSCP (Differentiated Services Code Point) für das Shaping des Datenverkehrs und dessen namentliche Kennzeichnung unterstützt. Die Schicht-2-CoS (Class of Service, Dienstklasse) ermöglicht die Festlegung einer Priorität für Datenpakete, wenn der Datenverkehr im Segment wegen Überlastung gepuffert wird. Der Schicht-3-DSCP ermittelt Pakete auf der Basis ihrer DSCP-Werte. CoS wird immer auf das Datenpaket angewendet, unabhängig vom vertrauenswürdigen Modus.

NSX-T Data Center stuft die von einer virtuellen Maschine übernommene DSCP-Einstellung oder den auf der Ebene des logischen Segments geänderten oder festgelegten DSCP-Wert als vertrauenswürdig ein. In beiden Fällen wird der DSCP-Wert an die Outer-IP-Kopfzeile der gekapselten Frames weitergegeben. Dies bietet dem externen physischen Netzwerk die Möglichkeit, dem Datenverkehr auf der Basis dieser DSCP-Einstellung in der äußeren Kopfzeile Priorität einzuräumen. Wenn für DSCP der Modus „Vertrauenswürdig“ eingestellt ist, wird der DSCP-Wert von der inneren Kopfzeile kopiert. Ist für DSCP der Modus „Nicht vertrauenswürdig“ eingestellt, wird der DSCP-Wert nicht für die innere Kopfzeile beibehalten.

---

**Hinweis** DSCP-Einstellungen sind nur für getunnelten Datenverkehr wirksam. Diese Einstellungen haben keine Auswirkungen auf den Datenverkehr innerhalb desselben Hypervisors.

---

Sie können mit dem QoS-Switching-Profil die durchschnittliche Bandbreite für den Ingress und Egress konfigurieren und so den Grenzwert für die Übertragungsrate festlegen. Die höchste Bandbreitenrate dient der Unterstützung des Burstdatenverkehrs, der für ein Segment zulässig ist, um eine Überlastung auf vertikalen Netzwerkverbindungen zu vermeiden. Diese Einstellungen gewährleisten nicht die Bandbreite, tragen jedoch zur Begrenzung der Netzwerkbandbreitennutzung bei. Die tatsächlich beobachtbare Bandbreite wird durch die Link-Geschwindigkeit des Ports oder die Werte im Switching-Profil bestimmt, je nachdem, welcher davon niedriger ist.

Die Einstellungen für das QoS-Switching-Profil gelten für das Segment und werden vom untergeordneten Segment-Port übernommen.

## Erstellen eines QoS-Segmentprofils

Sie können den DSCP-Wert definieren und die Ingress- und Egress-Einstellungen zum Erstellen eines benutzerdefinierten QoS-Switching-Profiles konfigurieren.

### Voraussetzungen

- Machen Sie sich mit dem Konzept des QoS-Switching-Profiles vertraut. Siehe [Grundlegendes zum QoS-Switching-Profil](#).
- Ermitteln Sie den Netzwerkdatenverkehr, der Priorität haben soll.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk > Segmente > Segmentprofile**.
- 3 Klicken Sie auf **Segmentprofil hinzufügen** und wählen Sie **QoS** aus.

#### 4 Vervollständigen Sie die Details des QoS-Switching-Profiles.

Option	Beschreibung
<b>Name</b>	Name des Profils.
<b>Modus</b>	<p>Wählen Sie die Option <b>Vertrauenswürdig</b> oder <b>Nicht vertrauenswürdig</b> aus dem Dropdown-Menü „Modus“ aus.</p> <p>Bei der Auswahl des Modus „Vertrauenswürdig“ wird der innere DSCP-Kopfzeilenwert von der äußeren IP-Kopfzeile für den IP-/IPv6-Datenverkehr übernommen. Für den Nicht-IP-/IPv6-Datenverkehr gilt für die äußere IP-Kopfzeile der Standardwert. Der Modus „Vertrauenswürdig“ wird auf einem Overlay-basierten logischen Port unterstützt. Der Standardwert ist 0.</p> <p>Der Modus „Nicht vertrauenswürdig“ wird auf einem Overlay-basierten und auf einem VLAN-basierten logischen Port unterstützt. Für den Overlay-basierten logischen Port wird der DSCP-Wert der äußeren IP-Kopfzeile auf den konfigurierten Wert festgelegt, unabhängig vom inneren Pakettyp für den logischen Port. Für den VLAN-basierten logischen Port wird der DSCP-Wert des IP-/IPv6-Pakets auf den konfigurierten Wert festgelegt. Der Bereich der DSCP-Werte für den Modus „Nicht vertrauenswürdig“ liegt zwischen 0 und 63.</p> <p><b>Hinweis</b> DSCP-Einstellungen sind nur für getunnelten Datenverkehr wirksam. Diese Einstellungen haben keine Auswirkungen auf den Datenverkehr innerhalb desselben Hypervisors.</p>
<b>Priorität</b>	<p>Legen Sie den CoS-Prioritätswert fest.</p> <p>Die Prioritätswerte liegen zwischen 0 und 63, wobei 0 der höchsten Priorität entspricht.</p>
<b>Dienstklasse</b>	<p>Legen Sie den CoS-Wert fest.</p> <p>CoS wird auf VLAN-basierten logischen Ports unterstützt. CoS fasst ähnliche Datenverkehrstypen im Netzwerk in Gruppen zusammen. Jeder Datenverkehrstyp wird als eine Klasse mit einer eigenen Stufe der Dienstpriorität behandelt. Der Datenverkehr mit geringerer Priorität wird verlangsamt bzw. in manchen Fällen sogar verworfen, um einen besseren Durchsatz für den Datenverkehr mit höherer Priorität zu gewährleisten. CoS kann für die VLAN-ID auch mit „Null-Paket“ konfiguriert werden.</p> <p>Die CoS-Werte reichen von 0 bis 7, wobei 0 für den maximalen Dienst steht.</p>
<b>Ingress</b>	<p>Legen Sie benutzerdefinierte Werte für den ausgehenden Netzwerkdatenverkehr von der VM zum logischen Netzwerk fest.</p> <p>Sie können mit der durchschnittlichen Bandbreite die Netzwerküberlastung reduzieren. Mit der Spitzenbandbreite wird der Burstdatenverkehr unterstützt. Die Burstgröße basiert auf der Dauer mit Spitzenbandbreite. Sie können die Burstdauer in der Einstellung für die Burstgröße festlegen. Sie können die Bandbreite nicht dauerhaft gewährleisten. Sie können jedoch die Einstellungen für Durchschnitt, Spitzenbandbreite und Burstgröße verwenden, um die Netzwerkbandbreite zu begrenzen.</p> <p>Wenn beispielsweise die durchschnittliche Bandbreite 30 Mbit/s, die Spitzenbandbreite 60 Mbit/s und die zulässige Dauer 0,1 Sekunden beträgt, beträgt die Burstgröße <math>60 \times 1000000 \times 0,1/8 = 750000</math> Byte.</p> <p>Der Standardwert 0 deaktiviert die Ratenbegrenzung für den Ingress-Datenverkehr.</p>



Option	Beschreibung
<b>Ingress Broadcast</b>	<p>Legen Sie benutzerdefinierte Werte für den eingehenden Netzwerkdatenverkehr von der VM zum logischen Netzwerk auf Broadcast-Basis fest.</p> <p>Wenn Sie beispielsweise die durchschnittliche Bandbreite für einen logischen Switch auf 3000 Kbit/s festlegen, die Spitzenbandbreite 6000 Kbit/s und die zulässige Dauer 0,1 Sekunden beträgt, beträgt die Burstgröße <math>6000 \times 1000 \times 0,1/8 = 75000</math> Byte.</p> <p>Der Standardwert 0 deaktiviert die Ratenbegrenzung für den Ingress Broadcast-Datenverkehr.</p>
<b>Egress</b>	<p>Legen Sie benutzerdefinierte Werte für den eingehenden Netzwerkdatenverkehr vom logischen Netzwerk zur VM fest.</p> <p>Der Standardwert 0 deaktiviert die Ratenbegrenzung für den ausgehenden Datenverkehr.</p>

Wenn die Ingress-, Ingress-Broadcast- und Egress-Optionen nicht konfiguriert sind, werden die Standardwerte verwendet.

## 5 Klicken Sie auf **Speichern**.

## Grundlegendes zum Segmentprofil für die IP Discovery

Die IP Discovery ruft MAC- und IP-Adressen mithilfe von DHCP- und DHCPv6-Snooping, ARP-Snooping (Address Resolution Protocol), ND-Snooping (Neighbor Discovery) und VM-Tools ab.

Die erkannten Mac- und IP-Adressen werden verwendet, um ARP-/ND-Unterdrückung zu erzielen und somit den Datenverkehr zwischen VMs zu minimieren, die mit demselben Segment verbunden sind. Die Adressen werden auch von den SpoofGuard-Komponenten und Komponenten der verteilten Firewall (DFW) verwendet. Anhand der Adressbindungen ermittelt DFW die IP-Adresse von Objekten in Firewallregeln.

Das DHCP/DHCPv6-Snooping prüft die DHCP/DHCPv6-Pakete, die zwischen dem DHCP/DHCPv6-Client und dem DHCP/DHCPv6-Server ausgetauscht werden, um die IP- und MAC-Adressen abzurufen.

Das ARP-Snooping überprüft die ausgehenden ARP- und GARP- (Gratuitous ARP-)Pakete der VM, um die IP- und MAC-Adressen abzurufen.

VM Tools ist eine Software, die auf einer ESXi-gehosteten virtuellen Maschine ausgeführt wird und die Konfigurationsdaten der virtuellen Maschine, einschließlich MAC- und IP- oder IPv6-Adressen, bereitstellen kann. Diese IP Discovery-Methode ist nur für VMs verfügbar, die auf ESXi-Hosts ausgeführt werden.

ND-Snooping ist das IPv6-Äquivalent zum ARP-Snooping. Es prüft Neighbor Solicitation (NS)- und Neighbor Advertisement (NA)-Nachrichten, um die IP- und MAC-Adressen zu ermitteln.

Die Erkennung von doppelten Adressen überprüft, ob eine neu ermittelte IP-Adresse bereits in der realisierten Bindungsliste für einen anderen Port vorhanden ist. Diese Prüfung wird für Ports durchgeführt, die sich im selben Segment befinden. Wenn eine doppelte Adresse erkannt wird, wird die neu ermittelte Adresse nicht zur realisierten Bindungsliste, sondern zur ermittelten Liste

hinzugefügt. Allen doppelten IPs ist ein Ermittlungszeitstempel zugeordnet. Wenn die IP, die sich in der realisierten Bindungsliste befindet, entweder durch Hinzufügen zur Ignorieren-Bindungsliste (siehe unten) oder durch Deaktivieren des Snooping entfernt wird, wird die doppelte IP mit dem ältesten Zeitstempel in die realisierte Bindungsliste verschoben. Die doppelten Adressinformationen sind über einen API-Aufruf verfügbar.

Standardmäßig arbeiten die Ermittlungsmethoden ARP-Snooping und ND-Snooping in einem Modus namens „Trust on First Use“ (TOFU). Wenn im TOFU-Modus eine Adresse ermittelt und zur realisierten Bindungsliste hinzugefügt wird, bleibt diese Bindung für immer in der realisierten Liste. TOFU gilt für die ersten „n“ eindeutigen <IP-, MAC-, VLAN->Bindungen, die mithilfe von ARP/ND-Snooping erkannt werden, wobei „n“ der Bindungsgrenzwert ist, den Sie konfigurieren können. Sie können TOFU für ARP-/ND-Snooping deaktivieren. Die Methoden werden dann im TOEU-Modus als vertrauenswürdig eingestuft. Wenn eine Adresse im TOEU-Modus ermittelt wird, wird Sie zur realisierten Bindungsliste hinzugefügt, und wenn sie gelöscht oder abgelaufen ist, wird sie aus der realisierten Bindungsliste entfernt. Die DHCP-Snooping- und VM-Tools-Methoden funktionieren immer im TOEU-Modus.

---

**Hinweis** TOFU ist nicht identisch mit SpoofGuard und blockiert nicht den Datenverkehr, wie dies bei SpoofGuard der Fall ist. Weitere Informationen zu SpoofGuard finden Sie unter [Grundlegendes zum Spoofguard-Segmentprofil](#).

---

NSX Manager verwaltet für jeden Port eine Ignorieren-Bindungsliste, die IP-Adressen enthält, die nicht an den Port gebunden werden können. Sie können diese Liste nur über die API aktualisieren. Sie können diese Methode auch durch Navigation verwenden, um eine zuvor ermittelte IP für einen bestimmten Port zu löschen. Weitere Informationen finden Sie in der Referenz zur NSX-T-API unter „ignore\_address\_bindings“.

---

**Hinweis** Für Linux-VMs kann das ARP-Flux-Problem möglicherweise dazu führen, dass das ARP-Snooping inkorrekte Informationen erhält. Das Problem kann durch einen ARP-Filter verhindert werden. Weitere Informationen finden Sie unter <http://linux-ip.net/html/ether-arp.html#ether-arp-flux>.

---

## Erstellen eines Segmentprofils für die IP-Ermittlung

NSX-T Data Center weist mehrere standardmäßige Switching-Profile für die IP-Ermittlung auf. Sie können auch weitere Profile erstellen.

### Voraussetzungen

Machen Sie sich mit dem Konzept des Switching-Profils für die IP-Ermittlung vertraut. Siehe [Grundlegendes zum Switching-Profil für die IP Discovery](#)

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk > Segmente > Segmentprofile**.

- 3 Klicken Sie auf **Segmentprofil hinzufügen** und wählen Sie **IP-Ermittlung** aus.
- 4 Geben Sie die Details des Switching-Profiles für die IP-Ermittlung an.

Option	Beschreibung
<b>Name</b>	Geben Sie einen Namen ein.
<b>ARP-Snooping</b>	Für eine IPv4-Umgebung. Anwendbar, wenn VMs statische IP-Adressen aufweisen.
<b>ARP-Bindungsgrenzwert</b>	Die maximale Anzahl von IPv4-IP-Adressen, die an einen Port gebunden werden können.
<b>Zeitüberschreitung bei ARP-ND-Bindungsgrenzwert</b>	Der Zeitüberschreitungswert in Minuten für IP-Adressen in der ARP-/ND-Bindungstabelle, wenn TOFU deaktiviert ist. Wenn für eine Adresse eine Zeitüberschreitung auftritt, wird sie durch eine neu erkannte Adresse ersetzt.
<b>DHCP-Snooping</b>	Für eine IPv4-Umgebung. Anwendbar, wenn VMs IPv4-Adressen aufweisen.
<b>DHCP-Snooping-V6</b>	Für eine IPv6-Umgebung. Anwendbar, wenn VMs IPv6-Adressen aufweisen.
<b>VM Tools</b>	Nur für ESXi-gehostete VMs verfügbar.
<b>VM-Tools für IPv6</b>	Nur für ESXi-gehostete VMs verfügbar.
<b>Überwachung (Snooping) der Nachbarermittlung</b>	Für eine IPv6-Umgebung. Anwendbar, wenn VMs statische IP-Adressen aufweisen.
<b>Bindungsgrenzwert für Nachbarermittlung</b>	Die maximale Anzahl an IPv6-Adressen, die an einen Port gebunden werden können.
<b>Vertrauen bei erster Nutzung</b>	Anwendbar auf ARP- und ND-Snooping.
<b>Doppelte IP-Erkennung</b>	Für alle Snooping-Methoden sowie für IPv4- und IPv6-Umgebungen.

- 5 Klicken Sie auf **Speichern**.

## Grundlegendes zum Spoofguard-Segmentprofil

Mit SpoofGuard unterstützt die Abwehr von bestimmten Angriffen wie „Web-Spoofing“ und „Phishing“. Eine SpoofGuard-Richtlinie blockiert Datenverkehr, der als manipuliert erkannt wird.

SpoofGuard ist ein Tool, das virtuelle Maschinen in Ihrer Umgebung daran hindert, Datenverkehr von einer nicht für das Senden berechtigten IP-Adresse zu senden. Wenn die IP-Adresse einer virtuellen Maschine nicht mit der IP-Adresse des zugehörigen logischen Ports und der Segmentadressbindung in Spoof Guard übereinstimmt, wird die vNIC der virtuellen Maschine vollständig am Zugriff auf das Netzwerk gehindert. SpoofGuard lässt sich auf Port- oder Segmentebene konfigurieren. SpoofGuard kann aus verschiedenen Gründen in Ihrer Umgebung verwendet werden:

- Zur Verhinderung der Erkennung der IP-Adresse einer vorhandenen VM durch eine nicht berechnete virtuelle Maschine.
- Zur Sicherstellung, dass sich die IP-Adressen von virtuellen Maschinen nicht ohne Eingriff verändern lassen. In einigen Umgebungen ist es wünschenswert, dass virtuelle Maschinen ihre IP-Adressen ohne ordnungsgemäße Änderungskontrolle nicht ändern können. Mit SpoofGuard lässt sich dies vereinfachen. Damit wird sichergestellt, dass der Besitzer der virtuellen Maschine die IP-Adresse nicht einfach ändern und seine Arbeit ungehindert fortsetzen kann.
- Zur Sicherstellung, dass Regeln der die verteilte Firewall nicht irrtümlich (oder absichtlich) umgangen werden. Bei Regeln für die verteilte Firewall, die unter Verwendung von IP Sets als Quelle oder Ziele erstellt wurden, besteht immer die Gefahr, dass die IP-Adresse einer virtuellen Maschine in der Paketkopfzeile gefälscht ist und so die betreffenden Regeln umgangen werden.

Die Konfiguration von NSX-T Data Center SpoofGuard umfasst die folgenden Elemente:

- MAC SpoofGuard – authentifiziert die MAC-Adresse des Pakets
- IP SpoofGuard – authentifiziert die MAC- und die IP-Adresse des Pakets
- Dynamische ARP (Address Resolution Protocol)-Untersuchung, d. h., es wird eine ARP-, GARP (Gratuitous Address Resolution Protocol)- und ND (Neighbor Discovery)-SpoofGuard-Überprüfung der Zuordnung der MAC-, IP- und IP-MAC-Quelle in der ARP-/GARP-/ND-Nutzlast durchgeführt.

Auf Portebene wird die Positivliste zulässiger MAC/VLAN/IP-Werte über die Adressbindungseigenschaft des Ports zur Verfügung gestellt. Wenn die virtuelle Maschine Datenverkehr sendet, wird dieser verworfen, wenn ihre IP-/MAC-/VLAN-Werte nicht mit den IP-/MAC-/VLAN-Eigenschaften des Ports übereinstimmen. SpoofGuard auf Portebene ist für die Authentifizierung des Datenverkehrs zuständig, d. h. für die Überprüfung, ob der Datenverkehr mit der VIF-Konfiguration in Einklang steht.

Auf Segmentebene wird die Positivliste zulässiger MAC-/VLAN-/IP-Werte über die Adressbindungseigenschaft des Segments zur Verfügung gestellt. Hierbei handelt es sich in der Regel um einen zulässigen IP-Bereich oder ein zulässiges Subnetz für das Segment. SpoofGuard ist auf Segmentebene für die Authentifizierung des Datenverkehrs zuständig.

Der Datenverkehr muss von SpoofGuard auf Port- UND Segmentebene gestattet werden, bevor er für das Segment zugelassen wird. Die Aktivierung/Deaktivierung von SpoofGuard auf Port- und Segmentebene kann mithilfe des SpoofGuard-Segmentprofils gesteuert werden.

## Erstellen eines SpoofGuard-Segmentprofils

Wenn sich bei konfigurierter SpoofGuard die IP-Adresse einer virtuellen Maschine ändert, kann der Datenverkehr aus der virtuellen Maschine so lange blockiert werden, bis die zugehörigen konfigurierten Port-/Segmentadressbindungen mit der neuen IP-Adresse aktualisiert werden.

Aktivieren Sie SpoofGuard für die Portgruppen, die die Gastbetriebssysteme enthalten. Wenn SpoofGuard für jeden Netzwerkadapter aktiviert ist, untersucht es Pakete für die vorgegebene MAC-Adresse und die zugehörige IP-Adresse.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk > Segmente > Segmentprofile**.
- 3 Klicken Sie auf **Segmentprofil hinzufügen** und wählen Sie **Spoof Guard** aus.
- 4 Geben Sie einen Namen ein.
- 5 Um SpoofGuard auf Portebene zu aktivieren, setzen Sie **Portbindungen** auf **Aktiviert**.
- 6 Klicken Sie auf **Speichern**.

## Grundlegendes zu Segmentprofilen für die Segmentsicherheit

Die Segmentsicherheit bietet die statusfreie Schicht-2- und Schicht-3-Sicherheit durch Überprüfung des Ingress-Datenverkehrs zum Segment und durch Verwerfung unberechtigter Pakete, die von VMs gesendet wurden. Dazu werden die IP- und die MAC-Adresse sowie die Protokolle mit einem Satz zulässiger Adressen und Protokolle verglichen. Sie können mit der Segmentsicherheit die Integrität des Segments durch Herausfiltern von Angriffen aus den VMs im Netzwerk schützen.

Sie haben die Möglichkeit, Filter für die BPDU (Bridge Protocol Data Unit), DHCP-Snooping, DHCP-Serverblock und Optionen zur Begrenzung der Übertragungsrate zu konfigurieren, um das Segmentsicherheitsprofil auf einem Segment anzupassen.

## Erstellen eines Segmentprofils für die Segmentsicherheit

Sie können ein benutzerdefiniertes Segmentprofil für die Segmentsicherheit mit MAC-Ziel-Adressen aus der BPDU-Liste zulässiger Adressen anlegen und die Beschränkung der Rate konfigurieren.

### Voraussetzungen

Machen Sie sich mit dem Konzept des Segmentprofils für die Segmentsicherheit vertraut. Siehe [Grundlegendes zum Switching-Profil für die Switch-Sicherheit](#).

### Verfahren

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

- 2 Wählen Sie **Netzwerk > Segmente > Segmentprofile**.
- 3 Klicken Sie auf **Segmentprofil hinzufügen** und wählen Sie **Segmentsicherheit** aus.
- 4 Vervollständigen Sie die Details des Segment-Sicherheitsprofils.

Option	Beschreibung
<b>Name</b>	Name des Profils.
<b>BPDU-Filter</b>	<p>Schalten Sie die Schaltfläche <b>BPDU-Filter</b> zur Aktivierung der BPDU-Filterung um. Standardmäßig deaktiviert.</p> <p>Wenn der BPDU-Filter aktiviert ist, wird der gesamte Datenverkehr zur BPDU-Ziel-MAC-Adresse blockiert. Dabei wird auch STP auf den logischen Switch-Ports deaktiviert, da davon ausgegangen wird, dass diese Ports nicht Bestandteil von STP sind.</p>
<b>Positivliste für den BPDU-Filter</b>	Klicken Sie auf die Ziel-MAC-Adresse aus der Liste der BPDU-Ziel-MAC-Adressen, um den Datenverkehr zum zugelassenen Ziel zu ermöglichen. Sie müssen <b>BPDU-Filter</b> aktivieren, um aus dieser Liste auswählen zu können.
<b>DHCP-Filter</b>	<p>Schalten Sie die Schaltflächen <b>Serverblock</b> und <b>Clientblock</b> zur Aktivierung der DHCP-Filterung um. Beide sind standardmäßig deaktiviert.</p> <p>Die DHCP-Serverblockierung blockiert Datenverkehr von einem DHCP-Server an einen DHCP-Client. Dabei wird kein Datenverkehr von einem DHCP-Server an einen DHCP-Relay-Agent blockiert.</p> <p>Die DHCP-Clientblockierung verhindert, dass eine VM eine DHCP-IP-Adresse erhält, indem DHCP-Anforderungen blockiert werden.</p>
<b>DHCPv6-Filter</b>	<p>Schalten Sie die Schaltflächen <b>V6-Serverblock</b> und <b>V6-Clientblock</b> zur Aktivierung der DHCP-Filterung um. Beide sind standardmäßig deaktiviert.</p> <p>Die DHCPv6-Serverblockierung blockiert Datenverkehr von einem DHCPv6-Server an einen DHCPv6-Client. Dabei wird kein Datenverkehr von einem DHCP-Server an einen DHCP-Relay-Agent blockiert. Pakete, deren UDP-Quellportnummer 547 beträgt, werden gefiltert.</p> <p>Die DHCPv6-Clientblockierung verhindert, dass eine VM eine DHCP-IP-Adresse erhält, indem DHCP-Anforderungen blockiert werden. Pakete, deren UDP-Quellportnummer 546 beträgt, werden gefiltert.</p>
<b>Nicht-IP-Datenverkehr blockieren</b>	<p>Schalten Sie die Schaltfläche <b>Nicht-IP-Datenverkehr blockieren</b> um, um nur IPv4-, IPv6-, ARP- und BPDU-Datenverkehr zuzulassen.</p> <p>Der übrige Nicht-IP-Datenverkehr wird blockiert. Der zugelassene IPv4-, IPv6-, ARP-, GARP- und BPDU-Datenverkehr basiert auf anderen Richtlinien, die in der Konfiguration der Adressbindung und von SpoofGuard festgelegt sind.</p> <p>Standardmäßig ist diese Option deaktiviert, d. h. der Nicht-IP-Datenverkehr wird als regulärer Datenverkehr behandelt.</p>

Option	Beschreibung
<b>RA-Guard</b>	Schalten Sie die Schaltfläche <b>RA-Guard</b> um, um Ingress-IPv6-Routerankündigungen herauszufiltern. ICMPv6-Pakete vom Typ 134 werden herausgefiltert. Diese Option ist standardmäßig aktiviert.
<b>Ratenbegrenzungen</b>	Legen Sie eine Ratenbegrenzung für Broadcast-und Multicast-Datenverkehr fest. Diese Option ist standardmäßig aktiviert.  Ratenbegrenzungen können verwendet werden, um den logischen Switch oder VMs vor Ereignissen wie Broadcast-Stürmen zu schützen.  Um Konnektivitätsprobleme zu vermeiden, muss die Mindestrate größer oder gleich 10 PPS sein.

5 Klicken Sie auf **Speichern**.

## Grundlegendes zum Segmentprofil für die MAC Discovery

Das Segmentprofil für die MAC-Verwaltung unterstützt zwei Funktionen: MAC Learning und MAC-Adressänderung.

Die Änderungsfunktion für die MAC-Adresse ermöglicht einem VM die Änderung der zugehörigen MAC-Adresse. Eine mit einem Port verbundene VM kann einen administrativen Befehl zur Änderung der MAC-Adresse ihrer vNIC ausführen, und es kann weiterhin Datenverkehr an diese vNIC gesendet bzw. von ihr empfangen werden. Diese Funktion wird nur für ESXi- und nicht für KVM-VMs unterstützt. Die Eigenschaft ist standardmäßig deaktiviert.

MAC Learning bietet eine Netzwerkkonnektivität für Bereitstellungen, in denen mehrere MAC-Adressen hinter einer vNIC konfiguriert sind. Ein Beispiel ist eine geschachtelte Hypervisor-Bereitstellung, in der eine ESXi-VM auf einem ESXi-Host ausgeführt wird und mehrere VMs innerhalb der ESXi-VM ausgeführt werden. Wenn die vNIC der ESXi-VM eine Verbindung mit einem Segment-Port herstellt, ist die MAC-Adresse ohne MAC Learning statisch. VMs, die innerhalb der ESXi-VM ausgeführt werden, verfügen über keine Netzwerkkonnektivität, da ihre Pakete über unterschiedliche MAC-Quelladressen verfügen. Beim MAC Learning überprüft vSwitch die MAC-Quelladresse jedes Pakets von der vNIC, ruft die MAC-Adresse ab und gestattet dem Paket die Weiterleitung. Wird eine erlernte MAC-Adresse eine bestimmte Zeit lang nicht verwendet, wird sie entfernt. Dieser Zeitraum ist nicht konfigurierbar. Das Feld **MAC Learning-Alterungszeit** zeigt den vordefinierten Wert an, der 600 ist.

MAC Learning unterstützt auch unbekanntes Unicast Flooding. Im Normalfall wird ein Paket, das von einem Port empfangen wird und über eine unbekannte Ziel-MAC-Adresse verfügt, verworfen. Bei aktiviertem Flooding des Datenverkehrs vom Typ „Unbekannter Unicast“ leitet der Port diesen Datenverkehr an jeden Port auf dem Switch weiter, für den MAC Learning und unbekanntes Unicast-Flooding aktiviert wurden. Diese Eigenschaft ist standardmäßig aktiviert, wenn MAC Learning aktiviert ist.

Die Anzahl erlernbarer MAC-Adressen ist konfigurierbar. Der Maximalwert ist 4096. Dies ist die Standardeinstellung. Sie können auch die Richtlinie für den Fall festlegen, dass der Grenzwert erreicht wird. Folgende Optionen stehen zur Verfügung:

- **Verwerfen** – Pakete von einer unbekannten MAC-Quelladresse werden verworfen. Pakete, die bei dieser MAC-Adresse eingehen, werden als unbekannte Unicast-Objekte behandelt. Der Port empfängt die Pakete nur dann, wenn unbekanntes Unicast-Flooding aktiviert ist.
- **Zulassen** – Pakete von einer unbekannten MAC-Quelladresse werden weitergeleitet, obwohl die Adresse nicht erlernt wird. Pakete, die bei dieser MAC-Adresse eingehen, werden als unbekannte Unicast-Objekte behandelt. Der Port empfängt die Pakete nur dann, wenn unbekanntes Unicast-Flooding aktiviert ist.

Wenn Sie MAC Learning und die MAC-Adressänderung aktiviert haben, müssen Sie zur Verbesserung der Sicherheit zusätzlich SpoofGuard konfigurieren.

## Erstellen eines MAC Discovery-Segmentprofils

Sie können ein MAC Discovery-Segmentprofil erstellen, um MAC-Adressen zu verwalten.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk > Segmente > Segmentprofile**.
- 3 Klicken Sie auf **Segmentprofil hinzufügen** und wählen Sie **MAC Discovery**.
- 4 Vervollständigen Sie die Details zum MAC Discovery-Profil.

Option	Beschreibung
<b>Name</b>	Name des Profils.
<b>MAC-Änderung</b>	Aktivieren oder deaktivieren Sie die Funktion zum Ändern der MAC-Adresse. Standardmäßig ist sie deaktiviert.
<b>MAC Learning</b>	Aktivieren oder deaktivieren Sie MAC Learning. Standardmäßig ist sie deaktiviert.
<b>MAC-Grenzwertrichtlinie</b>	Wählen Sie <b>Zulassen</b> oder <b>Verwerfen</b> aus. Die Standardeinstellung ist <b>Zulassen</b> . Diese Option ist verfügbar, wenn Sie Mac Learning aktivieren.
<b>Unbekanntes Unicast Flooding</b>	Aktivieren oder deaktivieren Sie die unbekannte Unicast Flooding-Funktion. Standardmäßig ist sie aktiviert. Diese Option ist verfügbar, wenn Sie Mac Learning aktivieren.
<b>MAC-Grenzwert</b>	Legen Sie die maximale Anzahl an MAC-Adressen fest. Die Standardeinstellung ist 4096. Diese Option ist verfügbar, wenn Sie Mac Learning aktivieren.
<b>MAC Learning-Alterungszeit</b>	Nur zur Information. Diese Option kann nicht konfiguriert werden. Der vordefinierte Wert lautet 600.

- 5 Klicken Sie auf **Speichern**.



## Hinzufügen eines Segments

Ein Segment stellt eine Verbindung zu Gateways und VMs her. Ein Segment führt die Funktionen eines logischen Switches aus.

Informationen zum Auffinden der VIF-ID einer VM finden Sie unter [Verbinden einer VM mit einem logischen Switch](#).

---

**Hinweis** Ein im Modus „Erweiterter Datenpfad“ konfigurierter N-VDS-Switch unterstützt IP Discovery-, SpoofGuard- und IPFIX-Profile.

---

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk > Segmente**.
- 3 Klicken Sie auf **Hinzufügen**.
- 4 Geben Sie einen Namen für das Segment ein.
- 5 Wählen Sie einen Uplink aus.  
  
Sie können ein vorhandenes Tier-0- oder Tier-1-Gateway oder die Option **Keine** auswählen. Bei Auswahl von **Keine** stellt das Segment lediglich einen logischen Switch dar. Mit einem konfigurierten Subnetz kann das Segment mit einem Tier-0- oder einem Tier-1-Gateway verbunden werden.
- 6 Handelt es sich bei dem Uplink um ein Tier-1-Gateway, wählen Sie den Typ **Flexibel** oder **Fest** aus.  
  
Die Verknüpfung eines flexiblen Segments mit einem Gateway kann aufgehoben werden. Ein festes Segment kann gelöscht werden. Die Verknüpfung eines festen Segments mit einem Gateway kann jedoch nicht aufgehoben werden.
- 7 Klicken Sie auf **Subnetze festlegen**, um ein Subnetz anzugeben.
- 8 Wählen Sie eine Transportzone aus.
- 9 Geben Sie bei einer Transportzone vom Typ „VLAN“ eine Liste der VLAN-IDs an.
- 10 Klicken Sie auf **Speichern**.
- 11 Klicken Sie auf **Ports** und **Festlegen**, um Segment-Ports hinzuzufügen.
  - a Klicken Sie auf **Segment-Port hinzufügen**.
  - b Geben Sie einen Portnamen ein.
  - c Geben Sie für **ID** die VIF-UUID der VM oder des Servers ein, der sich mit diesem Port verbindet.

- d Wählen Sie einen Typ aus: **Übergeordnet**, **Untergeordnet** oder **Unabhängig**.

Lassen Sie dieses Feld leer, außer für Anwendungsfälle wie Container oder VMware HCX. Soll dieser Port für einen Container in einer VM verwendet werden, wählen Sie **Untergeordnet** aus. Soll dieser Port für eine Container-Host-VM verwendet werden, wählen Sie **Übergeordnet** aus. Soll dieser Port für einen Bare-Metal-Container oder -Server verwendet werden, wählen Sie **Unabhängig** aus.

- e Geben Sie eine Kontext-ID ein.

Geben Sie die übergeordnete VIF-ID ein, wenn unter **Typ** der Wert **Untergeordnet** festgelegt wurde, oder die Transportknoten-ID, wenn unter **Typ** der Wert **Unabhängig** festgelegt wurde.

- f Geben Sie ein Datenverkehrs-Tag ein.

Geben Sie die VLAN-ID im Container und anderen Anwendungsfällen ein.

- g Wählen Sie eine Adresszuteilungsmethode aus: **IP-Pool**, **MAC-Pool**, **Beide** oder **Keine**.

- h Geben Sie Tags an.

- i Wählen Sie Segmentprofile für diesen Port aus.

**12** Klicken Sie auf **Segmentprofile**, um Segmentprofile auszuwählen.

**13** Klicken Sie auf **Speichern**.

# Virtual Private Network (VPN)

# 5

NSX-T Data Center unterstützt IPsec-Virtual Private Network (IPsec-VPN) und Layer 2 VPN (L2 VPN) auf einem NSX Edge-Knoten. IPsec-VPN bietet Site-to-Site-Konnektivität zwischen einem NSX Edge-Knoten und Remote-Sites. Mit L2 VPN können Sie Ihr Datacenter erweitern, indem Sie zulassen, dass virtuelle Maschinen ihre Netzwerkkonnektivität unter Verwendung derselben IP-Adresse über geografische Grenzen hinweg beibehalten.

---

**Hinweis** IPsec-VPNs und L2 VPNs werden in der NSX-T Data Center-Version mit Exportbeschränkung nicht unterstützt.

---

Sie müssen über einen funktionierenden NSX Edge-Knoten mit mindestens einem konfigurierten Tier-0-Gateway verfügen, bevor Sie einen VPN-Dienst konfigurieren können. Weitere Informationen finden Sie unter „NSX Edge-Installation“ im *NSX-T Data Center-Installationshandbuch*.

Ab NSX-T Data Center 2.4 können Sie auch neue VPN-Dienste mithilfe der NSX Manager-Benutzeroberfläche konfigurieren. In früheren Versionen von NSX-T Data Center können Sie VPN-Dienste nur mithilfe von REST-API-Aufrufen konfigurieren.

---

**Wichtig** Bei Nutzung von NSX-T Data Center 2.4 oder höher zur Konfiguration von VPN-Diensten müssen Sie neue Objekte verwenden, wie z. B. Tier-0-Gateways, die mithilfe der NSX Manager-Benutzeroberfläche oder der Richtlinien-APIs erstellt wurden, die sich im Lieferumfang von NSX-T Data Center 2.4 oder höher befinden. Für vorhandene logische Tier-0-Router, die vor NSX-T Data Center 2.4 konfiguriert wurden, müssen Sie weiterhin API-Aufrufe zum Konfigurieren eines VPN-Diensts verwenden.

---

Standardkonfigurationsprofile mit vordefinierten Werten und Einstellungen werden Ihnen während der Konfiguration eines VPN-Diensts zur Verfügung gestellt. Sie können auch neue Profile mit verschiedenen Einstellungen definieren und sie während der Konfiguration des VPN-Diensts auswählen.

Dieses Kapitel enthält die folgenden Themen:

- [Grundlegendes zu IPsec-VPNs](#)
- [Grundlegendes zu Layer 2-VPN](#)
- [Hinzufügen von VPN-Diensten](#)
- [Hinzufügen von IPsec-VPN-Sitzungen](#)

- [Hinzufügen von L2-VPN-Sitzungen](#)
- [Hinzufügen von lokalen Endpoints](#)
- [Hinzufügen von Profilen](#)
- [Überprüfen des realisierten Zustands einer IPSec-VPN-Sitzung](#)
- [Überwachung und Fehlerbehebung von VPN-Sitzungen](#)

## Grundlegendes zu IPSec-VPNs

IPSec-VPNs (Internet Protocol Security) sichern den Datenverkehr zwischen zwei Netzwerken, die über ein öffentliches Netzwerk durch IPSec-Gateways, sogenannte Endpoints, verbunden sind. NSX Edge unterstützt Site-to-Site-IPSec-VPN zwischen einem NSX Edge-Knoten und Remote-Sites.

IPSec-VPNs sichern den Datenverkehr zwischen zwei Netzwerken, die über ein öffentliches Netzwerk über IPSec-Gateways, sogenannte Endpoints, verbunden sind. NSX Edge unterstützt nur einen Tunnelmodus, der IP-Tunneling mit Encapsulating Security Payload (ESP) verwendet. ESP wird direkt auf der IP-Adresse mit der IP-Protokollnummer 50 ausgeführt.

IPSec-VPNs verwenden das IKE-Protokoll zum Aushandeln der Sicherheitsparameter. Der Standard-UDP-Port ist auf 500 festgelegt. Wenn NAT im Gateway erkannt wird, wird der Port auf UDP 4500 festgelegt.

In NSX-T Data Center werden IPSec-VPN-Dienste nur auf Tier-0-Gateways unterstützt, die im Hochverfügbarkeitsmodus Active-Standby ausgeführt werden müssen. Weitere Informationen finden Sie unter [Hinzufügen eines Tier-0-Gateways](#). Sie können Segmente verwenden, die mit Tier-0- oder Tier-1-Gateways verbunden sind, wenn Sie einen IPSec-VPN-Dienst konfigurieren.

Der IPsec-VPN-Dienst in NSX-T Data Center nutzt die Failover-Funktionalität auf Gateway-Ebene, um Hochverfügbarkeit zu unterstützen. Tunnel werden bei einem Failover neu eingerichtet und VPN-Konfigurationsdaten werden synchronisiert. Der Status des IPSec-VPN wird nicht synchronisiert, wenn Tunnel neu eingerichtet werden.

Authentifizierung mit vorinstalliertem Schlüssel und IP-Unicast-Datenverkehr werden zwischen dem NSX Edge-Knoten und Remote-VPN-Sites unterstützt. Darüber hinaus wird die Zertifikatsauthentifizierung ab NSX-T Data Center 2.4 unterstützt. Nur Zertifikatstypen, die mit einem der folgenden Hash-Signaturalgorithmen signiert sind, werden unterstützt.

- SHA256withRSA
- SHA384withRSA
- SHA512withRSA

NSX Edge unterstützt zwei Arten von IPSec-VPNs: richtlinienbasierte IPSec-VPNs und routenbasierte IPSec-VPNs.

## Verwendung von richtlinienbasiertem IPSec-VPN

Richtlinienbasiertes IPSec-VPN erfordert, dass eine VPN-Richtlinie auf Pakete angewendet wird, um festzustellen, welcher Datenverkehr durch IPSec geschützt werden soll, bevor er durch den VPN-Tunnel übergeben wird.

Diese Art von VPN wird als statisch angesehen, da bei Änderung einer lokalen Netzwerktopologie und -konfiguration auch die VPN-Richtlinieneinstellungen aktualisiert werden müssen, um den Änderungen Rechnung zu tragen.

Wenn Sie ein richtlinienbasiertes IPSec-VPN mit NSX-T Data Center verwenden, verbinden Sie mithilfe von IPSec-Tunneln ein oder mehrere lokale Subnetze hinter dem NSX Edge-Knoten mit den Peer-Subnetzen auf der Remote-VPN-Site.

Sie können einen NSX Edge-Knoten hinter einem NAT-Gerät bereitstellen. In dieser Bereitstellung übersetzt das NAT-Gerät die VPN-Adresse eines NSX Edge-Knotens in eine aus dem Internet zugängliche öffentliche Adresse. Remote-VPN-Sites verwenden diese öffentliche Adresse für den Zugriff auf den NSX Edge-Knoten.

Sie können Remote-VPN-Sites auch hinter einem NAT-Gerät platzieren. Zum Einrichten des IPSec-Tunnels müssen Sie die öffentliche IP-Adresse und die ID (FQDN oder IP-Adresse) der Remote-VPN-Site angeben. Für die VPN-Adresse ist auf beiden Seiten eine statische 1:1-Netzwerkadressübersetzung erforderlich.

Die Größe des NSX Edge-Knotens bestimmt die maximale Anzahl unterstützter Tunnel, wie in der folgenden Tabelle dargestellt.

**Tabelle 5-1. Anzahl der unterstützten IPSec-Tunnel**

Edge-Knotengröße	Anzahl der IPSec-Tunnel pro VPN-Sitzung (richtlinienbasiert)	Anzahl der Sitzungen pro VPN-Dienst	Anzahl der IPSec-Tunnel pro VPN-Dienst (16-Tunnel pro Sitzung)
Klein	N. v. (nur POC/Lab)	N. v. (nur POC/Lab)	N. v. (nur POC/Lab)
Mittel	128	128	2048
Groß	128 (weiche Grenze)	256	4096
Bare Metal	128 (weiche Grenze)	512	6000

**Einschränkung** Die vererbte Architektur des richtlinienbasierten IPSec-VPN schränkt Sie bei der Einrichtung einer VPN-Tunnel-Redundanz ein.

Weitere Informationen zum Konfigurieren eines richtlinienbasierten IPSec-VPN finden Sie unter [Hinzufügen eines IPSec-VPN-Dienstes](#).

## Verwenden von routenbasiertem IPSec-VPN

Routenbasierte IPSec-VPNs bieten Tunneling für Datenverkehr auf Basis der dynamisch über eine spezielle Schnittstelle (Virtual Tunnel Interface, VTI) erlernten Routen, indem z. B. BGP als

Protokoll verwendet wird. IPSec schützt den gesamten Datenverkehr, der über die VTI geleitet wird.

Das routenbasierte IPSec-VPN ähnelt GRE (Generic Routing Encapsulation) über IPSec mit der Ausnahme, dass dem Paket keine zusätzliche Kapselung hinzugefügt wird, bevor die IPSec-Verarbeitung angewendet wird.

Bei diesem VPN-Tunneling-Ansatz werden VTIs auf dem NSX Edge-Knoten erstellt. Jede VTI wird einem IPSec-Tunnel zugeordnet. Der verschlüsselte Datenverkehr wird über die VTI-Schnittstellen von einer Site zu einer anderen geleitet. Die IPSec-Verarbeitung erfolgt ausschließlich in der VTI.

## VPN-Tunnel-Redundanz

Sie können VPN-Tunnel-Redundanz mit einem routenbasierten IPSec-VPN-Dienst konfigurieren. Tunnel-Redundanz bietet unterbrechungsfreie Datenpfad-Konnektivität zwischen den beiden Sites, wenn der ISP-Link oder das Remote-VPN-Gateway fehlschlägt.

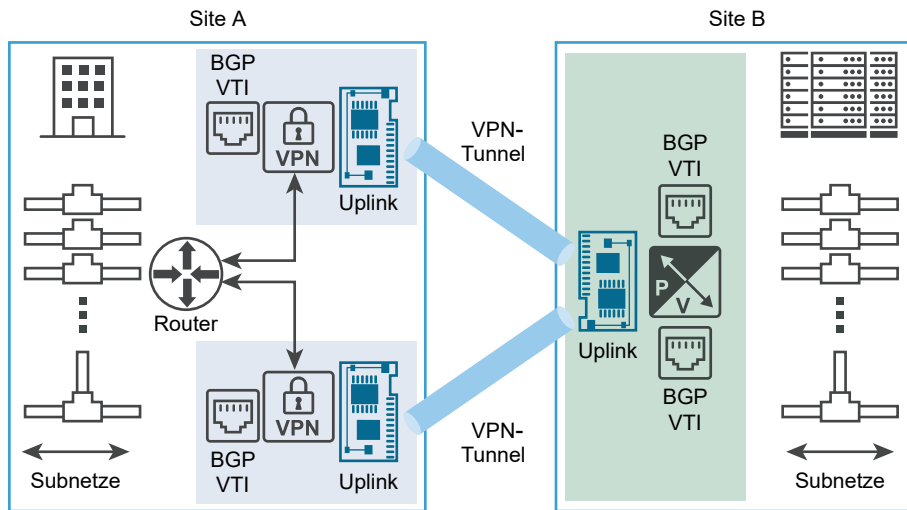
---

### Wichtig

- In NSX-T Data Center wird IPSec-VPN-Tunnel-Redundanz nur mithilfe von BGP unterstützt. Das dynamische OSPF-Routing wird nicht für das Routing über IPSec-VPN-Tunnel unterstützt.
  - Verwenden Sie kein statisches Routing für routenbasierte IPSec-VPN-Tunnel, um eine VPN-Tunnel-Redundanz zu erreichen.
- 

Die folgende Abbildung zeigt eine logische Darstellung der IPSec-VPN-Tunnel-Redundanz zwischen zwei Sites. In dieser Abbildung stellen Site A und Site B zwei Datacenter dar. In diesem Beispiel wird davon ausgegangen, dass NSX-T Data Center keine Edge-VPN-Gateways an Site A verwaltet und dass NSX-T Data Center eine virtuelle Edge-Gateway-Appliance an Site B verwaltet.

Abbildung 5-1. Tunnel-Redundanz in einem routenbasierten IPSec-VPN



Wie in der Abbildung gezeigt, können Sie zwei unabhängige IPSec-VPN-Tunnel mithilfe von VTIs konfigurieren. Das dynamische Routing wird mit einem BGP-Protokoll konfiguriert, um die Tunnel-Redundanz zu realisieren. Wenn beide IPSec-VPN-Tunnel verfügbar sind, werden beide weiterhin ausgeführt. Der gesamte Datenverkehr, der von Site A zu Site B über den NSX Edge-Knoten vorgesehen ist, wird über die VTI geleitet. Der Datenverkehr unterliegt der IPSec-Verarbeitung und verlässt die ihm zugeordnete Uplink-Schnittstelle des NSX Edge-Knotens. Der gesamte eingehende IPSec-Datenverkehr, der vom VPN-Gateway auf Site B an der Uplink-Schnittstelle des NSX Edge-Knotens empfangen wird, wird nach der Entschlüsselung an die VTI weitergeleitet. Im Anschluss daran erfolgt das normale Routing.

Sie müssen Werte für den BGP HoldDown-Timer und KeepAlive-Timer konfigurieren, um den Verlust der Konnektivität mit dem Peer innerhalb der erforderlichen Failover-Zeit erkennen zu können. Siehe [Konfigurieren des BGP-Protokolls](#).

Weitere Informationen zum Konfigurieren eines richtlinienbasierten IPSec-VPN finden Sie unter [Hinzufügen eines IPSec-VPN-Dienstes](#).

## Grundlegendes zu Layer 2-VPN

Mit Layer 2-VPN (L2 VPN) können Sie Layer 2-Netzwerke (VLANs oder VNIs) auf mehrere Sites in derselben Broadcast-Domäne erweitern. Virtuelle Maschinen (VMs) in Layer 2 können über L2 VPN nahtlos miteinander kommunizieren, auch wenn sie sich in verschiedenen Datacentern befinden.

Mit L2-VPN-Konnektivität können Layer 2-Netzwerke aus einem lokalen Datacenter auf die Cloud (z. B. VMware Cloud on Amazon, VMC) erweitert werden. Diese Verbindung ist mit einem routenbasierten IPSec-Tunnel zwischen dem L2-VPN-Client und dem L2-VPN-Server gesichert.

Jede L2-VPN-Sitzung verfügt über einen GRE-Tunnel (Generic Routing Encapsulation). Tunnelredundanz wird nicht unterstützt. Eine L2-VPN-Sitzung kann auf bis zu 4.094 Layer 2-Netzwerke erweitert werden.

L2-VPN-Dienste in NSX-T Data Center werden nur auf Tier-0-Gateways unterstützt. Segmente können entweder mit Tier-0- oder Tier-1-Gateways verbunden werden und L2-VPN-Dienste verwenden.

---

**Hinweis** Diese L2-VPN-Funktion ist nur für NSX-T Data Center verfügbar und weist keine Interoperabilität mit Drittanbietern auf.

---

Die Unterstützung für den L2-VPN-Dienst wird in folgenden Szenarien bereitgestellt.

- Zwischen einem L2-VPN-Server in NSX-T Data Center und einem L2-VPN-Client, der auf einer NSX Edge gehostet wird, die in einem NSX Data Center for vSphere verwaltet wird. Ein verwalteter L2-VPN-Client ist auf die Unterstützung virtueller Netzwerkkarten beschränkt.
- Zwischen einem L2-VPN-Server in NSX-T Data Center und einem L2-VPN-Client, der auf einer eigenständigen oder nicht verwalteten NSX Edge gehostet wird. Ein nicht verwalteter L2-VPN-Client unterstützt VLANs.
- Ab Version NSX-T Data Center 2.4 ist Unterstützung für den L2-VPN-Dienst zwischen einem L2-VPN-Server in NSX-T Data Center und L2-VPN-Clients in NSX-T Data Center verfügbar. In diesem Szenario können Sie die logischen L2-Segmente zwischen zwei lokalen softwaredefinierten Datencentern (SDDCs) erweitern.

Das erweiterte Netzwerk ist ein einzelnes Subnetz mit einer einzelnen Broadcast-Domäne. Somit verbleiben virtuelle Maschinen (VMs) im selben Subnetz, wenn sie zwischen Netzwerk-Sites verschoben werden, und ihre IP-Adressen bleiben gleich.

Sie können Arbeitslasten zwischen verschiedenen physischen Sites migrieren, wobei sich die zugehörigen IP-Adressen nicht ändern. Die Arbeitslasten können in VXLAN-basierten oder VLAN-basierten Netzwerken ausgeführt werden. Für Cloud-Anbieter stellt L2 VPN einen Mechanismus zur Integration von Mandanten zur Verfügung, ohne dass die bestehenden von den zugehörigen Arbeitslasten und Anwendungen verwendeten IP-Adressen geändert werden müssen.

Zusätzlich zur Unterstützung der Datencentermigration eignet sich ein mit einem L2 VPN erweitertes lokales Netzwerk für einen Notfallwiederherstellungsplan sowie für die dynamische Nutzung externer Computing-Ressourcen, um den erhöhten Bedarf zu decken.

## Hinzufügen von VPN-Diensten

Über die Benutzeroberfläche von NSX Manager können Sie entweder ein (richtlinienbasiertes oder routenbasiertes) IPSec-VPN oder ein L2-VPN hinzufügen.

In den folgenden Abschnitten finden Sie allgemeine Informationen zu den Workflows, die zum Einrichten des benötigten VPN-Dienstes erforderlich sind. In den nachfolgenden Themen in diesen Abschnitten wird beschrieben, wie Sie über die Benutzeroberfläche von NSX Manager entweder ein IPSec-VPN oder ein L2-VPN hinzufügen.



## Workflow für die Konfiguration eines richtlinienbasierten IPSec-VPN

Im Rahmen des Workflows für die Konfiguration eines richtlinienbasierten IPSec-VPN-Dienstes müssen Sie die folgenden allgemeinen Schritte ausführen:

- 1 Erstellen und aktivieren Sie einen IPSec-VPN-Dienst mithilfe eines vorhandenen Tier-0-Gateways. Siehe [Hinzufügen eines IPSec-VPN-Dienstes](#).
- 2 Erstellen Sie ein DPD-Profil (Dead Peer Detection), sofern Sie den Systemstandard nicht verwenden möchten. Siehe [Hinzufügen von DPD-Profilen](#).
- 3 Um ein IKE-Profil (Internet Key Exchange) zu verwenden, das sich vom Systemstandard unterscheidet, definieren Sie ein IKE-Profil. Siehe [Hinzufügen von IKE-Profilen](#).
- 4 Konfigurieren Sie ein IPSec-Profil mithilfe von [Hinzufügen von IPSec-Profilen](#).
- 5 Gehen Sie wie unter [Hinzufügen von lokalen Endpoints](#) beschrieben vor, um einen lokalen Endpoint zu erstellen.
- 6 Konfigurieren Sie eine richtlinienbasierte IPSec-VPN-Sitzung, wenden Sie die Profile an und hängen Sie den lokalen Endpoint dort an. Siehe [Hinzufügen einer richtlinienbasierten IPSec-Sitzung](#).

## Workflow für die Konfiguration eines routenbasierten IPSec-VPN

Im Rahmen des Workflows für die Konfiguration eines routenbasierten IPSec-VPN-Dienstes müssen Sie die folgenden allgemeinen Schritte ausführen:

- 1 Konfigurieren Sie einen IPSec-VPN-Dienst mithilfe eines vorhandenen Tier-0-Gateways und aktivieren Sie ihn. Siehe [Hinzufügen eines IPSec-VPN-Dienstes](#).
- 2 Geben Sie die lokalen Subnetze und Peer-Subnetze an, die für den Tunnel verwendet werden sollen.
- 3 Erstellen Sie ein DPD-Profil. Siehe [Hinzufügen von DPD-Profilen](#).
- 4 Definieren Sie ein IKE-Profil, sofern Sie das standardmäßige IKE-Profil nicht verwenden möchten. Siehe [Hinzufügen von IKE-Profilen](#).
- 5 Wenn Sie das standardmäßige IPSec-Profil des Systems nicht verwenden möchten, erstellen Sie eines mit [Hinzufügen von IPSec-Profilen](#).
- 6 Gehen Sie wie unter [Hinzufügen von lokalen Endpoints](#) beschrieben vor, um einen lokalen Endpoint hinzuzufügen.
- 7 Erstellen Sie eine routenbasierte IPSec-VPN-Sitzung. Siehe [Hinzufügen einer routenbasierten IPSec-Sitzung](#).

## Workflow für die Konfiguration eines L2-VPN

Für die Konfiguration eines L2-VPN müssen Sie einen L2-VPN-Dienst im Servermodus und dann einen anderen L2-VPN-Dienst im Clientmodus konfigurieren. Außerdem müssen Sie die Sitzungen für den L2-VPN-Server und den L2-VPN-Client konfigurieren. Nachfolgend wird ein allgemeiner Workflow zum Konfigurieren eines L2-VPN-Dienstes beschrieben.

- 1 Erstellen Sie einen L2 VPN-Dienst im Servermodus.
  - a Konfigurieren Sie einen routenbasierten IPSec-VPN-Tunnel mit einem Tier-0-Gateway und dann mithilfe dieses routenbasierten IPSec-Tunnels einen L2-VPN-Serverdienst. Siehe [Hinzufügen eines L2-VPN-Serverdienstes](#).
  - b Konfigurieren Sie eine L2-VPN-Serversitzung, die den neu erstellten routenbasierten IPSec-VPN-Dienst und den L2-VPN-Serverdienst bindet und die GRE-IP-Adressen automatisch zuweist. Siehe [Hinzufügen einer L2-VPN-Server-Sitzung](#).
  - c Fügen Sie den L2-VPN-Serversitzungen Segmente hinzu. Dieser Schritt wird auch in [Hinzufügen einer L2-VPN-Server-Sitzung](#) beschrieben.
  - d Ermitteln Sie mithilfe von [Herunterladen der L2-VPN-Konfiguration der Remote-Site](#) den Peer-Code für die Sitzung des L2-VPN-Serverdienstes. Die L2-VPN-Clientsitzung wird damit automatisch konfiguriert.
- 2 Erstellen Sie einen L2 VPN-Dienst im Clientmodus.
  - a Konfigurieren Sie einen weiteren routenbasierten IPSec-VPN-Dienst mit einem anderen Tier-0-Gateway und konfigurieren Sie dann mit diesem soeben konfigurierten Tier-0-Gateway einen L2-VPN-Clientdienst. Weitere Informationen finden Sie unter [Hinzufügen eines L2-VPN-Clientdienstes](#).
  - b Definieren Sie die L2-VPN-Clientsitzungen, indem Sie den vom L2-VPN-Serverdienst generierten Peer-Code importieren. Siehe [Hinzufügen einer L2-VPN-Clientsitzung](#).
  - c Fügen Sie den im vorherigen Schritt definierten L2-VPN-Clientsitzungen Segmente hinzu. Dieser Schritt wird unter [Hinzufügen einer L2-VPN-Clientsitzung](#) beschrieben.

## Hinzufügen eines IPSec-VPN-Dienstes

NSX-T Data Center unterstützt einen Site-to-Site-IPSec-VPN-Dienst zwischen einem Tier-0-Gateway und Remote-Sites. Sie können einen richtlinienbasierten oder einen routenbasierten IPSec-VPN-Dienst erstellen. Sie müssen zuerst den IPSec-VPN-Dienst erstellen, bevor Sie entweder eine richtlinienbasierte oder eine routenbasierte IPSec-VPN-Sitzung konfigurieren können.

---

**Hinweis** IPSec-VPNs werden in der NSX-T Data Center-Version mit Exportbeschränkung nicht unterstützt.

---

IPSec-VPN wird nicht unterstützt, wenn die IP-Adresse des lokalen Endpoints über NAT in denselben logischen Router geht, auf dem die IPSec-VPN-Sitzung konfiguriert ist.

## Voraussetzungen

- Machen Sie sich mit dem IPSec-VPN-Konzept vertraut. Siehe [Grundlegendes zu IPSec-VPNs](#).
- Mindestens ein Tier-O-Gateway muss konfiguriert und zur Verwendung verfügbar sein. Weitere Informationen hierzu finden Sie unter [Hinzufügen eines Tier-O-Gateways](#).

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Navigieren Sie zu **Netzwerk > VPN > VPN-Dienste**.
- 3 Wählen Sie **Dienst hinzufügen > IPSec** aus.
- 4 Geben Sie einen Namen für den IPSec-Dienst ein.  
Dieser Name ist erforderlich.
- 5 Wählen Sie im Dropdown-Menü **Tier-O-Gateway** das Tier-O-Gateway aus, das diesem IPSec-VPN-Dienst zugeordnet werden soll.
- 6 Aktivieren oder deaktivieren Sie **Verwaltungsstatus**.  
Standardmäßig ist der Wert auf **Enabled** festgelegt. Dies bedeutet, dass der IPSec-VPN-Dienst auf dem Tier-O-Gateway aktiviert wird, nachdem der neue IPSec-VPN-Dienst konfiguriert wurde.
- 7 Legen Sie den Wert für **IKE-Protokollebene** fest.  
Die IKE-Protokollierungsebene (Internet Key Exchange) bestimmt die Menge der Informationen, die Sie für den IPSec-VPN-Datenverkehr erfassen möchten. Als Standardeinstellung ist die Ebene **Info** festgelegt.
- 8 Geben Sie einen Wert für **Tags** ein, wenn Sie diesen Dienst in eine Tag-Gruppe aufnehmen möchten.
- 9 Klicken Sie auf **Globale Umgehungsregeln**, wenn Sie zulassen möchten, dass Datenpakete zwischen den angegebenen lokalen und Remote-IP-Adressen ohne IPSec-Schutz ausgetauscht werden, selbst wenn die IP-Adressen in den IPSec-Sitzungsregeln angegeben sind. Geben Sie unter **Lokale Netzwerke** und **Remote-Netzwerke** die Liste der lokalen Subnetze und der Remote-Subnetze ein, zwischen denen die Umgehungsregeln angewendet werden.

Standardmäßig wird der IPSec-Schutz verwendet, wenn Daten zwischen lokalen Sites und Remote-Sites ausgetauscht werden. Diese Regeln gelten für alle IPSec-VPN-Sitzungen, die innerhalb dieses IPSec-VPN-Dienstes erstellt werden.

**10** Klicken Sie auf **Speichern**.

Nachdem der neue IPSec-VPN-Dienst erfolgreich erstellt wurde, werden Sie gefragt, ob Sie mit der restlichen IPSec-VPN-Konfiguration fortfahren möchten. Wenn Sie auf **Ja** klicken, gelangen Sie wieder zum Bereich „IPSec-VPN-Dienst hinzufügen“. Der Link **Sitzung** ist jetzt aktiviert und Sie können darauf klicken, um eine IPSec-VPN-Sitzung hinzuzufügen.

**Nächste Schritte**

Die Informationen in [Hinzufügen von IPSec-VPN-Sitzungen](#) können Ihnen beim Hinzufügen einer IPSec-VPN-Sitzung als Anleitung dienen. Außerdem geben Sie Informationen zu den Profilen und zum lokalen Endpoint an, die erforderlich sind, um die IPSec-VPN-Konfiguration abzuschließen.

**Hinzufügen eines L2-VPN-Diensts**

Sie können einen L2-VPN-Dienst über einen IPSec-Tunnel konfigurieren, indem Sie zuerst einen routenbasierten IPSec-VPN-Tunnel erstellen. Anschließend konfigurieren Sie einen L2-VPN-Tunnel zwischen einem L2-VPN-Server (Ziel-Gateway) und einem L2-VPN-Client (Quell-Gateway), indem Sie den routenbasierten IPSec-VPN-Tunnel nutzen.

Zum Konfigurieren eines L2-VPN-Diensts über einen IPSec-Tunnel verwenden Sie die Informationen in den folgenden Themen in diesem Abschnitt.

**Voraussetzungen**

- Machen Sie sich mit IPsec-VPN und L2-VPN vertraut. Siehe [Grundlegendes zu IPSec-VPNs](#) und [Grundlegendes zu Layer 2-VPN](#).
- Mindestens ein Tier-0-Gateway muss konfiguriert und zur Verwendung verfügbar sein. Siehe [Hinzufügen eines Tier-0-Gateways](#).

**Verfahren****1** [Hinzufügen eines L2-VPN-Serverdienstes](#)

Um einen L2-VPN-Serverdienst zu konfigurieren, müssen Sie den L2-VPN-Dienst im Servermodus auf der Ziel-NSX Edge konfigurieren, mit der der L2-VPN-Client verbunden werden soll.

**2** [Hinzufügen eines L2-VPN-Clientdienstes](#)

Konfigurieren Sie nach dem L2-VPN-Server den L2-VPN-Dienst im Clientmodus auf einer anderen Edge-Instanz, bei der es sich um ein NSX-verwaltetes Edge, ein eigenständiges Edge oder ein NSX-T-Software-Defined Data Center (SDDC) handeln kann.

**Hinzufügen eines L2-VPN-Serverdienstes**

Um einen L2-VPN-Serverdienst zu konfigurieren, müssen Sie den L2-VPN-Dienst im Servermodus auf der Ziel-NSX Edge konfigurieren, mit der der L2-VPN-Client verbunden werden soll.

Bevor Sie einen L2-VPN-Server konfigurieren, müssen Sie zuerst einen routenbasierten IPSec-VPN-Tunnel erstellen. Anschließend erstellen Sie mithilfe dieses routenbasierten IPSec-VPN-Tunnels einen L2-VPN-Tunnel, der Ihre Schicht-2-Netzwerke zwischen zwei Sites ausdehnt.

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Erstellen Sie einen routenbasierten IPSec-Tunnel mit der NSX Edge, die Sie als L2-VPN-Servermodus konfigurieren möchten.
  - a Navigieren Sie zur Registerkarte **Netzwerk > VPN > VPN-Dienste** und wählen Sie **Dienst hinzufügen > IPSec** aus.
  - b Geben Sie einen Namen für den IPSec-VPN-Dienst ein.
  - c Wählen Sie im Dropdown-Menü **Tier-O-Gateway** ein Tier-O-Gateway aus, das mit dem L2-VPN-Server verwendet werden soll.
  - d Wenn Sie Werte verwenden möchten, die sich von den Systemstandardwerten unterscheiden, legen Sie die restlichen Eigenschaften im Bereich „IPSec-Dienst hinzufügen“ nach Bedarf fest.
  - e Klicken Sie auf **Speichern**. Wenn Sie gefragt werden, ob Sie mit der Konfiguration des IPSec-VPN-Dienstes fortfahren möchten, wählen Sie **Nein** aus.
- 3 Navigieren Sie zur Registerkarte **Netzwerk > VPN > VPN-Dienste**, und wählen Sie **Dienst hinzufügen > L2-VPN-Server** aus, um einen L2-VPN-Server zu erstellen.
- 4 Geben Sie einen Namen für den L2-VPN-Server ein.
- 5 Wählen Sie im Dropdown-Menü **Tier-O-Gateway** dasselbe Tier-O-Gateway aus, das Sie mit dem zuvor erstellten IPSec-Dienst verwendet haben.
- 6 Geben Sie eine optionale Beschreibung für diesen L2-VPN-Server ein.
- 7 Geben Sie einen Wert für **Tags** ein, wenn Sie diesen Dienst in eine Tag-Gruppe aufnehmen möchten.
- 8 Aktivieren oder deaktivieren Sie die **Hub-and-Spoke**-Eigenschaft.

Standardmäßig ist der Wert `Disabled` festgelegt. Das bedeutet, dass der von den L2-VPN-Clients empfangene Datenverkehr nur auf den mit dem L2-VPN-Server verbundenen Segmenten repliziert wird. Wenn diese Eigenschaft auf `Enabled` festgelegt ist, wird der Datenverkehr von einem beliebigen L2-VPN-Client auf allen anderen L2-VPN-Clients repliziert.

- 9 Klicken Sie auf **Speichern**.

Nachdem der neue L2-VPN-Server erfolgreich erstellt wurde, werden Sie gefragt, ob Sie mit der restlichen Konfiguration des L2-VPN-Dienstes fortfahren möchten. Wenn Sie auf **Ja** klicken, werden Sie zum Bereich „L2-VPN-Server hinzufügen“ zurückgeführt, und der Link **Sitzung** ist aktiviert. Über diesen Link können Sie eine L2-VPN-Serversitzung erstellen. Stattdessen können Sie auch die Registerkarte **Netzwerk > VPN > L2-VPN-Sitzungen** verwenden.

## Nächste Schritte

Konfigurieren Sie eine L2-VPN-Serversitzung für den L2-VPN-Server, den Sie anhand der Anleitung in [Hinzufügen einer L2-VPN-Server-Sitzung](#) konfiguriert haben.

## Hinzufügen eines L2-VPN-Clientdiensts

Konfigurieren Sie nach dem L2-VPN-Server den L2-VPN-Dienst im Clientmodus auf einer anderen Edge-Instanz, bei der es sich um ein NSX-verwaltetes Edge, ein eigenständiges Edge oder ein NSX-T-Software-Defined Data Center (SDDC) handeln kann.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Erstellen Sie einen routenbasierten IPSec-Tunnel für den L2-VPN-Clientdienst.
  - a Navigieren Sie zur Registerkarte **Netzwerk > VPN > VPN-Dienste** und wählen Sie **Dienst hinzufügen > IPSec** aus.
  - b Geben Sie einen Namen für den IPSec-VPN-Dienst ein.
  - c Wählen Sie im Dropdown-Menü **Tier-O-Gateway** ein Tier-O-Gateway aus, das mit dem L2-VPN-Client verwendet werden soll.
  - d Wenn Sie Werte verwenden möchten, die sich von den Systemstandardwerten unterscheiden, legen Sie die restlichen Eigenschaften im Bereich „IPSec-Dienst hinzufügen“ nach Bedarf fest.
  - e Klicken Sie auf **Speichern**. Wenn Sie gefragt werden, ob Sie mit der Konfiguration des IPSec-VPN-Dienstes fortfahren möchten, wählen Sie **Nein** aus.
- 3 Navigieren Sie zur Registerkarte **Netzwerk > VPN > VPN-Dienste** und wählen Sie **Dienst hinzufügen > L2-VPN-Client** aus.
- 4 Geben Sie einen Namen für den L2-VPN-Clientdienst ein.
- 5 Wählen Sie im Dropdown-Menü **Tier-O-Gateway** dasselbe Tier-O-Gateway aus, das Sie mit dem soeben erstellten routenbasierten IPSec-Tunnel verwendet haben.
- 6 Definieren Sie die anderen Eigenschaften im Bereich „L2-VPN-Client hinzufügen“, wenn Sie andere Werte als die Standardwerte des Systems verwenden möchten.
- 7 Klicken Sie auf **Speichern**.

Nach erfolgreicher Erstellung des neuen L2-VPN-Clientdiensts werden Sie gefragt, ob Sie mit der restlichen Konfiguration des L2-VPN-Clients fortfahren möchten. Wenn Sie auf **Ja** klicken, werden Sie zum Bereich „L2-VPN-Client hinzufügen“ zurückgeleitet und der Link **Sitzung** ist aktiviert. Sie können diesen Link zum Erstellen einer L2-VPN-Clientsitzung oder die Registerkarte **Netzwerk > VPN > L2-VPN-Sitzungen** verwenden.

## Nächste Schritte

Konfigurieren Sie eine L2-VPN-Clientsitzung für den von Ihnen konfigurierten L2-VPN-Clientdienst. Verwenden Sie die Informationen unter [Hinzufügen einer L2-VPN-Clientsitzung](#) als Leitfaden.

## Hinzufügen von IPSec-VPN-Sitzungen

Nachdem Sie einen IPSec-VPN-Dienst konfiguriert haben, müssen Sie je nach Typ des zu konfigurierenden IPSec-VPN entweder eine richtlinienbasierte IPSec-VPN-Sitzung oder eine routenbasierte IPSec-VPN-Sitzung hinzufügen. Außerdem geben Sie die Informationen für den lokalen Endpoint und die Profile an, die zum Abschließen der IPSec-VPN-Dienstkonfiguration verwendet werden sollen.

### Hinzufügen einer richtlinienbasierten IPSec-Sitzung

Wenn Sie ein richtlinienbasiertes IPSec-VPN hinzufügen, werden mithilfe von IPSec-Tunneln mehrere lokale Subnetze, die sich hinter dem NSX Edge-Knoten befinden, mit Peer-Subnetzen in der Remote-VPN-Site verbunden.

Bei den folgenden Schritten wird die Registerkarte **IPSec-Sitzungen** in der Benutzeroberfläche von NSX Manager verwendet, um eine richtlinienbasierte IPSec-Sitzung zu erstellen. Sie fügen außerdem Informationen für den Tunnel, IKE und DPD-Profil hinzu und wählen einen vorhandenen lokalen Endpoint aus, der mit dem richtlinienbasierten IPSec-VPN verwendet werden soll.

---

**Hinweis** Sie können auch die IPSec-VPN-Sitzungen sofort, nachdem Sie den IPSec-VPN-Dienst erfolgreich konfiguriert haben, hinzufügen. Sie klicken bei Aufforderung zum Fortfahren mit der IPSec-VPN-Dienstkonfiguration auf **Ja** und wählen im Bereich „IPSec-Sitzung hinzufügen“ **Sitzungen > Sitzungen hinzufügen** aus. Für die ersten Schritte im folgenden Verfahren wird davon ausgegangen, dass Sie **Nein** bei der Aufforderung zum Fortfahren mit der IPSec-VPN-Dienstkonfiguration ausgewählt haben. Wenn Sie **Ja** ausgewählt haben, gehen Sie in den folgenden Schritten weiter zu Schritt 3. Sie werden dann durch die restliche Konfiguration der richtlinienbasierten IPSec-VPN-Sitzung geführt.

---

### Voraussetzungen

- Sie müssen einen IPSec-VPN-Dienst konfiguriert haben, bevor Sie fortfahren können. Siehe [Hinzufügen eines IPSec-VPN-Dienstes](#).
- Holen Sie die Informationen für den lokalen Endpoint, die IP-Adresse für die Peer-Site, das lokale Netzwerk-Subnetz und das Remote-Netzwerk-Subnetz ein, die in der richtlinienbasierten IPSec-VPN-Sitzung verwendet werden sollen, die Sie hinzufügen. Informationen zum Erstellen eines lokalen Endpoints finden Sie unter [Hinzufügen von lokalen Endpoints](#).
- Wenn Sie einen vorinstallierten Schlüssel (PSK) für die Authentifizierung verwenden, rufen Sie den PSK-Wert ab.

- Wenn Sie ein Zertifikat für die Authentifizierung verwenden, stellen Sie sicher, dass die notwendigen Serverzertifikate und die entsprechenden ZS-signierten Zertifikate bereits importiert wurden. Siehe [Einrichten von Zertifikaten](#).
- Wenn Sie die von NSX-T Data Center bereitgestellten Standardeinstellungen für den IPSec-Tunnel, IKE oder Dead Peer Detection(DPD)-Profile nicht verwenden möchten, können Sie stattdessen die gewünschten Profile konfigurieren. Weitere Informationen finden Sie unter [Hinzufügen von Profilen](#).

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Navigieren zur Registerkarte **Netzwerk > VPN > IPSec-Sitzungen**.
- 3 Wählen Sie **IPSec-Sitzung hinzufügen > Richtlinienbasiert** aus.
- 4 Geben Sie einen Namen für die richtlinienbasierte IPSec-VPN-Sitzung ein.
- 5 Wählen Sie aus dem Dropdown-Menü **VPN-Dienst** den IPSec-VPN-Dienst aus, dem Sie diese neue IPSec-Sitzung hinzufügen möchten.

---

**Hinweis** Wenn Sie diese IPSec-Sitzung aus dem Dialogfeld **IPSec-Sitzungen hinzufügen** hinzufügen, wird der VPN-Dienst-Name bereits über der Schaltfläche **IPSec-Sitzung hinzufügen** angegeben.

---

- 6 Wählen Sie im Dropdown-Menü einen vorhandenen lokalen Endpoint aus.  
Dieser lokale Endpoint-Wert ist erforderlich und identifiziert den lokalen NSX Edge-Knoten. Wenn Sie einen anderen lokalen Endpoint erstellen möchten, klicken Sie auf das Drei-Punkte-Menü (⋮) und wählen Sie **Lokalen Endpoint hinzufügen**.
- 7 Geben Sie in das Textfeld **Remote-IP** die erforderliche IP-Adresse der Remote-Site ein.  
Dieser Wert ist erforderlich.
- 8 Geben Sie eine optionale Beschreibung für diese richtlinienbasierte IPSec-VPN-Sitzung ein.  
Die Längenbeschränkung beträgt 1024 Zeichen.
- 9 Klicken Sie zum Aktivieren oder Deaktivieren der IPSec-VPN-Sitzung auf **Verwaltungsstatus**.  
Als Standardwert ist **Enabled** festgelegt. Das bedeutet, dass die IPSec-VPN-Sitzung bis hinunter zum NSX Edge-Knoten konfiguriert werden muss.
- 10 Wählen Sie im Dropdown-Menü **Authentifizierungsmodus** einen Modus aus.  
Der verwendete Standard-Authentifizierungsmodus lautet PSK, d. h. ein geheimer Schlüssel, der zwischen NSX Edge und der Remote-Site gemeinsam verwendet wird, wird für die IPSec-VPN-Sitzung benutzt. Wenn Sie **Certificate** auswählen, wird das Sitezertifikat, das zum Konfigurieren des lokalen Endpoints verwendet wurde, für die Authentifizierung verwendet.



- 11** Wenn Sie PSK für den Authentifizierungsmodus ausgewählt haben, geben Sie den Schlüsselwert im Textfeld **Vorinstallierter Schlüssel** ein.

Dieser geheime Schlüssel kann eine Zeichenfolge mit einer Maximallänge von 128 Zeichen sein.

---

**Vorsicht** Seien Sie beim Freigeben und Speichern eines PSK-Werts vorsichtig, da er vertrauliche Informationen enthält.

---

- 12** Geben Sie in die Textfelder **Lokale Netzwerke** und **Remote-Netzwerke** mindestens eine IP-Subnetzadresse ein, die für diese richtlinienbasierte IPSec-VPN-Sitzung verwendet werden soll.

Diese Subnetze müssen im CIDR-Format vorliegen.

- 13** Geben Sie in **Remote-ID** einen Wert ein, um die Peer-Site anzugeben.

Bei Peer-Sites mit PSK-Authentifizierung muss dieser ID-Wert der öffentlichen IP-Adresse oder dem FQDN der Peer-Site entsprechen. Bei Peer-Sites mit Zertifikatsauthentifizierung muss dieser ID-Wert dem allgemeinen Namen (CN) oder dem definierten Namen (DN) im Zertifikat der Peer-Site entsprechen.

---

**Hinweis** Wenn das Zertifikat der Peer-Site eine E-Mail-Adresse in der DN-Zeichenfolge enthält, z. B.

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123/emailAddress=user1@mycompany.com
```

dann geben Sie den Wert für **Remote-ID** im gleichen Format wie in dem folgenden Beispiel ein.

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, MAILTO=user1@mycompany.com"
```

Wenn das Zertifikat der lokalen Site eine E-Mail-Adresse in der DN-Zeichenfolge enthält und die Peer-Site die strongSwan-IPsec-Implementierung verwendet, geben Sie den ID-Wert der lokalen Site in dieser Peer-Site ein, wie im folgenden Beispiel gezeigt.

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, E=user1@mycompany.com"
```

- 
- 14** Wenn Sie diese Sitzung als Teil einer bestimmten Gruppe aufnehmen möchten, geben Sie den Namen des Tags in **Tags** ein.

- 15** Um die Profile und den Initiierungsmodus, die von der richtlinienbasierten IPSec-VPN-Sitzung verwendet werden, zu ändern, klicken Sie auf **Profile und Initiierungsmodus**.

Standardmäßig werden die vom System generierte Profile verwendet. Wählen Sie ein anderes verfügbares Profil, wenn Sie nicht die Standardoption verwenden möchten. Wenn Sie ein Profil, das noch nicht konfiguriert ist, verwenden möchten, klicken Sie auf das Dreipunkte-Menü (⋮), um ein anderes Profil zu erstellen. Siehe [Hinzufügen von Profilen](#).

- a Wählen Sie im Dropdown-Menü **IKE-Profil** das zu verwendende IKE-Profil aus.
- b Wählen Sie das bevorzugte DPD-Profil aus dem Dropdown-Menü **DPD-Profil** aus.
- c Wählen Sie in **IPSec-Profil** das IPSec-Tunnel-Profil zur Verwendung mit der IPSec-Sitzung aus.
- d Wählen Sie im Dropdown-Menü **Verbindungs-Initiierungsmodus** den bevorzugten Modus aus.

Der Verbindungs-Initiierungsmodus definiert die Richtlinie, die vom lokalen Endpoint bei der Tunnel-Erstellung verwendet wird. Der Standardwert lautet **Initiator**. Die folgende Tabelle beschreibt die unterschiedlichen verfügbaren Verbindungs-Initiierungsmodi.

**Tabelle 5-2. Verbindungs-Initiierungsmodi**

Initiierungsmodus der Verbindung	Beschreibung
Initiator	Der Standardwert In diesem Modus initiiert der lokale Endpoint die IPSec-VPN-Tunnel-Erstellung und reagiert auf eingehende Anforderungen des Tunnel-Setups vom Peer-Gateway.
On Demand	In diesem Modus initiiert der lokale Endpoint die IPSec-VPN-Tunnel-Erstellung, nachdem das erste Paket, das mit der Richtlinienregel übereinstimmt, empfangen wird. Er reagiert auch auf die eingehende Initiierungsanforderung.
Respond Only	Der IPSec-VPN initiiert nie eine Verbindung. Die Peer-Site initiiert immer die Verbindungsanforderung, und der lokale Endpoint reagiert auf diese Verbindungsanfrage.

- 16** Klicken Sie auf **Speichern**.

### Ergebnisse

Wenn die neue richtlinienbasierte IPSec-VPN-Sitzung erfolgreich konfiguriert wurde, wird sie der Liste verfügbarer IPSec-VPN-Sitzungen hinzugefügt. Sie befindet sich im schreibgeschützten Modus.

### Nächste Schritte

- Stellen Sie sicher, dass der IPSec VPN-Tunnel-Status Aktiv ist. Weitere Informationen finden Sie unter [Überwachung und Fehlerbehebung von VPN-Sitzungen](#).

- Verwalten Sie bei Bedarf die Sitzungsinformationen für die IPSec-VPN, indem Sie auf das Drei-Punkte-Menü (⋮) auf der linken Seite der Sitzung Zeile klicken. Wählen Sie eine der Aktionen, die Sie berechtigt sind, durchführen.

## Hinzufügen einer routenbasierten IPSec-Sitzung

Wenn Sie ein routenbasiertes IPSec-VPN hinzufügen, wird Tunneling für Datenverkehr bereitgestellt, der auf Routen basiert, die dynamisch über eine virtuelle Tunnelschnittstelle (VTI) unter Verwendung eines bevorzugten Protokolls wie BGP erlernt wurden. IPSec schützt den gesamten Datenverkehr, der über die VTI geleitet wird.

Für die in diesem Thema verwendeten Schritte wird die Registerkarte **IPSec-Sitzungen** verwendet, um eine routenbasierte IPSec-Sitzung zu erstellen. Sie fügen auch Informationen für die Tunnel-, IKE- und DPD-Profil hinzu und wählen einen vorhandenen lokalen Endpoint aus, der mit dem routenbasierten IPSec-VPN verwendet werden soll.

---

**Hinweis** Sie können auch die IPSec-VPN-Sitzungen sofort, nachdem Sie den IPSec-VPN-Dienst erfolgreich konfiguriert haben, hinzufügen. Sie klicken bei Aufforderung zum Fortfahren mit der IPSec-VPN-Dienstkonfiguration auf **Ja** und wählen im Bereich „IPSec-Dienst hinzufügen“ **Sitzungen > Sitzungen hinzufügen** aus. Für die ersten Schritte im folgenden Verfahren wird davon ausgegangen, dass Sie **Nein** bei der Aufforderung zum Fortfahren mit der IPSec-VPN-Dienstkonfiguration ausgewählt haben. Falls Sie **Ja** ausgewählt haben, fahren Sie mit Schritt 3 in den folgenden Schritten fort, um Sie beim Rest der Konfiguration der routenbasierten IPSec-VPN-Sitzung anzuleiten.

---

### Voraussetzungen

- Sie müssen einen IPSec-VPN-Dienst konfiguriert haben, bevor Sie fortfahren können. Siehe [Hinzufügen eines IPSec-VPN-Dienstes](#).
- Besorgen Sie sich die Informationen für den lokalen Endpoint, die IP-Adresse für die Peer-Site und IP-Subnetz-Adresse des Tunnel-Diensts, die mit der routenbasierten IPSec-Sitzung verwendet werden soll, die Sie hinzufügen. Informationen zum Erstellen eines lokalen Endpoints finden Sie unter [Hinzufügen von lokalen Endpoints](#).
- Wenn Sie einen vorinstallierten Schlüssel (PSK) für die Authentifizierung verwenden, rufen Sie den PSK-Wert ab.
- Wenn Sie ein Zertifikat für die Authentifizierung verwenden, stellen Sie sicher, dass die notwendigen Serverzertifikate und die entsprechenden ZS-signierten Zertifikate bereits importiert wurden. Siehe [Einrichten von Zertifikaten](#).
- Wenn Sie nicht die Standardwerte für den IPSec-Tunnel, IKE oder DPD-Profil (Dead Peer Detection), die von NSX-T Data Center bereitgestellt werden, verwenden möchten, konfigurieren Sie die Profile, die Sie stattdessen verwenden möchten. Weitere Informationen finden Sie unter [Hinzufügen von Profilen](#).

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Navigieren Sie zu **Netzwerk > VPN > IPSec-Sitzungen**.
- 3 Wählen Sie **IPSec-Sitzung hinzufügen > Routenbasiert** aus.
- 4 Geben Sie einen Namen für die routenbasierte IPSec-Sitzung ein.
- 5 Wählen Sie aus dem Dropdown-Menü **VPN-Dienst** den IPSec-VPN-Dienst aus, dem Sie diese neue IPSec-Sitzung hinzufügen möchten.

---

**Hinweis** Wenn Sie diese IPSec-Sitzung aus dem Dialogfeld **IPSec-Sitzungen hinzufügen** hinzufügen, wird der VPN-Dienst-Name bereits über der Schaltfläche **IPSec-Sitzung hinzufügen** angegeben.

---

- 6 Wählen Sie im Dropdown-Menü einen vorhandenen lokalen Endpoint aus.  
Dieser lokale Endpoint-Wert ist erforderlich und identifiziert den lokalen NSX Edge-Knoten. Wenn Sie einen anderen lokalen Endpoint erstellen möchten, klicken Sie auf das Drei-Punkte-Menü (⋮) und wählen Sie **Lokalen Endpoint hinzufügen**.
- 7 Geben Sie im Textfeld **Remote-IP** die IP-Adresse der Remote-Site ein.  
Dieser Wert ist erforderlich.
- 8 Geben Sie eine optionale Beschreibung für diese routenbasierte IPSec-VPN-Sitzung ein.  
Die Längenbeschränkung beträgt 1024 Zeichen.
- 9 Klicken Sie zum Aktivieren oder Deaktivieren der IPSec-Sitzung auf **Administrativer Status**.  
Als Standardwert ist `Enabled` festgelegt. Das bedeutet, dass die IPSec-Sitzung bis hinunter zum NSX Edge-Knoten konfiguriert werden muss.
- 10 Wählen Sie im Dropdown-Menü **Authentifizierungsmodus** einen Modus aus.  
Der verwendete Standard-Authentifizierungsmodus lautet PSK, d. h. ein geheimer Schlüssel, der zwischen NSX Edge und der Remote-Site gemeinsam verwendet wird, muss für die IPSec-VPN-Sitzung verwendet werden. Wenn Sie `Certificate` auswählen, wird das Sitezertifikat, das zum Konfigurieren des lokalen Endpoints verwendet wurde, für die Authentifizierung verwendet.
- 11 Wenn Sie PSK für den Authentifizierungsmodus ausgewählt haben, geben Sie den Schlüsselwert im Textfeld **Vorinstallierter Schlüssel** ein.  
Dieser geheime Schlüssel kann eine Zeichenfolge mit einer Maximallänge von 128 Zeichen sein.

---

**Vorsicht** Seien Sie beim Freigeben und Speichern eines PSK-Werts vorsichtig, da er vertrauliche Informationen enthält.

---

- 12** Geben Sie eine IP-Subnetz-Adresse in **Tunnelschnittstelle** in der CIDR-Notation ein.

Diese Adresse ist erforderlich.

- 13** Geben Sie einen Wert **Remote-ID** ein.

Bei Peer-Sites mit PSK-Authentifizierung muss dieser ID-Wert der öffentlichen IP-Adresse oder dem FQDN der Peer-Site entsprechen. Bei Peer-Sites mit Zertifikatsauthentifizierung muss dieser ID-Wert dem allgemeinen Namen (CN) oder dem definierten Namen (DN) im Zertifikat der Peer-Site entsprechen.

**Hinweis** Wenn das Zertifikat der Peer-Site eine E-Mail-Adresse in der DN-Zeichenfolge enthält, z. B.

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123/emailAddress=user1@mycompany.com
```

dann geben Sie den Wert für **Remote-ID** im gleichen Format wie in dem folgenden Beispiel ein.

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, MAILTO=user1@mycompany.com"
```

Wenn das Zertifikat der lokalen Site eine E-Mail-Adresse in der DN-Zeichenfolge enthält und die Peer-Site die strongSwan-IPsec-Implementierung verwendet, geben Sie den ID-Wert der lokalen Site in dieser Peer-Site ein. Im Folgenden finden Sie ein Beispiel.

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, E=user1@mycompany.com"
```

- 14** Wenn Sie diese IPSec-Sitzung als Teil eines bestimmten Gruppentags einschließen möchten, geben Sie den Namen des Tags in **Tags** ein.
- 15** Um die Profile und den Initiierungsmodus, die von der routenbasierten IPSec-VPN-Sitzung verwendet werden, zu ändern, klicken Sie auf **Profile und Initiierungsmodus**.

Standardmäßig werden die vom System generierten Profile verwendet. Wählen Sie ein anderes verfügbares Profil, wenn Sie nicht die Standardoption verwenden möchten. Wenn Sie ein Profil verwenden möchten, das noch nicht konfiguriert ist, klicken Sie auf das Drei-Punkte-Menü (⋮), um ein anderes Profil zu erstellen. Siehe [Hinzufügen von Profilen](#).

- a Wählen Sie im Dropdown-Menü **IKE-Profile** das zu verwendende IKE-Profil aus.
- b Wählen Sie das bevorzugte DPD-Profil aus dem Dropdown-Menü **DPD-Profile** aus.

- c Wählen Sie in **IPSec-Profile** das IPSec-Tunnel-Profil zur Verwendung mit der IPSec-Sitzung aus.
- d Wählen Sie im Dropdown-Menü **Initiierungsmodus der Verbindung** den bevorzugten Modus aus.

Der Verbindungs-Initiierungsmodus definiert die Richtlinie, die vom lokalen Endpoint bei der Tunnel-Erstellung verwendet wird. Der Standardwert lautet **Initiator**. Die folgende Tabelle beschreibt die unterschiedlichen verfügbaren Verbindungs-Initiierungsmodi.

**Tabelle 5-3. Verbindungs-Initiierungsmodi**

Initiierungsmodus der Verbindung	Beschreibung
Initiator	Der Standardwert In diesem Modus initiiert der lokale Endpoint die IPSec-VPN-Tunnel-Erstellung und reagiert auf eingehende Anforderungen des Tunnel-Setups vom Peer-Gateway.
On Demand	Verwenden Sie diesen Modus nicht mit dem routenbasierten VPN. Dieser Modus gilt nur für das richtlinienbasierte VPN.
Respond Only	Der IPSec-VPN initiiert nie eine Verbindung. Die Peer-Site initiiert immer die Verbindungsanforderung, und der lokale Endpoint reagiert auf diese Verbindungsanfrage.

**16** Klicken Sie auf **Speichern**.

### Ergebnisse

Wenn die neue routenbasierte IPSec-VPN-Sitzung erfolgreich konfiguriert ist, wird sie zur Liste der verfügbaren IPSec-VPN-Sitzungen hinzugefügt. Sie befindet sich im schreibgeschützten Modus.

### Nächste Schritte

- Stellen Sie sicher, dass der IPSec VPN-Tunnel-Status Aktiv ist. Weitere Informationen finden Sie unter [Überwachung und Fehlerbehebung von VPN-Sitzungen](#).
- Konfigurieren Sie das Routing entweder mit einer statischen Route oder mit BGP. Siehe [Konfigurieren einer statischen Route](#) oder [Konfigurieren des BGP-Protokolls](#).
- Verwalten Sie bei Bedarf die Sitzungsinformationen für die IPSec-VPN, indem Sie auf das Drei-Punkte-Menü (⋮) auf der linken Seite der Sitzungszeile klicken. Wählen Sie eine der Aktionen aus, zu deren Durchführung Sie berechtigt sind.

## Hinzufügen von L2-VPN-Sitzungen

Nachdem Sie einen L2-VPN-Server und einen L2-VPN-Client konfiguriert haben, müssen Sie L2-VPN-Sitzungen für beide hinzufügen, um die Konfiguration des L2-VPN-Diensts abzuschließen.

## Hinzufügen einer L2-VPN-Server-Sitzung

Nach dem Erstellen eines L2-VPN-Server-Diensts müssen Sie eine L2-VPN-Sitzung hinzufügen und sie an ein vorhandenes Segment anhängen.

Die folgenden Schritte verwenden die Registerkarte **L2-VPN-Sitzungen** auf der NSX Manager-Benutzeroberfläche, um eine L2-VPN-Server-Sitzung zu erstellen. Sie können auch einen vorhandenen lokalen Endpoint und ein Segment auswählen, die an die L2-VPN-Server-Sitzung angehängt werden sollen.

---

**Hinweis** Sie können auch eine L2-VPN-Server-Sitzung sofort hinzufügen, nachdem Sie den L2-VPN-Server-Dienst erfolgreich konfiguriert haben. Sie klicken bei Aufforderung zum Fortfahren mit der L2-VPN-Serverkonfiguration auf **Ja** und wählen im Bereich „L2-VPN-Server hinzufügen“ **Sitzungen > Sitzungen hinzufügen** aus. Für die ersten Schritten im folgenden Verfahren wird davon ausgegangen, dass Sie **Nein** bei der Aufforderung zum Fortfahren mit der L2-VPN-Server-Konfiguration ausgewählt haben. Falls Sie **Ja** ausgewählt haben, fahren Sie mit Schritt 3 in den folgenden Schritten fort, um Sie beim Rest der Konfiguration der L2-VPN-Server-Sitzung anzuleiten.

---

### Voraussetzungen

- Sie müssen einen L2-VPN-Server-Dienst konfiguriert haben, bevor Sie fortfahren. Siehe [Hinzufügen eines L2-VPN-Serverdienstes](#).
- Rufen Sie die Informationen für den lokalen Endpoint und die Remote-IP-Adresse ab, die mit der L2-VPN-Server-Sitzung, die Sie gerade hinzufügen, verwendet werden sollen. Informationen zum Erstellen eines lokalen Endpoints finden Sie unter [Hinzufügen von lokalen Endpoints](#).
- Rufen Sie die Werte für den vorinstallierten Schlüssel (PSK) und das Subnetz der Tunnel-Schnittstelle ab, die mit der L2-VPN-Server-Sitzung verwendet werden soll.
- Rufen Sie den Namen des vorhandenen Segments ab, das Sie an die L2-VPN-Server-Sitzung, die Sie gerade erstellen, anhängen möchten. Weitere Informationen finden Sie unter [Hinzufügen eines Segments](#).

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Navigieren zur Registerkarte **Netzwerk > VPN > L2-VPN-Sitzungen**.
- 3 Wählen Sie **L2-VPN-Sitzung hinzufügen > L2-VPN-Server** aus.
- 4 Geben Sie einen Namen für die L2-VPN-Server-Sitzung ein.

- 5 Wählen Sie aus dem Dropdown-Menü **L2 VPN-Dienst** den L2-VPN-Server-Dienst aus, für den die L2 VPN-Sitzung gerade erstellt wird.

---

**Hinweis** Wenn Sie diese L2-VPN-Server-Sitzung über das Dialogfeld „L2VPN-Server-Sitzungen festlegen“ hinzufügen, wird der L2-VPN-Server-Dienst bereits über der Schaltfläche **L2-Sitzung hinzufügen** angegeben.

---

- 6 Wählen Sie im Dropdown-Menü einen vorhandenen lokalen Endpoint aus.  
Wenn Sie einen anderen lokalen Endpoint erstellen möchten, klicken Sie auf das Drei-Punkte-Menü (⋮) und wählen Sie **Lokalen Endpoint hinzufügen**.

- 7 Geben Sie die IP-Adresse der Remote-Sie ein.

- 8 Klicken Sie zum Aktivieren oder Deaktivieren der L2-VPN-Server-Sitzung auf **Administrativer Status**.

Standardmäßig ist der Wert auf **Aktiviert** festgelegt, was bedeutet, dass die L2-VPN-Server-Sitzung bis hinunter zum NSX Edge-Knoten konfiguriert werden muss.

- 9 Geben Sie den geheimen Schlüssel-Wert in **Vorinstallierter Schlüssel** ein.

---

**Vorsicht** Seien Sie beim Freigeben und Speichern eines PSK-Werts vorsichtig, da er vertrauliche Informationen enthält.

---

- 10 Geben Sie eine IP-Subnetz-Adresse in die **Tunnel Schnittstelle** mithilfe der CIDR-Notation ein.  
Zum Beispiel 4.5.6.6/24. Diese Subnetzadresse muss angegeben werden.

- 11 Geben Sie einen Wert in **Remote-ID** ein.

Bei Peer-Sites mit Zertifikatsauthentifizierung muss diese ID der allgemeine Name im Zertifikat des Peer-Sites sein. Bei PSK-Peers kann diese ID eine beliebige Zeichenfolge sein. Verwenden Sie vorzugsweise die öffentliche IP-Adresse des VPN oder einen FQDN für die VPN-Dienste als Remote ID.

- 12 Wenn Sie diese Sitzung als Teil einer bestimmten Gruppe aufnehmen möchten, geben Sie den Namen des Tags in **Tags** ein.

- 13 Klicken Sie auf **Speichern**, und klicken Sie auf **Ja**, wenn Sie aufgefordert werden, wenn Sie mit der Konfiguration des VPN-Dienstes fortfahren möchten.

Sie werden zum Fenster „L2VPN-Sitzungen hinzufügen“ zurückgeleitet, und der Link **Segmente** ist jetzt aktiviert.

- 14 Hängen Sie ein vorhandenes Segment an die L2-VPN-Server-Sitzung an.

- a Klicken Sie auf **Segmente > Segmente festlegen**.
- b Klicken Sie im Dialogfeld **Segmente festlegen** auf **Segment festlegen**, um ein vorhandenes Segment an die L2-VPN-Server-Sitzung anzuhängen.
- c Wählen Sie aus dem Dropdown-Menü **Segment** das Segment aus, das Sie an die Sitzung anhängen möchten.



- d Geben Sie einen Wert im Feld **VPN-Tunnel-ID** ein, der verwendet wird, um das von Ihnen ausgewählte Segment eindeutig zu identifizieren.
- e Klicken Sie auf **Speichern** und anschließend auf **Schließen**.

Im Bereich „L2VPN-Sitzungen festlegen“ im Dialogfeld hat das System die Anzahl für **Segmente** für die L2-VPN-Server-Sitzung erhöht.

- 15 Um die Konfiguration der L2-VPN-Server-Sitzung abzuschließen, klicken Sie auf **Bearbeitung schließen**.

### Ergebnisse

Auf der Registerkarte **VPN-Dienste** hat das System die Anzahl an **Sitzungen** für den L2-VPN-Server-Dienst erhöht, den Sie konfiguriert haben.

### Nächste Schritte

Um die Konfiguration des L2-VPN-Dienstes abzuschließen, müssen Sie auch einen L2-VPN-Dienst im Client-Modus und eine L2-VPN-Client-Sitzung erstellen. Siehe [Hinzufügen eines L2-VPN-Clientdiensts](#) und [Hinzufügen einer L2-VPN-Clientsitzung](#).

## Hinzufügen einer L2-VPN-Clientsitzung

Nach dem Erstellen eines L2-VPN-Clientdiensts müssen Sie eine L2-VPN-Clientsitzung hinzufügen und an ein vorhandenes Segment anhängen.

Bei den folgenden Schritten wird die Registerkarte **L2-VPN-Sitzungen** in der Benutzeroberfläche von NSX Manager verwendet, um eine L2-VPN-Clientsitzung zu erstellen. Sie können auch einen vorhandenen lokalen Endpoint und ein vorhandenes Segment auswählen, um diese an die L2-VPN-Clientsitzung anzuhängen.

---

**Hinweis** Sie können auch unmittelbar, nachdem Sie den L2-VPN-Clientdienst erfolgreich konfiguriert haben, eine L2-VPN-Clientsitzung hinzufügen. Klicken Sie auf **Ja**, wenn Sie aufgefordert werden, mit der Konfiguration des L2-VPN-Clients fortzufahren, und wählen Sie im Bereich „L2-VPN-Client hinzufügen“ **Sitzungen > Sitzungen hinzufügen** aus. In den ersten Schritten im folgenden Verfahren wird davon ausgegangen, dass Sie bei der Aufforderung, mit der Konfiguration des L2-VPN-Clients fortzufahren, **Nein** gewählt haben. Wenn Sie **Ja** ausgewählt haben, gehen Sie in den folgenden Schritten weiter zu Schritt 3. Sie werden dann durch die restliche Konfiguration der L2-VPN-Clientsitzung geführt.

---

### Voraussetzungen

- Sie müssen einen L2-VPN-Clientdienst konfiguriert haben, bevor Sie fortfahren. Siehe [Hinzufügen eines L2-VPN-Clientdiensts](#).
- Rufen Sie die IP-Adresseninformationen für die lokale IP und die Remote-IP ab, die mit der hinzugefügten L2-VPN-Clientsitzung verwendet werden sollen.
- Rufen Sie die Peer-Codes ab, die während der Konfiguration des L2-VPN-Servers generiert wurden. Siehe [Herunterladen der L2-VPN-Konfiguration der Remote-Site](#).

- Ermitteln Sie den Namen des vorhandenen Segments, das Sie an die von Ihnen erstellte L2-VPN-Clientsitzung anhängen möchten. Siehe [Hinzufügen eines Segments](#).

#### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk > VPN > L2-VPN-Sitzungen** aus.
- 3 Wählen Sie **L2-VPN-Sitzung hinzufügen > L2-VPN-Client** aus.
- 4 Geben Sie einen Namen für die L2-VPN-Clientsitzung ein.
- 5 Wählen Sie im Dropdown-Menü **VPN-Dienst** den L2-VPN-Clientdienst aus, dem die L2-VPN-Sitzung zugeordnet werden soll.

---

**Hinweis** Wenn Sie diese L2-VPN-Clientsitzung im Dialogfeld „L2-VPN-Clientsitzungen festlegen“ hinzufügen, wird der L2-VPN-Clientdienst bereits über der Schaltfläche **L2-Sitzung hinzufügen** angezeigt.

---

- 6 Geben Sie im Textfeld **Lokale IP-Adresse** die IP-Adresse der L2-VPN-Clientsitzung ein.
- 7 Geben Sie die Remote-IP-Adresse des IPSec-Tunnels ein, der für den L2-VPN-Clientdienst verwendet wird.
- 8 Geben Sie im Textfeld **Peer-Konfiguration** den Peer-Code ein, der bei der Konfiguration des L2-VPN-Serverdienstes generiert wurde.
  - a Navigieren Sie zu dem Speicherort, in dem Sie mit [Herunterladen der L2-VPN-Konfiguration der Remote-Site](#) die Datei `L2VPNSession_<L2VPN-Server-Session>_config.txt` heruntergeladen haben.
  - b Kopieren Sie den Inhalt der Datei und fügen Sie ihn in das Textfeld **Peer-Konfiguration** ein.
- 9 Aktivieren oder deaktivieren Sie **Verwaltungsstatus**.  
Standardmäßig ist der Wert auf **Aktiviert** festgelegt, was bedeutet, dass die L2-VPN-Server-Sitzung bis hinunter zum NSX Edge-Knoten konfiguriert werden muss.
- 10 Klicken Sie auf **Speichern**, und klicken Sie auf **Ja**, wenn Sie aufgefordert werden, wenn Sie mit der Konfiguration des VPN-Dienstes fortfahren möchten.
- 11 Hängen Sie ein vorhandenes Segment an die L2-VPN-Clientsitzung an.
  - a Wählen Sie **Segmente > Segmente hinzufügen** aus.
  - b Klicken Sie im Dialogfeld **Segmente festlegen** auf **Segment hinzufügen**.
  - c Wählen Sie im Dropdown-Menü **Segment** das Segment aus, das Sie an die L2-VPN-Serversitzung anhängen möchten.
  - d Geben Sie einen Wert in das Feld **VPN-Tunnel-ID** ein.
  - e Klicken Sie auf **Schließen**.

- 12 Klicken Sie auf **Bearbeiten schließen**, um die Konfiguration der L2-VPN-Clientsitzung abzuschließen.

### Ergebnisse

Auf der Registerkarte **VPN-Dienste** wird die Anzahl der Sitzungen für den konfigurierten L2-VPN-Clientdienst aktualisiert.

## Herunterladen der L2-VPN-Konfiguration der Remote-Site

Zum Konfigurieren der L2-VPN-Clientsitzung müssen Sie den Peer-Code abrufen, der bei der Konfiguration der L2-VPN-Serversitzung erzeugt wurde.

### Voraussetzungen

- Sie können erst fortfahren, wenn Sie einen L2-VPN-Serverdienst und eine Sitzung erfolgreich konfiguriert haben. Siehe [Hinzufügen eines L2-VPN-Serverdienstes](#).

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Navigieren zur Registerkarte **Netzwerk > VPN > L2-VPN-Sitzungen**.
- 3 Erweitern Sie in der Tabelle der L2-VPN-Sitzungen die Zeile für die L2-VPN-Serversitzung, die Sie zur Konfiguration der L2-VPN-Clientsitzung verwenden möchten.
- 4 Klicken Sie auf **Konfiguration herunterladen** und klicken Sie im Dialogfeld „Warnung“ auf **Ja**.

Eine Textdatei mit dem Namen `L2VPNSession_<name-of-L2-VPN-server-session>.config.txt` wird heruntergeladen. Sie enthält den Peer-Code für die L2-VPN-Konfiguration der Remotesite.

**Vorsicht** Passen Sie auf, wie Sie den Peer-Code speichern und freigeben, da er einen PSK-Wert enthält, bei dem es sich um vertrauliche Informationen handelt.

`L2VPNSession_L2VPNSess1_config.txt` enthält beispielsweise die folgende Konfiguration.

```
[{"transport_tunnel_path":"/infra/tier-0s/T0-gateway-1-AS/locale-services/1f309c00-277f-11e9-8074-a18943ad6b99/ipsec-vpn-services/IPS01-01/sessions/093ad8d0-2fad-11e9-8e5b-15a7211d1582",
"peer_code":"MCxiYTNjZmIwLHsic2l0ZU5hbWUiOiJMMlZQTi1MMLTZTXNzMSIsInNyY1RhcElwIjoiMTY5LjI1NC42NC4yIiwZHN0VGFWsXAiOiIxNjkuMjU0LjY0LjEiLCJpa2VpChRpb24iOiJpa2V2MiIsImVuY2FwUHJvdG8iOiJncmUvaXBzZWMiLCJkaEduY2VwIjoiZGxNCIsImVuY2J3JScHBBmREaWdlc3QiOiJhZXMtZ2NtL3NoYS0yNTYiLCJwc2siOiIxMTIyMz0NDU1NjYiLCJ0dW5uZWxzIjpbeyJsb2NhbnBzZW50IjoiNC41LjYyNiIsInBlZXJJZCI6IjEuMS4yLjIiLCJsb2NhbnBzZW50IjoiNC41LjYyMS8yNCJ9XX0="}]2NhbfZ0aUlwIjoiNC41LjYyMS8yNCJ9XX0="}]
```

## Nächste Schritte

Konfigurieren Sie den L2-VPN-Clientdienst und die L2-VPN-Clientsitzung. Siehe [Hinzufügen eines L2-VPN-Clientdiensts](#) und [Hinzufügen einer L2-VPN-Clientsitzung](#).

## Hinzufügen von lokalen Endpoints

Sie müssen einen lokalen Endpoint konfigurieren, der mit der IPSec-VPN verwendet werden soll, die Sie gerade konfigurieren.

Für die folgenden Schritte wird die Registerkarte **Lokale Endpoints** auf der NSX Manager-Benutzeroberfläche verwendet. Während Sie eine IPSec-VPN-Sitzung hinzufügen, können Sie auch einen lokalen Endpoint erstellen, indem Sie auf das Drei-Punkte-Menü (⋮) klicken und **Lokalen Endpoint hinzufügen** wählen. Wenn Sie gerade dabei sind, eine IPSec-VPN-Sitzung zu konfigurieren, fahren Sie mit Schritt 3 in den folgenden Schritten fort, die Sie bei der Erstellung eines neuen lokalen Endpoints anleiten sollen.

### Voraussetzungen

- Wenn Sie einen zertifikatbasierten Authentifizierungsmodus für die IPSec-VPN-Sitzung verwenden, der den lokalen Endpoint verwenden soll, welchen Sie gerade konfigurieren, rufen Sie die Information über das Zertifikat ab, das der lokale Endpoint verwenden muss.
- Stellen Sie sicher, dass Sie einen IPSec-VPN-Dienst konfiguriert haben, dem dieser lokale Endpoint zugeordnet werden soll.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wechseln Sie zu **Netzwerk > VPN > Lokale Endpoints** und klicken Sie auf **Lokalen Endpoint hinzufügen**.
- 3 Geben Sie einen Namen für den lokalen Endpoint ein.
- 4 Wählen Sie aus dem Dropdown-Menü **VPN-Dienst** den IPSec-VPN-Dienst aus, mit dem dieser lokale Endpoint verknüpft werden soll.
- 5 Geben Sie eine IP-Adresse oder einen lokalen Endpoint ein.
- 6 Wenn Sie einen zertifikatbasierten Authentifizierungsmodus für die IPSec-VPN-Sitzung verwenden, wählen Sie aus dem Dropdown-Menü **Site-Zertifikat** das Zertifikat aus, das vom lokalen Endpoint verwendet werden soll.
- 7 Geben Sie den Wert für die **Lokale ID** ein, die zum Identifizieren der lokalen NSX Edge-Instanz verwendet werden soll.

Diese lokale ID ist die Peer-ID auf der Remote-Site. Die lokale ID muss entweder die öffentliche IP-Adresse oder der FQDN der Remote-Site sein. Für zertifikatsbasierte VPN-

Verbindungen, die mithilfe des lokalen Endpoints definiert wurden, wird die lokale ID aus dem Zertifikat abgeleitet, das dem lokalen Endpoint zugeordnet ist. Die ID, die im Textfeld **Lokale ID** angegeben ist, wird ignoriert. Die vom Zertifikat für eine VPN-Sitzung abgeleitete lokale ID hängt von den im Zertifikat vorhandenen Erweiterungen ab.

- Wenn die X509v3-Erweiterung X509v3 Subject Alternative Name nicht im Zertifikat vorhanden ist, wird der Distinguished Name (DN) als lokaler ID-Wert verwendet.
- Wenn die X509v3-Erweiterung X509v3 Subject Alternative Name im Zertifikat gefunden wird, wird einer der alternativen Antragstellernamen als lokaler ID-Wert verwendet.

- 8 Wählen Sie aus den Dropdown-Menüs **Vertrauenswürdiges CA-Zertifikat** und **Vertrauenswürdiges CLR-Zertifikat** die entsprechenden erforderlichen Zertifikate.
- 9 Geben Sie bei Bedarf ein Tag an.
- 10 Klicken Sie auf **Speichern**.

## Hinzufügen von Profilen

NSX-T Data Center stellt das vom System generierte IPSec-Tunnelprofil und ein IKE-Profil bereit, die standardmäßig zugewiesen werden, wenn Sie einen IPSec-VPN- oder L2-VPN-Dienst konfigurieren. Für eine IPSec-VPN-Konfiguration wird ein vom System generiertes DPD-Profil erstellt.

Die IKE- und IPSec-Profile enthalten Informationen zu den Algorithmen, die zum Authentifizieren, Verschlüsseln und Einrichten eines gemeinsamen geheimen Schlüssels zwischen Netzwerk-Sites verwendet werden. Das DPD-Profil liefert Informationen darüber, wie viele Sekunden zwischen den Prüfpunkten abgewartet werden muss.

Wenn Sie die von NSX-T Data Center bereitgestellten Standardprofile nicht verwenden möchten, können Sie stattdessen anhand der Informationen in den nachfolgenden Themen in diesem Abschnitt eigene Profile konfigurieren.

## Hinzufügen von IKE-Profilen

Die IKE-Profile (Internet Key Exchange) enthalten Informationen zu den Algorithmen, die zum Authentifizieren, Verschlüsseln und Einrichten eines gemeinsamen geheimen Schlüssels zwischen Netzwerk-Sites verwendet werden, wenn Sie einen IKE-Tunnel einrichten.

NSX-T Data Center bietet vom System generierte IKE-Profile, die standardmäßig zugewiesen werden, wenn Sie einen IPSec-VPN- oder L2-VPN-Dienst konfigurieren. In der folgenden Tabelle sind die bereitgestellten Standardprofile aufgeführt.

Tabelle 5-4. Für IPSec-VPN- oder L2-VPN-Dienste verwendete standardmäßige IKE-Profile

Name des Standard-IKE-Profils	Beschreibung
nsx-default-l2vpn-ike-profile	<ul style="list-style-type: none"> <li>■ Wird für eine L2-VPN-Dienstkonfiguration verwendet.</li> <li>■ Mit IKE V2, Verschlüsselungsalgorithmus AES 128, Algorithmus SHA2 256 und Schlüsselaustauschalgorithmus Diffie-Hellman Group 14 konfiguriert.</li> </ul>
nsx-default-l3vpn-ike-profile	<ul style="list-style-type: none"> <li>■ Wird für eine IPSec-VPN-Dienstkonfiguration verwendet.</li> <li>■ Mit IKE V2, Verschlüsselungsalgorithmus AES 128, Algorithmus SHA2 256 und Schlüsselaustauschalgorithmus Diffie-Hellman Group 14 konfiguriert.</li> </ul>

Wenn Sie sich gegen die Verwendung der bereitgestellten standardmäßigen IKE-Profile entscheiden, können Sie Ihre eigenen Profile konfigurieren. Gehen Sie dazu wie folgt vor:

#### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Klicken Sie auf die Registerkarte **Netzwerk > VPN > Profile**.
- 3 Wählen Sie den Profiltyp **IKE-Profile** aus und klicken Sie auf **IKE-Profil hinzufügen**.
- 4 Geben Sie einen Namen für das IKE-Profil ein.
- 5 Wählen Sie im Dropdown-Menü **IKE-Version** die IKE-Version aus, die bei der Einrichtung einer Sicherheitsverbindung (SA) in der IPSec-Protokollsuite verwendet werden soll.

Tabelle 5-5. IKE-Versionen

IKE-Version	Beschreibung
IKEv1	Wenn diese Version ausgewählt wurde, initiiert das IPSec-VPN nur ein IKEv1-Protokoll und reagiert darauf.
IKEv2	Dies ist die Standardversion. Wenn diese Version ausgewählt wurde, initiiert das IPSec-VPN nur ein IKEv2-Protokoll und reagiert darauf.
IKE-Flex	Wenn diese Version ausgewählt wurde und der Tunnelaufbau mit dem IKEv2-Protokoll fehlschlägt, wird nicht auf die Quell-Site zurückgegriffen und es wird auch keine Verbindung mit dem IKEv1-Protokoll initiiert. Stattdessen wird die Verbindung akzeptiert, wenn die Remote-Site eine Verbindung mit dem IKEv1-Protokoll initiiert.

- 6 Wählen Sie in den Dropdown-Menüs die Verschlüsselungs-, Digest- und Diffie-Hellman Group-Algorithmen aus. Sie können mehrere Algorithmen auswählen, die angewendet werden sollen, oder die Auswahl aller ausgewählten Algorithmen aufheben, die nicht angewendet werden sollen.

Tabelle 5-6. Verwendete Algorithmen

Art des Algorithmus	Gültige Werte	Beschreibung
Verschlüsselung	<ul style="list-style-type: none"> <li>■ AES 128 (Standard)</li> <li>■ AES 256</li> <li>■ AES GCM 128</li> <li>■ AES GCM 192</li> <li>■ AES GCM 256</li> </ul>	<p>Der Verschlüsselungsalgorithmus, der während der IKE-Verhandlung (Internet Key Exchange) verwendet wird.</p> <p>Die AES-GCM-Algorithmen werden bei Verwendung mit IKEv2 unterstützt. Sie werden nicht unterstützt, wenn Sie mit IKEv1 verwendet werden.</p>
Digest	<ul style="list-style-type: none"> <li>■ SHA2 256 (Standard)</li> <li>■ SHA 1</li> <li>■ SHA2 384</li> <li>■ SHA2 512</li> </ul>	<p>Der sichere Hashing-Algorithmus, der während der IKE-Verhandlung verwendet wird.</p> <p>Wenn AES-GCM der einzige im Textfeld <b>Verschlüsselungsalgorithmus</b> ausgewählte Verschlüsselungsalgorithmus ist, können gemäß Abschnitt 8 in RFC 5282 im Textfeld <b>Digest-Algorithmus</b> keine Hash-Algorithmen angegeben werden. Darüber hinaus wird der Pseudo-Random Function-(PRF-)Algorithmus PRF-HMAC-SHA2-256 implizit ausgewählt und in der Aushandlung der IKE-Sicherheitsverbindung verwendet. Der Algorithmus PRF-HMAC-SHA2-256 muss auch auf dem Peer-Gateway konfiguriert werden, damit die Phase 1 der IKE-SA-Aushandlung erfolgreich ausgeführt werden kann.</p> <p>Wenn im Textfeld <b>Verschlüsselungsalgorithmus</b> zusätzlich zum AES-GCM-Algorithmus weitere Algorithmen angegeben sind, können im Textfeld <b>Digest-Algorithmus</b> mehrere Hash-Algorithmen ausgewählt werden. Darüber hinaus wird der in der IKE-SA-Aushandlung verwendete PRF-Algorithmus implizit basierend auf den konfigurierten Hash-Algorithmen bestimmt. Mindestens einer der übereinstimmenden PRF-Algorithmen muss auch auf dem Peer-Gateway konfiguriert sein, damit die Phase 1 der IKE-SA-Verhandlung erfolgreich ausgeführt werden kann. Wenn beispielsweise das Textfeld <b>Verschlüsselungsalgorithmus</b> „AES 128“ und „AES GCM 128“ enthält und „SHA1“ im Textfeld <b>Digest-Algorithmus</b> angegeben ist, wird der Algorithmus PRF-HMAC-SHA1 während der IKE-SA-Aushandlung verwendet. Dieser muss dann auch im Peer-Gateway konfiguriert werden.</p>
Diffie-Hellman Group	<ul style="list-style-type: none"> <li>■ Gruppe 14 (Standard)</li> <li>■ Gruppe 2</li> <li>■ Gruppe 5</li> <li>■ Gruppe 15</li> </ul>	<p>Die Kryptografieschemata, die die Peer-Site und die NSX Edge verwenden, um einen gemeinsamen geheimen Schlüssel über einen unsicheren Kommunikationskanal zu etablieren.</p>

Tabelle 5-6. Verwendete Algorithmen (Fortsetzung)

Art des Algorithmus	Gültige Werte	Beschreibung
	■ Gruppe 16	
	■ Gruppe 19	
	■ Gruppe 20	
	■ Gruppe 21	

**Hinweis** Wenn Sie versuchen, einen IPSec-VPN-Tunnel mit einem GUARD-VPN-Client (zuvor QuickSec-VPN-Client) unter Verwendung von zwei Verschlüsselungsalgorithmen oder zwei Digest-Algorithmen einzurichten, fügt der GUARD-VPN-Client zusätzliche Algorithmen in die vorgeschlagene Aushandlungsliste ein. Wenn Sie beispielsweise AES 128 und AES 256 als Verschlüsselungsalgorithmen sowie SHA2 256 und SHA2 512 als Digest-Algorithmen angegeben haben, die im IKE-Profil verwendet werden sollen, das Sie zum Aufbau des IPSec-VPN-Tunnels verwenden, schlägt der GUARD-VPN-Client auch AES 192 und SHA2 384 in der Aushandlungsliste vor. In diesem Fall verwendet NSX-T Data Center den ersten Verschlüsselungsalgorithmus, den Sie beim Einrichten des IPSec-VPN-Tunnels ausgewählt haben.

- 7 Geben Sie einen Lebensdauerwert der Sicherheitsverbindung (SA) in Sekunden ein, wenn ein anderer Wert als der Standardwert von 86400 Sekunden (24 Stunden) verwendet werden soll.
- 8 Geben Sie eine Beschreibung an und fügen Sie nach Bedarf ein Tag hinzu.
- 9 Klicken Sie auf **Speichern**.

### Ergebnisse

Der Tabelle der verfügbaren IKE-Profile wird eine neue Zeile hinzugefügt. Um ein nicht vom System erstelltes Profil zu bearbeiten oder zu löschen, klicken Sie auf das Dreipunkt-Menü (⋮) und wählen Sie aus der Liste der verfügbaren Aktionen eine aus.

## Hinzufügen von IPSec-Profilen

Die IPSec-Profile (Internet Protocol Security) enthalten Informationen zu den Algorithmen, die zum Authentifizieren, Verschlüsseln und Einrichten eines gemeinsamen geheimen Schlüssels zwischen Netzwerk-Sites verwendet werden, wenn Sie einen IPSec-Tunnel einrichten.

NSX-T Data Center bietet vom System generierte IPSec-Profile, die standardmäßig zugewiesen werden, wenn Sie einen IPSec-VPN- oder L2-VPN-Dienst konfigurieren. In der folgenden Tabelle sind die bereitgestellten Standardprofile aufgeführt.



Tabelle 5-7. Für IPSec-VPN- oder L2-VPN-Dienste verwendete standardmäßige IPSec-Profile

Dateiname des standardmäßigen IPSec-Profils	Beschreibung
nsx-default-l2vpn-tunnel-profile	<ul style="list-style-type: none"> <li>■ Wird für das L2-VPN verwendet.</li> <li>■ Mit dem Verschlüsselungsalgorithmus AES GCM 128 und dem Schlüsselaustauschalgorithmus Diffie-Hellman Group 14 konfiguriert.</li> </ul>
nsx-default-l3vpn-tunnel-profile	<ul style="list-style-type: none"> <li>■ Wird für das IPSec-VPN verwendet.</li> <li>■ Mit dem Verschlüsselungsalgorithmus AES GCM 128 und dem Schlüsselaustauschalgorithmus Diffie-Hellman Group 14 konfiguriert.</li> </ul>

Wenn Sie sich gegen die Verwendung der bereitgestellten standardmäßigen IPSec-Profile entscheiden, können Sie Ihre eigenen Profile konfigurieren. Gehen Sie dazu wie folgt vor:

#### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Navigieren zur Registerkarte **Netzwerk > VPN > Profile**.
- 3 Wählen Sie den Profiltyp **IPSec-Profile** aus und klicken Sie auf **IPSec-Profil hinzufügen**.
- 4 Geben Sie einen Namen für das IPSec-Profil ein.
- 5 Wählen Sie in den Dropdown-Menüs die Verschlüsselungs-, Digest- und Diffie-Hellman-Algorithmen aus. Sie können mehrere Algorithmen auswählen, die angewendet werden sollen.  
Deaktivieren Sie diejenigen, die Sie nicht verwenden möchten.
- 6 Deaktivieren Sie **PFS-Gruppe**, wenn Sie das PFS-Gruppenprotokoll bei Ihrem VPN-Dienst nicht verwenden möchten.  
Standardmäßig ist diese Option aktiviert.
- 7 Ändern Sie im Textfeld **SA-Lebensdauer** die Standardanzahl von Sekunden, bevor der IPSec-Tunnel wieder hergestellt werden muss.  
Standardmäßig wird eine SA-Lebensdauer von 24 Stunden (86400 Sekunden) verwendet.
- 8 Wählen Sie den Wert für das **DF-Bit**, das mit dem IPSec-Tunnel verwendet werden soll.  
Der Wert bestimmt, wie mit dem in dem empfangenen Datenpaket enthaltene DF-Bit (Don't Fragment, „Nicht fragmentieren“) verfahren wird. Die zulässigen Werte werden in der folgenden Tabelle beschrieben.

Tabelle 5-8. DF-Bit-Werte

DF-Bit-Wert	Beschreibung
COPY	Der Standardwert. Wenn dieser Wert ausgewählt ist, kopiert NSX-T Data Center den Wert des DF-Bits aus dem empfangenen Paket in das weitergeleitete Paket. Wenn im empfangenen Datenpaket das DF-Bit gesetzt ist, bedeutet dieser Wert, dass das DF-Bit im Paket nach der Verschlüsselung ebenfalls gesetzt ist.
CLEAR	Wenn dieser Wert ausgewählt ist, ignoriert NSX-T Data Center den Wert der des DF-Bits im empfangenen Datenpaket und das DF-Bit ist im verschlüsselten Paket immer 0.

9 Geben Sie eine Beschreibung an und fügen Sie bei Bedarf ein Tag hinzu.

10 Klicken Sie auf **Speichern**.

### Ergebnisse

Der Tabelle der verfügbaren IPSec-Profile wird eine neue Zeile hinzugefügt. Um ein nicht vom System erstelltes Profil zu bearbeiten oder zu löschen, klicken Sie auf das Dreipunkt-Menü (⋮) und wählen Sie aus der Liste der verfügbaren Aktionen eine aus.

## Hinzufügen von DPD-Profilen

Ein DPD-Profil (Dead Peer Detection) enthält Informationen zur Anzahl der Sekunden, die zwischen Prüfungen gewartet werden muss, um zu erkennen, ob ein IPSec-Peer aktiv ist.

NSX-T Data Center stellt ein vom System erzeugtes DPD-Profil mit der Bezeichnung `nsx-default-l3vpn-dpd-profile` bereit, das beim Konfigurieren des IPSec-VPN-Diensts standardmäßig zugewiesen wird.

Wenn Sie das DPD-Standardprofil nicht verwenden möchten, können Sie Ihr eigenes Profil mithilfe der folgenden Schritte konfigurieren.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Navigieren Sie zu **Netzwerk > VPN > Profile**.
- 3 Wählen Sie den Profiltyp **DPD-Profil** aus und klicken Sie auf **DPD-Profil hinzufügen**.
- 4 Geben Sie einen Namen für das DPD-Profil ein.
- 5 Geben Sie im Textfeld **DPD-Prüfintervall** die Anzahl der Sekunden ein, die NSX-T Data Center warten soll, bevor der nächste DPD-Prüfpunkt gesendet wird. Die Standardeinstellung ist 60 Sekunden.

Wenn der NSX Edge-Knoten eine Antwort von der Remote-Peer-Site erhält, wird der Timer des DPD-Prüfintervalls neu gestartet. Wenn der NSX Edge-Knoten nicht innerhalb von 0,5 Sekunden nach dem Senden des nächsten DPD-Prüfpunkts eine Antwort von der Peer-

Site erhält, wird ein Neuübertragungs-Timer auf 0,5 Sekunden festgelegt. Der NSX Edge-Knoten überträgt den nächsten DPD-Prüfpunkt erneut, nachdem der Timer für die erneute Übertragung erreicht wurde. Wenn die Remote-Peer-Site weiterhin nicht antwortet, wird der Timer für die erneute Übertragung exponentiell auf den Maximalwert von 6 Sekunden erhöht. Der NSX Edge-Knoten sendet die DPD-Prüfung weiterhin jedes Mal erneut, wenn der Timer für die erneute Übertragung abläuft. Der NSX Edge-Knoten wiederholt die Übertragung bis zu 30-mal, bevor er die Peer-Site als inaktiv deklariert und die Sicherheitsverbindung auf dem Link des inaktiven Peers abbricht. Die Gesamtzeit für die 30 Wiederholungen der Übertragung des DPD-Prüfpunkts beträgt etwa 2 Minuten und 45 Sekunden.

**6** Geben Sie eine Beschreibung an und fügen Sie nach Bedarf ein Tag hinzu.

**7** Klicken Sie auf **Speichern**.

### Ergebnisse

Der Tabelle der verfügbaren DPD-Profilen wird eine neue Zeile hinzugefügt. Um ein nicht vom System erstelltes Profil zu bearbeiten oder zu löschen, klicken Sie auf das Dreipunkt-Menü (⋮) und wählen Sie aus der Liste der verfügbaren Aktionen eine aus.

## Überprüfen des realisierten Zustands einer IPSec-VPN-Sitzung

Nachdem Sie eine Anfrage zum Aktualisieren der Konfiguration für eine IPSec-VPN-Sitzung gesendet haben, können Sie überprüfen, ob der angeforderte Status in der lokalen NSX-T Data Center-Control Plane auf den Transportknoten erfolgreich verarbeitet wurde.

Wenn Sie eine IPSec-VPN-Sitzung erstellen, werden mehrere Entitäten angelegt: IKE-Profil, DPD-Profil, Tunnelprofil, lokaler Endpoint, IPSec-VPN-Dienst und IPSec-VPN-Sitzung. Diese Entitäten verwenden gemeinsam denselben `IPSecVPNSession-Span`, damit Sie den Umsetzungsstatus aller Entitäten der IPSec-VPN-Sitzung mithilfe desselben GET-API-Aufrufs abrufen können. Sie können den Umsetzungsstatus nur mithilfe der API überprüfen.

### Voraussetzungen

- Machen Sie sich mit IPSec-VPN vertraut. Siehe [Grundlegendes zu IPSec-VPNs](#).
- Stellen Sie sicher, dass das IPSec-VPN erfolgreich konfiguriert wurde. Siehe [Hinzufügen eines IPSec-VPN-Dienstes](#).
- Sie müssen auf die NSX Manager-API zugreifen können.

### Verfahren

**1** Senden Sie einen API-Aufruf für eine POST-, PUT- oder DELETE-Anforderung.

Beispiel:

```
PUT https://<nsx-mgr>/api/v1/vpn/ipsec/sessions/8dd1c386-9b2c-4448-85b8-51ff649fae4f
{
  "resource_type": "PolicyBasedIPSecVPNSession",
  "id": "8dd1c386-9b2c-4448-85b8-51ff649fae4f",
  "display_name": "Test RZ_UPDATED",
  "ipsec_vpn_service_id": "7adfa455-a6fc-4934-a919-f5728957364c",
  "peer_endpoint_id": "17263ca6-dce4-4c29-bd8a-e7d12bd1a82d",
  "local_endpoint_id": "91ebfa0a-820f-41ab-bd87-f0fb1f24e7c8",
  "enabled": true,
  "policy_rules": [
    {
      "id": "1026",
      "sources": [
        {
          "subnet": "1.1.1.0/24"
        }
      ],
      "logged": true,
      "destinations": [
        {
          "subnet": "2.1.4..0/24"
        }
      ],
      "action": "PROTECT",
      "enabled": true,
      "_revision": 1
    }
  ]
}
```

- 2 Suchen Sie nach dem Wert von x-nsx-requestid und kopieren Sie ihn aus dem zurückgegebenen Antwort-Header.

Beispiel:

```
x-nsx-requestid    e550100d-f722-40cc-9de6-cf84d3da3ccb
```

- 3 Fordern Sie den Umsetzungsstatus der IPSec-VPN-Sitzung mithilfe des folgenden GET-Aufrufs an.

```
GET https://<nsx-mgr>/api/v1/vpn/ipsec/sessions/<ipsec-vpn-session-id>/state?request_id=<request-id>
```

Der folgende API-Aufruf verwendet die Werte id und x-nsx-requestid in den Beispielen aus den vorherigen Schritten.

```
GET https://<nsx-mgr>/api/v1/vpn/ipsec/sessions/8dd1c386-9b2c-4448-85b8-51ff649fae4f/state?
request_id=e550100d-f722-40cc-9de6-cf84d3da3ccb
```

Bei Folgendem handelt es sich um eine Beispielantwort, die Sie bei einem Umsetzungsstatus von `in_progress` erhalten.

```
{
  "details": [
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "fe651e63-04bd-43a4-a8ec-45381a3b71b9",
      "state": "in_progress",
      "failure_message": "CCP Id:ab5958df-d98a-468e-a72b-d89dcdae5346, Message:State realization is in progress at the node."
    },
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "ebe174ac-e4f1-4135-ba72-3dd2eb7099e3",
      "state": "in_sync"
    }
  ],
  "state": "in_progress",
  "failure_message": "The state realization is in progress at transport nodes."
}
```

Bei Folgendem handelt es sich um eine Beispielantwort, die Sie bei einem Umsetzungsstatus von `in_sync` erhalten.

```
{
  "details": [
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "7046e8f4-a680-11e8-9bc3-020020593f59",
      "state": "in_sync"
    }
  ],
  "state": "in_sync"
}
```

Bei Folgendem handelt es sich um mögliche Beispielantworten, die Sie bei einem Umsetzungsstatus von `unknown` erhalten.

```
{
  "state": "unknown",
  "failure_message": "Unable to get response from any CCP node. Please retry operation after some time."
}
```

```
{
  "details": [
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "3e643776-5def-11e8-94ae-020022e7749b",
      "state": "unknown",
      "failure_message": "CCP Id:ab5958df-d98a-468e-a72b-d89dcdae5346, Message: Unable to get response from the node. Please retry operation after some time."
    }
  ]
}
```

```

    },
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "4784ca0a-5def-11e8-93be-020022f94b73",
      "state": "in_sync"
    }
  ],
  "state": "unknown",
  "failure_message": "The state realization is unknown at transport nodes"
}

```

Nach dem Durchführen eines DELETE-Vorgangs für eine Entität erhalten Sie unter Umständen den Status NOT\_FOUND (siehe folgendes Beispiel).

```

{
  "http_status": "NOT_FOUND",
  "error_code": 600,
  "module_name": "common-services",
  "error_message": "The operation failed because object identifier LogicalRouter/61746f54-7ab8-4702-93fe-6ddeb804 is missing: Object identifiers are case sensitive.."
}

```

Wenn der mit der Sitzung verknüpfte IPSec-VPN-Dienst deaktiviert ist, erhalten Sie die Antwort BAD\_REQUEST (siehe folgendes Beispiel).

```

{
  "httpStatus": "BAD_REQUEST",
  "error_code": 110199,
  "module_name": "VPN",
  "error_message": "VPN service f9cfe508-05e3-4e1d-b253-fed096bb2b63 associated with the session 8dd1c386-9b2c-4448-85b8-51ff649fae4f is disabled. Can not get the realization status."
}

```

## Überwachung und Fehlerbehebung von VPN-Sitzungen

Nach der Konfiguration einer IPSec- oder L2-VPN-Sitzung können Sie den Status des VPN-Tunnels überwachen und Fehlerbehebung für alle gemeldeten Tunnelprobleme mithilfe der NSX Manager-Benutzeroberfläche durchführen.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Navigieren Sie zur Registerkarte **Netzwerk > VPN > IPSec-Sitzungen** oder **Netzwerk > VPN > L2-VPN-Sitzungen**.
- 3 Erweitern Sie die Zeile für die VPN-Sitzung, die überwacht oder für die eine Fehlerbehebung durchgeführt werden soll.

- 4 Zum Anzeigen des Status des VPN-Tunnels klicken Sie auf das Infosymbol.

Das Dialogfeld „Status“ mit den verfügbaren Status wird angezeigt.

- 5 Klicken Sie zum Anzeigen der Datenverkehrsstatistiken des VPN-Tunnels in der Spalte „Status“ auf **Statistik anzeigen**.

Im Dialogfeld „Statistik“ wird die Datenverkehrsstatistik für den VPN-Tunnel angezeigt.

- 6 Klicken Sie zum Anzeigen der Fehlerstatistik im Dialogfeld „Statistik“ auf die Verknüpfung **Mehr anzeigen**.

- 7 Klicken Sie zum Schließen des Dialogfelds **Statistik** auf **Schließen**.

# Netzwerkadressübersetzung (NAT)

# 6

Bei der Netzwerkadressübersetzung (NAT) wird ein IP-Adressbereich einem anderen zugeordnet. Sie können NAT auf Tier-0- und Tier-1-Gateways konfigurieren.

Dieses Kapitel enthält die folgenden Themen:

- Konfigurieren von NAT auf einem Gateway

## Konfigurieren von NAT auf einem Gateway

Sie können Quell-NAT (SNAT), Ziel-NAT (DNAT) oder reflexive NAT auf einem Tier-0- oder Tier-1-Gateway konfigurieren.

Wenn ein Tier-0-Gateway im Modus „Aktiv/Aktiv“ ausgeführt wird, können Sie weder SNAT noch DNAT konfigurieren, da asymmetrische Pfade unter Umständen zu Problemen führen. Sie können nur reflexive NAT (gelegentlich als „statusfreie NAT“ bezeichnet) konfigurieren. Wenn ein Tier-0-Gateway im Modus „Aktiv/Standby“ ausgeführt wird, können Sie SNAT, DNAT oder reflexive NAT konfigurieren.

Sie können SNAT oder DNAT auch für eine IP-Adresse oder einen Adressbereich deaktivieren. Weist eine Adresse mehrere NAT-Regeln auf, wird die Regel mit der höchsten Priorität angewendet.

Auf der externen Schnittstelle eines logischen Tier-0-Gateways konfigurierte SNAT verarbeitet Datenverkehr aus einem Tier-1-Gateway sowie aus einer anderen externen Schnittstelle auf dem Tier-0-Gateway.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk > NAT**.
- 3 Wählen Sie ein Gateway aus.
- 4 Klicken Sie auf **NAT-Regel hinzufügen**.



**5** Wählen Sie eine Aktion aus.

Für ein Tier-1-Gateway lauten die verfügbaren Aktionen **SNAT**, **DNAT**, **Reflexiv**, **KEINE SNAT** und **KEINE DNAT**.

Für ein Tier-0-Gateway im Modus „Aktiv/Standby“ lauten die verfügbaren Aktionen **SNAT**, **DNAT**, **KEINE SNAT** und **KEINE DNAT**.

Für ein Tier-0-Gateway im Modus „Aktiv/Aktiv“ steht die Aktion **Reflexiv** zur Verfügung.

**6** Klicken Sie in der Spalte **Dienst** auf **Festlegen**, um Dienste auszuwählen.

**7** (Erforderlich) Geben Sie für **Quell-IP** eine IP-Adresse oder einen IP-Adressbereich im CIDR-Format an.

Wenn Sie dieses Feld leer lassen, gilt diese NAT-Regel für alle Quellen außerhalb des lokalen Subnetzes.

**8** Geben Sie für **Ziel-IP** eine IP-Adresse oder einen IP-Adressbereich im CIDR-Format an.

**9** Geben Sie für **Übersetzte IP** eine IP-Adresse oder einen IP-Adressbereich im CIDR-Format an.

**10** Geben Sie einen Wert für **Übersetzter Port** ein.

**11** Wählen Sie eine FirewallEinstellung aus den folgenden Optionen aus:

- **Externe Adresse abgleichen:** Das Paket wird von Firewallregeln verarbeitet, die der Kombination aus übersetzter IP-Adresse und übersetztem Port entsprechen.
- **Interne Adresse abgleichen:** Das Paket wird von Firewallregeln verarbeitet, die der Kombination aus ursprünglicher IP-Adresse und ursprünglichem Port entsprechen.
- **Umgehung:** Das Paket umgeht Firewallregeln.

**12** (Erforderlich) Ändern Sie den Status der Protokollierung.

**13** (Erforderlich) Wählen Sie für **Angewendet auf** die Objekte aus, für die diese Regel gilt.

Zu den verfügbaren Objekten gehören **Tier-0-Gateways**, **Schnittstellen**, **Bezeichnungen**, **Dienstinstanz-Endpoints** und **Virtuelle Endpoints**.

**14** Geben Sie einen Prioritätswert an.

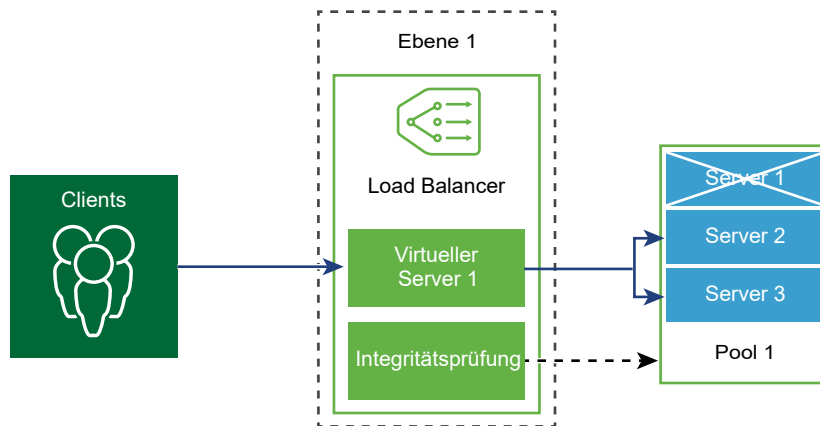
Ein niedrigerer Wert bedeutet eine höhere Priorität. Die Standardeinstellung ist 100.

**15** Klicken Sie auf **Speichern**.

# Lastausgleich

# 7

Der logische NSX-T Data Center-Load Balancer bietet einen Hochverfügbarkeitsdienst für Anwendungen und verteilt die Datenverkehrslast im Netzwerk auf mehrere Server.



Der Load Balancer verteilt eingehende Dienstanforderungen über mehrere Server gleichmäßig auf eine Weise, dass die Lastverteilung für die Benutzer transparent ist. Der Lastausgleich trägt dazu dabei, optimale Ressourcennutzung, maximalen Durchsatz und minimale Reaktionszeit zu erreichen sowie Überlastung zu vermeiden.

Sie können eine virtuelle IP-Adresse mehreren Poolservern für den Lastausgleich zuordnen. Der Load Balancer akzeptiert TCP-, UDP-, HTTP- oder HTTPS-Anforderungen über die virtuelle IP-Adresse und entscheidet, welcher Poolserver verwendet werden soll.

Abhängig von den Umgebungsanforderungen können Sie die Load Balancer-Leistung skalieren, indem Sie die Anzahl der vorhandenen virtuellen Server und Poolmitglieder zur Verarbeitung hoher Datenverkehrslasten erhöhen.

---

**Hinweis** Der logische Load Balancer wird nur auf dem Tier-1-Gateway unterstützt. Ein Load Balancer kann nur an ein Tier-1-Gateway angehängt werden.

---

Dieses Kapitel enthält die folgenden Themen:

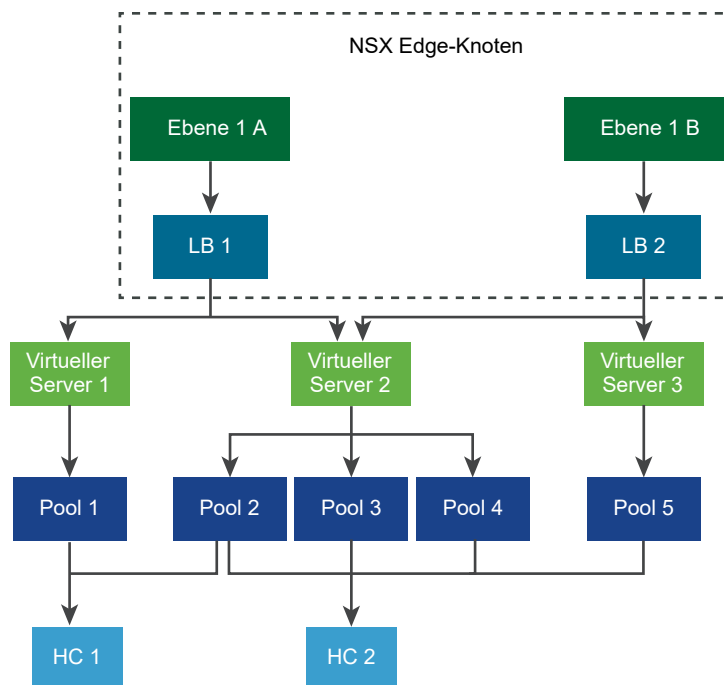
- [Wichtige Load Balancer-Konzepte](#)
- [Einrichten von Load Balancer-Komponenten](#)

## Wichtige Load Balancer-Konzepte

Der Load Balancer beinhaltet virtuelle Server, Serverpools und Systemdiagnoseüberwachungen.

Ein Load Balancer ist mit einem logischen Tier-1-Router verbunden. Der Load Balancer hostet einen einzelnen oder mehrere virtuelle Server. Bei einem virtuellen Server handelt es sich um einen Anwendungsdienst, der durch eine eindeutige Kombination aus IP, Port und Protokoll dargestellt wird. Der virtuelle Server ist einem einzelnen Serverpool oder mehreren Serverpools zugeordnet. Ein Serverpool besteht aus einer Gruppe von Servern. Die Serverpools enthalten einzelne Mitglieder des Serverpools.

Wenn Sie die ordnungsgemäße Ausführung der Anwendung auf jedem Server prüfen möchten, können Sie Systemdiagnoseüberwachungen hinzufügen, die den Systemzustand eines Servers überprüfen.



## Skalieren von Load Balancer-Ressourcen

Load Balancer sind in den Größen klein, mittel und groß verfügbar. Je nach Größe des Load Balancers kann dieser verschiedene virtuelle Server und Poolmitglieder hosten.

---

**Hinweis** Auf der Registerkarte **Netzwerk und Sicherheit – Erweitert** wird der Begriff logischer Tier-1-Router verwendet, um ein Ebene-1-Gateway zu beschreiben.

---

Tabelle 7-1. Load Balancer-Größe für den Load-Balancer-Dienst

<b>Load Balancer-Dienst</b>	<b>Kleiner Load Balancer</b>	<b>Mittlerer Load Balancer</b>	<b>Großer Load Balancer</b>
Anzahl der virtuellen Server pro Load Balancer	20	100	1000
Anzahl der Pools pro Load Balancer	60	300	3000
Anzahl der Poolmitglieder pro Load Balancer	300	2000	7500

Ein Load Balancer ist an einen logischen Tier-1-Router angehängt. Dieser logische Tier-1-Router, der sich im Aktiv-Standby-Modus befinden muss, wird auf den NSX Edge-Knoten gehostet.

NSX Edge hat den Formfaktor BareMetal sowie kleine, mittlere und große VM-Appliances. Je nach Formfaktor kann der NSX Edge-Knoten unterschiedliche viele Load Balancer hosten.

Tabelle 7-2. Load Balancer-Größe für NSX Edge-Knoten

<b>Load Balancer pro NSX Edge-Knoten</b>	<b>Kleiner Load Balancer</b>	<b>Mittlerer Load Balancer</b>	<b>Großer Load Balancer</b>	<b>Maximale Anzahl Poolmitglieder</b>
NSX Edge-VM – Klein	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar
NSX Edge VM - Mittel	1	Nicht verfügbar	Nicht verfügbar	300
NSX Edge-VM – Groß	40	4	1	7500
NSX Edge-VM – Bare Metal	750	75	18	30.000

## Unterstützte Load Balancer-Funktionen

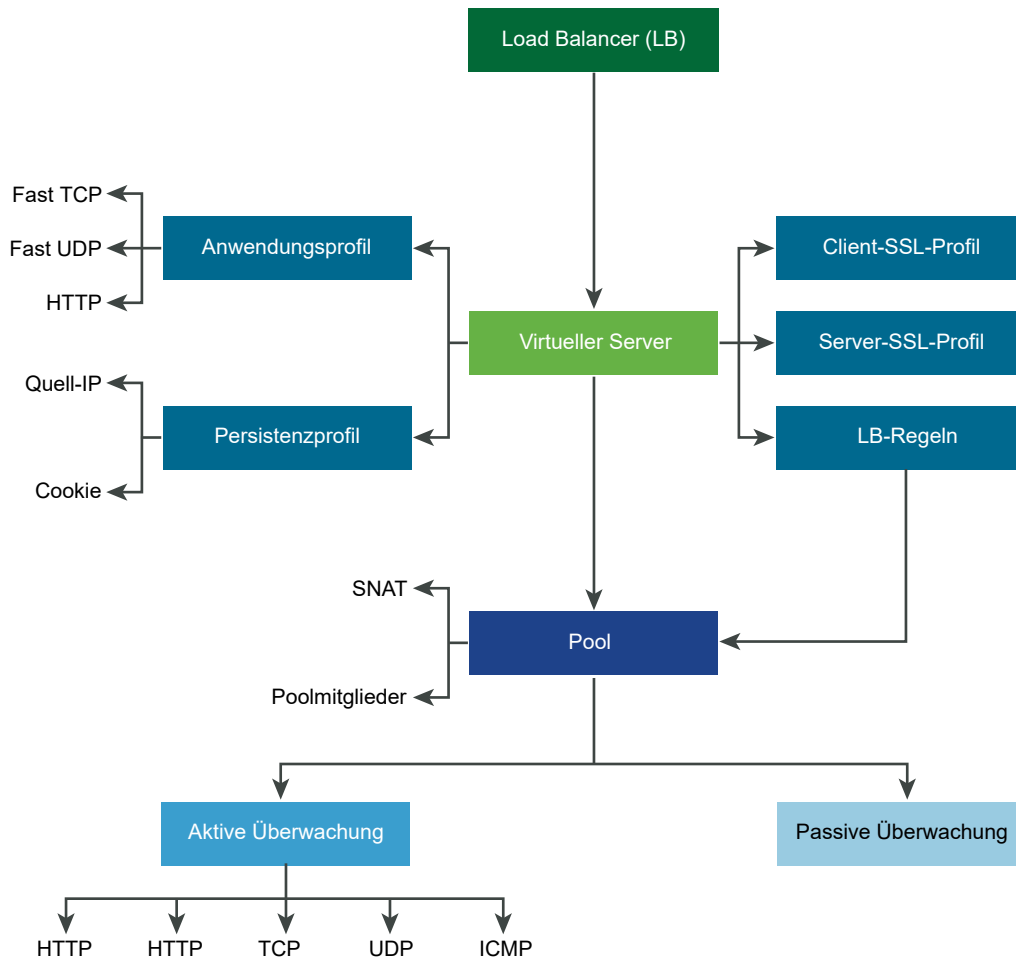
Der NSX-T Data Center-Load Balancer unterstützt die folgenden Funktionen:

- Schicht 4 – TCP und UDP
- Schicht 7 – HTTP und HTTPS mit Unterstützung von Load Balancer-Regeln
- Serverpools – Statisch und dynamisch mit NSGroup
- Persistenz – Quell-IP- und Cookie-Persistenzmodus
- Systemdiagnoseüberwachungen – Aktive Überwachung, die HTTP, HTTPS, TCP, UDP und ICMP sowie die passive Überwachung beinhaltet
- SNAT – Transparent, automatische Zuordnung und IP-Liste

- HTTP Upgrade – bei Anwendungen, die HTTP Upgrade nutzen wie z. B. WebSocket, werden vom Client oder Server HTTP Upgrade-Anforderungen übermittelt, was unterstützt wird. NSX-T Data Center unterstützt und akzeptiert standardmäßig HTTPS Upgrade-Anforderungen von Clients über das HTTP-Anwendungsprofil.

Um eine inaktive Client- oder Server-Kommunikation zu erkennen, verwendet der Load Balancer die Antwortzeitüberschreitungsfunktion des HTTP-Anwendungsprofils, die auf 60 Sekunden eingestellt ist. Wenn der Server während des 60-Sekunden-Intervalls keine Daten sendet, beendet NSX-T Data Center die Verbindung auf Client- und Serverseite.

Hinweis: Der SSL-Beendigungs- und der SSL-Proxymodus werden in der NSX-T Data Center Limited Export-Version nicht unterstützt.

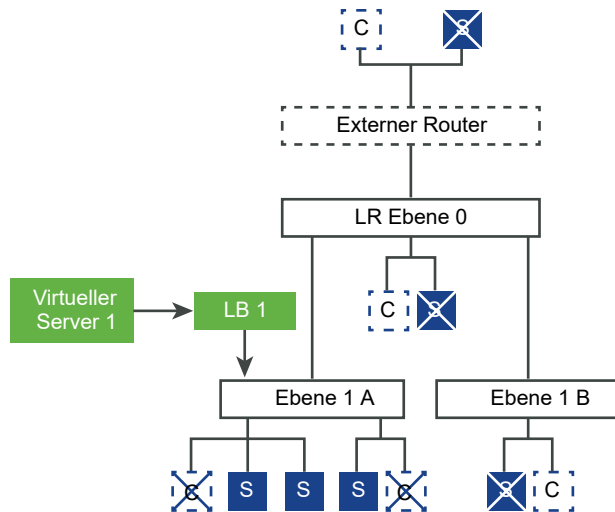


## Load Balancer-Topologien

Load Balancer werden üblicherweise im Inline- oder One-Arm-Modus (einarmer Modus) bereitgestellt. Der einarmige Modus erfordert die Konfiguration der virtuellen Quell-NAT (SNAT), und der Inlinemodus ist nicht möglich.

## Inline-Topologie

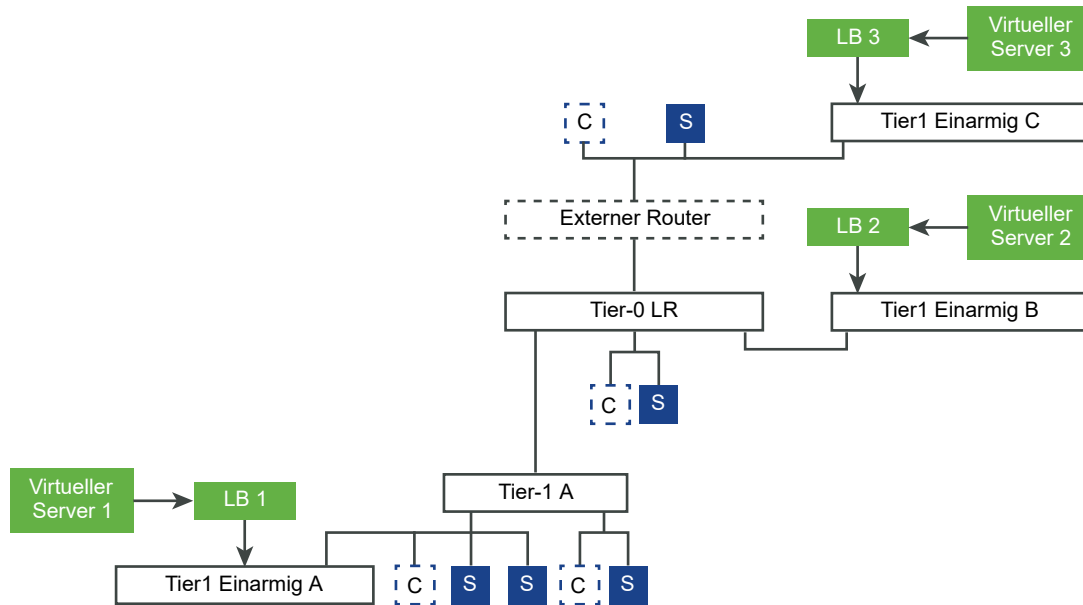
Im Inline-Modus befindet sich der Load Balancer im Datenverkehrspfad zwischen dem Client und dem Server. Clients und Server sollten nicht mit Überlagerungssegmenten auf demselben logischen Tier-1-Router verbunden sein, wenn SNAT auf dem Load Balancer nicht erwünscht ist. Wenn Clients und Server mit Überlagerungssegmenten auf demselben logischen Tier-1-Router verbunden sind, ist SNAT erforderlich.



## One-Arm-Topologie

Im One-Arm-Modus befindet sich der Load Balancer nicht im Datenverkehrspfad zwischen dem Client und dem Server. In diesem Modus können sich der Client und der Server an einem beliebigen Ort befinden. Der Load Balancer führt die Source Network Address Translation (SNAT) durch, um zu erzwingen, dass der zurückgegebene Datenverkehr vom Server, der für den Client bestimmt ist, durch den Load Balancer geleitet wird. Diese Topologie erfordert die Aktivierung der SNAT des virtuellen Servers.

Wenn der Load Balancer den Clientdatenverkehr an die virtuelle IP-Adresse empfängt, wählt er ein Mitglied des Serverpools aus und leitet den Clientdatenverkehr an dieses Mitglied weiter. Im einarmigen Modus ersetzt der Load Balancer die Client-IP-Adresse durch die IP-Adresse des Load Balancers, damit die Antwort des Servers immer an den Load Balancer gesendet wird. Der Load Balancer leitet die Antwort an den Client weiter.



## Tier-1-Dienstverkettung

Wenn ein Tier-1-Gateway oder ein logischer Router verschiedene Dienste hostet, z. B. NAT, Firewall und Load Balancer, werden die Dienste in der folgenden Reihenfolge angewendet:

- Ingress

DNAT – Firewall – Load Balancer

Hinweis: Wenn DNAT mit Firewall-Umgehung konfiguriert ist, wird die Firewall übersprungen, nicht jedoch der Load Balancer.

- Egress

Load Balancer – Firewall – SNAT

## Einrichten von Load Balancer-Komponenten

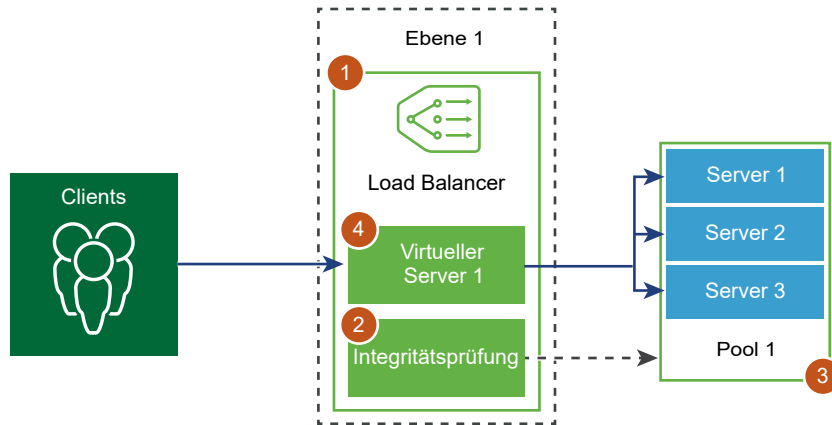
Zur Verwendung logischer Load Balancer müssen Sie zuerst einen Load Balancer konfigurieren und ihn dann an ein Tier-1-Gateway anhängen.

---

**Hinweis** Auf der Registerkarte **Netzwerk und Sicherheit – Erweitert** wird der Begriff logischer Tier-1-Router verwendet, um ein Ebene-1-Gateway zu beschreiben.

---

Im nächsten Schritt richten Sie die Überwachung der Integritätsprüfung für Ihre Server ein. In diesem Fall müssen Sie Serverpools für den Load Balancer konfigurieren. Zum Schluss müssen Sie einen virtuellen Server der Schicht 4 oder der Schicht 7 für Ihren Load Balancer erstellen und den neu erstellten virtuellen Server an den Load Balancer anhängen.



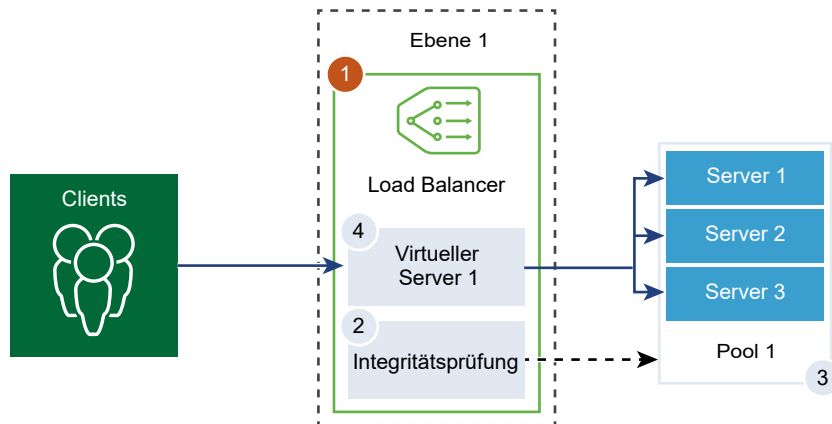
## Hinzufügen von Load Balancern

Der Load Balancer wird erstellt und an das Tier-1-Gateway angehängt.

**Hinweis** Auf der Registerkarte **Netzwerk und Sicherheit – Erweitert** wird der Begriff logischer Tier-1-Router verwendet, um ein Ebene-1-Gateway zu beschreiben.

Sie können die Ebene der Fehlermeldungen konfigurieren, die vom Load Balancer zum Fehlerprotokoll hinzugefügt werden soll.

**Hinweis** Setzen Sie für Load Balancer mit erheblichem Datenverkehr die Protokollebene nicht auf DEBUG, da aufgrund der hohen Anzahl der in das Protokoll geschriebenen Meldungen die Leistung beeinträchtigt wird.



### Voraussetzungen

Stellen Sie sicher, dass ein Tier-1-Gateway konfiguriert ist. Siehe [Kapitel 3 Tier-1-Gateway](#).

### Verfahren

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



- 2 Wählen Sie **Netzwerk > Load Balancing > Load Balancer hinzufügen** aus.
- 3 Geben Sie einen Namen und eine Beschreibung für den Load Balancer ein.
- 4 Wählen Sie auf Basis der verfügbaren Ressourcen die Größe des virtuellen Servers und die Anzahl der Poolmitglieder für den Load Balancer aus.
- 5 Wählen Sie das bereits konfigurierte Tier-1-Gateway, das an diesen Load Balancer angehängt werden soll, im Dropdown-Menü aus.  
  
Das Tier-1-Gateway muss im Modus „Aktiv/Standby“ ausgeführt werden.
- 6 Definieren Sie den Schweregrad des Eintrags im Fehlerprotokolls über das Dropdown-Menü.  
  
Der Load Balancer erfasst Informationen über aufgetretene Probleme verschiedener Schweregrade im Fehlerprotokoll.
- 7 (Optional) Geben Sie Tags ein, um die Suche zu vereinfachen.  
  
Sie können ein Tag angeben, um einen Geltungsbereich des Tags festzulegen.
- 8 Verwenden Sie die Umschaltfläche, um den administrativen Zustand des Load Balancers zu deaktivieren.
- 9 Klicken Sie auf **Speichern**.  
  
Das Erstellen und Anhängen des Load Balancers an das Tier-1-Gateway dauert etwa drei Minuten. Danach wird der Konfigurationsstatus als „Aktiv“ (grün) angezeigt.  
  
Lautet der Status „Inaktiv“, klicken Sie auf das Informationssymbol und beheben Sie den Fehler, bevor Sie fortfahren.
- 10 (Optional) Löschen Sie den Load Balancer.
  - a Trennen Sie den Load Balancer vom virtuellen Server und Tier-1-Gateway.
  - b Wählen Sie den Load Balancer aus.
  - c Klicken Sie auf die Schaltfläche mit den vertikalen Auslassungspunkten.
  - d Wählen Sie **Löschen** aus.

## Hinzufügen einer aktiven Überwachung

Mit der aktiven Systemzustandsüberwachung können Sie testen, ob ein Server verfügbar ist. Die aktive Systemzustandsüberwachung verwendet verschiedene Arten von Tests zur Überwachung des Anwendungszustands, wie z. B. das Senden eines einfachen Pings an Server oder erweiterte HTTP-Anfragen.

---

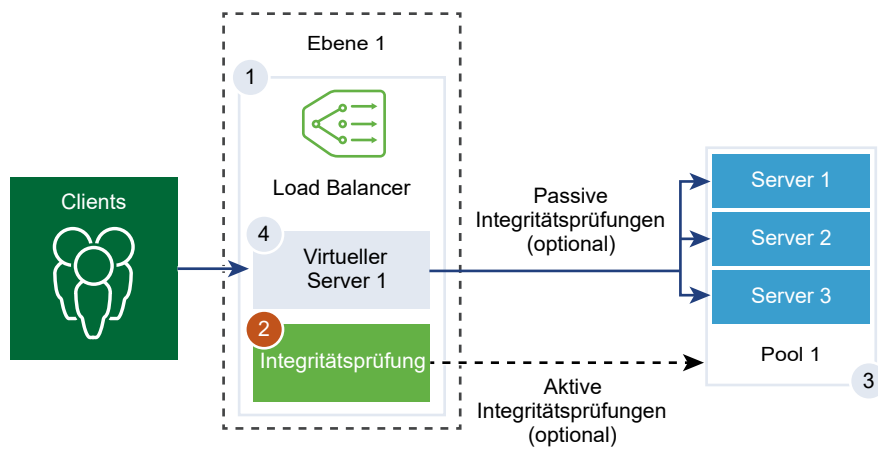
**Hinweis** Auf der Registerkarte **Netzwerk und Sicherheit – Erweitert** wird der Begriff logischer Tier-1-Router verwendet, um ein Ebene-1-Gateway zu beschreiben.

---

Server, die innerhalb eines bestimmten Zeitraums nicht oder mit Fehlern reagieren, werden solange aus der künftigen Verbindungsverarbeitung ausgeschlossen, bis durch eine nachträgliche regelmäßig durchgeführte Systemdiagnose sichergestellt wird, dass die betreffenden Server ordnungsgemäß ausgeführt werden.

Aktive Systemdiagnosen werden auf Serverpoolmitgliedern durchgeführt, nachdem das Poolmitglied an einen virtuellen Server und dieser virtuelle Server dann an ein Tier-1-Gateway angehängt wird. Die IP-Adresse des Tier-1-Uplinks wird für die Systemdiagnose verwendet.

**Hinweis** Pro Serverpool kann genau eine aktive Systemzustandsüberwachung konfiguriert werden.



## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk > Load Balancing > Überwachungen > Aktiv > Aktive Überwachung hinzufügen** aus.
- 3 Wählen Sie im Dropdown-Menü ein Protokoll für den Server aus.  
Sie können auch vordefinierte Protokolle verwenden: HTTP, HTTPS, ICMP, TCP und UDP für NSX Manager.
- 4 Wählen Sie das **HTTP**-Protokoll aus.
- 5 Konfigurieren Sie die Werte zum Überwachen eines Dienstpools.

Sie können auch die Standardwerte der aktiven Systemzustandsüberwachung übernehmen.

Option	Beschreibung
<b>Name und Beschreibung</b>	Geben Sie einen Namen und eine Beschreibung für die aktive Systemzustandsüberwachung ein.
<b>Überwachungsport</b>	Legen Sie den Wert des Überwachungsports fest.
<b>Überwachungsintervall</b>	Geben Sie den Zeitraum in Sekunden an, nach dem von der Überwachung eine weitere Verbindungsanfrage an den Server gesendet wird.

Option	Beschreibung
<b>Zeitüberschreitung</b>	Legen Sie fest, wie oft der Server getestet wird, bevor er als INAKTIV angesehen wird.
<b>Fehleranzahl</b>	Legen Sie einen Wert fest. Wenn die aufeinander folgenden Fehler diesen Wert erreichen, wird der Server als vorübergehend nicht verfügbar betrachtet.
<b>Anzahl bis zum erneuten Versuch</b>	Legen Sie einen Wert fest, der angibt, nach welcher Zeit ein erneuter Verbindungsversuch mit dem Server unternommen wird, um herauszufinden, ob er verfügbar ist.
<b>Tags</b>	Geben Sie Tags ein, um die Suche zu vereinfachen. Sie können ein Tag angeben, um einen Geltungsbereich des Tags festzulegen.

Wenn das Überwachungsintervall beispielsweise auf 5 Sekunden und das Zeitlimit auf 15 Sekunden festgelegt ist, sendet der Load Balancer alle 5 Sekunden Anfragen an den Server. Wenn die erwartete Antwort innerhalb von 15 Sekunden vom Server empfangen wird, lautet das Ergebnis der Systemdiagnose „OK“. Ist dies nicht der Fall, lautet das Ergebnis KRITISCH. Wenn die letzten drei Systemdiagnosen alle AKTIV ergeben haben, wird der Server als AKTIV gekennzeichnet.

**6** Klicken Sie auf **Konfigurieren**.

**7** Geben Sie die HTTP-Anforderung und Antwort-Konfigurationsdetails ein.

Option	Beschreibung
<b>HTTP-Methode</b>	Wählen Sie die Methode (GET, OPTIONS, POST, HEAD und PUT) zur Erkennung des Serverstatus im Dropdown-Menü aus.
<b>HTTP-Anforderungs-URL</b>	Geben Sie die Anforderungs-URI für die Methode ein.
<b>HTTP-Anforderungsversion</b>	Wählen Sie die unterstützte Anforderungsversion im Dropdown-Menü aus. Sie können auch die Standardversion HTTP_VERSION_1 übernehmen.
<b>HTTP-Antwort-Header</b>	Klicken Sie auf <b>Hinzufügen</b> und geben Sie den Namen des HTTP-Antwort-Headers und den entsprechenden Wert ein. Der Standard-Headerwert ist 4000. Der Maximal-Headerwert ist 64.000.
<b>HTTP-Anforderungstext</b>	Geben Sie den Anforderungstext ein. Gültig für die Methoden POST und PUT.
<b>HTTP-Antwortcode</b>	Geben Sie die Zeichenfolge, die bei der Überprüfung als Übereinstimmung erwartet wird, in der Statuszeile des HTTP-Antworttexts ein. Der Antwortcode ist eine durch Komma getrennte Liste. Beispiel: 200,301,302,401.
<b>HTTP-Antworttext</b>	Wenn der HTTP-Antworttext und der HTTP-Antworttext der Systemdiagnose übereinstimmen, wird der Server als fehlerfrei betrachtet.

**8** Wählen Sie das **HTTPS**-Protokoll aus.

**9** Führen Sie Schritt 5 aus.

**10** Klicken Sie auf **Konfigurieren**.

**11** Geben Sie HTTP-Anforderung und Antwort und die Details der SSL-Konfiguration ein.

Option	Beschreibung
<b>Name und Beschreibung</b>	Geben Sie einen Namen und eine Beschreibung für die aktive Systemzustandsüberwachung ein.
<b>HTTP-Methode</b>	Wählen Sie die Methode (GET, OPTIONS, POST, HEAD und PUT) zur Erkennung des Serverstatus im Dropdown-Menü aus.
<b>HTTP-Anforderungs-URL</b>	Geben Sie die Anforderungs-URI für die Methode ein.
<b>HTTP-Anforderungsversion</b>	Wählen Sie die unterstützte Anforderungsversion im Dropdown-Menü aus. Sie können auch die Standardversion HTTP_VERSION_1 übernehmen.
<b>HTTP-Antwort-Header</b>	Klicken Sie auf <b>Hinzufügen</b> und geben Sie den Namen des HTTP-Antwort-Headers und den entsprechenden Wert ein. Der Standard-Headerwert ist 4000. Der Maximal-Headerwert ist 64.000.
<b>HTTP-Anforderungstext</b>	Geben Sie den Anforderungstext ein. Gültig für die Methoden POST und PUT.
<b>HTTP-Antwortcode</b>	Geben Sie die Zeichenfolge, die bei der Überprüfung als Übereinstimmung erwartet wird, in der Statuszeile des HTTP-Antworttexts ein. Der Antwortcode ist eine durch Komma getrennte Liste. Beispiel: 200,301,302,401.
<b>HTTP-Antworttext</b>	Wenn der HTTP-Antworttext und der HTTP-Antworttext der Systemdiagnose übereinstimmen, wird der Server als fehlerfrei betrachtet.
<b>Server-SSL</b>	Schalten Sie die Schaltfläche um, um den SSL-Server zu aktivieren.
<b>Clientzertifikat</b>	(Optional) Wählen Sie ein Zertifikat aus dem Dropdown-Menü, das verwendet werden soll, wenn der Server nicht mehrere Hostnamen auf derselben IP-Adresse hosten soll oder wenn der Client keine SNI-Erweiterung unterstützt.
<b>SSL-Profil des Servers</b>	(Optional) Weisen Sie ein Standard-SSL-Profil aus dem Dropdown-Menü zu, das wiederverwendbare und anwendungsunabhängige, clientseitige SSL-Eigenschaften definiert. Klicken Sie auf die vertikale Auslassungspunkte und erstellen Sie ein benutzerdefiniertes SSL-Profil.
<b>Vertrauenswürdige CA-Zertifikate</b>	(Optional) Sie können den Client so konfigurieren, dass er ein CA-Zertifikat für die Authentifizierung haben muss.
<b>Obligatorische Serverauthentifizierung</b>	(Optional) Schalten Sie die Schaltfläche um, um die Server-Authentifizierung zu aktivieren.
<b>Tiefe der Zertifikatskette</b>	(Optional) Legen Sie die Authentifizierungstiefe für die Client-Zertifikatskette fest.
<b>Zertifikatswiderrufsliste</b>	(Optional) Legen Sie eine Zertifikatswiderrufsliste (CRL) im clientseitigen SSL-Profil fest, um manipulierte Clientzertifikate abzulehnen.

**12** Wählen Sie das **ICMP**-Protokoll aus.**13** Führen Sie Schritt 5 aus und weisen Sie die Datengröße in Byte des Pakets zur ICMP-Integritätsprüfung zu.**14** Wählen Sie das **TCP**-Protokoll aus.

- 15** Führen Sie Schritt 5 aus. Dabei können Sie die TCP-Daten-Parameter leer lassen.

Wenn sowohl gesendete als auch erwartete Daten nicht aufgelistet werden, wird eine TCP-Verbindung mit Dreiwege-Handshake eingerichtet, um den Zustand des Servers zu überprüfen. Keine Daten werden gesendet.

Erwartete Daten, falls aufgeführt, müssen eine Zeichenfolge sein. Reguläre Ausdrücke werden nicht unterstützt.

- 16** Wählen Sie das **UDP**-Protokoll aus.
- 17** Führen Sie Schritt 5 aus und konfigurieren Sie die UDP-Daten.

Erforderliche Option	Beschreibung
<b>Gesendete UDP-Daten</b>	Geben Sie die Zeichenfolge ein, die nach dem Verbindungsaufbau an den Server gesendet werden soll.
<b>Erwartete UDP-Daten</b>	Geben Sie die Zeichenfolge ein, die vom Server gesendet werden soll. Der Server wird nur dann als AKTIV eingestuft, wenn die empfangene Zeichenfolge mit dieser Definition übereinstimmt.

#### Nächste Schritte

Verknüpfen Sie die aktive Systemzustandsüberwachung mit einem Serverpool. Siehe [Hinzufügen eines Serverpools](#).

## Hinzufügen einer passiven Überwachung

Load Balancer führen passive Systemdiagnosen durch, um Fehler bei Clientverbindungen zu überwachen und Server, die durchgängig Fehler verursachen, als INAKTIV zu markieren.

Die passive Systemdiagnose überwacht den Clientdatenverkehr, der durch den Load Balancer geleitet wird, auf Fehler. Wenn ein Poolmitglied beispielsweise als Reaktion auf eine Clientverbindung ein TCP Reset (RST) sendet, erkennt der Load Balancer diesen Fehler. Treten mehrere aufeinander folgende Fehler auf, sieht der Load Balancer dieses Mitglied des Serverpools als vorübergehend nicht verfügbar an und sendet eine Weile keine Verbindungsanforderungen mehr an dieses Poolmitglied. Nach einem festgelegten Zeitraum sendet der Load Balancer eine Verbindungsanforderung, um sicherzustellen, dass das Poolmitglied wiederhergestellt wurde. Wenn diese Verbindung erfolgreich hergestellt werden kann, wird das Poolmitglied als fehlerfrei angesehen. Andernfalls wartet der Load Balancer eine Zeit lang und versucht es dann erneut.

Die passive Systemdiagnose sieht die folgenden Szenarien als Fehler im Clientdatenverkehr an.

- Wenn bei Serverpools, die virtuellen Servern der Schicht 7 zugeordnet sind, die Verbindung zum Poolmitglied fehlschlägt. Sendet das Poolmitglied beispielsweise ein TCP RST, während der Load Balancer versucht, eine Verbindung herzustellen oder ein SSL-Handshake zwischen dem Load Balancer und dem Poolmitglied durchzuführen, schlägt dieser Vorgang fehl.

- Wenn bei Serverpools, die virtuellen TCP-Servern der Schicht 4 zugeordnet sind, das Poolmitglied ein TCP RST als Reaktion auf ein TCP SYN des Clients sendet oder überhaupt nicht reagiert.
- Wenn bei Serverpools, die virtuellen UDP-Servern der Schicht 4 zugeordnet sind, ein Port nicht erreichbar ist oder eine ICMP-Fehlermeldung bezüglich eines nicht erreichbaren Ziels als Reaktion auf ein UDP-Clientpaket empfangen wird.

Bei Serverpools, die virtuellen Servern der Schicht 7 zugeordnet sind, wird die Anzahl der fehlgeschlagenen Verbindungen erhöht, wenn TCP-Verbindungsfehler, z. B. TCP-RST-Fehler beim Senden von Daten, oder SSL-Handshake-Fehler auftreten.

Wenn in Serverpools, die virtuellen Servern der Schicht 4 zugeordnet sind, keine Antwort auf ein an das Mitglied des Serverpools gesendetes TCP SYN eingeht oder ein TCP RST als Reaktion auf ein TCP SYN empfangen wird, wird das Mitglied des Serverpools als INAKTIV angesehen. Die Fehleranzahl wird entsprechend erhöht.

Wenn bei virtuellen UDP-Servern der Schicht 4 ein ICMP-Fehler, beispielsweise eine Meldung über einen nicht erreichbaren Port oder ein nicht erreichbares Ziel, als Reaktion auf den Clientdatenverkehr empfangen wird, wird der Server als INAKTIV angesehen.

---

**Hinweis** Pro Serverpool kann eine passive Systemzustandsüberwachung konfiguriert werden.

---

#### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk > Load Balancing > Überwachungen > Passiv > Passive Überwachung hinzufügen** aus.
- 3 Geben Sie einen Namen und eine Beschreibung für die passive Systemzustandsüberwachung ein.
- 4 Konfigurieren Sie die Werte zum Überwachen eines Dienstpools.

Sie können auch die Standardwerte der aktiven Systemzustandsüberwachung übernehmen.

Option	Beschreibung
<b>Fehleranzahl</b>	Legen Sie einen Wert fest. Wenn die aufeinander folgenden Fehler diesen Wert erreichen, wird der Server als vorübergehend nicht verfügbar betrachtet.
<b>Zeitüberschreitung</b>	Legen Sie fest, wie oft der Server getestet wird, bevor er als INAKTIV angesehen wird.
<b>Tags</b>	Geben Sie Tags ein, um die Suche zu vereinfachen. Sie können ein Tag angeben, um einen Geltungsbereich des Tags festzulegen.

Wenn die aufeinander folgenden Fehler beispielsweise den konfigurierten Wert 5 erreicht haben, wird dieses Mitglied 5 Sekunden lang als vorübergehend nicht verfügbar angesehen. Nach Ablauf dieses Zeitraums wird wieder versucht, eine neue Verbindung mit diesem

Mitglied herzustellen, um seine Verfügbarkeit zu prüfen. Bei einer erfolgreichen Verbindung wird das Mitglied als verfügbar angesehen, und die Fehleranzahl wird auf Null gesetzt. Schlägt diese Verbindung jedoch fehl, wird das Mitglied während eines weiteren 5 Sekunden langen Zeitüberschreitungsintervalls nicht verwendet.

#### Nächste Schritte

Verknüpfen Sie die passive Systemzustandsüberwachung mit einem Serverpool. Siehe [Hinzufügen eines Serverpools](#).

## Hinzufügen eines Serverpools

Ein Serverpool besteht aus einem oder mehreren Servern, die konfiguriert sind und die gleiche Anwendung ausführen. Ein einzelner Pool kann virtuellen Servern der Schicht 4 und 7 zugeordnet werden.

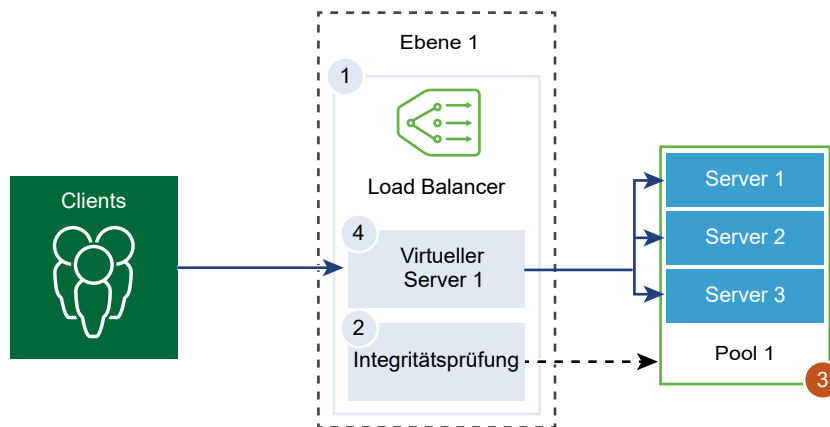
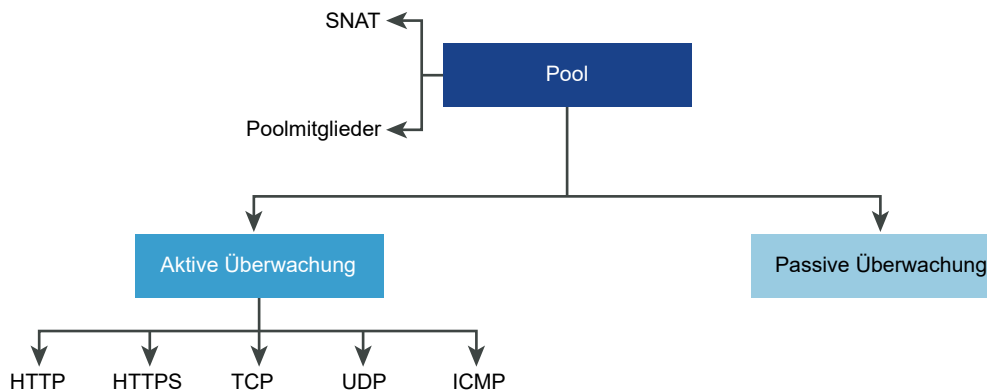


Abbildung 7-1. Konfiguration der Serverpool-Parameter



#### Voraussetzungen

- Wenn Sie dynamische Poolmitglieder verwenden, muss eine NS-Gruppe konfiguriert werden. Siehe [Erstellen einer NS-Gruppe](#).
- Vergewissern Sie sich, dass eine passive Systemzustandsüberwachung konfiguriert ist. Siehe [Hinzufügen einer passiven Überwachung](#).

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk > Load Balancing > Serverpools > Serverpool hinzufügen** aus.
- 3 Geben Sie einen Namen und eine Beschreibung für den Load Balancer-Serverpool ein.  
Optional können Sie die vom Serverpool verwalteten Verbindungen beschreiben.
- 4 Wählen Sie die Algorithmus-Ausgleichsmethode für den Serverpool aus.

Der Lastausgleichs-Algorithmus steuert, wie die eingehenden Verbindungen zwischen den Mitgliedern verteilt werden. Der Algorithmus kann direkt auf einem Serverpool oder einem Server verwendet werden.

Alle Lastausgleichs-Algorithmen überspringen Server, die eine der folgenden Bedingungen erfüllen:

- Admin-Zustand ist auf DISABLED festgelegt
- Admin-Zustand ist auf GRACEFUL\_DISABLED und keinen übereinstimmenden Persistenzeintrag festgelegt
- Zustand der aktiven oder passiven Systemdiagnose ist DOWN
- Verbindungsgrenzwert für die maximale Anzahl gleichzeitiger Verbindungen des Serverpools ist erreicht.

Option	Beschreibung
<b>ROUND_ROBIN</b>	Eingehende Clientanforderungen werden durch eine Liste verfügbarer Server geleitet, die in der Lage sind, die Anforderung zu bearbeiten. Ignoriert die Gewichtungen der Serverpoolmitglieder, auch wenn sie konfiguriert sind.
<b>WEIGHTED_ROUND_ROBIN</b>	Jedem Server wird ein Gewichtungswert zugewiesen, der angibt, wie sich dieser Server im Vergleich zu anderen Servern im Pool verhält. Der Wert legt fest, wie viele Clientanforderungen im Vergleich zu anderen Servern im Pool an einen Server gesendet werden. Dieser Lastausgleichs-Algorithmus konzentriert sich auf eine gerechte Verteilung der Last auf die verfügbaren Serverressourcen.
<b>LEAST_CONNECTION</b>	Verteilt basierend auf der Anzahl der bereits auf den Servern aktiven Verbindungen die Client-Anforderungen an mehrere Server. Neue Verbindungen werden an den Server mit der geringsten Anzahl an Verbindungen gesendet. Ignoriert die Gewichtungen der Serverpoolmitglieder, auch wenn sie konfiguriert sind.



Option	Beschreibung
<b>WEIGHTED_LEAST_CONNECTION</b>	<p>Jedem Server wird ein Gewichtungswert zugewiesen, der angibt, wie sich dieser Server im Vergleich zu anderen Servern im Pool verhält. Der Wert legt fest, wie viele Clientanforderungen im Vergleich zu anderen Servern im Pool an einen Server gesendet werden.</p> <p>Dieser Lastausgleichs-Algorithmus konzentriert sich auf die Verteilung der Last auf die verfügbaren Serverressourcen anhand des Gewichtungswerts. Standardmäßig ist der Gewichtungswert 1, wenn der Wert nicht konfiguriert ist und langsamer Start aktiviert ist.</p>
<b>IP-HASH</b>	Wählt einen Server auf der Basis eines Hash der Quell-IP-Adresse und der gesamten Gewichtung aller ausgeführten Server aus.

## 5 Wählen Sie die Serverpoolmitglieder aus.

Der Serverpool besteht aus einem oder mehreren Poolmitgliedern.

Option	Beschreibung
<b>Einzelne Mitglieder eingeben</b>	<p>Geben Sie einen Poolmitgliedsnamen, eine IP-Adresse und einen Port ein.</p> <p>Jedes Serverpoolmitglied kann mit einer Gewichtung für die Verwendung im Lastausgleichs-Algorithmus konfiguriert werden. Die Gewichtung gibt an, wie viel mehr oder weniger Last ein bestimmtes Poolmitglied im Vergleich zu anderen Mitgliedern im selben Pool verarbeiten kann.</p> <p>Sie können den Admin-Zustand des Serverpools festlegen. Wenn ein Serverpoolmitglied hinzugefügt wird, ist die Option standardmäßig aktiviert. Wenn die Option deaktiviert ist, werden aktive Verbindungen verarbeitet und das Serverpoolmitglied wird nicht für neue Verbindungen ausgewählt. Neue Verbindungen werden anderen Mitgliedern des Pools zugewiesen. Wenn die Option deaktiviert ist, können Sie Server für Wartungszwecke entfernen. Die vorhandenen Verbindungen zu einem Mitglied im Serverpool in diesem Zustand werden weiterhin verarbeitet.</p> <p>Klicken Sie auf die Schaltfläche, um ein Poolmitglied als Backup-Mitglied zuzuweisen, das zusammen mit der Systemzustandsüberwachung dazu eingesetzt wird, einen Aktiv-Standby-Zustand anzugeben. Datenverkehr-Failover tritt für Backup-Mitglieder ein, wenn die Systemdiagnose für aktive Mitglieder fehlschlägt. Backup-Mitglieder werden während der Serverauswahl übersprungen. Wenn der Serverpool inaktiv ist, werden die eingehenden Verbindungen nur an die Backup-Mitglieder gesendet, die so konfiguriert sind, dass eine Fehlermeldungsseite auf die Nichtverfügbarkeit einer Anwendung hinweist.</p> <p>Der Wert für „Max. Anzahl gleichzeitiger Verbindungen“ weist eine Höchstzahl von Verbindungen zu, sodass die Serverpoolmitglieder nicht überlastet und bei der Serverauswahl übersprungen werden. Wenn kein Wert angegeben ist, ist die Anzahl der gleichzeitigen Verbindungen unbegrenzt.</p>
<b>Gruppe auswählen</b>	<p>Wählen Sie eine vorkonfigurierte Gruppe von Serverpoolmitgliedern aus. Geben Sie einen Gruppennamen, optional eine Beschreibung sowie die Domäne ein. Beachten Sie, dass das Domänenobjekt eine experimentelle Funktion in NSX-T Data Center 2.4 ist, aber in NSX-T Data Center 2.4.1 nicht verfügbar ist.</p> <p>Legen Sie ein vorhandenes Mitglied aus der Liste als Computing-Mitglied fest oder erstellen Sie ein neues Mitglied. Sie können Mitgliedschaftskriterien angeben, Mitglieder der Gruppe auswählen, IP- und MAC-Adressen als Gruppenmitglieder hinzufügen und Active Directory-Gruppen hinzufügen. Es wird eine Schnittmenge der Identitätsmitglieder mit dem Computing-Mitglied gebildet, um die Mitgliedschaft der Gruppe zu definieren.</p> <p>Geben Sie Tags ein, um die Suche zu vereinfachen. Sie können ein Tag angeben, um einen Geltungsbereich des Tags festzulegen.</p> <p>Optional können Sie die maximale IP-Adressen-Gruppenliste definieren.</p>

- Wählen Sie im Dropdown-Menü die aktive Systemzustandsüberwachung für den Serverpool aus.

Der Lastausgleich sendet in regelmäßigen Abständen einen ICMP-Ping an die Server, um den Systemzustand unabhängig vom Datenverkehr zu überprüfen. Sie können nur eine aktive Systemzustandsüberwachung pro Serverpool konfigurieren.

## 7 Wählen Sie den SNAT-Übersetzungsmodus (Source NAT, Quell-NAT) aus.

Abhängig von der Topologie kann SNAT erforderlich sein, damit der Load Balancer Datenverkehr von dem Server empfängt, der für den Client bestimmt ist. SNAT kann pro Serverpool aktiviert werden.

Modus	Beschreibung
<b>Modus für die automatische Zuordnung</b>	<p>Der Load Balancer verwendet die IP-Adresse der Schnittstelle und den flüchtigen Port, um die Kommunikation mit einem Client fortzusetzen, der ursprünglich mit einem der etablierten Überwachungsports des Servers verbunden war.</p> <p>SNAT ist erforderlich.</p> <p>Aktivieren Sie die Portüberlastung, damit dieselbe SNAT-IP und derselbe Port für mehrere Verbindungen verwendet werden können, wenn das Tupel (Quell-IP, Quellport, Ziel-IP, Zielport und IP-Protokoll) nach der Ausführung des SNAT-Prozesses eindeutig ist.</p> <p>Sie können auch den Portüberlastungsfaktor so festlegen, dass die maximale Anzahl der gleichzeitigen Nutzung eines Ports für mehrere Verbindungen möglich ist.</p>
<b>Deaktivieren</b>	Deaktivieren Sie den SNAT-Übersetzungsmodus.
<b>IP-Pool</b>	<p>Geben Sie einen einzigen IP-Adressbereich an, z. B. 1.1.1.1-1.1.1.10, der für SNAT verwendet werden soll, während Sie eine Verbindung zu einem der Server im Pool herstellen.</p> <p>Standardmäßig wird der Portbereich von 4000 bis 64000 für alle konfigurierten SNAT-IP-Adressen verwendet. Die Portbereiche von 1000 bis 4000 sind für bestimmte Zwecke wie z. B. Systemdiagnosen und von Linux-Anwendungen initiierte Verbindungen reserviert. Wenn mehrere IP-Adressen vorhanden sind, werden sie auf Grundlage von Round-Robin ausgewählt.</p> <p>Aktivieren Sie die Portüberlastung, damit dieselbe SNAT-IP und derselbe Port für mehrere Verbindungen verwendet werden können, wenn das Tupel (Quell-IP, Quellport, Ziel-IP, Zielport und IP-Protokoll) nach der Ausführung des SNAT-Prozesses eindeutig ist.</p> <p>Sie können auch den Portüberlastungsfaktor so festlegen, dass die maximale Anzahl der gleichzeitigen Nutzung eines Ports für mehrere Verbindungen möglich ist.</p>

## 8 Klicken Sie auf den Schalter, um TCP-Multiplexing zu aktivieren.

Mit der Funktion „TCP-Multiplexing“ können Sie dieselbe TCP-Verbindung zwischen einem Lastausgleich und dem Server verwenden, um mehrere Clientanforderungen über verschiedene Client-TCP-Verbindungen zu senden.

## 9 Legen Sie die maximale Anzahl der TCP-Multiplexing-Verbindungen pro Pool fest, die zum Senden von zukünftigen Clientanforderungen beibehalten werden.

## 10 Geben Sie die minimale Anzahl von aktiven Mitgliedern ein, die der Serverpool immer beibehalten muss.

## 11 Wählen Sie im Dropdown-Menü eine passive Systemzustandsüberwachung für den Serverpool aus.

## 12 Geben Sie Tags ein, um die Suche zu vereinfachen.

Sie können ein Tag angeben, um einen Geltungsbereich des Tags festzulegen.

## Einrichten von Komponenten des virtuellen Servers

Sie können die virtuellen Server der Schicht 4 und der Schicht 7 einrichten und mehrere virtuelle Serverkomponenten konfigurieren, z. B. Anwendungsprofile, persistente Profile und Load Balancer-Regeln.

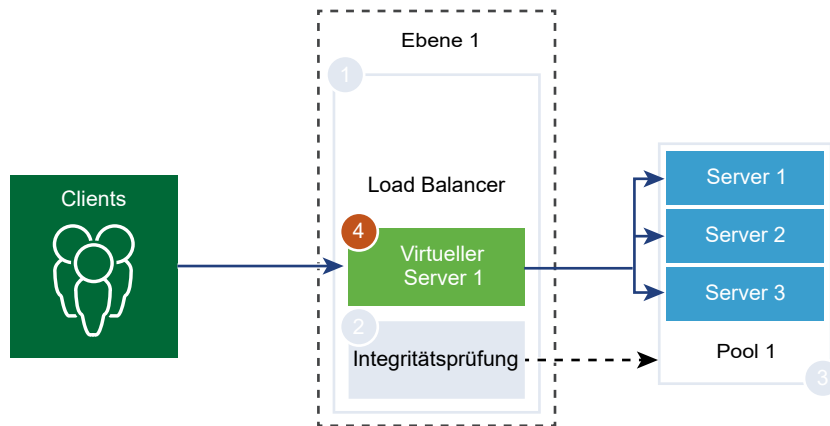
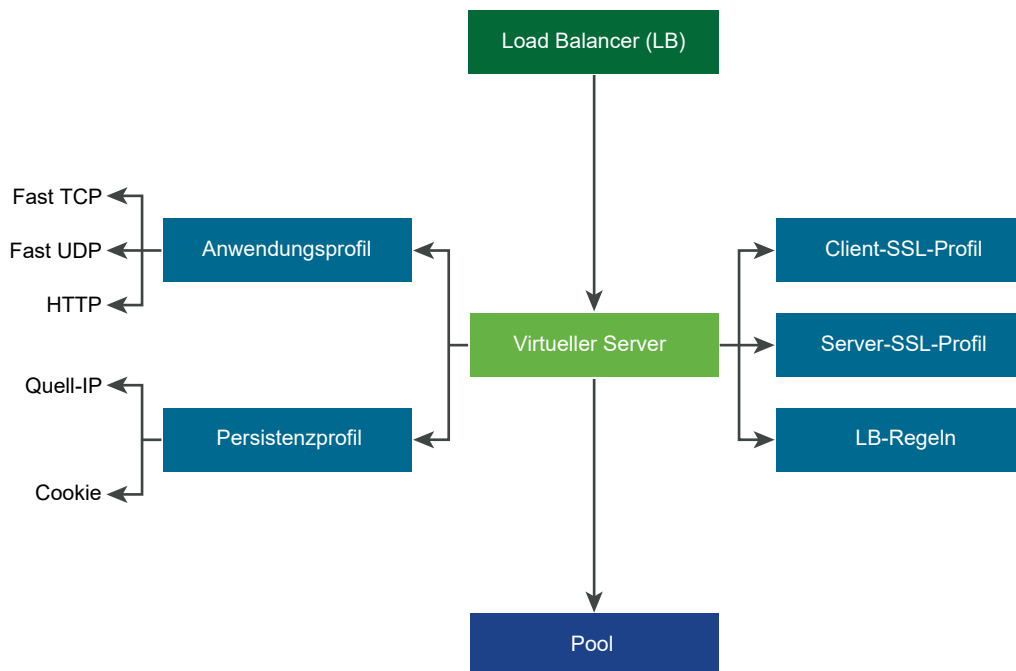


Abbildung 7-2. Komponenten des virtuellen Servers



## Hinzufügen eines Anwendungsprofils

Anwendungsprofile sind mit virtuellen Servern verknüpft, um das Load Balancing im Netzwerkverkehr zu verbessern und Aufgaben zur Verwaltung des Datenverkehrs zu vereinfachen.

Mit Anwendungsprofilen definieren Sie das Verhalten eines bestimmten Netzwerkverkehrstyps. Der verknüpfte virtuelle Server verarbeitet den Datenverkehr gemäß den im Anwendungsprofil angegebenen Werten. Fast TCP-, Fast UDP- und HTTP- Anwendungsprofile sind die unterstützten Profiltypen.

Das Anwendungsprofil TCP wird verwendet, wenn standardmäßig kein Anwendungsprofil mit einem virtuellen Server verknüpft ist. TCP- und UDP-Anwendungsprofile werden verwendet, wenn eine Anwendung auf einem TCP- oder UDP-Protokoll ausgeführt wird und kein Load Balancing auf Anwendungsebene benötigt, wie z. B. HTTP-URL-Load Balancing. Diese Profile werden auch verwendet, wenn Sie nur Load Balancing der Schicht 4 benötigen, der leistungsfähiger ist und Verbindungsspiegelung unterstützt.

Das HTTP-Anwendungsprofil wird für HTTP- und HTTPS-Anwendungen verwendet, wenn der Load Balancer Aktionen auf Grundlage von Schicht 7 durchführen muss, wie z. B. das Durchführen von Load Balancing für alle Bildanforderungen auf einem bestimmten Serverpoolmitglied oder das Beenden von HTTPS zum Auslagern von SSL aus Poolmitgliedern. Im Gegensatz zum TCP-Anwendungsprofil hält das HTTP-Anwendungsprofil die TCP-Verbindung des Clients vor der Auswahl des Serverpoolmitglieds an.

Abbildung 7-3. TCP- und UDP-Anwendungsprofil der Schicht 4

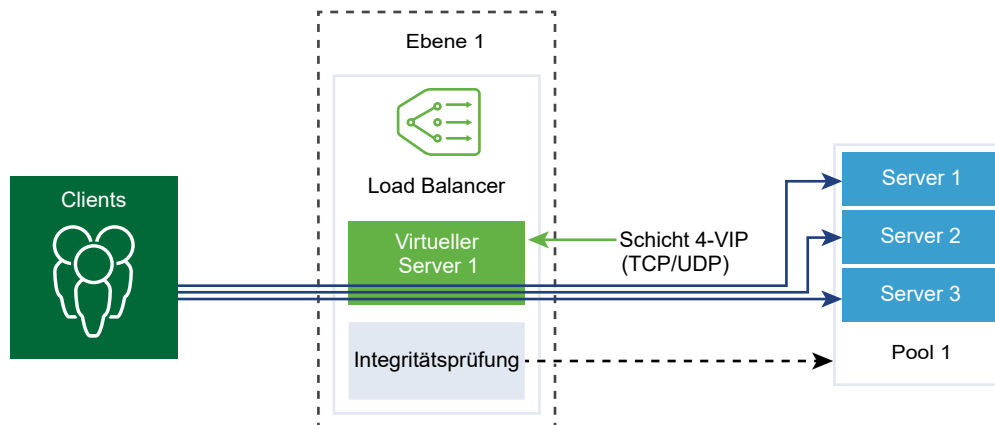
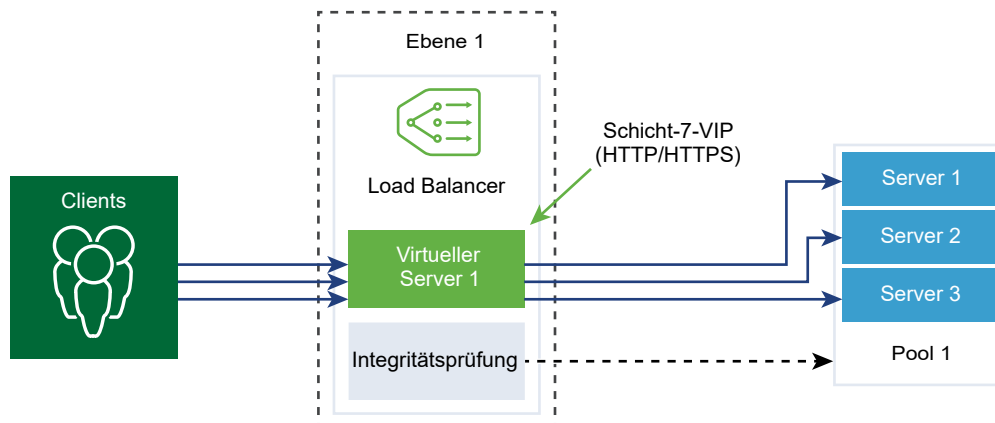


Abbildung 7-4. HTTPS-Anwendungsprofil der Schicht 7



## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk > Load Balancing > Profile > Anwendung > Anwendungsprofil hinzufügen** aus.
- 3 Wählen Sie ein **Fast TCP**-Anwendungsprofil aus und geben Sie die Profildetails ein.  
Sie können auch die Standardprofileinstellungen für FAST TCP übernehmen.

Option	Beschreibung
<b>Name und Beschreibung</b>	Geben Sie einen Namen und eine Beschreibung für das Fast TCP-Anwendungsprofil ein.
<b>Leerlaufzeitlimit</b>	Geben Sie den Zeitraum in Sekunden ein, während dem ein Server im Leerlauf ausgeführt werden kann, nachdem eine TCP-Verbindung eingerichtet wurde.  Legen Sie die Leerlaufzeit auf die Leerlaufzeit der tatsächlichen Anwendung fest und fügen Sie ein paar Sekunden hinzu, damit der Load Balancer seine Verbindungen nicht vor der Anwendung schließt.
<b>HA-Flow-Mirroring</b>	Schalten Sie die Schaltfläche um, um alle Flows zum zugehörigen virtuellen Server auf den HA-Standby-Knoten zu spiegeln.
<b>Zeitlimit vor Schließen der Verbindung</b>	Geben Sie den Zeitraum in Sekunden ein, während dem eine TCP-Verbindung (FIN und RST) für eine Anwendung bestehen bleiben muss, bevor die Verbindung geschlossen wird.  Ein kurzes Zeitlimit ist unter Umständen erforderlich, um schnelle Verbindungsraten zu unterstützen.
<b>Tags</b>	Geben Sie Tags ein, um die Suche zu vereinfachen.  Sie können ein Tag angeben, um einen Geltungsbereich des Tags festzulegen.

- 4 Wählen Sie ein **Fast UDP**-Anwendungsprofil aus und geben Sie die Profildetails ein.  
Sie können auch die Standardprofileinstellungen für UDP übernehmen.

Option	Beschreibung
<b>Name und Beschreibung</b>	Geben Sie einen Namen und eine Beschreibung für das Fast UDP-Anwendungsprofil ein.
<b>Leerlaufzeitlimit</b>	Geben Sie den Zeitraum in Sekunden ein, während dem ein Server im Leerlauf ausgeführt werden kann, nachdem eine UDP-Verbindung eingerichtet wurde.  UDP ist ein verbindungsloses Protokoll. Zu Load Balancing-Zwecken wird davon ausgegangen, dass alle UDP-Pakete mit derselben Flow-Signatur (wie z. B. IP-Quell- und IP-Zieladresse oder -ports) und IP-Protokolle, die während des Leerlaufzeitlimits empfangen wurden, zur selben Verbindung gehören und an denselben Server gesendet werden.  Werden während des Leerlaufzeitlimits keine Pakete empfangen, wird die Verbindung, die als Verknüpfung zwischen der Flow-Signatur und dem ausgewählten Server fungiert, getrennt.

Option	Beschreibung
<b>HA-Flow-Mirroring</b>	Schalten Sie die Schaltfläche um, um alle Flows zum zugehörigen virtuellen Server auf den HA-Standby-Knoten zu spiegeln.
<b>Tags</b>	Geben Sie Tags ein, um die Suche zu vereinfachen. Sie können ein Tag angeben, um einen Geltungsbereich des Tags festzulegen.

**5** Wählen Sie ein **HTTP** Anwendungsprofil aus und geben Sie die Profildetails ein.

Sie können auch die Standardprofileinstellungen für HTTP übernehmen.

Das HTTP-Anwendungsprofil wird für HTTP- und HTTPS-Anwendungen verwendet.

Option	Beschreibung
<b>Name und Beschreibung</b>	Geben Sie einen Namen und eine Beschreibung für das HTTP-Anwendungsprofil ein.
<b>Leerlaufzeitlimit</b>	Geben Sie anstelle der TCP-Socket-Einstellung, die im TCP-Anwendungsprofil konfiguriert werden muss, den Zeitraum in Sekunden an, während dem eine HTTP-Anwendung im Leerlauf ausgeführt werden kann.
<b>Größe des Anforderungsheaders</b>	Geben Sie die maximale Puffergröße in Byte an, die zum Speichern von HTTP-Anforderungsheadern verwendet wird.
<b>XFF (X-Forwarded-For)</b>	<ul style="list-style-type: none"> <li>■ <b>Einfügen</b> – Wenn der XFF-HTTP-Header nicht in der eingehenden Anfrage enthalten ist, fügt der Load Balancer einen neuen XFF-Header mit der IP-Adresse des Clients ein. Wenn der XFF-HTTP-Header in der eingehenden Anfrage enthalten ist, hängt der Load Balancer den XFF-Header mit der IP-Adresse des Clients an.</li> <li>■ <b>Ersetzen</b> – Wenn der XFF-HTTP-Header in der eingehenden Anfrage enthalten ist, ersetzt der Load Balancer den Header.</li> </ul> <p>Webserver protokollieren jede Anfrage, die sie verarbeiten, mit der IP-Adresse des anfragenden Clients. Diese Protokolle werden zur Fehlerbehebung und Analyse verwendet. Wenn die Bereitstellungstopologie SNAT auf dem Load Balancer erfordert, verwendet der Server die IP-Adresse der Client-SNAT, was dem Zweck der Protokollierung widerspricht. Zur Umgehung dieses Problems kann der Load Balancer so konfiguriert werden, dass der XFF-HTTP-Header mit der IP-Adresse des ursprünglichen Clients eingefügt wird. Server können so konfiguriert werden, dass anstelle der IP-Quelladresse der Verbindung die IP-Adresse im XFF-Header aufgezeichnet wird.</p>
<b>Größe des Anforderungstexts</b>	Geben Sie einen Wert für die maximale Größe des Puffers ein, der zum Speichern des HTTP-Anforderungstexts verwendet wird. Wenn die Größe nicht angegeben wird, ist die Größe des Anforderungshauptteils unbegrenzt.

Option	Beschreibung
<b>Umleitung</b>	<ul style="list-style-type: none"> <li>■ Keine – Wenn eine Website vorübergehend nicht verfügbar ist, erhält der Benutzer eine Meldung mit dem Hinweis, dass die Seite nicht gefunden werden konnte.</li> <li>■ HTTP-Umleitung – Wenn eine Website vorübergehend nicht verfügbar ist oder verschoben wurde, können eingehende Anfragen für diesen virtuellen Server vorübergehend an eine hier angegebene URL umgeleitet werden. Nur eine statische Umleitung wird unterstützt.  Wenn „HTTP-Umleitung“ beispielsweise auf <code>http://sitedown.abc.com/sorry.html</code> gesetzt ist, werden ungeachtet der tatsächlichen Anfrage (z. B. <code>http://original_app.site.com/home.html</code> oder <code>http://original_app.site.com/somepage.html</code>) eingehende Anfragen an die angegebene URL umgeleitet, wenn die ursprüngliche Website nicht erreichbar ist.</li> <li>■ HTTP an HTTPS umleiten – Bestimmte sichere Anwendungen möchten unter Umständen Kommunikation über SSL erzwingen, aber statt Nicht-SSL-Verbindungen abzulehnen, können sie die Clientanfrage zur Verwendung von SSL umleiten. Mithilfe von „HTTP an HTTPS umleiten“ können Sie den Host und die URI-Pfade beibehalten und die Clientanfrage zur Verwendung von SSL umleiten.  Zur Verwendung von „HTTP an HTTPS umleiten“ muss der virtuelle HTTPS-Server Port 443 aufweisen und dieselbe IP-Adresse des virtuellen Servers muss auf demselben Load Balancer konfiguriert sein.  Eine Clientanfrage für <code>http://app.com/path/page.html</code> wird beispielsweise an <code>https://app.com/path/page.html</code> umgeleitet. Wenn entweder der Hostname oder die URI während der Umleitung geändert werden muss, z. B. Umleitung an <code>https://secure.app.com/path/page.html</code>, müssen Load Balancing-Regeln verwendet werden.</li> </ul>



Option	Beschreibung
<b>NTLM-Authentifizierung</b>	<p>Schalten Sie die Schaltfläche für den Load Balancer um, um TCP-Multiplexing zu deaktivieren und HTTP-Keep-Alive zu aktivieren.</p> <p>NTLM ist ein Authentifizierungsprotokoll, das über HTTP verwendet werden kann. Für Load Balancing mit NTLM-Authentifizierung muss TCP-Multiplexing für die Serverpools deaktiviert werden, die NTLM-basierte Anwendungen hosten. Andernfalls kann eine mit den Anmeldedaten eines Clients eingerichtete serverseitige Verbindung möglicherweise dazu verwendet werden, die Anfragen eines anderen Clients zu beantworten.</p> <p>Wenn NTLM im Profil aktiviert ist und einem virtuellen Server zugeordnet wurde und TCP-Multiplexing im Serverpool aktiviert ist, hat NTLM Vorrang. TCP-Multiplexing wird für diesen virtuellen Server nicht durchgeführt. Wenn derselbe Pool jedoch einem anderen virtuellen Server ohne NTLM zugeordnet wird, steht TCP-Multiplexing für Verbindungen mit diesem virtuellen Server zur Verfügung.</p> <p>Wenn der Client HTTP/1.0 verwendet, führt der Load Balancer ein Upgrade auf das HTTP/1.1-Protokoll durch und HTTP-Keep-Alive wird eingerichtet. Alle HTTP-Anforderungen, die über dieselbe clientseitigen TCP-Verbindung empfangen wurden, werden über eine einzige TCP-Verbindung an denselben Server gesendet, um sicherzustellen, dass keine erneute Autorisierung erforderlich ist.</p>
<b>Tags</b>	<p>Geben Sie Tags ein, um die Suche zu vereinfachen.</p> <p>Sie können ein Tag angeben, um einen Geltungsbereich des Tags festzulegen.</p>

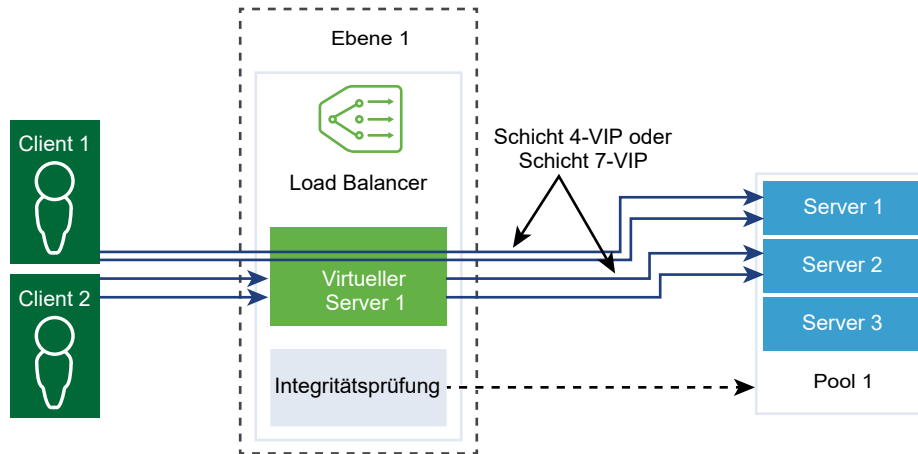
## Hinzufügen eines Persistenzprofils

Zur Gewährleistung der Stabilität von statusbehafteten Anwendungen implementieren Load Balancer Persistenz, die alle zugehörigen Verbindungen an denselben Server weiterleitet. Es werden verschiedene Arten von Persistenz unterstützt, um die unterschiedlichen Anwendungsanforderungen zu erfüllen.

Einige Anwendungen verwalten den Serverstatus, z. B. Einkaufswagen. Dieser Status kann pro Client gelten und anhand der Client-IP-Adresse oder über die HTTP-Sitzung ermittelt werden. Anwendungen können während der Verarbeitung nachfolgender zugehöriger Verbindungen von demselben Client oder derselben HTTP-Sitzung auf diesen Status zugreifen oder ihn ändern.

Das Quell-IP-Persistenzprofil verfolgt Sitzungen basierend auf der Quell-IP-Adresse. Wenn ein Client eine Verbindung mit einem virtuellen Server anfordert, der die Persistenz der Quelladresse ermöglicht, überprüft der Load Balancer, ob dieser Client zuvor verbunden war. Wenn dies der Fall ist, gibt er den Client an denselben Server zurück. Andernfalls können Sie basierend auf dem Load Balancing-Algorithmus des Pools ein Mitglied des Serverpools auswählen. Das Quell-IP-Persistenzprofil wird von virtuellen Servern der Schichten 4 und 7 verwendet.

Das Cookie-Persistenzprofil fügt ein eindeutiges Cookie zur Identifizierung der Sitzung beim ersten Zugriff eines Clients auf die Site ein. Das HTTP-Cookie wird durch den Client in nachfolgenden Anforderungen weitergeleitet, und der Load Balancer verwendet diese Informationen zur Bereitstellung der Cookiepersistenz. Virtuelle Server der Ebene 7 können nur das Cookie-Persistenzprofil verwenden.



## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk > Load Balancing > Profile > Persistenz > Persistenzprofil hinzufügen** aus.
- 3 Wählen Sie **Quell-IP** aus, um ein Quell-IP-Persistenzprofil hinzuzufügen, und geben Sie die Profildetails ein.

Sie können auch die Standardeinstellungen des Quell-IP-Profiles übernehmen.

Option	Beschreibung
<b>Name und Beschreibung</b>	Geben Sie einen Namen und eine Beschreibung für das Quell-IP-Persistenzprofil ein.
<b>Persistenz freigeben</b>	<p>Schalten Sie die Schaltfläche um, um die Persistenz freizugeben, sodass alle virtuellen Server, denen dieses Profil zugewiesen ist, die Persistenztabelle gemeinsam nutzen können.</p> <p>Wenn die Persistenzfreigabe in dem Quell-IP-Persistenzprofil, das einem virtuellen Server zugeordnet ist, nicht aktiviert ist, verwaltet jeder virtuelle Server, dem das Profil zugeordnet wird, eine private Persistenztabelle.</p>

Option	Beschreibung
<b>Zeitüberschreitung für Persistenzeintrag</b>	<p>Geben Sie den Zeitraum für die Persistenz bis zum Ablauf in Sekunden ein. Die Persistenztabelle des Load Balancers enthält Einträge, die die Weiterleitung von Clientanforderungen an denselben Server aufzeichnen.</p> <ul style="list-style-type: none"> <li>■ Wenn von demselben Client keine neuen Verbindungsanforderungen innerhalb des festgelegten Zeitraums empfangen werden, verfällt der Persistenzeintrag und wird gelöscht.</li> <li>■ Geht von demselben Client innerhalb des festgelegten Zeitraums eine neue Verbindungsanforderung ein, wird der Timer zurückgesetzt und die Clientanforderung an ein verfügbares Poolmitglied gesendet.</li> </ul> <p>Nach Ablauf des festgelegten Zeitraums werden neue Verbindungsanforderungen an einen über den Load Balancing-Algorithmus bestimmten Server gesendet. Für den Fall einer TCP-Quell-IP-Persistenz mit dem L7-Load Balancing legt der Persistenzeintrag den Zeitpunkt fest, ab dem einige Zeit lang keine neuen TCP-Verbindungen erstellt werden, auch wenn die vorhandenen Verbindungen weiterhin aktiv sind.</p>
<b>Bei voller Tabelle Einträge löschen</b>	<p>Schalten Sie die Schaltfläche um, um Einträge zu löschen, wenn die Persistenztabelle voll ist.</p> <p>Ein hoher Wert für die Zeitüberschreitung führt möglicherweise dazu, dass die Persistenztabelle sich schnell füllt, wenn der Datenverkehr hoch ist. Wenn die Persistenztabelle voll ist, wird für den aktuellen Eintrag der älteste Eintrag gelöscht.</p>
<b>HA-Persistenzspiegelung</b>	Schalten Sie die Schaltfläche um, um Persistenzeinträge mit dem HA-Peer zu synchronisieren.
<b>Tags</b>	<p>Geben Sie Tags ein, um die Suche zu vereinfachen.</p> <p>Sie können ein Tag angeben, um einen Geltungsbereich des Tags festzulegen.</p>

#### 4 Wählen Sie ein **Cookie**-Persistenzprofil und geben Sie die Profildetails ein.

Option	Beschreibung
<b>Name und Beschreibung</b>	Geben Sie einen Namen und eine Beschreibung für das Cookie-Persistenzprofil ein.
<b>Persistenz freigeben</b>	<p>Schalten Sie die Schaltfläche um, Persistenz für mehrere virtuelle Server freizugeben, die denselben Poolmitgliedern zugeordnet sind.</p> <p>Das Cookie-Persistenzprofil fügt ein Cookie mit dem Format <code>&lt;name&gt;.&lt;profile-id&gt;.&lt;pool-id&gt;</code> ein.</p> <p>Wenn die freigegebene Persistenz in dem einem virtuellen Server zugeordneten Cookie-Persistenzprofil nicht aktiviert ist, wird für jeden virtuellen Server die private Cookie-Persistenz verwendet und durch das Poolmitglied qualifiziert. Der Load Balancer fügt ein Cookie mit dem Format <code>&lt;name&gt;.&lt;virtual_server_id&gt;.&lt;pool_id&gt;</code> ein.</p>

Option	Beschreibung
<b>Cookiemodus</b>	<p>Wählen Sie im Dropdown-Menü einen Modus aus.</p> <ul style="list-style-type: none"> <li>■ <b>EINFÜGEN</b> – Fügt ein eindeutiges Cookie zur Identifizierung der Sitzung hinzu.</li> <li>■ <b>PRÄFIX</b> – Wird an die vorhandenen HTTP-Cookie-Informationen angefügt.</li> <li>■ <b>UMSCHREIBEN</b> – Schreibt die vorhandenen HTTP-Cookie-Informationen um.</li> </ul>
<b>Cookiename</b>	Geben Sie den Cookienamen ein.
<b>Cookie-domäne</b>	<p>Geben Sie den Domännennamen ein.</p> <p>Die HTTP-Cookie-domäne kann nur im Modus EINFÜGEN konfiguriert werden.</p>
<b>Cookie-Fallback</b>	<p>Schalten Sie die Schaltfläche um, sodass die Clientanforderung abgelehnt wird, wenn ein Cookie auf einen Server verweist, der sich im Status DEAKTIVIERT oder INAKTIV befindet.</p> <p>Wählt einen neuen Server für die Verarbeitung einer Clientanforderung aus, wenn das Cookie auf einen Server verweist, der sich im Status DEAKTIVIERT oder INAKTIV befindet.</p>
<b>Cookiepfad</b>	<p>Geben Sie den URL-Pfad des Cookies ein.</p> <p>Der HTTP-Cookiepfad kann nur im Modus EINFÜGEN festgelegt werden.</p>
<b>Cookieverschlüsselung</b>	<p>Schalten Sie die Schaltfläche um, um die Verschlüsselung zu deaktivieren.</p> <p>Wenn die Verschlüsselung deaktiviert ist, liegen die Informationen zu IP-Adresse und Port des Cookieservers unverschlüsselt vor. Verschlüsseln Sie die Informationen zu IP-Adresse und Port des Cookieservers.</p>
<b>Cookie-Typ</b>	<p>Wählen Sie im Dropdown-Menü einen Cookietyp aus.</p> <p><b>Sitzungs-Cookie</b> – wird nicht gespeichert. Geht verloren, wenn der Browser geschlossen wird.</p> <p><b>Persistenz-Cookie</b> – wird vom Browser gespeichert. Geht nicht verloren, wenn der Browser geschlossen wird.</p>
<b>Maximale Leerlaufzeit</b>	Geben Sie die Zeit in Sekunden ein, in der der Cookietyp im Leerlauf verweilen kann, bevor ein Cookie abläuft.
<b>Maximales Cookie-Alter</b>	Geben Sie für Sitzungscookies die Zeit in Sekunden ein, die ein Cookie verfügbar ist.
<b>Tags</b>	<p>Geben Sie Tags ein, um die Suche zu vereinfachen.</p> <p>Sie können ein Tag angeben, um einen Geltungsbereich des Tags festzulegen.</p>

## Hinzufügen eines SSL-Profiles

SSL-Profile konfigurieren anwendungsunabhängige SSL-Eigenschaften, beispielsweise Verschlüsselungslisten, und verwenden diese Listen für mehrere Anwendungen. SSL-Eigenschaften sind unterschiedlich, wenn der Load Balancer als Client und als Server dient. Daher werden separate SSL-Profile für die Client- und die Serverseite unterstützt.

**Hinweis** SSL-Profile werden in der Version NSX-T Data Center Limited Export nicht unterstützt.

Das clientseitige SSL-Profil verweist auf den Load Balancer, der als SSL-Server agiert und die SSL-Verbindung des Clients beendet. Das serverseitige SSL-Profil verweist auf den Load Balancer, der als Client agiert und eine Verbindung mit dem Server herstellt.

Sie können sowohl in den client- als auch in den serverseitigen SSL-Profilen eine Verschlüsselungsliste angeben.

Durch das Caching von SSL-Sitzungen sind SSL-Client und -Server in der Lage, zuvor ausgehandelte Sicherheitsparameter wiederzuverwenden. Hierdurch wird das aufwändige Verfahren mit öffentlichen Schlüsseln während des SSL-Handshakes vermieden. Das Caching von SSL-Sitzungen ist standardmäßig sowohl auf Client- als auch auf Serverseite deaktiviert.

Bei SSL-Sitzungstickets handelt es sich um ein alternatives Verfahren, das dem SSL-Client und -Server die Wiederverwendung von zuvor ausgehandelten Sitzungsparametern ermöglicht. In SSL-Sitzungstickets handeln der Client und der Server aus, ob sie während des Handshake-Austauschs SSL-Sitzungstickets unterstützen. Wenn beide die Tickets unterstützen, kann der Server ein SSL-Ticket mit verschlüsselten SSL-Sitzungsparametern an den Client senden. Der Client kann dieses Ticket in nachfolgenden Verbindungen verwenden, um die Sitzung wiederzuverwenden. SSL-Sitzungstickets sind auf der Clientseite aktiviert und auf der Serverseite deaktiviert.

**Abbildung 7-5. SSL-Offloading**

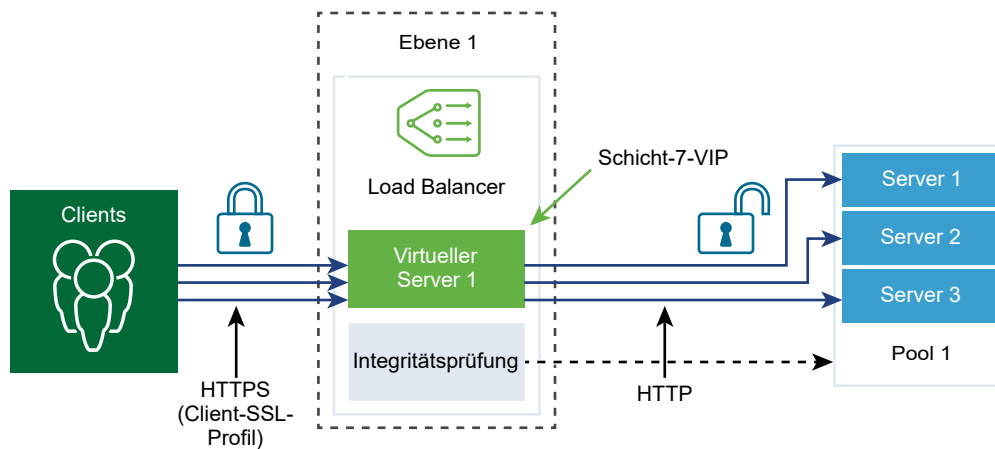
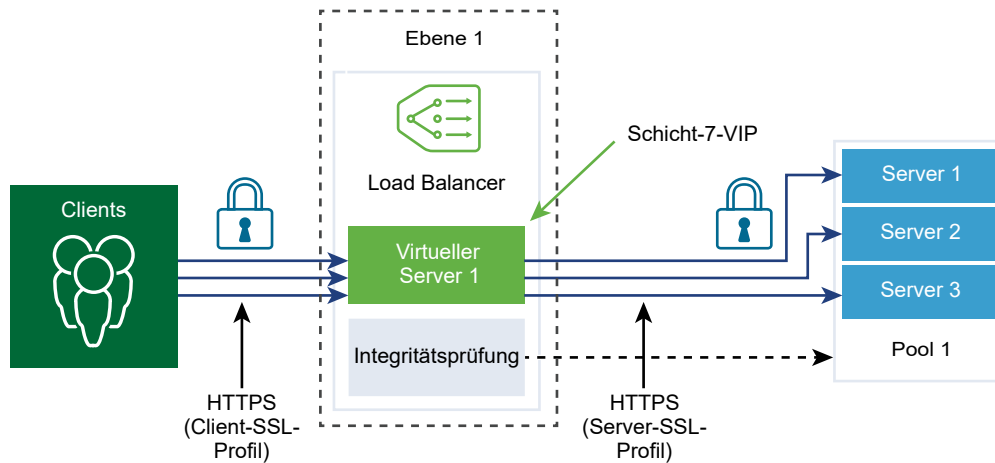


Abbildung 7-6. End-to-End-SSL



### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk > Load Balancing > Profile > SSL-Profil** aus.
- 3 Wählen Sie ein **SSL-Profil des Clients** aus und geben Sie die Profildetails ein.

Option	Beschreibung
<b>Name und Beschreibung</b>	Geben Sie einen Namen und eine Beschreibung für das SSL-Clientprofil ein.
<b>SSL-Suite</b>	Wählen Sie die SSL-Verschlüsselungsgruppe im Dropdown-Menü aus, und die in das Client-SSL-Profil aufzunehmenden verfügbaren SSL-Verschlüsselungen und -Protokolle werden befüllt. Die SSL-Verschlüsselungsgruppe „Ausgeglichen“ stellt den Standardwert dar.
<b>Sitzungs-Caching</b>	Verwenden Sie die Umschaltfläche, damit der SSL-Client und -Server zuvor ausgehandelte Sicherheitsparameter wiederverwenden kann. Hierdurch wird das aufwändige Verfahren mit öffentlichen Schlüsseln während eines SSL-Handshakes vermieden.
<b>Tags</b>	Geben Sie Tags ein, um die Suche zu vereinfachen. Sie können ein Tag angeben, um einen Geltungsbereich des Tags festzulegen.
<b>Unterstützte SSL-Verschlüsselungen</b>	Je nach zugewiesener SSL-Suite werden die unterstützten SSL-Verschlüsselungen hier aufgefüllt. Klicken Sie auf <b>Mehr anzeigen</b> , um die gesamte Liste anzuzeigen. Bei Auswahl von <b>Benutzerdefiniert</b> müssen Sie die SSL-Verschlüsselungen im Dropdown-Menü auswählen.
<b>Unterstützte SSL-Protokolle</b>	Je nach zugewiesener SSL-Suite werden die unterstützten SSL-Protokolle hier aufgefüllt. Klicken Sie auf <b>Mehr anzeigen</b> , um die gesamte Liste anzuzeigen. Bei Auswahl von <b>Benutzerdefiniert</b> müssen Sie die SSL-Verschlüsselungen im Dropdown-Menü auswählen.

Option	Beschreibung
<b>Zeitüberschreitung für Cache-Eintrag der Sitzung</b>	Geben Sie die Zeitüberschreitung für den Cache in Sekunden an, um festzulegen, wie lange die SSL-Sitzungsparameter beibehalten werden müssen und wiederverwendet werden können.
<b>Serververschlüsselung bevorzugen</b>	Schalten Sie die Schaltfläche um, sodass der Server die erste unterstützte Verschlüsselung aus der Liste auswählen kann, die er unterstützen kann. Während eines SSL-Handshakes sendet der Client eine sortierte Liste der unterstützten Verschlüsselungen an den Server.

#### 4 Wählen Sie ein **SSL-Profil des Servers** aus und geben Sie die Profildetails ein.

Option	Beschreibung
<b>Name und Beschreibung</b>	Geben Sie einen Namen und eine Beschreibung für das SSL-Serverprofil ein.
<b>SSL-Suite</b>	Wählen Sie die SSL-Verschlüsselungsgruppe im Dropdown-Menü aus, und die in das Server-SSL-Profil aufzunehmenden verfügbaren SSL-Verschlüsselungen und -Protokolle werden befüllt. Die SSL-Verschlüsselungsgruppe „Ausgeglichen“ stellt den Standardwert dar.
<b>Sitzungs-Caching</b>	Verwenden Sie die Umschaltfläche, damit der SSL-Client und -Server zuvor ausgehandelte Sicherheitsparameter wiederverwenden kann. Hierdurch wird das aufwändige Verfahren mit öffentlichen Schlüsseln während eines SSL-Handshakes vermieden.
<b>Tags</b>	Geben Sie Tags ein, um die Suche zu vereinfachen. Sie können ein Tag angeben, um einen Geltungsbereich des Tags festzulegen.
<b>Unterstützte SSL-Verschlüsselungen</b>	Je nach zugewiesener SSL-Suite werden die unterstützten SSL-Verschlüsselungen hier aufgefüllt. Klicken Sie auf <b>Mehr anzeigen</b> , um die gesamte Liste anzuzeigen. Bei Auswahl von <b>Benutzerdefiniert</b> müssen Sie die SSL-Verschlüsselungen im Dropdown-Menü auswählen.
<b>Unterstützte SSL-Protokolle</b>	Je nach zugewiesener SSL-Suite werden die unterstützten SSL-Protokolle hier aufgefüllt. Klicken Sie auf <b>Mehr anzeigen</b> , um die gesamte Liste anzuzeigen. Bei Auswahl von <b>Benutzerdefiniert</b> müssen Sie die SSL-Verschlüsselungen im Dropdown-Menü auswählen.
<b>Zeitüberschreitung für Cache-Eintrag der Sitzung</b>	Geben Sie die Zeitüberschreitung für den Cache in Sekunden an, um festzulegen, wie lange die SSL-Sitzungsparameter beibehalten werden müssen und wiederverwendet werden können.
<b>Serververschlüsselung bevorzugen</b>	Schalten Sie die Schaltfläche um, sodass der Server die erste unterstützte Verschlüsselung aus der Liste auswählen kann, die er unterstützen kann. Während eines SSL-Handshakes sendet der Client eine sortierte Liste der unterstützten Verschlüsselungen an den Server.

## Hinzufügen von virtuellen Servern der Schicht 4

Virtuelle Server empfangen alle Clientverbindungen und verteilen diese an die Server. Ein virtueller Server verfügt über eine IP-Adresse, einen Port und ein Protokoll. Für virtuelle Server

der Schicht 4 können anstelle einzelner TCP- oder UDP-Ports Listen mit Portbereichen angegeben werden, um komplexe Protokolle mit dynamischen Ports zu unterstützen.

Ein virtueller Server der Schicht 4 muss mit einem primären Serverpool, der auch als Standardpool bezeichnet wird, verknüpft werden.

Wenn der Status eines virtuellen Servers „Deaktiviert“ lautet, werden alle neuen Verbindungsversuche mit dem virtuellen Server abgelehnt, indem entweder ein TCP RST für die TCP-Verbindung oder eine ICMP-Fehlermeldung für UDP gesendet wird. Neue Verbindungen werden abgelehnt, selbst wenn passende Persistenzeinträge für sie vorhanden sind. Aktive Verbindungen werden weiterhin verarbeitet. Wenn ein virtueller Server gelöscht oder von einem Load Balancer getrennt wird, schlagen aktive Verbindungen mit diesem virtuellen Server fehl.

### Voraussetzungen

- Stellen Sie sicher, dass Anwendungsprofile verfügbar sind. Siehe [Hinzufügen eines Anwendungsprofils](#).
- Stellen Sie sicher, dass persistente Profile verfügbar sind. Siehe [Hinzufügen eines Persistenzprofils](#).
- Stellen Sie sicher, dass SSL-Profile für Client und Server verfügbar sind. Siehe [Hinzufügen eines SSL-Profils](#).
- Stellen Sie sicher, dass Serverpools verfügbar sind. Siehe [Hinzufügen eines Serverpools](#).
- Stellen Sie sicher, dass der Load Balancer verfügbar ist. Siehe [Hinzufügen von Load Balancern](#).

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk > Load Balancing > Virtuelle Server > Virtuellen Server hinzufügen** aus.
- 3 Wählen Sie ein **L4-TCP**-Protokoll aus und geben Sie die Protokolldetails ein.

Virtuelle Server der Schicht 4 unterstützen entweder das Fast TCP- oder das Fast UDP-Protokoll.

Damit das Fast TCP- oder das Fast UDP-Protokoll für dieselbe IP-Adresse und denselben Port unterstützt wird, wie z. B. DNS, muss für jedes Protokoll ein virtueller Server erstellt werden.

Option	Beschreibung
<b>Name und Beschreibung</b>	Geben Sie einen Namen und eine Beschreibung für den virtuellen Server der Schicht 4 ein.
<b>IP-Adresse</b>	Geben Sie die IP-Adresse des virtuellen Servers ein.
<b>Ports</b>	Geben Sie die Portnummer des virtuellen Servers ein.



Option	Beschreibung
<b>Load Balancer</b>	Wählen Sie im Dropdown-Menü einen vorhandenen Load Balancer aus, der an diesen virtuellen Server der Schicht 4 angehängt werden soll.
<b>Serverpool</b>	<p>Wählen Sie im Dropdown-Menü einen vorhandenen Serverpool aus.</p> <p>Der Serverpool besteht aus einem oder mehreren auch als Poolmitglieder bezeichneten Servern mit ähnlicher Konfiguration, auf denen dieselbe Anwendung ausgeführt wird.</p> <p>Sie können auf die vertikalen Punkte klicken, um einen Serverpool zu erstellen.</p>
<b>Anwendungsprofil</b>	<p>Je nach Protokolltyp wird das vorhandene Anwendungsprofil automatisch befüllt.</p> <p>Sie können auf die vertikalen Punkte klicken, um ein Anwendungsprofil zu erstellen.</p>
<b>Persistenz</b>	<p>Wählen Sie im Dropdown-Menü ein vorhandenes Persistenzprofil aus.</p> <p>Das Persistenzprofil kann auf einem virtuellen Server aktiviert werden, damit auf die Quell-IP bezogene Clientverbindungen an denselben Server gesendet werden können.</p>
<b>Max. Anzahl gleichzeitiger Verbindungen</b>	Legen Sie die maximale Anzahl gleichzeitiger Verbindungen fest, die für einen virtuellen Server zulässig sind, damit der virtuelle Server nicht die Ressourcen anderer Anwendung verbraucht, die vom selben Load Balancer gehostet werden.
<b>Max. Anzahl neuer Verbindungen</b>	Legen Sie die maximale Anzahl neuer Verbindungen für ein Serverpoolmitglied fest, damit ein virtueller Server die Ressourcen nicht überlastet.
<b>Sorry-Serverpool</b>	<p>Wählen Sie im Dropdown-Menü einen vorhandenen Sorry-Serverpool aus.</p> <p>Der Sorry-Serverpool stellt die Anforderung zu, wenn ein Load Balancer keinen Backend-Server auswählen kann, um die Anforderung aus dem Standardpool zuzustellen.</p> <p>Sie können auf die vertikalen Punkte klicken, um einen Serverpool zu erstellen.</p>
<b>Standardport des Poolmitglieds</b>	<p>Geben Sie den Standardport eines Poolmitglieds ein, wenn der Port des Poolmitglieds für einen virtuellen Server nicht definiert ist.</p> <p>Wenn ein virtueller Server beispielsweise mit dem Portbereich 2000-2999 definiert ist und der Standardportbereich des Poolmitglieds auf 8000-8999 festgelegt ist, wird eine eingehende Clientverbindung für Port 2500 des virtuellen Servers an ein Poolmitglied mit einem auf 8500 gesetzten Zielport gesendet.</p>
<b>Administrativer Zustand</b>	Klicken Sie auf den Schalter, um den Admin-Zustand des virtuellen Servers der Schicht 4 zu deaktivieren.
<b>Zugriffsprotokoll</b>	Klicken Sie auf den Schalter, um die Protokollierung für den virtuellen Server der Schicht 4 zu aktivieren.
<b>Tags</b>	<p>Geben Sie Tags ein, um die Suche zu vereinfachen.</p> <p>Sie können ein Tag angeben, um einen Geltungsbereich des Tags festzulegen.</p>

#### 4 Wählen Sie ein **L4-UDP**-Protokoll aus und geben Sie die Protokolldetails ein.

Option	Beschreibung
<b>Name und Beschreibung</b>	Geben Sie einen Namen und eine Beschreibung für den virtuellen Server der Schicht 4 ein.
<b>IP-Adresse</b>	Geben Sie die IP-Adresse des virtuellen Servers ein.
<b>Ports</b>	Geben Sie die Portnummer des virtuellen Servers ein.
<b>Load Balancer</b>	Wählen Sie im Dropdown-Menü einen vorhandenen Load Balancer aus, der an diesen virtuellen Server der Schicht 4 angehängt werden soll.
<b>Serverpool</b>	<p>Wählen Sie im Dropdown-Menü einen vorhandenen Serverpool aus.</p> <p>Der Serverpool besteht aus einem oder mehreren auch als Poolmitglieder bezeichneten Servern mit ähnlicher Konfiguration, auf denen dieselbe Anwendung ausgeführt wird.</p> <p>Sie können auf die vertikalen Punkte klicken, um einen Serverpool zu erstellen.</p>
<b>Anwendungsprofil</b>	<p>Je nach Protokolltyp wird das vorhandene Anwendungsprofil automatisch befüllt.</p> <p>Sie können auf die vertikalen Punkte klicken, um ein Anwendungsprofil zu erstellen.</p>
<b>Persistenz</b>	<p>Wählen Sie im Dropdown-Menü ein vorhandenes Persistenzprofil aus.</p> <p>Das Persistenzprofil kann auf einem virtuellen Server aktiviert werden, damit auf die Quell-IP bezogene Clientverbindungen an denselben Server gesendet werden können.</p>
<b>Max. Anzahl gleichzeitiger Verbindungen</b>	Legen Sie die maximale Anzahl gleichzeitiger Verbindungen fest, die für einen virtuellen Server zulässig sind, damit der virtuelle Server nicht die Ressourcen anderer Anwendung verbraucht, die vom selben Load Balancer gehostet werden.
<b>Max. Anzahl neuer Verbindungen</b>	Legen Sie die maximale Anzahl neuer Verbindungen für ein Serverpoolmitglied fest, damit ein virtueller Server die Ressourcen nicht überlastet.
<b>Sorry-Serverpool</b>	<p>Wählen Sie im Dropdown-Menü einen vorhandenen Sorry-Serverpool aus.</p> <p>Der Sorry-Serverpool stellt die Anforderung zu, wenn ein Load Balancer keinen Backend-Server auswählen kann, um die Anforderung aus dem Standardpool zuzustellen.</p> <p>Sie können auf die vertikalen Punkte klicken, um einen Serverpool zu erstellen.</p>
<b>Standardport des Poolmitglieds</b>	<p>Geben Sie den Standardport eines Poolmitglieds ein, wenn der Port des Poolmitglieds für einen virtuellen Server nicht definiert ist.</p> <p>Wenn ein virtueller Server beispielsweise mit dem Portbereich 2000-2999 definiert ist und der Standardportbereich des Poolmitglieds auf 8000-8999 festgelegt ist, wird eine eingehende Clientverbindung für Port 2500 des virtuellen Servers an ein Poolmitglied mit einem auf 8500 gesetzten Zielport gesendet.</p>
<b>Administrativer Zustand</b>	Klicken Sie auf den Schalter, um den Admin-Zustand des virtuellen Servers der Schicht 4 zu deaktivieren.

Option	Beschreibung
<b>Zugriffsprotokoll</b>	Klicken Sie auf den Schalter, um die Protokollierung für den virtuellen Server der Schicht 4 zu aktivieren.
<b>Tags</b>	Geben Sie Tags ein, um die Suche zu vereinfachen. Sie können ein Tag angeben, um einen Geltungsbereich des Tags festzulegen.

## Hinzufügen von virtuellen HTTP-Servern der Schicht 7

Virtuelle Server empfangen alle Clientverbindungen und verteilen diese an die Server. Ein virtueller Server verfügt über eine IP-Adresse, einen Port und ein TCP-Protokoll.

Load Balancer-Regeln werden nur für virtuelle Server der Schicht 7 unterstützt, die ein HTTP-Anwendungsprofil aufweisen. Verschiedene Load Balancer-Dienste können Load Balancer-Regeln verwenden.

Jede Load Balancer-Regel besteht aus einzelnen oder mehreren Übereinstimmungsbedingungen und Aktionen. Wenn keine Übereinstimmungsbedingungen angegeben sind, stimmt die Load Balancer-Regel immer überein und wird zum Definieren von Standardregeln verwendet. Wenn mehr als eine Übereinstimmungsbedingung angegeben wird, bestimmt die Übereinstimmungsstrategie, ob alle Bedingungen oder eine beliebige Bedingung erfüllt sein muss, damit die Load Balancer-Regel als Übereinstimmung angesehen wird.

Jede Load Balancer-Regel wird während einer bestimmten Phase der Load Balancing-Verarbeitung implementiert (Umschreiben der HTTP-Anfrage, Weiterleiten der HTTP-Anfrage und Umschreiben der HTTP-Antwort). Nicht alle Übereinstimmungsbedingungen und Aktionen sind auf jede Phase anwendbar.

---

**Hinweis** Schicht-7-SSL-Passthrough wird in NSX-T Data Center 3.0 und höher unterstützt.

---

Wenn der Status eines virtuellen Servers „Deaktiviert“ lautet, werden alle neuen Verbindungsversuche mit dem virtuellen Server abgelehnt, indem entweder ein TCP RST für die TCP-Verbindung oder eine ICMP-Fehlermeldung für UDP gesendet wird. Neue Verbindungen werden abgelehnt, selbst wenn passende Persistenzeinträge für sie vorhanden sind. Aktive Verbindungen werden weiterhin verarbeitet. Wenn ein virtueller Server gelöscht oder von einem Load Balancer getrennt wird, schlagen aktive Verbindungen mit diesem virtuellen Server fehl.

---

**Hinweis** SSL-Profil werden in der Version NSX-T Data Center Limited Export nicht unterstützt.

---

Wenn eine clientseitige, nicht aber eine serverseitige SSL-Profilbindung auf einem virtuellen Server konfiguriert wurde, wird der virtuelle Server im SSL-Terminate-Modus ausgeführt, der eine verschlüsselte Verbindung zum Client und eine Klartextverbindung zum Server aufweist. Wenn sowohl die clientseitigen als auch die serverseitigen SSL-Profilbindungen konfiguriert sind, wird der virtuelle Server im SSL-Proxy-Modus ausgeführt, der eine verschlüsselte Verbindung zum Client und Server aufweist.

Das Zuordnen einer serverseitigen SSL-Profilbindung ohne Zuordnung einer clientseitigen SSL-Profilbindung wird aktuell nicht unterstützt. Wenn weder eine clientseitige noch eine serverseitige SSL-Profilbindung mit einem virtuellen Server verknüpft und die Anwendung SSL-basiert ist, wird der virtuelle Server im SSL-Unaware-Modus ausgeführt. In diesem Fall muss der virtuelle Server für Schicht 4 konfiguriert werden. Der virtuelle Server kann beispielsweise einem Fast TCP-Profil zugeordnet werden.

#### Voraussetzungen

- Stellen Sie sicher, dass Anwendungsprofile verfügbar sind. Siehe [Hinzufügen eines Anwendungsprofils](#).
- Stellen Sie sicher, dass persistente Profile verfügbar sind. Siehe [Hinzufügen eines Persistenzprofils](#).
- Stellen Sie sicher, dass SSL-Profile für Client und Server verfügbar sind. Siehe [Hinzufügen eines SSL-Profils](#).
- Stellen Sie sicher, dass Serverpools verfügbar sind. Siehe [Hinzufügen eines Serverpools](#).
- Stellen Sie sicher, dass Zertifizierungsstelle und Clientzertifikat verfügbar sind. Siehe [Erstellen einer Datei für die Zertifikatsignieranforderung](#).
- Stellen Sie sicher, dass eine Zertifikatssperrliste (CRL) verfügbar ist. Siehe [Importieren einer Zertifikatswiderrufsliste](#).
- Stellen Sie sicher, dass der Load Balancer verfügbar ist. Siehe [Hinzufügen von Load Balancern](#).

#### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk > Load Balancing > Virtuelle Server > Virtuellen Server hinzufügen** aus.
- 3 Wählen Sie ein **L7-HTTP**-Protokoll aus und geben Sie die Protokolldetails ein.

Virtuelle Server der Schicht 7 unterstützen das HTTP- und HTTPS-Protokoll.

Option	Beschreibung
<b>Name und Beschreibung</b>	Geben Sie einen Namen und eine Beschreibung für den virtuellen Server der Schicht ein.
<b>IP-Adresse</b>	Geben Sie die IP-Adresse des virtuellen Servers ein.
<b>Ports</b>	Geben Sie die Portnummer des virtuellen Servers ein.
<b>Load Balancer</b>	Wählen Sie im Dropdown-Menü einen vorhandenen Load Balancer aus, der an diesen virtuellen Server der Schicht 4 angehängt werden soll.

Option	Beschreibung
<b>Serverpool</b>	<p>Wählen Sie im Dropdown-Menü einen vorhandenen Serverpool aus.</p> <p>Der Serverpool besteht aus einem oder mehreren auch als Poolmitglieder bezeichneten Servern mit ähnlicher Konfiguration, auf denen dieselbe Anwendung ausgeführt wird.</p> <p>Sie können auf die vertikalen Punkte klicken, um einen Serverpool zu erstellen.</p>
<b>Anwendungsprofil</b>	<p>Je nach Protokolltyp wird das vorhandene Anwendungsprofil automatisch befüllt.</p> <p>Sie können auf die vertikalen Punkte klicken, um ein Anwendungsprofil zu erstellen.</p>
<b>Persistenz</b>	<p>Wählen Sie im Dropdown-Menü ein vorhandenes Persistenzprofil aus.</p> <p>Das Persistenzprofil kann auf einem virtuellen Server aktiviert werden, damit auf die Quell-IP und auf Cookies bezogene Clientverbindungen an denselben Server gesendet werden können.</p>

- 4 Klicken Sie auf **Konfigurieren**, um SSL für den virtuellen Server der Schicht 7 festzulegen.  
Sie können Client-SSL und Server-SSL konfigurieren.
- 5 Konfigurieren Sie Client-SSL.

Option	Beschreibung
<b>Client-SSL</b>	<p>Klicken Sie auf den Schalter, um das Profil zu aktivieren.</p> <p>Clientseitige SSL-Profilbindung ermöglicht mehrere Zertifikate, damit verschiedene Hostnamen mit demselben virtuellen Server verbunden werden können.</p>
<b>Standardzertifikat</b>	<p>Wählen Sie im Dropdown-Menü ein Standardzertifikat aus.</p> <p>Dieses Zertifikat wird verwendet, wenn der Server nicht mehrere Hostnamen auf derselben IP-Adresse hostet oder wenn der Client keine Unterstützung für SNI-Erweiterungen (Server Name Indication) bietet.</p>
<b>SSL-Profil des Clients</b>	Wählen Sie das clientseitige SSL-Profil im Dropdown-Menü aus.
<b>SNI-Zertifikate</b>	Wählen Sie das verfügbare SNI-Zertifikat im Dropdown-Menü aus.
<b>Vertrauenswürdige CA-Zertifikate</b>	Wählen Sie das verfügbare CA-Zertifikat aus.
<b>Obligatorische Clientauthentifizierung</b>	Klicken Sie auf den Schalter, um dieses Menüelement zu aktivieren.
<b>Tiefe der Zertifikatskette</b>	Legen Sie die Tiefe der Zertifikatskette fest, um die Tiefe in der Serverzertifikatskette zu überprüfen.
<b>Zertifikatswiderrufsliste</b>	Wählen Sie die verfügbare Zertifikatswiderrufsliste (CRL) aus, um gefährdete Serverzertifikate zu deaktivieren.

## 6 Konfigurieren Sie Server-SSL.

Option	Beschreibung
<b>Server-SSL</b>	Klicken Sie auf den Schalter, um das Profil zu aktivieren.
<b>Clientzertifikat</b>	Wählen Sie im Dropdown-Menü ein Clientzertifikat aus. Dieses Zertifikat wird verwendet, wenn der Server nicht mehrere Hostnamen auf derselben IP-Adresse hostet oder wenn der Client keine Unterstützung für SNI-Erweiterungen (Server Name Indication) bietet.
<b>SSL-Profil des Servers</b>	Wählen Sie das serverseitige SSL-Profil im Dropdown-Menü aus.
<b>Vertrauenswürdige CA-Zertifikate</b>	Wählen Sie das verfügbare CA-Zertifikat aus.
<b>Obligatorische Serverauthentifizierung</b>	Klicken Sie auf den Schalter, um dieses Menüelement zu aktivieren. Eine serverseitige SSL-Profilbindung gibt an, ob das dem Load Balancer während des SSL-Handshakes präsentierte Serverzertifikat validiert werden muss. Bei aktivierter Validierung muss das Serverzertifikat von einer der vertrauenswürdigen Zertifizierungsstellen signiert sein, deren selbstsignierte Zertifikate in derselben serverseitigen SSL-Profilbindung angegeben sind.
<b>Tiefe der Zertifikatskette</b>	Legen Sie die Tiefe der Zertifikatskette fest, um die Tiefe in der Serverzertifikatskette zu überprüfen.
<b>Zertifikatswiderrufsliste</b>	Wählen Sie die verfügbare Zertifikatswiderrufsliste (CRL) aus, um gefährdete Serverzertifikate zu deaktivieren. OCSP und OCSP-Heftung werden serverseitig nicht unterstützt.

## 7 Konfigurieren Sie weitere Eigenschaften des virtuellen Servers der Schicht 7.

Option	Beschreibung
<b>Max. Anzahl gleichzeitiger Verbindungen</b>	Legen Sie die maximale Anzahl gleichzeitiger Verbindungen fest, die für einen virtuellen Server zulässig sind, damit der virtuelle Server nicht die Ressourcen anderer Anwendung verbraucht, die vom selben Load Balancer gehostet werden.
<b>Max. Anzahl neuer Verbindungen</b>	Legen Sie die maximale Anzahl neuer Verbindungen für ein Serverpoolmitglied fest, damit ein virtueller Server die Ressourcen nicht überlastet.
<b>Sorry-Serverpool</b>	Wählen Sie im Dropdown-Menü einen vorhandenen Sorry-Serverpool aus. Der Sorry-Serverpool stellt die Anforderung zu, wenn ein Load Balancer keinen Backend-Server auswählen kann, um die Anforderung aus dem Standardpool zuzustellen. Sie können auf die vertikalen Punkte klicken, um einen Serverpool zu erstellen.
<b>Standardport des Poolmitglieds</b>	Geben Sie den Standardport eines Poolmitglieds ein, wenn der Port des Poolmitglieds für einen virtuellen Server nicht definiert ist. Wenn ein virtueller Server beispielsweise mit dem Portbereich 2000-2999 definiert ist und der Standardportbereich des Poolmitglieds auf 8000-8999 festgelegt ist, wird eine eingehende Clientverbindung für Port 2500 des virtuellen Servers an ein Poolmitglied mit einem auf 8500 gesetzten Zielpport gesendet.
<b>Administrativer Zustand</b>	Klicken Sie auf den Schalter, um den administrativen Zustand des virtuellen Servers der Schicht 7 zu deaktivieren.

Option	Beschreibung
<b>Zugriffsprotokoll</b>	Klicken Sie auf den Schalter, um die Protokollierung für den virtuellen Server der Schicht 7 zu aktivieren.
<b>Tags</b>	Geben Sie Tags ein, um die Suche zu vereinfachen. Sie können ein Tag angeben, um einen Geltungsbereich des Tags festzulegen.

## Anzeigen von Load Balancer-Regeln

Auf virtuellen HTTP-Servern der Schicht 7 können Sie optional Load Balancer-Regeln konfigurieren und das Lastausgleichsverhalten unter Verwendung von Übereinstimmungs- oder Aktionsregeln anpassen.

Load Balancer-Regeln unterstützen die Verwendung von regulären Ausdrücken (Regex) für Übereinstimmungstypen. Regex-Muster nach PCRE-Art werden mit einigen Einschränkungen für anspruchsvollere Anwendungsfälle unterstützt. Wenn Regex in Übereinstimmungsbedingungen verwendet wird, werden benannte erfassende Gruppierungskonstrukte unterstützt.

Bezüglich der Verwendung von Regex gelten folgende Einschränkungen:

- Vereinigungen und Schnittmengen von Zeichenklassen werden nicht unterstützt. Verwenden Sie beispielsweise nicht `[a-z[0-9]]` und `[a-z&&[aeiou]]`, sondern stattdessen `[a-z0-9]` bzw. `[aeiou]`.
- Es werden nur 9 Rückverweise unterstützt, und man kann sie mit Hilfe von `\1` bis `\9` referenzieren.
- Verwenden Sie zum Abgleichen von Oktalzeichen das `\Odd`-Format, nicht das `\ddd`-Format.
- Eingebettete Flags werden auf der obersten Ebene nicht unterstützt. Sie können nur innerhalb von Gruppen verwendet werden. Verwenden Sie beispielsweise nicht „Case (?i:sensitive“, sondern stattdessen „Case ((?i:sensitive)“.
- Die Vorverarbeitungsoperationen `\l`, `\u`, `\L` und `\U` werden nicht unterstützt. Dabei steht `\l` für Kleinschreibung des nächsten Zeichens, `\u` für Großschreibung des nächsten Zeichens, `\L` für Kleinschreibung bis `\E` und `\U` für Großschreibung bis `\E`.
- „`(?(condition)X)`“, „`(?{Code})`“, „`(??{Code})`“ und „`(?#comment)`“ werden nicht unterstützt.
- Die vordefinierte Unicode-Zeichenklasse `\X` wird nicht unterstützt
- Die Verwendung von benannten Zeichenkonstrukten für Unicode-Zeichen wird nicht unterstützt. Verwenden Sie beispielsweise nicht „`\N{name}`“, sondern stattdessen „`\u2018`“.

Wenn Regex in Übereinstimmungsbedingungen verwendet wird, werden benannte erfassende Gruppierungskonstrukte unterstützt. Beispielsweise kann das Regex-Übereinstimmungsmuster „`/news/(?<year>\d+)-(?(month>\d+)-(?(day>\d+)/(?<article>.*))`“ für den Abgleich mit einem URI wie „`/news/2018-06-15/news1234.html`“ verwendet werden.

Dann werden die Variablen wie folgt belegt: `$year = "2018"`, `$month = "06"`, `$day = "15"` und `$article = "news1234.html"`. Nachdem Sie die Variablen festgelegt haben, können diese in Regeln eines Load Balancers verwendet werden. Der URI kann z. B. mithilfe der übereinstimmenden Variablen wie `„/news.py?year=$year&month=$month&day=$day&article=$article“` umgeschrieben werden. Dann wird der URI in `„/news.py?year=2018&month=06&day=15&article=news1234.html“` umgeschrieben.

Umschreibungsaktionen können eine Kombination von benannten Erfassungsgruppen und integrierten Variablen verwenden. Der URI kann beispielsweise als `„/news.py?year=$year&month=$month&day=$day&article=$article&user_ip=$_remote_addr“` geschrieben werden. Der Beispiel-URI wird dann in `„/news.py?year=2018&month=06&day=15&article=news1234.html&user_ip=1.1.1.1“` umgeschrieben.

---

**Hinweis** Der Name einer benannten Erfassungsgruppe darf nicht mit einem Unterstrich (`_`) beginnen.

---

Zusätzlich zu benannten Erfassungsgruppen können die folgenden integrierten Variablen in Umschreibungsaktionen verwendet werden. Alle Namen der integrierten Variablen beginnen mit Unterstrich (`_`).

- `$_args` – Argumente der Anforderung
- `$_cookie_<name>` – Wert des `<name>`-Cookies
- `$_host` – in der folgenden Rangfolge: der Hostname aus der Anforderungszeile oder der Hostname im Anforderungsheader-Feld „Host“ oder der mit einer Anforderung übereinstimmende Servername
- `$_hostname` – Hostname
- `$_http_<name>` – beliebiges Feld des Anforderungsheaders; `<name>` ist der Name des Felds, konvertiert in Kleinbuchstaben, in dem Bindestriche durch Unterstriche ersetzt wurden.
- `$_https` – „on“, wenn die Verbindung im SSL-Modus arbeitet, andernfalls „“
- `$_is_args` – „?“ , wenn eine Anforderungszeile Argumente enthält, andernfalls „“
- `$_query_string` – identisch mit „`$_args`“
- `$_remote_addr` – Client-Adresse
- `$_remote_port` – Client-Port
- `$_request_uri` – vollständiger ursprünglicher Anforderungs-URI (mit Argumenten)
- `$_scheme` – Anforderungsschema, „http“ oder „https“
- `$_server_addr` – Adresse des Servers, der eine Anforderung akzeptiert hat
- `$_server_name` – Name des Servers, der eine Anforderung akzeptiert hat
- `$_server_port` – Port des-Servers, der eine Anforderung akzeptiert hat
- `$_server_protocol` – Anforderungsprotokoll, in der Regel „HTTP/1.0“ oder „HTTP/1.1“



- `$_ssl_client_cert` – gibt für eine eingerichtete SSL-Verbindung das Client-Zertifikat im PEM-Format zurück, wobei jeder Zeile außer der ersten ein Tabulatorzeichen vorangestellt ist
- `$_ssl_server_name` – gibt den über SNI angeforderten Servernamen zurück
- `$_uri` – URI-Pfad in der Anforderung

### Voraussetzungen

Stellen Sie sicher, dass ein virtueller HTTP-Server der Schicht 7 verfügbar ist. Siehe [Hinzufügen von virtuellen HTTP-Servern der Schicht 7](#).

### Verfahren

- 1 Öffnen Sie den virtuellen HTTP-Server der Schicht 7.
- 2 Klicken Sie im Abschnitt Load Balancer-Regeln auf **Festlegen > Regel hinzufügen**, um die Load Balancer-Regel für die Phase „HTTP-Anforderungsrewrite“ zu konfigurieren.

Zu den unterstützten Übereinstimmungstypen gehören REGEX, STARTS\_WITH, ENDS\_WITH usw. sowie die Inverse-Option.

Unterstützte Übereinstimmungsbedingung	Beschreibung
<b>HTTP-Anforderungsmethode</b>	Zuordnen einer HTTP-Anforderungsmethode. <code>http_request.method</code> – zuzuordnender Wert
<b>HTTP-Anforderungs-URI</b>	Zuordnen einer HTTP-Anforderungs-URI ohne Abfrageargumente. <code>http_request.uri</code> – zuzuordnender Wert
<b>Argumente des HTTP-Anforderungs-URI</b>	Zuordnen des Abfragearguments eines HTTP-Anforderungs-URI. <code>http_request.uri_arguments</code> – zuzuordnender Wert
<b>HTTP-Anforderungsversion</b>	Zuordnen einer HTTP-Anforderungsversion. <code>http_request.version</code> – zuzuordnender Wert
<b>HTTP-Anforderungs-Header</b>	Zuordnen eines beliebigen HTTP-Anforderungs-Headers. <code>http_request.header_name</code> – zuzuordnender Header-Name <code>http_request.header_value</code> – zuzuordnender Wert
<b>HTTP-Anforderungs-Cookie</b>	Zuordnung eines beliebigen HTTP-Anforderungs-Cookies. <code>http_request.cookie_value</code> – zuzuordnender Wert
<b>HTTP-Anforderungstext</b>	Zuordnen des Inhalts eines HTTP-Anforderungstexts. <code>http_request.body_value</code> – zuzuordnender Wert
<b>Client-SSL</b>	Zuordnen der Client-SSL-Profil-ID. <code>ssl_profile_id</code> – zuzuordnender Wert
<b>Port des TCP-Headers</b>	Zuordnen einer TCP-Quelle oder des Zielports. <code>Tcp_header.source_port</code> – zuzuordnender Quellport <code>tcp_header.destination_port</code> – zuzuordnender Zielport
<b>Quelle des IP-Headers</b>	Zuordnen einer IP-Quelladresse oder -Zieladresse <code>ip_header.source_address</code> – zuzuordnende Quelladresse <code>ip_header.destination_address</code> – zuzuordnende Zieladresse

Unterstützte Übereinstimmungsbedingung	Beschreibung
<b>Variable</b>	Erstellen einer Variablen und Zuweisen eines Wertes zu der Variablen.
<b>Groß-/Kleinschreibung beachten</b>	Festlegen eines Flags für den HTTP-Kopfzeilenwertvergleich. Bei dem Flag wird die Groß-/Kleinschreibung beachtet.
Aktionen	Beschreibung
<b>HTTP-Anforderungs-URI umschreiben</b>	Ändern eines URI. http_request.uri – zu schreibender URI (ohne Abfrageargumente) http_request.uri_args – zu schreibende URI-Abfrageargumente
<b>HTTP-Anforderungs-Header umschreiben</b>	Ändern des Werts eines HTTP-Headers. http_request.header_name – Name des Headers http_request.header_value – zu schreibender Wert
<b>HTTP-Anforderungsheader löschen</b>	Löschen des HTTP-Headers. http_request.header_delete – Name des Headers http_request.header_delete – zu schreibender Wert

- 3 Klicken Sie auf **Anforderungsweiterleitung > Regel hinzufügen**, um die Lastausgleichsregeln für die Weiterleitung von HTTP-Anforderungen zu konfigurieren.

Alle Übereinstimmungswerte akzeptieren reguläre Ausdrücke.

Unterstützte Übereinstimmungsbedingung	Beschreibung
<b>HTTP-Anforderungsmethode</b>	Zuordnen einer HTTP-Anforderungsmethode. http_request.method – zuzuordnender Wert
<b>HTTP-Anforderungs-URI</b>	Zuordnen eines HTTP-Anforderungs-URI. http_request.uri – zuzuordnender Wert
<b>HTTP-Anforderungsversion</b>	Zuordnen einer HTTP-Anforderungsversion. http_request.version – zuzuordnender Wert
<b>HTTP-Anforderungs-Header</b>	Zuordnen eines beliebigen HTTP-Anforderungs-Headers. http_request.header_name – zuzuordnender Header-Name http_request.header_value – zuzuordnender Wert
<b>HTTP-Anforderungs-Cookie</b>	Zuordnung eines beliebigen HTTP-Anforderungs-Cookies. http_request.cookie_value – zuzuordnender Wert
<b>HTTP-Anforderungstext</b>	Zuordnen des Inhalts eines HTTP-Anforderungstexts. http_request.body_value – zuzuordnender Wert
<b>Client-SSL</b>	Zuordnen der Client-SSL-Profil-ID. ssl_profile_id – zuzuordnender Wert
<b>Port des TCP-Headers</b>	Zuordnen einer TCP-Quelle oder des Zielports. tcp_header.source_port – zuzuordnender Quellport tcp_header.destination_port – zuzuordnender Zielport

Unterstützte Übereinstimmungsbedingung	Beschreibung
<b>Quelle des IP-Headers</b>	Zuordnen einer IP-Quelladresse oder -Zieladresse ip_header.source_address – zuzuordnende Quelladresse ip_header.destination_address – zuzuordnende Zieladresse
<b>Variable</b>	Erstellen einer Variablen und Zuweisen eines Wertes zu der Variablen.
<b>Groß-/Kleinschreibung beachten</b>	Festlegen eines Flags für den HTTP-Kopfzeilenwertvergleich. Bei dem Flag wird die Groß-/Kleinschreibung beachtet.
Aktion	Beschreibung
<b>HTTP-Ablehnung</b>	Ablehnen einer Anforderung, beispielsweise durch Setzen des Status auf 5xx. http_forward.reply_status – zum Ablehnen verwendeter HTTP-Statuscode http_forward.reply_message – HTTP-Ablehnungsnachricht
<b>HTTP-Umleitung</b>	Umleiten einer Anforderung. Statuscode muss auf 3xx gesetzt werden. http_forward.redirect_status – HTTP-Statuscode für Umleiten http_forward.redirect_url – HTTP-Umleitungs-URL
<b>Pool auswählen</b>	Erzwingen der Anforderung auf einem bestimmten Serverpool. Der konfigurierte Algorithmus (Prognose) der angegebenen Poolmitglieder wird verwendet, um einen Server im Serverpool auszuwählen. http_forward.select_pool – UUID des Serverpools
<b>Antwortstatus</b>	Zeigt den Status der Antwort an.
<b>Antwortnachricht</b>	Der Server antwortet mit einer Antwortnachricht, die bestätigte Adressen und die Konfiguration enthält.

- 4 Klicken Sie auf **Antwortrewrite > Regel hinzufügen**, um die Load Balancer-Regeln für das HTTP-Antwortrewrite zu konfigurieren.

Alle Übereinstimmungswerte akzeptieren reguläre Ausdrücke.

Unterstützte Übereinstimmungsbedingung	Beschreibung
<b>HTTP-Antwort-Header</b>	Zuordnen eines beliebigen HTTP-Antwort-Headers. http_response.header_name – zuzuordnender Header-Name http_response.header_value – zuzuordnender Wert
<b>HTTP-Antwortmethode</b>	Zuordnen einer HTTP-Antwortmethode. http_response.method – zuzuordnender Wert
<b>HTTP-Antwort-URI</b>	Zuordnen eines HTTP-Antwort-URI. http_response.uri – zuzuordnender Wert
<b>Argumente des HTTP-Antwort-URI</b>	Zuordnen der Argumente eines HTTP-Antwort-URI. http_response.uri_args – zuzuordnender Wert
<b>HTTP-Antwortversion</b>	Zuordnen einer HTTP-Antwortversion. http_response.version – zuzuordnender Wert

<b>Unterstützte Übereinstimmungsbedingung</b>	<b>Beschreibung</b>
<b>HTTP-Antwort-Cookie</b>	Zuordnen eines beliebigen HTTP-Antwort-Cookies. http_response.cookie_value – zuzuordnender Wert
<b>Client-SSL</b>	Zuordnen der Client-SSL-Profil-ID. ssl_profile_id – zuzuordnender Wert
<b>Port des TCP-Headers</b>	Zuordnen einer TCP-Quelle oder des Zielports. tcp_header.source_port – zuzuordnender Quellport tcp_header.destination_port – zuzuordnender Zielport
<b>Quelle des IP-Headers</b>	Zuordnen einer IP-Quelladresse oder -Zieladresse ip_header.source_address – zuzuordnende Quelladresse ip_header.destination_address – zuzuordnende Zieladresse
<b>Variable</b>	Erstellen einer Variablen und Zuweisen eines Wertes zu der Variablen.
<b>Groß-/Kleinschreibung beachten</b>	Festlegen eines Flags für den HTTP-Kopfzeilenwertvergleich. Bei dem Flag wird die Groß-/Kleinschreibung beachtet.
<b>Aktion</b>	<b>Beschreibung</b>
<b>HTTP-Antwort-Header umschreiben</b>	Ändern des Werts eines HTTP-Antwort-Headers. http_response.header_name – Name des Headers http_response.header_value – zu schreibender Wert
<b>HTTP-Antwort-Header löschen</b>	Löschen des HTTP-Headers. http_request.header_delete – Name des Headers http_request.header_delete – zu schreibender Wert

# Weiterleitungsrichtlinien

## 8

Diese Funktion gehört zu NSX Cloud.

Weiterleitungsrichtlinien oder Regeln für richtlinienbasiertes Routing (Policy-Based Routing, PBR) definieren, wie NSX-T den Datenverkehr von einer NSX-verwalteten VM verarbeitet. Dieser Datenverkehr kann zum NSX-T-Overlay geleitet werden oder über das (Underlay-)Netzwerk des Cloud-Anbieters geroutet werden.

---

**Hinweis** Die Arbeitslast-VMs in Ihrer Public Cloud werden von NSX-T verwaltet, nachdem Sie sie mit `nsx.network=default` in Ihrer Public Cloud gekennzeichnet und den NSX-Agent darauf installiert haben. Weitere Informationen finden Sie unter [Onboarden von Workload-VMs](#).

---

Drei Standard-Weiterleitungsrichtlinien werden automatisch eingerichtet, nachdem Sie entweder ein PCG in einer Transit-VPC bzw. einem Transit-VNet bereitgestellt haben oder eine Computing-VPC bzw. ein Computing-VNet mit der Transit-VPC bzw. dem Transit-VNet verknüpft haben.

- 1 **Route zum Underlay** für den gesamten Datenverkehr innerhalb einer Transit-/Computing-VPC bzw. eines Transit-/Computing-VNet.
- 2 **Route zum Underlay** für den gesamten Datenverkehr an die Metadatendienste der Public Cloud.
- 3 **Route zum Overlay** für allen anderen Datenverkehr, der z. B. an ein Ziel außerhalb der Transit-/Computing-VPC bzw. des Transit-/Computing-VNet gesendet wird. Dieser Datenverkehr wird über den NSX-T-Overlay-Tunnel zum PCG und weiter zum Ziel geroutet.

---

**Hinweis Für Datenverkehr an andere VPCs/VNETs, die vom gleichen PCG verwaltet werden:** Der Datenverkehr wird von der NSX-verwalteten Quell-VPC bzw. dem Quell-VNet über den NSX-T-Overlay-Tunnel zum PCG und dann zur Ziel-VPC bzw. zum Ziel-VNet geroutet.

**Für Datenverkehr an andere VPCs/VNets, die von einem anderen PCG verwaltet werden:** Der Datenverkehr wird von der NSX-verwalteten Quell-VPC bzw. dem Quell-VNet über den NSX-T-Overlay-Tunnel an das PCG der Quell-VPC bzw. des Quell-VNet geroutet und dann zum PCG der NSX-verwalteten Ziel-VPC bzw. des Ziel-VNet weitergeleitet.

Wenn der Datenverkehr für das Internet vorgesehen ist, dann leitet ihn das PCG an das Ziel im Internet weiter.

---

## Mikrosegmentierung beim Routing zum Underlay

Die Mikrosegmentierung wird auch für Arbeitslast-VMs erzwungen, deren Datenverkehr an das Underlay-Netzwerk weitergeleitet wird.

Wenn eine NSX-verwaltete Arbeitslast-VM direkt mit einem Ziel außerhalb der verwalteten VPC bzw. des verwalteten VNet verbunden ist und Sie das PCG umgehen möchten, richten Sie eine Weiterleitungsrichtlinie ein, um den Datenverkehr von dieser VM über das Underlay weiterzuleiten.

Wenn der Datenverkehr über das Underlay-Netzwerk geroutet wird, dann wird das PCG umgangen. Daher trifft der Datenverkehr nicht auf die Nord-Süd-Firewall. Sie müssen jedoch weiterhin Regeln für die Ost-West- oder Distributed Firewall (DFW) verwalten, da diese Regeln auf VM-Ebene angewendet werden, bevor das PCG erreicht wird.

## Aktuell unterstützte Weiterleitungsrichtlinien

Im Dropdown-Menü wird möglicherweise eine ganze Liste von Weiterleitungsrichtlinien angezeigt, in dieser Version werden jedoch nur die folgenden Weiterleitungsrichtlinien unterstützt:

- **Route zum Underlay:** für den Zugriff von einer NSX-verwalteten VM auf einen Underlay-Dienst. Beispiel: Zugriff auf den AWS S3-Dienst im AWS-Underlay-Netzwerk.
- **Route vom Underlay:** für den Zugriff vom Underlay-Netzwerk auf einen Dienst, der auf einer NSX-verwalteten VM gehostet wird. Beispiel: Zugriff von AWS ELB auf die NSX-verwaltete VM.

Dieses Kapitel enthält die folgenden Themen:

- [Hinzufügen oder Bearbeiten von Weiterleitungsrichtlinien](#)

## Hinzufügen oder Bearbeiten von Weiterleitungsrichtlinien

Sie können die automatisch erstellten Weiterleitungsrichtlinien bearbeiten oder neue hinzufügen.

Für die Verwendung der von der Public Cloud bereitgestellten Dienste (z. B. S3 von AWS) können Sie z. B. eine Richtlinie erstellen, die zulässt, dass ein Satz IP-Adressen durch Routing über das Underlay auf diesen Dienst zugreift.

### Voraussetzungen

Dazu benötigen Sie eine VPC oder ein VNet, auf dem PCG bereitgestellt ist.

### Verfahren

- 1 Klicken Sie auf **Abschnitt hinzufügen**. Benennen Sie den Abschnitt entsprechend, z. B. **AWS-Dienste**.

- 2** Aktivieren Sie das Kontrollkästchen neben dem Abschnitt und klicken Sie auf **Regel hinzufügen**. Benennen Sie die Regel, z. B. **S3-Regeln**.
- 3** Wählen Sie auf der Registerkarte **Quellen** die VPC oder das VNet aus, auf der bzw. dem sich die Arbeitslast-VMs befinden, für die Sie den Dienstzugriff bereitstellen möchten, z. B. die AWS VPC. Sie können hier auch eine **Gruppe** erstellen, um mehrere VMs einzubeziehen, die einem oder mehreren Kriterien entsprechen.
- 4** Wählen Sie auf der Registerkarte **Ziele** die VPC oder das VNet aus, auf der bzw. dem der Service gehostet wird, z. B. eine **Gruppe**, die die IP-Adresse des S3-Dienstes in AWS enthält.
- 5** Wählen Sie den Dienst auf der Registerkarte **Dienste** aus dem Dropdown-Menü aus. Wenn der Dienst nicht vorhanden ist, können Sie ihn hinzufügen. Sie können die Auswahl auch auf **Beliebig** belassen, da Sie die Routingdetails unter **Ziele** angeben können.
- 6** Geben Sie auf der Registerkarte **Aktion** an, wie das Routing funktionieren soll. Wählen Sie z. B. die Option **Route zum Underlay**, wenn Sie diese Richtlinie für den AWS S3-Dienst einrichten.
- 7** Klicken Sie auf **Veröffentlichen**, um die Einrichtung der Weiterleitungsrichtlinie abzuschließen.

# IP-Adressverwaltung (IPAM)

# 9

Zur Verwaltung von IP-Adressen können Sie DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), IP-Adresspools und IP-Adressblöcke konfigurieren.

---

**Hinweis** IP-Blöcke werden von NSX Container Plug-in (NCP) verwendet. Weitere Informationen über NCP finden Sie im *Installations- und Administratorhandbuch zum NSX Container Plug-in für Kubernetes und Cloud Foundry*.

---

Dieses Kapitel enthält die folgenden Themen:

- [Hinzufügen einer DNS-Zone](#)
- [Hinzufügen eines DNS-Weiterleitungsdiensts](#)
- [Hinzufügen eines DHCP-Servers](#)
- [Konfigurieren eines DHCP-Relay-Servers für ein Tier-0- oder Tier-1-Gateway](#)
- [Hinzufügen eines IP-Adressenpools](#)
- [Hinzufügen eines IP-Adressblocks](#)

## Hinzufügen einer DNS-Zone

Sie können DNS-Zonen für Ihren DNS-Dienst konfigurieren. Eine DNS-Zone ist ein eindeutiger Teil des Domänen-Namespaces in DNS.

Wenn Sie eine DNS-Zone konfigurieren, können Sie eine Quell-IP für eine DNS-Weiterleitung angeben, die bei der Weiterleitung von DNS-Abfragen an einen Upstream-DNS-Server verwendet werden soll. Wenn Sie keine Quell-IP angeben, wird die Quell-IP des DNS-Abfragepakets zur Listener-IP der DNS-weitergeleiteten Instanz. Die Angabe einer Quell-IP ist erforderlich, wenn es sich bei der Listener-IP um eine interne Adresse handelt, die vom externen Upstream-DNS-Server aus nicht erreichbar ist. Um sicherzustellen, dass die DNS-Antwortpakete an die weiterleitende Instanz zurückgeleitet werden, ist eine dedizierte Quell-IP erforderlich. Alternativ können Sie SNAT auf dem logischen Router konfigurieren, um die Listener-IP in eine öffentliche IP-Adresse zu übersetzen. In diesem Fall müssen Sie keine Quell-IP angeben.



## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk > IP-Adressverwaltung > DNS**.
- 3 Klicken Sie auf die Registerkarte **DNS-Zonen**.
- 4 Wählen Sie **DNS-Zone hinzufügen > Standardzone hinzufügen** aus, um eine Standardzone hinzuzufügen.
  - a Geben Sie einen Namen und optional eine Beschreibung ein.
  - b Geben Sie die IP-Adressen von bis zu drei DNS-Servern ein.
  - c (Optional) Geben Sie eine IP-Adresse im Feld **Quell-IP** ein.
- 5 Wählen Sie **DNS-Zone hinzufügen > FQDN-Zone hinzufügen** aus, um eine FQDN-Zone hinzuzufügen.
  - a Geben Sie einen Namen und optional eine Beschreibung ein.
  - b Geben Sie einen FQDN für die Domäne ein.
  - c Geben Sie die IP-Adressen von bis zu drei DNS-Servern ein.
  - d (Optional) Geben Sie eine IP-Adresse im Feld **Quell-IP** ein.
- 6 Klicken Sie auf **Speichern**.

## Hinzufügen eines DNS-Weiterleitungsdiensts

Sie können eine DNS-Weiterleitung konfigurieren, um DNS-Abfragen an externe DNS-Server weiterzuleiten.

Bevor Sie eine DNS-Weiterleitung konfigurieren, müssen Sie eine DNS-Standardzone konfigurieren. Optional können Sie eine oder mehrere FQDN-DNS-Zonen konfigurieren. Jede DNS-Zone ist mit bis zu 3 DNS-Servern verknüpft. Wenn Sie eine FQDN-DNS-Zone konfigurieren, geben Sie einen oder mehrere Domännennamen an. Eine DNS-Weiterleitung ist mit einer DNS-Standardzone und bis zu 5 FQDN-DNS-Zonen verknüpft. Wenn eine DNS-Abfrage empfangen wird, vergleicht die DNS-Weiterleitung den Domännennamen in der Abfrage mit den Domännennamen in den FQDN-DNS-Zonen. Wenn eine Übereinstimmung gefunden wird, wird die Abfrage an die DNS-Server weitergeleitet, die in der FQDN-DNS-Zone angegeben sind. Wenn keine Übereinstimmung gefunden wird, wird die Abfrage an die DNS-Server weitergeleitet, die in der DNS-Standardzone angegeben sind.

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk > IP-Adressverwaltung > DNS**.

- 3 Klicken Sie auf **DNS-Dienst hinzufügen**.
- 4 Geben Sie einen Namen und optional eine Beschreibung ein.
- 5 Wählen Sie ein Tier-0- oder Tier-1-Gateway aus.
- 6 Geben Sie die IP-Adresse des DNS-Diensts ein.  
Clients senden DNS-Abfragen an diese IP-Adresse, die auch als Listener-IP der DNS-Weiterleitung bezeichnet wird.
- 7 Wählen Sie eine DNS-Standardzone aus.
- 8 Wählen Sie eine Protokollebene aus.
- 9 Wählen Sie bis zu fünf FQDN-Zonen aus.
- 10 Klicken Sie auf die Umschaltfläche **Administrativer Status**, um den DNS-Dienst zu aktivieren oder zu deaktivieren.
- 11 Klicken Sie auf **Speichern**.

## Hinzufügen eines DHCP-Servers

Mit DHCP (Dynamic Host Configuration Protocol) können Clients die Netzwerkkonfiguration, wie IP-Adresse, Subnetzmaske, Standard-Gateway und DNS-Konfiguration, automatisch von einem DHCP-Server abrufen. Sie können DHCP-Server erstellen, um DHCP-Anforderungen zu verarbeiten.

---

**Hinweis** Der mit diesem Verfahren erstellte DHCP-Server wird in einem VLAN-gestützten Segment nicht unterstützt. Sie müssen die DHCP-Funktion unter **Netzwerk und Sicherheit – Erweitert** verwenden, um einen DHCP-Server zu erstellen, der auf einem VLAN-gestützten logischen Switch unterstützt wird.

---

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk > IP-Adressverwaltung > DHCP**.
- 3 Klicken Sie auf **Server hinzufügen**.
- 4 Wählen Sie **DHCP-Server** als Servertyp aus.
- 5 Geben Sie einen Namen für den Server ein.
- 6 Geben Sie die IP-Adresse des Servers im CIDR-Format ein.

In diesem Schritt werden zwei logische Ports erstellt (einer für eine logische Schnittstelle und einer für den DHCP-Server selbst). Außerdem wird der DHCP-Server mit einem bestimmten logischen DHCP-Switch verbunden. Diese Schnittstelle wird auf dem Tier-0- oder Tier-1-Gateway als verbundene Schnittstelle angezeigt. Stellen Sie daher sicher, dass Sie ein nicht

überlappendes Subnetz für das Tier-1- oder Tier-0-Gateway auswählen, dem Sie den DHCP-Server zuweisen möchten. Sie können für diesen Zweck <IP-Adresse>/30 angeben. Der hier verwendete Subnetzbereich wird nicht für das verbundene Tier-0-Gateway angekündigt, aber in der Weiterleitungstabelle des Tier-1-Gateways angezeigt.

- 7 Geben Sie eine Lease-Zeit ein.
- 8 Wählen Sie einen NSX Edge-Cluster aus.
- 9 Klicken Sie auf **Speichern**.
- 10 So weisen Sie einem Tier-0- oder Tier-1-Gateway einen DHCP-Server zu:
  - a Navigieren Sie zu **Netzwerk > Tier-0-Gateways** oder **Netzwerk > Tier-1-Gateways**.
  - b Bearbeiten Sie ein vorhandenes Gateway.
  - c Klicken Sie im Feld **IP-Adressverwaltung** auf **Keine IP-Zuteilung**.
  - d Wählen Sie **Lokaler DHCP-Server** in der Dropdown-Liste „Typ“ aus.
  - e Wählen Sie einen DHCP-Server aus.
  - f Klicken Sie auf **Speichern**.
  - g Klicken Sie auf **Speichern**.
- 11 So weisen Sie einem Segment einen DHCP-Server zu:
  - a Navigieren Sie zu **Netzwerk > Segmente**.
  - b Fügen Sie ein Segment hinzu oder bearbeiten Sie eines.  
Das Segment muss einem Tier-0- oder Tier-1-Gateway zugeordnet sein.
  - c Klicken Sie auf **Subnetze festlegen**, wenn Sie ein neues Segment hinzufügen, oder klicken Sie auf die Zahl unter **Subnetze**, um ein Subnetz hinzuzufügen oder zu ändern.
  - d Geben Sie die entsprechenden DHCP-Bereiche ein.
  - e Klicken Sie auf **Übernehmen**.
  - f Klicken Sie auf **Speichern**.

## Konfigurieren eines DHCP-Relay-Servers für ein Tier-0- oder Tier-1-Gateway

Mit DHCP (Dynamic Host Configuration Protocol) können Clients die Netzwerkkonfiguration, wie IP-Adresse, Subnetzmaske, Standard-Gateway und DNS-Konfiguration, automatisch von einem DHCP-Server abrufen. Sie können einen DHCP-Relay-Server erstellen, um DHCP-Datenverkehr an externe DHCP-Server weiterzuleiten.

### Verfahren

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

- 2** Wählen Sie **Netzwerk > IP-Adressverwaltung > DHCP**.
- 3** Klicken Sie auf **Server hinzufügen**.
- 4** Wählen Sie **DHCP-Relay** als Servertyp aus.
- 5** Geben Sie einen Namen für den Relay-Server ein.
- 6** Geben Sie mindestens eine IP-Adresse für den Server ein.
- 7** Klicken Sie auf **Speichern**.
- 8** Navigieren Sie zu **Netzwerk > Tier-0-Gateways** oder **Netzwerk > Tier-1-Gateways**, um einen DHCP-Relay-Server für ein Gateway zu konfigurieren.
- 9** Bearbeiten Sie das entsprechende Gateway.
- 10** Klicken Sie im Feld **IP-Adressverwaltung** auf **Keine IP-Zuteilung** für ein Tier-0-Gateway oder auf **Keine IP-Zuteilung festgelegt** für ein Tier-1-Gateway.
- 11** Wählen Sie im Feld **Typ** die Option **DHCP-Relay** aus.
- 12** Wählen Sie im Feld **DHCP-Relay** den zuvor erstellten DHCP-Relay-Server aus.
- 13** Klicken Sie auf **Speichern**.
- 14** Für jedes mit dem Gateway verbundene Segment, das diesen DHCP-Relay-Dienst verwendet, müssen Sie DHCP-Bereiche angeben, damit das Relay funktioniert.
  - a** Navigieren Sie zu **Netzwerk > Segmente**.
  - b** Fügen Sie ein Segment hinzu oder bearbeiten Sie eines.
  - c** Klicken Sie auf **Subnetze festlegen**, wenn Sie ein neues Segment hinzufügen, oder klicken Sie auf die Zahl unter **Subnetze**, um ein Subnetz zu ändern.
  - d** Geben Sie einen oder mehrere DHCP-Bereiche an.

Dies ist erforderlich, damit das Relay funktioniert.
  - e** Klicken Sie auf **Übernehmen**.
  - f** Klicken Sie auf **Speichern**.

## Hinzufügen eines IP-Adressenpools

Sie können IP-Adresspools für die Verwendung durch Komponenten konfigurieren, wie z. B. DHCP.

### Verfahren

- 1** Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2** Wählen Sie **Netzwerk > IP-Adressverwaltung > IP-Adresspools**.
- 3** Klicken Sie auf **IP-Adresspool hinzufügen**.

- 4 Geben Sie einen Namen und optional eine Beschreibung ein.
- 5 Zur Angabe eines Adressblocks wählen Sie **Subnetz hinzufügen > IP-Block** aus.
  - a Wählen Sie einen IP-Block aus.
  - b Geben Sie eine Größe an.
  - c Klicken Sie auf **Hinzufügen**.
- 6 Zur Angabe von IP-Bereichen wählen Sie **Subnetz hinzufügen > IP-Bereiche** aus.
  - a Geben Sie IPv4- oder IPv6-Bereiche ein.
  - b Geben Sie IP-Bereiche im CIDR-Format ein.
  - c Geben Sie eine Adresse unter **Gateway-IP** ein.
  - d Klicken Sie auf **Hinzufügen**.
- 7 Klicken Sie auf **Speichern**.

## Hinzufügen eines IP-Adressblocks

Sie können IP-Adressblöcke für die Verwendung durch andere Komponenten konfigurieren.

---

**Hinweis** Sie können auch einen IP-Adressblock hinzufügen, indem Sie zu **Netzwerk und Sicherheit – Erweitert > Netzwerk > IPAM** navigieren.

---

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk > IP-Adressverwaltung > IP-Adresspools**.
- 3 Klicken Sie auf die Registerkarte **IP-Adressblöcke**.
- 4 Klicken Sie auf **IP-Adressblock hinzufügen**.
- 5 Geben Sie einen Namen und optional eine Beschreibung ein.
- 6 Geben Sie einen IP-Block im CIDR-Format ein.
- 7 Klicken Sie auf **Speichern**.

Die Themen in diesem Abschnitt beziehen sich auf die Nord-Süd- und Ost-West-Sicherheit für Regeln für verteilte Firewalls, Identitäts-Firewalls, Netzwerk-Introspektion, Gateway-Firewall und Endpoint-Schutzrichtlinien.

Dieses Kapitel enthält die folgenden Themen:

- [Überblick über die Sicherheitskonfiguration](#)
- [Sicherheit – Terminologie](#)
- [Identitätsbasierte Firewall](#)
- [Kontextprofil der Schicht 7](#)
- [Verteilte Firewall](#)
- [Konfigurieren einer Gateway-Firewall](#)
- [Konfigurieren der Netzwerk-Introspektion \(Ost-West\)](#)
- [Konfigurieren der Netzwerk-Introspektion \(Nord-Süd\)](#)
- [Konfigurieren von Endpoint-Schutz](#)

## Überblick über die Sicherheitskonfiguration

Konfigurieren Sie Ost-West- und Nord-Süd-Firewallrichtlinien unter vordefinierten Kategorien für Ihre Umgebung.

Verteilte Firewall (Ost-West) und Gateway-Firewall (Nord-Süd) bieten mehrere Sätze konfigurierbarer Regeln, die in Kategorien unterteilt sind. Sie können eine Ausschlussliste mit logischen Switches, logischen Ports oder Gruppen konfigurieren, die von der Firewallerzwingung ausgeschlossen werden sollen.

Sicherheitsrichtlinien werden wie folgt durchgesetzt:

- Regeln werden in Kategorien und von links nach rechts verarbeitet.
- Die Regeln werden von oben nach unten verarbeitet.
- Jedes Paket wird anhand der obersten Regel in der Regeltabelle überprüft, bevor zu den nächsten Regeln in der Tabelle nach unten übergegangen wird.

- Die erste Regel in der Tabelle, die den Datenverkehrsparametern entspricht, wird erzwungen.

Es können keine nachfolgenden Regeln angewendet werden, da die Suche für dieses Paket dann beendet wird. Aufgrund dieses Verhaltens ist es empfehlenswert, immer die detailliertesten Richtlinien an den Anfang der Regeltabelle zu stellen. Damit wird sichergestellt, dass diese vor den spezifischeren Regeln durchgesetzt werden.

## Sicherheit – Terminologie

Die folgenden Begriffe werden im Zusammenhang mit verteilten Firewalls verwendet.

**Tabelle 10-1. Sicherheitsbezogene Terminologie**

Konstrukt	Definition
Domäne	Bei einer Domäne handelt es sich um eine Umgebung oder Sicherheitszone, die Firewallregeln und Gruppen enthält. Das Erstellen einer Domäne ist optional. Die Standarddomäne stellt die gesamte NSX-Umgebung dar. Regeln in einer Domäne benötigen mindestens eine Gruppe in der Quelle oder im Ziel, die Mitglied derselben Domäne ist. Beachten Sie, dass das Domänenobjekt eine experimentelle Funktion in NSX-T Data Center 2.4 ist, aber in NSX-T Data Center 2.4.1 nicht verfügbar ist.
Richtlinie	Eine Sicherheitsrichtlinie enthält verschiedene Sicherheitselemente, einschließlich Firewallregeln und Dienstkonfigurationen. Richtlinien wurden zuvor als Firewallabschnitte bezeichnet.
Regel	Eine Gruppe von Parametern, mit denen Abläufe bewertet werden und die die Aktionen definieren, die bei einer Übereinstimmung durchgeführt werden. Regeln enthalten Parameter, wie z. B. Quelle und Ziel, Dienst, Kontextprofil, Protokollierung und Tags.
Gruppe	Gruppen enthalten verschiedene Objekte, die sowohl statisch als auch dynamisch hinzugefügt werden und als Quell- und Zielfeld einer Firewallregel verwendet werden können. Gruppen können so konfiguriert werden, dass sie eine Kombination aus virtuellen Maschinen, IP Sets, MAC Sets, logischen Ports, logischen Switches, AD-Benutzergruppen und anderen verschachtelten Gruppen enthalten. Gruppen können auf Basis von Tags, Maschinen-, Betriebssystem- oder Computernamen dynamisch aufgenommen werden.  Beim Erstellen einer Gruppe müssen Sie eine Domäne einbeziehen, zu der die Gruppe gehört. Hierbei handelt es sich in der Regel um die Standarddomäne.  Gruppen wurden zuvor als NS-Gruppe oder Sicherheitsgruppe bezeichnet.
Dienst	Definiert eine Kombination aus Port und Protokoll. Wird verwendet, um Datenverkehr basierend auf Port und Protokoll zu klassifizieren. Vordefinierte und benutzerdefinierte Dienste können in Firewallregeln verwendet werden.
Kontextprofil	Definiert kontextsensitive Attribute, einschließlich APP-ID und Domänenname. Enthält auch Unterattribute, wie z. B. Anwendungsversion oder Verschlüsselungssatz. Firewallregeln können ein Kontextprofil enthalten, um Schicht-7-Firewallregeln zu aktivieren.

## Identitätsbasierte Firewall

Mit den Funktionen für eine identitätsbasierte Firewall (IDFW) haben NSX-Administratoren die Möglichkeit, DFW-Regeln anhand der Active Directory-Benutzer zu erstellen.

Eine IDFW kann für virtuelle Desktop- (VDI) oder Remote-Desktop-Sitzungen (RDSH-Unterstützung) verwendet werden. Dies ermöglicht eine gleichzeitige Anmeldung mehrerer Benutzer, einen Benutzerzugriff auf Anwendungen basierend auf Anforderungen sowie die Beibehaltung unabhängiger Benutzerumgebungen. VDI-Verwaltungssysteme steuern, welchen Benutzern Zugriff auf die virtuellen VDI-Maschinen gewährt wird. NSX-T steuert den Zugriff auf die Zielservers von der Quell-VM. IDFW wird bei der Quell-VM verarbeitet. Erstellen Sie mit RDSH-Administratoren Sicherheitsgruppen mit verschiedenen Benutzern in Active Directory (AD), und gewähren oder verweigern Sie diesen Benutzern basierend auf ihrer Rolle den Zugriff auf einen Anwendungsserver. Beispielsweise können sich Personalabteilung und Konstruktionsabteilung mit demselben RDSH-Server verbinden und von diesem Server aus auf verschiedene Anwendungen zugreifen.

---

**Hinweis** IDFW stützt sich auf die Sicherheit und Integrität des Gastbetriebssystems. Es gibt mehrere Methoden für einen böswilligen lokalen Administrator, seine Identität zu manipulieren, um Firewallregeln zu umgehen. Benutzeridentitätsinformationen werden vom Guest Introspection-Agent innerhalb von Gast-VMs bereitgestellt. Sicherheitsadministratoren müssen sicherstellen, dass der NSX Guest Introspection-Agent in jeder Gast-VM installiert ist und ausgeführt wird. Angemeldete Benutzer sollten nicht über die Berechtigung zum Entfernen oder Beenden des Agents verfügen.

---

Linux-basierte Betriebssysteme werden nicht unterstützt.

IDFW wird unterstützt von:

Microsoft Active Directory Windows Server:

- 2008
- 2012
- 2012R2
- 2016
- 2019

VMware Tools Version 10.3 oder höher: NSX-Datei-Introspektion-Treiber, NSX-Netzwerk-Introspektion-Treiber, VMCI-Treiber.

Hostbetriebssystem: nur ESXi

Gastbetriebssysteme:

- Desktoperzwingung: Windows 8, Windows 10
- RDSH-Erzwingung: Windows 2012 R2, Windows 2016

Ein Überblick auf oberster Ebene über den Workflow der IDFW-Konfiguration beginnt mit der Vorbereitung der Infrastruktur. Dazu gehört die Installation der Komponenten der Hostvorbereitung in jedem geschützten Cluster durch den Administrator und die Einrichtung der Active Directory-Synchronisierung, damit NSX AD-Benutzer und -Gruppen verwenden kann. Als Nächstes muss IDFW wissen, bei welchem Desktop sich ein Active Directory-Benutzer anmeldet,



um die IDFW-Regeln zuzuweisen. Wenn Netzwerkereignisse von einem Benutzer generiert werden, erfasst der mit VMware Tools auf der VM installierte Thin Agent die Informationen und leitet sie an die Context Engine weiter. Diese Informationen werden verwendet, um die Erzwingung für die verteilte Firewall bereitzustellen.

Workflow der IDFW:

- 1 Ein Benutzer meldet sich bei einer VM an und startet eine Netzwerkverbindung, indem er Skype oder Outlook öffnet.
- 2 Der Thin Agent erfasst ein Benutzeranmeldeereignis. Er erfasst die Verbindungsinformationen und Identitätsinformationen und sendet sie an die Context Engine.
- 3 Die Context Engine leitet die Verbindungs- und Identitätsinformationen zur Erzwingung etwaiger anwendbarer Regeln an die verteilte Firewall weiter.

## Workflow für die identitätsbasierte Firewall

Der Workflow für die identitätsbasierte Firewall erweitert herkömmliche Firewalls, indem Firewallregeln auf Basis der Benutzeridentität zugelassen werden. Administratoren können Mitarbeitern des Kundensupports beispielsweise erlauben, mit einer einzigen Firewallrichtlinie auf die HR-Datenbank zuzugreifen.

Benutzerbasierte Regeln für die verteilte Firewall werden von der Mitgliedschaft in einer Active Directory-Gruppe bestimmt. Die identitätsbasierte Firewall benötigt einen Thin Agent.

---

**Hinweis** IDFW stützt sich auf die Sicherheit und Integrität des Gastbetriebssystems. Es gibt mehrere Methoden für einen böswilligen lokalen Administrator, seine Identität zu manipulieren, um Firewallregeln zu umgehen. Benutzeridentitätsinformationen werden vom Guest Introspection-Agent innerhalb von Gast-VMs bereitgestellt. Sicherheitsadministratoren müssen sicherstellen, dass der NSX Guest Introspection-Agent in jeder Gast-VM installiert ist und ausgeführt wird. Angemeldete Benutzer sollten nicht über die Berechtigung zum Entfernen oder Beenden des Agents verfügen.

---

**Hinweis** Zur Erzwingung der identitätsbasierten Firewallregel sollte für den Windows-Zeitdienst **ein** für alle VMs festgelegt sein, die Active Directory verwenden. Dadurch wird sichergestellt, dass Datum und Uhrzeit zwischen Active Directory und VMs synchronisiert werden. Darüber hinaus werden Änderungen der AD-Gruppenmitgliedschaft, einschließlich der Aktivierung und Löschung von Benutzern, nicht sofort für angemeldete Benutzer wirksam. Damit die Änderungen wirksam werden, müssen sich die Benutzer abmelden und erneut anmelden. AD-Administratoren sollten eine Abmeldung erzwingen, wenn die Gruppenmitgliedschaft geändert wird. Dieses Verhalten ist eine Beschränkung von Active Directory.

---

### Voraussetzungen

Microsoft Active Directory Windows Server:

- 2008
- 2012

- 2012R2
- 2016
- 2019

VMware Tools Version 10.3 oder höher: NSX-Datei-Introspektion-Treiber, NSX-Netzwerk-Introspektion-Treiber, VMCI-Treiber.

Hostbetriebssystem: nur ESXi

Gastbetriebssysteme:

- Desktoperzwingung: Windows 8, Windows 10
- RDSH-Erzwingung: Windows 2012 R2, Windows 2016

#### Verfahren

- 1 Aktivieren des NSX-Datei-Introspektion- und des NSX-Netzwerk-Introspektion-Treibers Bei einer vollständigen Installation von VMware Tools werden folgende Standardwerte hinzugefügt.
- 2 Aktivieren des Workflows für die identitätsbasierte Firewall auf einem Cluster oder eigenständigen Host: [Identitätsbasierte Firewall aktivieren](#).
- 3 Konfigurieren der Active Directory-Domäne: [Hinzufügen von Active Directory](#).
- 4 Konfigurieren von Active Directory-Synchronisierungsvorgängen: [Synchronisieren von Active Directory](#).
- 5 Erstellen von Sicherheitsgruppen (SG) mit Active Directory-Gruppenmitgliedern: [Hinzufügen einer Gruppe](#).
- 6 Zuweisen von Sicherheitsgruppen mit AD-Gruppenmitgliedern zu einer Regel für verteilte Firewalls: [Hinzufügen einer verteilten Firewall](#).

### Identitätsbasierte Firewall aktivieren

„Identitätsbasierte Firewall“ muss aktiviert sein, damit die IDFW-Firewallregeln wirksam werden.

#### Verfahren

- 1 Wählen Sie im Navigationsbereich **Sicherheit > Verteilte Firewall**.
- 2 Klicken Sie im Banner auf **IDFW aktivieren**.
- 3 Klicken Sie noch einmal im Banner auf **IDFW aktivieren**. Klicken Sie auf die Schaltfläche „Status“, um IDFW zu aktivieren.  
Der Bildschirm **Identitätsbasierte Firewall bearbeiten** wird angezeigt.
- 4 Klicken Sie auf den Schalter „Status“, um IDFW zu aktivieren.
- 5 (Optional) Klicken Sie auf den Schalter „Status“, um IDFW auf eigenständigen Hosts zu aktivieren.

- 6 (Optional) Ändern Sie den Status der einzelnen verfügbaren Cluster, damit IDFW clusterweise aktiviert wird.
- 7 Klicken Sie auf **Speichern**.

## Best Practices für die identitätsbasierte Firewall

Die folgenden Best Practices helfen, den Erfolg von identitätsbasierten Firewallregeln zu maximieren.

- IDFW unterstützt nur TCP-basierte Firewallregeln.
- Eine einzelne ID-basierte Gruppe kann innerhalb einer Firewallregel verwendet werden. Wenn IP- und ID-basierte Gruppen für die Quelle benötigt werden, erstellen Sie zwei separate Firewallregeln.
- Windows 2008 wird nicht als Active Directory-Server oder RDSH-Server-Betriebssystem unterstützt.
- Jede Änderung einer Domäne, einschließlich einer Änderung des Domänennamens, löst eine vollständige Synchronisierung mit Active Directory aus. Da eine vollständige Synchronisierung viel Zeit in Anspruch nehmen kann, wird empfohlen, die Synchronisierung außerhalb der Spitzenzeiten oder außerhalb der Geschäftszeiten durchzuführen.
- Der standardmäßige LDAP-Port 389 und der LDAPS-Port 636 werden für die Active Directory-Synchronisierung verwendet und dürfen nicht über die Standardwerte bearbeitet werden. Benutzerdefinierte Ports werden nicht unterstützt.

## Kontextprofil der Schicht 7

Die Anwendungsidentität der Schicht 7 wird im Rahmen eines Kontextprofils konfiguriert.

Ein Kontextprofil kann eine oder mehrere [Anwendungsidentifikations-GUIDs](#) angeben und auch Unterattribute enthalten. Wenn ein Unterattribut, z. B. TLS Version 1.2, definiert ist, werden mehrere Anwendungsidentitätsattribute nicht unterstützt. Zusätzlich zu den APP-IDs kann ein vollqualifizierter Domänenname (FQDN) oder eine URL in einem Kontextprofil für die Aufnahme von FQDN in die Whitelist festgelegt werden. FQDN kann zusammen mit APP-ID in einem Kontextprofil konfiguriert werden, oder sie können jeweils in verschiedenen Kontextprofilen festgelegt werden. Sobald ein Kontextprofil definiert wurde, kann es auf eine oder mehrere verteilte Firewallregeln angewendet werden.

Wenn ein Kontextprofil in einer Regel verwendet wurde, wird jeder Datenverkehr, der von einer virtuellen Maschine eingeht, auf der Basis von 5-Tupel mit der Regeltabelle abgeglichen. Wenn die Regel mit dem Flow übereinstimmt und auch ein Kontextprofil der Schicht 7 enthält, wird dieses Paket an eine Benutzerbereichskomponente umgeleitet, die als DPI-Engine (Deep Packet Inspection) bezeichnet wird. Eine kleine Anzahl nachfolgender Pakete wird für jeden Flow an diese DPI-Engine weitergegeben. Sobald die APP\_ID ermittelt wurde, werden diese Informationen in der kernelinternen Kontexttabelle gespeichert. Wenn das nächste Paket für den Flow eingeht, werden die Informationen in der Kontexttabelle mit der Regeltabelle verglichen und auf einem 5-Tupel sowie auf der APP-ID der Schicht 7 abgeglichen. Die entsprechende Aktion,

wie in der Regel definiert, wird ausgeführt, und im Falle einer ALLOW-Regel werden alle nachfolgenden Pakete für den Flow im Kernel verarbeitet und mit der Verbindungstabelle abgeglichen. Von der verteilten Firewall generierte Protokolle enthalten die APP\_ID der Schicht 7 wenn dieser Flow an DPI weitergegeben wurde.

Regelverarbeitung für ein eingehendes Paket:

- 1 Nach dem Festlegen eines DFW-Filters werden die Pakete basierend auf einem 5-Tupel mit der Flow-Tabelle abgeglichen.
- 2 Wenn kein Flow-Status gefunden werden kann, wird der Flow anhand der Regeltabelle basierend auf einem 5-Tupel abgeglichen. Daraufhin wird ein Eintrag in der Flow-Tabelle erstellt.
- 3 Wenn der Flow mit einer Regel mit einem Schicht-7-Dienstobjekt übereinstimmt, wird der Status der Flow-Tabelle mit „DPI in Bearbeitung“ gekennzeichnet.
- 4 Der Datenverkehr wird daraufhin an die DPI-Engine weitergegeben. Die DPI-Engine bestimmt die APP\_ID.
- 5 Wenn die APP\_ID bestimmt wurde, versendet die DPI-Engine das Attribut, das in die Kontexttabelle für diesen Flow eingefügt wird. Die Kennzeichnung „DPI In Progress“ wird entfernt und der Datenverkehr wird nicht mehr an die DPI-Engine weitergegeben.
- 6 Der Flow (jetzt mit APP-ID) wird erneut anhand aller Regeln überprüft, die der APP\_ID entsprechen, angefangen bei der ursprünglichen Regel, bei der die Übereinstimmung auf dem 5-Tupel basierte. Dabei wird sichergestellt, dass übereinstimmende L4-Regeln keinen Vorrang haben. Die entsprechende Aktion wird ausgeführt (zulassen/verweigern) und der Eintrag in der Flowtabelle wird entsprechend aktualisiert.

## Layer 7-Workflow für Regeln für verteilte Firewall

Layer 7-App-IDs werden beim Erstellen eines Kontextprofils und anschließend beim Erstellen von Regeln für verteilte Firewall verwendet. Auf Anwendungsidentität basierende Regelerzwingung ermöglicht Benutzern, die Ausführung von Anwendungen auf einem beliebigen Port zuzulassen oder zu verweigern.

NSX-T bietet integrierte [Anwendungsidentifikations-GUIDs](#) für gemeinsame Infrastruktur- und Unternehmensanwendungen. App-IDs umfassen Versionen (SSL/TLS und CIFS/SMB) sowie die Verschlüsselungs-Suite (SSL/TLS). App-IDs werden über Kontextprofile in Regeln verwendet und können mit FQDN-Whitelists und -Blacklists kombiniert werden. Unterstützung steht nur auf ESXi-Hosts bereit.

Unterstützte App-IDs und FQDNs:

- Für FQDN müssen Benutzer eine Regel mit hoher Priorität mit einer DNS-App-ID für die angegebenen DNS-Server auf Port 53 konfigurieren.
- Die ALG-App-IDs (FTP, ORACLE, DCERPC, TFTP) erfordern den entsprechenden ALG-Dienst für die Firewallregel.
- Die SYSLOG-App-ID wird nur auf Standard-Ports erkannt.

## Verfahren

- 1 Erstellen eines benutzerdefinierten Kontextprofils: [Hinzufügen eines Kontextprofils](#).
- 2 Verwenden des Kontextprofils in einer Regel für verteilte Firewall: [Hinzufügen einer verteilten Firewall](#).

## Anwendungsidentifikations-GUIDs

Durch die Identifikation von Schicht-7-Anwendungen wird bestimmt, von welcher Anwendung ein bestimmtes Paket oder ein bestimmter Flow unabhängig vom verwendeten Port generiert wird.

Die auf der Anwendungsidentität basierende Erzwingung ermöglicht es Benutzern, das Ausführen von Anwendungen auf beliebigen Ports zuzulassen oder zu verweigern, oder zu erzwingen, dass Anwendungen auf ihrem standardmäßigen Port ausgeführt werden. DPI (Deep Packet Inspection) ermöglicht die Abstimmung der Paketnutzlast auf definierte Muster. Diese werden in der Regel als Signaturen bezeichnet. Mithilfe der signaturbasierten Identifikation und Erzwingung können Kunden nicht nur die jeweilige Anwendung bzw. das jeweilige Protokoll abgleichen, zu der bzw. dem ein Flow gehört, sondern auch die Version dieses Protokolls, zum Beispiel TLS Version 1.0, TLS Version 1.2 oder verschiedene Versionen von CIFS-Datenverkehr. Dadurch erhalten Kunden für alle bereitgestellten Anwendungen und ihre Ost-West-Flows innerhalb des Datacenters Einblick in die Verwendung von Protokollen mit bekannten Sicherheitslücken und können die Verwendung dieser Protokolle beschränken.

Unterstützte App-IDs und FQDNs:

- Für FQDN müssen Benutzer eine Regel mit hoher Priorität mit einer DNS-App-ID für die angegebenen DNS-Server auf Port 53 konfigurieren.
- Die ALG-App-IDs (FTP, ORACLE, DCERPC, TFTP) erfordern den entsprechenden ALG-Dienst für die Firewallregel.
- Die SYSLOG-App-ID wird nur auf Standard-Ports erkannt.

Von KVM unterstützte App-IDs und FQDNs:

- Von KVM werden keine Unterattribute unterstützt.
- FTP- und TFTP-ALG-App-IDs werden von KVM unterstützt.

APP-IDs der Schicht 7 werden in Kontextprofilen in der verteilten Firewall verwendet und werden nur auf ESXi-Hosts unterstützt.

GUID	Beschreibung	Typ
360ANTIV	360 Safeguard ist ein vom chinesischen IT-Unternehmen Qihoo 360 entwickeltes Programm.	Webdienste
ACTIVDIR	Microsoft Active Directory	Netzwerk
AD_BKUP	Microsoft Active Directory-Backupdienst	Netzwerk
AD_NSP	Microsoft Active Directory-Dienstanbieter	Netzwerk

GUID	Beschreibung	Typ
AMQP	Advanced Messaging Queuing Protocol ist ein Protokoll auf Anwendungsebene, das die Business-Nachrichten-Kommunikation zwischen Anwendungen oder Organisationen unterstützt	Netzwerk
AVAST	Von der offiziellen Avast.com-Webseite von Avast! generierter Datenverkehr Antivirus-Downloads	Webdienste
AVG	Download und Updates für AVG Antivirus-/Sicherheitssoftware	Dateiübermittlung
AVIRA	Download und Updates für Avira Antivirus-/Sicherheitssoftware	Dateiübermittlung
BLAST	Ein Remotezugriffsprotokoll, das die Datenverarbeitung in einem Rechenzentrum komprimiert, verschlüsselt und codiert und diese über ein beliebiges Standard-IP-Netzwerk für VMware Horizon-Desktops übermittelt.	Remotezugriff
BDEFENDER	Download und Updates für BitDefender Antivirus-/Sicherheitssoftware	Dateiübermittlung
CA_CERT	Zertifizierungsstellen (CA) stellen digitale Zertifikate aus, die den Besitz eines öffentlichen Schlüssels für die Nachrichtenverschlüsselung zertifizieren.	Netzwerk
CIFS	CIFS (Common Internet File System) wird verwendet, um den gemeinsamen Zugriff auf Verzeichnisse, Dateien, Drucker, serielle Ports sowie diverse Kommunikationswege zwischen Knoten in einem Netzwerk zu ermöglichen.	Dateiübermittlung
CLDAP	Das CLDAP (Connectionless Lightweight Directory Access Protocol) ist ein Anwendungsprotokoll für den Zugriff auf und die Verwaltung von verteilten Verzeichnis-Informationsdiensten über ein IP (Internet Protocol)-Netzwerk mithilfe von UDP.	
CLRCASE	Ein Software-Tool zur Versionsverwaltung des Quellcodes sowie weiterer Softwareentwicklungs-Assets. Es wird von der Rational Software-Abteilung von IBM entwickelt. ClearCase bildet die Basis für die Versionsverwaltung vieler großer und mittelständischer Unternehmen und bietet Kapazitäten für Projekte mit Hunderten oder sogar Tausenden von Entwicklern.	Netzwerk
CTRXCGP	Das CTRXCGP (Citrix Common Gateway Protocol) ist ein Anwendungsprotokoll für den Zugriff auf und die Verwaltung von verteilten Verzeichnis-Informationsdiensten über ein IP (Internet Protocol)-Netzwerk mithilfe von UDP.	Datenbank
CTRKGOTO	Für das Hosten von Citrix GoToMeeting-Sitzungen oder vergleichbaren Sitzungen, die auf der GoToMeeting-Plattform basieren. Enthält Voice- und Video- sowie begrenzte Crowd Management-Funktionen	Zusammenarbeit
CTRICA	ICA (Independent Computing Architecture) ist ein von Citrix Systems entwickeltes proprietäres Protokoll für Anwendungsserver-Systeme.	Remotezugriff
DCERPC	Distributed Computing Environment / Remote Procedure Calls ist das für die Distributed Computing Environment (DCE) entwickelte Remoteprozeduraufruf-System.	Netzwerk

GUID	Beschreibung	Typ
DIAMETER	Ein Authentifizierungs-, Autorisierungs- und Accounting-Protokoll für Computernetzwerke	Netzwerk
DNS	Abfragen eines DNS-Servers über TCP oder UDP	Netzwerk
EPIC	EPIC EMR ist eine Anwendung für elektronische Patientenakten, die Informationen zur Patientenpflege und zum Gesundheitswesen bietet.	Client-Server
ESET	Download und Updates für Eset Antivirus-/Sicherheitssoftware	Dateiübermittlung
FPROT	Download und Updates für F-Prot Antivirus-/Sicherheitssoftware	Dateiübermittlung
FTP	FTP (File Transfer Protocol, Dateiübermittlungsprotokoll) wird verwendet, um Dateien von einem Dateiserver auf einen lokalen Rechner zu übertragen	Dateiübermittlung
GITHUB	Webbasiertes Git oder Repository für Versionskontrolle und Internethostingdienst	Zusammenarbeit
HTTP	(HyperText Transfer Protocol) ist das wichtigste Transportprotokoll für das World Wide Web.	Webdienste
HTTP2	Generierter Datenverkehr von Webseiten, die das HTTP 2.0-Protokoll unterstützen	Webdienste
IMAP	IMAP (Internet Message Access Protocol) ist ein Standard-Internet-Protokoll für den Zugriff auf E-Mail auf einem Remote-Server.	E-Mail
KASPRSKY	Download und Updates für Kaspersky Antivirus-/Sicherheitssoftware	Dateiübermittlung
KERBEROS	Kerberos ist ein Netzwerk-Authentifizierungsprotokoll, das entwickelt wurde, um mithilfe der Geheimschlüssel-Kryptografie eine starke Authentifizierung für Client-/Server-Anwendungen zu bieten.	Netzwerk
LDAP	LDAP (Lightweight Directory Access Protocol) ist ein Protokoll für das Lesen und Bearbeiten von Verzeichnissen über ein IP-Netzwerk.	Datenbank
MAXDB	SQL-Verbindungen zu und Abfragen an einen MaxDB-SQL-Server	Datenbank
MCAFEE	Download und Updates für McAfee Antivirus-/Sicherheitssoftware	Dateiübermittlung
MSSQL	Microsoft SQL Server ist eine relationale Datenbank.	Datenbank
NFS	Ermöglicht Benutzern auf einem Client-Computer den Zugriff auf Dateien über ein Netzwerk auf eine Art und Weise, die dem Zugriff auf den lokalen Speicher ähnelt.	Dateiübermittlung
NNTP	Dies ist ein Internet-Anwendungsprotokoll für die Übertragung von Usenet-News-Artikeln (Netnews) zwischen Newsservern sowie für das Lesen und Bereitstellen von Beiträgen durch Endbenutzer-Clientanwendungen.	Dateiübermittlung

GUID	Beschreibung	Typ
NTBIOSNS	NetBIOS-Namensdienst. Um Sitzungen zu starten oder Datagramme zu verteilen, müssen Anwendungen ihren NetBIOS-Namen mithilfe des Namensdienstes registrieren.	Netzwerk
NTP	Das NTP (Network Time Protocol) wird zur Synchronisation der Uhren in Computersystemen über das Netzwerk verwendet.	Netzwerk
OCSP	Ein OCSP-Responder, der sicherstellt, dass der private Schlüssel eines Benutzers nicht kompromittiert oder widerrufen wurde	Netzwerk
ORACLE	Ein objektrelationales Datenbankverwaltungssystem (ORDBMS), das von der Oracle Corporation entwickelt und vertrieben wird	Datenbank
PANDA	Download und Updates für Panda Antivirus-/Sicherheitssoftware	Dateiübermittlung
PCOIP	Ein Remotezugriffsprotokoll, das die Datenverarbeitung in einem Rechenzentrum komprimiert, verschlüsselt und codiert und diese über ein beliebiges Standard-IP-Netzwerk übermittelt	Remotezugriff
POP2	Das POP (Post Office Protocol) ist ein Protokoll, das von lokalen E-Mail-Clients für das Abrufen von E-Mails von einem Remote-Server verwendet wird.	E-Mail
POP3	Die Microsoft-Implementierung eines NetBIOS-Namensdiensts (NBNS), einem Server und Dienst für NetBIOS-Computernamen	E-Mail
RADIUS	Bietet eine zentralisierte AAA-Verwaltung (Authentifizierung, Autorisierung und Accounting), damit Computer eine Verbindung zu einem Netzwerk-Dienst aufbauen und diesen verwenden können	Netzwerk
POSTGRES		
RDP	Das RDP (Remote Desktop Protocol) bietet Benutzern eine grafische Schnittstelle zu einem anderen Computer.	Remotezugriff
RTCP	Das RTCP (Real-Time Transport Control Protocol) ist ein Schwesterprotokoll des Real-time Transport Protocol (RTP). Das RTCP bietet Out-of-Band-Kontrollinformationen für einen RTP-Strom.	Streaming Media
RTP	Das RTP (Real-Time Transport Protocol) dient in erster Linie zur Echtzeit-Bereitstellung von Audio und Video.	Streaming Media
RTSP	Das RTSP (Real Time Streaming Protocol) wird für das Einrichten und die Steuerung von Mediensitzungen zwischen Endpunkten verwendet.	Streaming Media
RTSPS	Ein sicheres Netzwerkprotokoll, das für die Verwendung in Unterhaltungs- und Kommunikationssystemen zur Steuerung von Streaming Media-Servern entwickelt wurde. Das Protokoll wird für das Einrichten und die Steuerung von Mediensitzungen zwischen Endpunkten verwendet.	Streaming Media
SAP	Verbindungen zu generischen Komponenten mehrerer SAP-Produkte, wie Netweaver, BusinessObjects XI und Crystal Enterprise Server.	Zusammenarbeit



GUID	Beschreibung	Typ
SIP	Das SIP (Session Initiation Protocol) ist ein allgemeines Steuerungsprotokoll für die Einrichtung und die Steuerung von Sprach- und Videoanrufen.	Streaming Media
SKIP	Simple Key Management for Internet Protocols (SKIP) ist ein Hybrid-Schlüsselverteilungsprotokoll. Simple Key Management for Internet Protocols (SKIP) ähnelt SSL, der Unterschied liegt jedoch darin, dass einmalig ein langfristiger Schlüssel festgelegt wird und anschließend keine weitere Kommunikation erforderlich ist, um für einzelne Sitzungen Schlüssel festzulegen oder auszutauschen.	Netzwerk
SMTP	Das SMTP (Simple Mail Transfer Protocol) ist ein Internetstandard für die Übertragung elektronischer Nachrichten (E-Mail) über Internet Protocol (IP)-Netzwerke.	E-Mail
SNMP	Das SNMP (Simple Network Management Protocol) ist ein Internet-Standard-Protokoll für die Verwaltung von Geräten in IP-Netzwerken.	Netzwerküberwachung
SQLNET	Netzwerk-Software, die einen Remote-Datenzugriff zwischen Programmen und der Oracle-Datenbank oder zwischen mehreren Oracle-Datenbanken ermöglicht	Datenbank
SQLSERV	SQL-Dienste	Datenbank
SSH	SSH (Secure Shell) ist ein Netzwerkprotokoll, das den Austausch von Daten zwischen zwei vernetzten Geräten über einen sicheren Kanal ermöglicht.	Remotezugriff
SSL	SSL (Secure Sockets Layer) ist ein kryptografisches Protokoll, das Sicherheit über das Internet bietet.	Webdienste
SVN	Verwalten von Inhalten auf einem Subversion-Server.	Datenbank
SYMUPDAT	Symantec LiveUpdate-Datenverkehr; dies umfasst Spyware-Definitionen, Firewall-Regeln, Antivirus-Signaturdateien und Software-Updates.	Dateiübermittlung
SYSLOG	Symantec LiveUpdate-Datenverkehr; dies umfasst Spyware-Definitionen, Firewall-Regeln, Antivirus-Signaturdateien und Software-Updates.	Netzwerküberwachung
TELNET	Ein Netzwerkprotokoll, das im Internet oder bei LAN-Verbindungen verwendet wird, um eine bidirektionale interaktive textorientierte Kommunikationseinrichtung mit einer virtuellen Terminal-Verbindung bereitzustellen	Remotezugriff
TFTP	Das TFTP (Trivial File Transfer Protocol) wird verwendet, um Dateien unter Verwendung eines Clients wie WinAgents TFTP-Client aufzulisten, herunterzuladen und zu einem TFTP-Server wie beispielsweise SolarWinds TFTP Server hochzuladen.	Dateiübermittlung
VNC	Virtual Network Computing-Datenverkehr:	Remotezugriff
WINS	Die Microsoft-Implementierung eines NetBIOS-Namensdiensts (NBNS), einem Server und Dienst für NetBIOS-Computernamen	Netzwerk

## Verteilte Firewall

Die verteilte Firewall enthält vordefinierte Kategorien für Firewallregeln. Die Regeln werden von oben nach unten und von links nach rechts ausgewertet. Die Kategorienamen können über die API geändert werden.

**Tabelle 10-2. Kategorien**

Ethernet	Wird für Schicht-2-basierte Regeln verwendet
Notfall	Für Quarantäne- und Zulassungsregeln verwendet
Infrastruktur	Definieren Sie den Zugriff auf gemeinsam genutzte Dienste. Globale Regeln – AD-, DNS-, NTP-, DHCP-, Sicherungs-, Verwaltungsserver
Umgebung	Regeln zwischen den Zonen – Produktion bzw. Entwicklung, Regeln für geschäftseinheitsübergreifenden Datenverkehr
Anwendung	Regeln zwischen Anwendungen, Anwendungsebenen oder die Regeln zwischen Mikrodiensten

## Hinzufügen einer verteilten Firewall

Eine verteilte Firewall überwacht den gesamten Ost-West-Datenverkehr auf Ihren virtuellen Maschinen.

### Voraussetzungen

Damit virtuelle Gastmaschinen per DFW geschützt sind, muss ihr vNIC mit einem logischen NVDS-Switch verbunden sein, der mit einer Transportzone verknüpft ist.

Wenn Sie Regeln für die identitätsbasierte Firewall erstellen, müssen Sie zuerst eine Gruppe mit Active Directory-Mitgliedern erstellen. IDFW unterstützt nur TCP-basierte Firewallregeln.

**Hinweis** Zur Erzwingung der identitätsbasierten Firewallregel sollte für den Windows-Zeitdienst **ein** für alle VMs festgelegt sein, die Active Directory verwenden. Dadurch wird sichergestellt, dass Datum und Uhrzeit zwischen Active Directory und VMs synchronisiert werden. Darüber hinaus werden Änderungen der AD-Gruppenmitgliedschaft, einschließlich der Aktivierung und Löschung von Benutzern, nicht sofort für angemeldete Benutzer wirksam. Damit die Änderungen wirksam werden, müssen sich die Benutzer abmelden und erneut anmelden. AD-Administratoren sollten eine Abmeldung erzwingen, wenn die Gruppenmitgliedschaft geändert wird. Dieses Verhalten ist eine Beschränkung von Active Directory.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie im Navigationsbereich **Sicherheit > Verteilte Firewall**.

- 3 Vergewissern Sie sich, dass Sie sich in der richtigen vordefinierten Kategorie befinden, und klicken Sie auf **Richtlinie hinzufügen**. Weitere Informationen über Kategorien finden Sie unter [Verteilte Firewall](#).
- 4 Geben Sie einen **Namen** für den Abschnitt mit der neuen Richtlinie ein.
- 5 Wählen Sie die **Ziel**-Domäne für die Richtlinie aus. Behalten Sie die Standarddomäne für die Richtlinie bei, fügen Sie eine andere Domäne hinzu oder erstellen Sie eine neue Domäne. Eine Domäne ist ein logisches Konstrukt, das eine Sicherheitszone und alle Sicherheitsgruppen und Regeln darstellt.

Beachten Sie, dass das Domänenobjekt eine experimentelle Funktion in NSX-T Data Center 2.4 ist, die in NSX-T Data Center 2.4.1 nicht verfügbar ist.

- 6 (Optional) Klicken Sie auf das Zahnradsymbol, um die folgenden Richtlinieneinstellungen zu konfigurieren:

Menüoption	Beschreibung
Strenges TCP	<p>Eine TCP-Verbindung beginnt mit einem Dreizeige-Handshake (SYN, SYN-ACK, ACK) und endet in der Regel mit einem Zweizeige-Austausch (FIN, ACK). Unter bestimmten Umständen sieht die verteilte Firewall den Dreizeige-Handshake für einen bestimmten Flow möglicherweise nicht (z. B. aufgrund des asymmetrischen Datenverkehrs oder der Aktivierung der verteilten Firewall, während ein Flow vorhanden ist). Standardmäßig erzwingt die verteilte Firewall nicht die Notwendigkeit, einen Dreizeige-Handshake zu sehen, und nimmt bereits bestehende Sitzungen auf. „Strenges TCP“ kann pro Abschnitt aktiviert werden, um das Abrufen mitten in der Sitzung zu deaktivieren und die Anforderung für einen 3-Wege-Handshake zu erzwingen.</p> <p>Wenn Sie den Modus „Strenges TCP“ für einen bestimmten Abschnitt der verteilten Firewall aktivieren und eine standardmäßige Blockregel vom Typ ANY-ANY verwenden, werden Pakete, die die Dreizeige-Handshake-Verbindungsanforderungen nicht erfüllen und die mit einer TCP-basierten Regel in diesem Abschnitt übereinstimmen, verworfen. „Streng“ wird nur auf statusbehaftete TCP-Regeln angewendet und auf der Abschnittsebene der verteilten Firewall aktiviert. „Strenges TCP“ wird nicht für Pakete erzwungen, die mit einer standardmäßigen ANY-ANY-Zulassung übereinstimmen, wofür kein TCP-Dienst angegeben wurde.</p>
Statusbehaftet	<p>Eine statusbehaftete Firewall überwacht den Zustand der aktiven Verbindungen und verwendet diese Informationen, um zu ermitteln, welche Pakete die Firewall passieren dürfen.</p>
Gesperrt	<p>Die Richtlinie kann gesperrt werden, um zu verhindern, dass mehrere Benutzer Änderungen an denselben Abschnitten vornehmen. Wenn Sie einen Abschnitt sperren, müssen Sie einen Kommentar einfügen.</p> <p>Einige Rollen, beispielsweise der Enterprise-Administrator, verfügen über Anmeldedaten mit Vollzugriff und können nicht gesperrt werden. Siehe <a href="#">Rollenbasierte Zugriffssteuerung</a>.</p>

- 7 Klicken Sie auf **Veröffentlichen**. Mehrere Richtlinien können hinzugefügt und anschließend in einem Arbeitsschritt zusammen veröffentlicht werden.

Die neue Richtlinie wird auf dem Bildschirm angezeigt.

- 8 Wählen Sie einen Richtlinienabschnitt aus und klicken Sie auf **Regel hinzufügen**.
- 9 Geben Sie einen Namen für die Regel ein.

- 10 Klicken Sie in der Spalte **Quellen** auf das Symbol „Bearbeiten“ und wählen Sie die Quelle der Regel aus. Gruppen mit Active Directory-Mitgliedern können für das Quelltextfeld einer IDFW-Regel verwendet werden. Weitere Informationen hierzu finden Sie unter [Hinzufügen einer Gruppe](#).
- 11 Klicken Sie in der Spalte **Ziele** auf das Symbol „Bearbeiten“ und wählen Sie das Ziel der Regel aus. Wenn nicht definiert, bezieht sich die Regel auf alle Ziele. Weitere Informationen hierzu finden Sie unter [Hinzufügen einer Gruppe](#).
- 12 Klicken Sie in der Spalte **Dienste** auf das Symbol „Bearbeiten“ und wählen Sie Dienste aus. Wenn nicht definiert, bezieht sich die Regel auf **alle** Dienste.
- 13 Diese Spalte **Profile** ist nicht verfügbar, wenn Sie der Ethernet-Kategorie eine Regel hinzufügen. Klicken Sie für alle anderen Regelkategorien in der Spalte **Profile** auf das Symbol „Bearbeiten“ und wählen Sie ein Kontextprofil aus. Siehe [Hinzufügen eines Kontextprofils](#).  
  
Kontextprofile verwenden APP-ID-Attribute der Schicht 7 für die Verwendung in Regeln für eine verteilte Firewall.
- 14 Standardmäßig ist für die Spalte **Angewendet auf** der Wert „DFW“ festgelegt und die Regel wird auf alle Arbeitslasten angewendet. Sie können die Regel oder Richtlinie auch auf ausgewählte Gruppen anwenden. **Angewendet auf** definiert den Erzwingungsumfang für jede Regel und wird hauptsächlich für die Optimierung oder für Ressourcen auf ESXi- und KVM-Hosts verwendet. Diese Einstellung ist hilfreich, wenn eine gezielte Richtlinie für bestimmte Zonen und Mandanten definiert werden soll, ohne dass es zu Konflikten mit einer anderen Richtlinie kommt, die für andere Mandanten und Zonen definiert wurde.  
  
Gruppen, die nur aus IP-Adressen bestehen, MAC-Adressen oder Active Directory-Gruppen können im Textfeld **Angewendet auf** nicht verwendet werden.

- 15 Wählen Sie eine Aktion in der Spalte **Aktion** aus.

Option	Beschreibung
<b>Zulassen</b>	Ermöglicht dem gesamten L3- oder L2-Datenverkehr mit der angegebenen Quelle, dem angegebenen Ziel und Protokoll das Passieren des aktuellen Firewallkontexts. Pakete, die der Regel genügen und akzeptiert werden, durchlaufen das System wie beim Fehlen einer Firewall.
<b>Verwerfen</b>	Verwirft Pakete mit der angegebenen Quelle, dem angegebenen Ziel und Protokoll. Das Verwerfen eines Pakets erfolgt im Hintergrund ohne Benachrichtigung der Quell- oder Zielsysteme. Das Verwerfen des Pakets führt dazu, dass erneut versucht wird, die Verbindung herzustellen, bis der entsprechende Schwellenwert erreicht wird.
<b>Ablehnen</b>	Lehnt Pakete mit der angegebenen Quelle, dem angegebenen Ziel und Protokoll ab. Das Ablehnen eines Pakets ist der elegantere Weg, um das Senden eines Pakets zu verweigern. Dabei wird an den Sender eine Meldung übermittelt, dass das Ziel nicht erreichbar ist. Bei Verwendung des TCP-Protokolls wird eine TCP RST-Meldung gesendet. ICMP-Meldungen mit vom Administrator verbotenen Code werden für UDP-, ICMP- und andere IP-Verbindungen versendet. Die Methode des Ablehnens hat den Vorteil, dass die sendende Anwendung bereits nach einem Versuch benachrichtigt wird, dass die Verbindung nicht aufgebaut werden kann.

- 16 Mit einem Klick auf den Schalter „Status“ können Sie die Regel aktivieren bzw. deaktivieren.

- 17 (Optional) Klicken Sie auf das Zahnradsymbol, um die folgenden Richtlinienoptionen zu konfigurieren:

Option	Beschreibung
<b>Protokollierung</b>	Die Protokollierung ist standardmäßig deaktiviert. Die Protokolle werden in der Datei „/var/log/dfwpktlogs.log“ auf ESXi- und KVM-Hosts gespeichert.
<b>Richtung</b>	Dieses Textfeld bezieht sich auf die Richtung des Datenverkehrs aus der Sicht des Zielobjekts. „Eingehend“ bedeutet, dass nur Datenverkehr an das Objekt überprüft wird, „Ausgehend“ bedeutet, dass nur Datenverkehr aus dem Objekt überprüft wird, und „Eingehend/Ausgehend“ bedeutet, dass Datenverkehr in beide Richtungen überprüft wird.
<b>IP-Protokoll</b>	Erzwingen Sie die Regel auf der Basis von IPv4, IPv6 oder beiden (IPv4-IPv6).
<b>Tag</b>	Mit Tags lässt sich die Suche vereinfachen.

- 18 Klicken Sie auf **Veröffentlichen**. Mehrere Regeln können hinzugefügt und in einem Arbeitsschritt zusammen veröffentlicht werden.

## Hinzufügen einer Firewallregel für die Aufnahme von FQDN/URLs in die Whitelist

Richten Sie eine Regel für die verteilte Firewall ein, um bestimmten Ost-West-Datenverkehr zu bestimmten mit FQDN/URLs identifizierten Domänen zuzulassen, z. B. *\*.office365.com*.

Derzeit wird eine vordefinierte Liste der Domänen unterstützt. Sie können die Liste der FQDNs sehen, wenn Sie ein neues Kontextprofil mit dem Attributtyp *Domänenname (FQDN)* hinzufügen.

Sie müssen zuerst eine DNS-Regel einrichten. Richten Sie dann unterhalb dieser Regel die FQDN-Whitelistregel ein. Der Grund hierfür ist, dass NSX-T Data Center DNS-Snooping verwendet, um eine Zuordnung zwischen der IP-Adresse und dem FQDN zu erhalten. Zum Schutz gegen DNS-Spoofing-Angriffe, bei denen eine bössartige VM gefälschte DNS-Antworten einfügen kann, um Datenverkehr an bössartige Endpoints umzuleiten oder die DFW zu umgehen, sollte Spoofguard über den Switch auf allen logischen Ports aktiviert werden. Weitere Informationen zu Spoofguard finden Sie unter [Grundlegendes zum Spoofguard-Segmentprofil](#).

FQDN-basierte Regeln werden während vMotion beibehalten.

---

**Hinweis** In der aktuellen Version wird nur ESXi unterstützt.

---

## Voraussetzungen

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie im Navigationsbereich **Sicherheit > Verteilte Firewall**.
- 3 Befolgen Sie die Schritte unter [Hinzufügen einer verteilten Firewall](#) und fügen Sie einen Abschnitt für eine Firewallrichtlinie hinzu. Alternativ können Sie einen vorhandenen Firewallrichtlinienabschnitt verwenden.
- 4 Wählen Sie zuerst den neuen oder vorhandenen Firewallrichtlinienabschnitt aus und klicken Sie auf **Regel hinzufügen**, um die DNS-Firewallregel zu erstellen.
- 5 Geben Sie einen Namen für die Firewallregel ein, beispielsweise **DNS-Regel1**, und geben Sie die folgenden Details ein:

Option	Beschreibung
<b>Dienste</b>	Klicken Sie auf das Symbol „Bearbeiten“ und wählen Sie den DNS- oder DNS-UDP-Dienst aus, je nachdem, was für Ihre Umgebung zutreffend ist.
<b>Profil</b>	Klicken Sie auf das Symbol „Bearbeiten“ und wählen Sie die DNS-Kontextprofil aus. Dieses wird vorab erstellt und ist standardmäßig in Ihrer Bereitstellung verfügbar.
<b>Angewendet auf</b>	Wählen Sie je nach Bedarf „DFW“ oder eine Gruppe aus.
<b>Aktion</b>	Wählen Sie <b>Zulassen</b> .

- 6 Klicken Sie noch einmal auf **Regel hinzufügen**, um die FQDN-Whitelistregel einzurichten.
- 7 Benennen Sie die Regel mit einem aussagekräftigen Namen, beispielsweise **FQDN/URL-Whitelist**. Ziehen Sie die Regel unter die DNS-Regel unter diesem Richtlinienabschnitt.

## 8 Geben Sie die folgenden Details an:

Option	Beschreibung
Dienste	Klicken Sie auf das Symbol „Bearbeiten“ und wählen Sie den Dienst aus, der mit dieser Regel verknüpft werden soll, z. B. „HTTP“.
Profil	Klicken Sie auf das Symbol „Bearbeiten“ und klicken Sie auf <b>Neues Kontextprofil hinzufügen</b> . Klicken Sie in die Spalte mit der Überschrift <b>Attribut</b> und wählen Sie <b>Domänenname (FQDN)</b> aus. Wählen Sie die Liste der Attributnamen/-werte aus der vordefinierten Liste aus. Klicken Sie auf <b>Hinzufügen</b> . Weitere Informationen finden Sie unter <a href="#">Hinzufügen eines Kontextprofils</a> .
Angewendet auf	Wählen Sie je nach Bedarf „DFW“ oder eine Gruppe aus.
Aktion	Wählen Sie <b>Zulassen</b> .

## 9 Klicken Sie auf **Veröffentlichen**.

## Protokolle des verteilten Firewallpakets

Wenn die Protokollierung für Firewallregeln aktiviert ist, können Sie zur Fehlerbehebung die Protokolle der Firewallpakete durchsehen.

Die Protokolldatei für ESXi- und KVM-Hosts lautet jeweils `/var/log/dfwpktlogs.log`.

Im Folgenden finden Sie ein reguläres Protokollbeispiel für Regeln für verteilte Firewalls:

```
2018-07-03T19:44:09.749Z b6507827 INET match PASS mainrs/1024 IN 52 TCP 192.168.4.3/49627->192.168.4.4/49153 SEW

2018-07-03T19:46:02.338Z 7396c504 INET match DROP mainrs/1024 OUT 52 TCP 192.168.4.3/49676->192.168.4.4/135 SEW

2018-07-06T18:15:49.647Z 028cd586 INET match DROP mainrs/1027 IN 36 PROTO 2 0.0.0.0->224.0.0.1

2018-07-06T18:19:54.764Z 028cd586 INET6 match DROP mainrs/1027 OUT 143 UDP
fe80:0:0:0:68c2:8472:2364:9be/546->ff02:0:0:0:0:1:2/547
```

Die Elemente eines DFW-Protokolldateiformats enthalten Folgendes, getrennt durch ein Leerzeichen:

- Zeitstempel:
- die letzten acht Ziffern der VIF-ID der Schnittstelle
- INET-Typ (v4 oder v6)
- Grund (Übereinstimmung)
- Aktion (ÜBERGEBEN, ABLEGEN, ABLEHNEN)
- Regelsatzname/-ID
- Paketrichtung (EIN-/AUSGEHEND)
- Paketgröße



- Protokoll (TCP, UDP oder PROTO #)
- SVM-Richtung für netX-Regeltreffer
- IP-Adresse/Port der Quelle > IP-Adresse/Port des Ziels
- TCP-Flags (SEW)

Für übergebene TCP-Pakete gibt es ein Beendigungsprotokoll, wenn die Sitzung beendet ist:

```
2018-07-03T19:44:30.585Z 7396c504 INET TERM mainrs/1024 OUT TCP RST 192.168.4.3/49627-
>192.168.4.4/49153 20/16 1718/76308
```

Die Elemente eines TCP-Beendigungsprotokolls enthalten Folgendes, getrennt durch einen Leerzeichen:

- Zeitstempel:
- die letzten 8 Ziffern der VIF-ID der Schnittstelle
- INET-Typ (v4 oder V6)
- Aktion (LAUFZEIT)
- Regelsatzname/Regel-ID
- Paketrichtung (EIN-/AUSGEHEND)
- Protokoll (TCP, UDP oder PROTO #)
- TCP RST-Flag
- SVM-Richtung für netX-Regeltreffer
- IP-Adresse/Port der Quelle > IP-Adresse/Port des Ziels
- Anzahl EINGEHENDER/AUSGEHENDER Pakete (insgesamt)
- Größe des EINGEHENDEN/AUSGEHENDEN Pakets

Im Folgenden finden Sie ein Beispiel für eine FQDN-Protokolldatei für Regeln verteilter Firewalls:

```
2019-01-15T00:34:45.903Z 7c607b29 INET match PASS 1031 OUT 48 TCP 10.172.178.226/32808-
>23.72.199.234/80 S www.sway.com(034fe78d-5857-0680-81e4-d8da6b28d1b4)
```

Die Elemente eines FQDN-Protokolls enthalten Folgendes, getrennt durch einen Leerzeichen:

- Zeitstempel:
- die letzten acht Ziffern der VIF-ID der Schnittstelle
- INET-Typ (v4 oder V6)
- Grund (Übereinstimmung)
- Aktion (ÜBERGEBEN, ABLEGEN, ABLEHNEN)
- Regelsatzname/Regel-ID
- Paketrichtung (EIN-/AUSGEHEND)

- Paketgröße
- Protokoll (TCP, UDP oder PROTO #)
- IP-Adresse/Port der Quelle > IP-Adresse/Port des Ziels
- Domänenname/UUID, wobei die UUID die binäre interne Darstellung für den Domännennamen ist

Im Folgenden finden Sie ein Beispiel für eine Schicht-7-Protokolldatei für Regeln verteilter Firewalls:

```
2019-01-15T00:35:07.221Z 82f365ae INET match REJECT 1034 OUT 48 TCP 10.172.179.6/49818-
>23.214.173.202/80 S APP_HTTP

2019-01-15T00:34:46.486Z 7c607b29 INET match PASS 1030 OUT 48 UDP 10.172.178.226/42035-
>10.172.40.1/53 APP_DNS
```

Die Elemente eines Schicht-7-Protokolls enthalten Folgendes, getrennt durch ein Leerzeichen:

- Zeitstempel:
- die letzten acht Ziffern der VIF-ID der Schnittstelle
- INET-Typ (v4 oder V6)
- Grund (Übereinstimmung)
- Aktion (ÜBERGEBEN, ABLEGEN, ABLEHNEN)
- Regelsatzname/Regel-ID
- Paketrichtung (EIN-/AUSGEHEND)
- Paketgröße
- Protokoll (TCP, UDP oder PROTO #)
- IP-Adresse/Port der Quelle > IP-Adresse/Port des Ziels
- APP\_XXX ist die erkannte Anwendung

## Auswählen einer Standard-Konnektivitätsstrategie

Sie können eine Standard-Konnektivitätsstrategie auswählen, um Ihr Sicherheitsmodell zu erzwingen.

Die Standard-Konnektivitätsstrategie erstellt zusätzlich zu den anderen von Ihnen erstellten Firewallregeln entweder eine Blacklist- oder eine Whitelist-Firewallrichtlinie, anstatt einzelne Regeln zu ändern. Bei einer Blacklist-Richtlinie werden alle Verbindungen zugelassen, die nicht auf die Blacklist gesetzt werden; bei einer Whitelist-Richtlinie werden alle Verbindungen abgelehnt, die nicht auf die Whitelist gesetzt werden.

Folgende Optionen sind verfügbar:

- **Blacklist (mit oder ohne Protokollierung):** Dies ist die Standardoption. Mit dieser Einstellung wird eine „Alle zulassen“-Regel für die DFW erstellt.

- **Whitelist (mit oder ohne Protokollierung):** Erstellt eine Firewallregel, die den gesamten Datenverkehr ablehnt. Nur die Kommunikation von Sites oder Anwendungen, die in Firewallregeln definiert wurden, ist zulässig. Alle anderen Kommunikationen erhalten keinen Zugriff. Dazu gehört auch der DHCP-Datenverkehr.
- **Keine:** Wählen Sie diese Option, um Firewallregeln per Blacklist und Whitelist zu deaktivieren. Dies ist nützlich, wenn Sie bereits eine Reihe von Regeln mit früheren Versionen von NSX-T Data Center konfiguriert haben.

## Konfigurieren einer Gateway-Firewall

Eine Gateway-Firewall enthält Regeln, die in der Perimeterfirewall angewendet werden.

In der Ansicht **Alle freigegeben Regeln**, in der Regeln für alle Gateways angezeigt werden, stehen vordefinierte Kategorien zur Verfügung. Die Regeln werden von oben nach unten und von links nach rechts ausgewertet. Die Kategorienamen können über die API geändert werden.

**Tabelle 10-3. Kategorien für Gateway-Firewallregeln**

Regelkategorie	Zweck
Notfall	Wird für Quarantäne verwendet. Kann auch für Zulassungsregeln verwendet werden.
System	Diese Regeln werden automatisch von NSX-T Data Center erzeugt und sind für Datenverkehr der internen Steuerungskomponente spezifisch, wie z. B. BFD-, VPN-Regeln usw.  <b>Hinweis</b> Systemregeln sollten nicht bearbeitet werden.
Gemeinsam genutzte Vorabregeln	Diese Regeln werden global auf mehrere Gateways angewendet.
Lokales Gateway	Diese Regeln sind für ein bestimmtes Gateway spezifisch.
Automatische Dienstregeln	Hierbei handelt es sich um automatisch ausgeführte Regeln, die auf die Datenebene angewendet werden. Sie können diese Regeln nach Bedarf bearbeiten.
Standard	Diese Regeln definieren das Standardverhalten der Gateway-Firewall.

## Hinzufügen von Regeln und Richtlinien für eine Gateway-Firewall

Implementieren Sie Regeln für eine Gateway-Firewall, indem Sie sie unter einem Abschnitt der Firewallrichtlinie hinzufügen, der zu einer vordefinierten Kategorie gehört.

### Verfahren

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

- 2 Wählen Sie **Sicherheit > Vertikale Sicherheit > Gateway-Firewall** und wechseln Sie zu der Kategorie, in der Sie die neue Richtlinie hinzufügen möchten.
- 3 Klicken Sie auf **Richtlinie hinzufügen**. Weitere Informationen über Kategorien finden Sie unter [Konfigurieren einer Gateway-Firewall](#).
- 4 Geben Sie einen **Namen** für den Abschnitt mit der neuen Richtlinie ein.
- 5 Wählen Sie die **Ziel**-Domäne für die Richtlinie aus. Behalten Sie die Standarddomäne für die Richtlinie bei, fügen Sie eine andere Domäne hinzu oder erstellen Sie eine neue Domäne. Eine Domäne ist ein logisches Konstrukt, das aus einer Sicherheitszone und allen Sicherheitsgruppen und -regeln besteht.

Beachten Sie, dass das Domänenobjekt eine experimentelle Funktion in NSX-T Data Center 2.4 ist, aber in NSX-T Data Center 2.4.1 nicht verfügbar ist.

- 6 Klicken Sie auf das Zahnradsymbol, um die folgenden Richtlinieneinstellungen zu konfigurieren:

Menüoption	Beschreibung
Strenges TCP	<p>Eine TCP-Verbindung beginnt mit einem Dreizeige-Handshake (SYN, SYN-ACK, ACK) und endet in der Regel mit einem Zweizeige-Austausch (FIN, ACK). Unter bestimmten Umständen sieht die Firewall den Dreizeige-Handshake für einen bestimmten Flow möglicherweise nicht (z. B. aufgrund von asymmetrischem Datenverkehr). Standardmäßig erzwingt die Firewall nicht die Notwendigkeit, einen Dreizeige-Handshake zu sehen, und nimmt bereits bestehende Sitzungen auf. „Strenges TCP“ kann pro Abschnitt aktiviert werden, um das Abrufen mitten in der Sitzung zu deaktivieren und die Anforderung für einen Dreizeige-Handshake zu erzwingen.</p> <p>Wenn Sie den Modus „Strenges TCP“ für eine bestimmte Firewallrichtlinie aktivieren und eine standardmäßige Blockregel vom Typ ANY-ANY verwenden, werden Pakete, die die Dreizeige-Handshake-Verbindungsanforderungen nicht erfüllen und die mit einer TCP-basierten Regel in diesem Richtlinienabschnitt übereinstimmen, verworfen. „Streng“ wird nur auf statusbehaftete TCP-Regeln angewendet und auf der Richtlinienzebene der Gatewayfirewall aktiviert. „Strenges TCP“ wird nicht für Pakete erzwungen, die mit einer standardmäßigen ANY-ANY-Zulassung übereinstimmen, wofür kein TCP-Dienst angegeben wurde.</p>
Statusbehaftet	<p>Eine statusbehaftete Firewall überwacht den Zustand der aktiven Verbindungen und verwendet diese Informationen, um zu ermitteln, welche Pakete die Firewall passieren dürfen.</p>
Gesperrt	<p>Die Richtlinie kann gesperrt werden, um zu verhindern, dass mehrere Benutzer Änderungen an denselben Abschnitten vornehmen. Wenn Sie einen Abschnitt sperren, müssen Sie einen Kommentar einfügen.</p>

- 7 Klicken Sie auf **Veröffentlichen**. Mehrere Richtlinien können hinzugefügt und anschließend in einem Arbeitsschritt zusammen veröffentlicht werden.
- Die neue Richtlinie wird auf dem Bildschirm angezeigt.
- 8 Wählen Sie einen Richtlinienabschnitt aus und klicken Sie auf **Regel hinzufügen**.
- 9 Geben Sie einen Namen für die Regel ein.
- 10 Klicken Sie in der Spalte **Quellen** auf das Symbol „Bearbeiten“ und wählen Sie die Quelle der Regel aus. Weitere Informationen hierzu finden Sie unter [Hinzufügen einer Gruppe](#).

- 11 Klicken Sie in der Spalte **Ziele** auf das Symbol „Bearbeiten“ und wählen Sie das Ziel der Regel aus. Wenn nicht definiert, bezieht sich die Regel auf alle Ziele. Weitere Informationen hierzu finden Sie unter [Hinzufügen einer Gruppe](#).
- 12 Klicken Sie in der Spalte **Dienste** auf das Symbol „Bearbeiten“ und wählen Sie Dienste aus. Wenn nicht definiert, bezieht sich die Regel auf alle Dienste.
- 13 In der Spalte **Angewendet auf** wird der Umfang der Durchsetzung pro Regel definiert. Diese Spalte wird hauptsächlich zur Optimierung von Ressourcen auf ESXi- und KVM-Hosts verwendet. Sie können eine zielgerichtete Richtlinie für bestimmte Zonen und Mandanten definieren, ohne die für andere Mandanten und Zonen definierte Richtlinie zu beeinträchtigen. Sie können einen logischen Router (Tier-0 oder Tier-1) oder Schnittstellen auf logischen Routern oder routenbasierte VPN-Sitzungen in dieser Spalte auswählen.
- 14 Wählen Sie eine Aktion in der Spalte **Aktion** aus.

Option	Beschreibung
<b>Zulassen</b>	Ermöglicht dem gesamten Datenverkehr mit der angegebenen Quelle, dem angegebenen Ziel und Protokoll das Passieren des aktuellen Firewallkontexts. Pakete, die der Regel genügen und akzeptiert werden, durchlaufen das System wie beim Fehlen einer Firewall.
<b>Verwerfen</b>	Verwirft Pakete mit der angegebenen Quelle, dem angegebenen Ziel und Protokoll. Das Verwerfen eines Pakets erfolgt im Hintergrund ohne Benachrichtigung der Quell- oder Zielsysteme. Das Verwerfen des Pakets führt dazu, dass erneut versucht wird, die Verbindung herzustellen, bis der entsprechende Schwellenwert erreicht wird.

- 15 Mit einem Klick auf den Schalter „Status“ können Sie die Regel aktivieren bzw. deaktivieren.
- 16 Klicken Sie auf das Zahnradsymbol, um Protokollierung, Richtung, IP-Protokoll, Tag und Hinweise festzulegen.

Option	Beschreibung
<b>Protokollierung</b>	Die Protokollierung lässt sich deaktivieren/aktivieren. Die Protokolle werden in der Datei „/var/log/dfwptlogs.log“ auf ESXi- und KVM-Hosts gespeichert.
<b>Richtung</b>	Die Optionen sind <b>Ein</b> , <b>Aus</b> und <b>Ein/Aus</b> . Die Standardeinstellung ist <b>Ein/Aus</b> . Dieses Feld bezieht sich auf die Richtung des Datenverkehrs aus der Sicht des Zielobjekts. <b>Ein</b> bedeutet, dass nur Datenverkehr an das Objekt überprüft wird, <b>Aus</b> bedeutet, dass nur Datenverkehr aus dem Objekt überprüft wird, und <b>Ein/Aus</b> bedeutet, dass Datenverkehr in beide Richtungen überprüft wird.
<b>IP-Protokoll</b>	Die Optionen sind <b>IPv4</b> , <b>IPv6</b> und <b>IPv4_IPv6</b> . Die Standardeinstellung ist <b>IPv4_IPv6</b> .
<b>Tags</b>	Tags, die der Regel hinzugefügt wurden.

**Hinweis** Klicken Sie auf das Diagrammsymbol, um die Datenstromstatistik der Firewallregel anzuzeigen. Sie können Informationen anzeigen, wie z. B. die Byte- und Paketanzahl sowie Sitzungen.

- 17 Klicken Sie auf **Veröffentlichen**. Mehrere Regeln können hinzugefügt und in einem Arbeitsschritt zusammen veröffentlicht werden.

## Konfigurieren der Netzwerk-Introspektion (Ost-West)

Nachdem Partner Netzwerkdienste, wie z. B. IDS (Intrusion Detection System) oder IPS (Intrusion Protection System), mit NSX-T Data Center registriert haben, können Sie als Administrator Netzwerkdienste konfigurieren, um Ost-West-Datenverkehr zwischen VMs in einem lokalen Datencenter zu überprüfen.

## Allgemeine Aufgaben für die Ost-West-Netzwerksicherheit

Führen Sie die folgenden Schritte aus, um die Netzwerksicherheit für den Ost-West-Datenverkehr einzurichten.

Tabelle 10-4. Liste der Aufgaben zum Konfigurieren der Ost-West-Netzwerk-Introspektion

Workflow-Aufgaben	Persona	Implementierung
Registrieren des Diensts	Partner	Nur API
Registrieren der Anbietervorlage	Partner	Nur API
Registrieren des Service Managers	Partner	Nur API
<a href="#">Bereitstellen eines Diensts für die Selbstprüfung von Ost-West-Datenverkehr</a>	Administrator	API und NSX Manager-Benutzeroberfläche
<a href="#">Hinzufügen eines Dienstprofils</a>	Administrator	API und NSX Manager-Benutzeroberfläche
<a href="#">Hinzufügen einer Dienstkette</a>	Administrator	API und NSX Manager-Benutzeroberfläche
<a href="#">Hinzufügen von Umleitungsregeln für Ost-West-Datenverkehr</a>	Administrator	API und NSX Manager-Benutzeroberfläche

## Wichtige Konzepte des Netzwerkschutzes (Ost-West)

Datenverkehr zwischen Gast-VMs in einem lokalen Datencenter wird von Drittanbieterdiensten geschützt, die von Partnern bereitgestellt werden. Es gibt einige Konzepte, die Ihnen dabei helfen, den Workflow zu verstehen.

- **Dienst:** Partner registrieren Dienste mit NSX-T Data Center. Ein Dienst stellt die vom Partner angebotene Sicherheitsfunktionalität dar. Zu den Details der Dienstbereitstellung gehören beispielsweise OVF-URL von Dienst-VMs, Punkt zum Anhängen des Diensts, Status des Diensts.

- **Anbietervorlage:** Sie enthält Funktionen, die ein Dienst für Netzwerkdatenverkehr durchführen kann. Partner definieren Anbietervorlagen. Eine Anbietervorlage kann beispielsweise einen Netzwerkvorgangsdienst bereitstellen, wie z. B. Tunneling mit dem IPSec-Dienst.
- **Dienstprofil:** Hierbei handelt es sich um eine Instanz einer Anbietervorlage. Ein NSX-T Data Center-Administrator kann ein Dienstprofil erstellen, das von Dienst-VMs verwendet wird.
- **Gast-VM:** Quelle oder Ziel des Datenverkehrs im Netzwerk. Der eingehende oder ausgehende Datenverkehr wird von einer Dienstkette geprüft, die für eine Regel definiert ist, die Ost-West-Netzwerkdienste ausführt.
- **Dienst-VM:** Eine VM, die die von einem Dienst angegebene OVA- oder OVF-Appliance ausführt. Sie ist über die Dienstebene verbunden, um umgeleiteten Datenverkehr zu empfangen.
- **Dienstinstanz:** Wird erstellt, wenn ein Dienst auf einem Host bereitgestellt wird. Jede Dienstinstanz verfügt über eine entsprechende Dienst-VM.
- **Dienstsegment:** Ein Segment einer Dienstebene, die mit einer Transportzone verknüpft ist. Jeder Dienstanhang wird von anderen Dienstanhängen und von den regulären L2- oder L3-Netzwerksegmenten getrennt, die von NSX-T bereitgestellt werden. Die Dienstebene verwaltet Dienstanhänge.
- **Service Manager:** Ist der Partner Service Manager, der auf einen Satz von Diensten verweist.
- **Dienstkette:** Ist eine logische Abfolge von Dienstprofilen, die vom Administrator definiert werden. Dienstprofile überprüfen Netzwerkdatenverkehr gemäß der in der Dienstkette angegebenen Reihenfolge. Das erste Dienstprofil ist beispielsweise „Firewall“, das zweite Dienstprofil ist „Überwachung“ usw. Dienstketten können verschiedene Dienstprofilabfolgen für unterschiedliche Richtungen des Datenverkehrs (Egress/Ingress) angeben.
- **Umleitungsrichtlinie:** Stellt sicher, dass für eine bestimmte Dienstkette klassifizierter Datenverkehr an diese Dienstkette umgeleitet wird. Sie basiert auf Datenverkehrsmustern, die der NSX-T Data Center-Sicherheitsgruppe und einer Dienstkette entsprechen. Der gesamte dem Muster entsprechende Datenverkehr wird entlang der Dienstkette umgeleitet.
- **Dienstpfad:** Ist eine Abfolge von Dienst-VMs, die die Dienstprofile einer Dienstkette implementieren. Ein Administrator definiert die Dienstkette, die aus einer vordefinierten Reihenfolge von Dienstprofilen besteht. NSX-T Data Center erzeugt basierend auf der Anzahl und den Speicherorten der Gast- und Dienst-VMs mehrere Dienstpfade anhand einer Dienstkette. Ausgewählt wird der optimale Dienstpfad für den zu prüfenden Datenverkehr. Jeder Dienstpfad wird durch einen Dienstpfadindex (Service Path Index, SPI) angegeben und jeder Hop entlang eines Pfads weist einen eindeutigen Dienstindex (Service Index, SI) auf.

## Bereitstellen eines Diensts für die Selbstprüfung von Ost-West-Datenverkehr

Nachdem Partner Dienste registriert haben, müssen Sie als Administrator eine Instanz des Diensts auf Mitgliederhosts eines Clusters bereitstellen.



Stellen Sie VMs des Partnerdiensts, auf denen die Sicherheits-Engine des Partners ausgeführt wird, auf allen NSX-T Data Center-Hosts in einem Cluster bereit. Nach dem Bereitstellen der SVMs können Sie Richtlinienregeln erstellen, die von SVM zum Schutz der Gast-VMs verwendet werden.

### Voraussetzungen

- Alle Hosts werden von einem vCenter Server verwaltet.
- Partnerdienste werden mit NSX-T Data Center registriert und können bereitgestellt werden.
- NSX-T Data Center-Administratoren können auf Partnerdienste und Anbietervorlagen zugreifen.
- Sowohl die Dienst-VM als auch der Partner Service Manager (Konsole) müssen auf der Ebene des Verwaltungsnetzwerks miteinander kommunizieren können.

### 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 > Dienstbereitstellungen > Bereitstellung > Dienst bereitstellen** aus.
- 3 Wählen Sie im Feld „Partnerdienst“ den Partnerdienst aus.
- 4 Geben Sie den Namen der Dienstbereitstellung ein.
- 5 Wählen Sie im Feld „Berechnungsmanager“ die Computing-Ressource auf dem vCenter Server aus, auf dem der Dienst bereitgestellt werden soll.
- 6 Wählen Sie im Feld „Cluster“ den Cluster aus, auf dem die Dienste bereitgestellt werden müssen.
- 7 Wählen Sie im Dropdown-Menü „Datenspeicher“ einen Datenspeicher als Repository für die Dienst-VM aus.
- 8 Klicken Sie in der Spalte „Netzwerk“ auf **Festlegen** und geben Sie die Schnittstelle des Verwaltungsnetzwerks ein, indem Sie den DHCP- oder statischen IP-Adresstyp, das Steuerungs- und Datennetzwerk auswählen.
- 9 Wählen Sie im Feld „Dienstsegmente“ ein Dienstsegment in der Liste aus oder klicken Sie auf das Symbol „Aktion“, um ein Dienstsegment hinzuzufügen oder zu bearbeiten. Ein Dienstsegment bestimmt die mit einer Overlay-Transportzone verknüpften Gast-VMs, denen Schutz für Ost-West-Netzwerkdatenverkehr bereitgestellt werden soll.
- 10 Wählen Sie im Feld „Bereitstellungsspezifikation“ den Dienst und den Formfaktor der Dienst-VM aus, die auf Clusterhosts bereitgestellt werden soll. Mehrere Dienste können für die Bereitstellung zur Verfügung stehen.
- 11 Wählen Sie im Feld „Bereitstellungsvorlage“ die Anbietervorlage mit Attributen zum Schutz der Arbeitslast aus, die in Gast-VM-Gruppen ausgeführt werden soll.

**12** Geben Sie unter „Anzahl der geclusterten Bereitstellung“ die Anzahl der Dienst-VMs ein, die auf dem Cluster bereitgestellt werden sollen. Der vCenter Server entscheidet, auf welchem Host die Dienst-VMs bereitgestellt werden.

**13** Klicken Sie auf **Speichern**.

#### Ergebnisse

Nach der Dienstbereitstellung wird der Partner Service Manager über das Update informiert.

#### Nächste Schritte

Informieren Sie sich über die Bereitstellungsdetails und den Systemzustand von Dienstinstanzen, die auf den Hosts bereitgestellt werden. Siehe [Anzeigen von Details der Dienstinstanz](#).

## Hinzufügen eines Dienstprofils

Ein Dienstprofil ist eine Instanz einer Partneranbietervorlage. Administratoren können die Attribute einer Anbietervorlage zum Erstellen einer Instanz der Vorlage anpassen.

#### Verfahren

- 1** Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2** Navigieren Sie zu **Sicherheit > Horizontale Sicherheit > Netzwerk-Introspektion > Dienstprofile**.
- 3** Wählen Sie im Dropdown-Feld „Partnerdienst“ einen Dienst aus. Sie können ein Dienstprofil für den ausgewählten Dienst erstellen.
- 4** Geben Sie den Namen des Dienstprofils ein und wählen Sie die Anbietervorlage aus.
- 5** Klicken Sie auf **Speichern**.

#### Ergebnisse

Für den Partnerdienst wird ein neues Dienstprofil erstellt.

#### Nächste Schritte

Fügen Sie eine Dienstkette hinzu. Siehe [Hinzufügen einer Dienstkette](#).

## Hinzufügen einer Dienstkette

Eine Dienstkette ist eine logische Abfolge von Dienstprofilen, die vom Netzwerkadministrator definiert werden.

#### Verfahren

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

- 2 Wählen Sie **Sicherheit > Horizontale Sicherheit > Netzwerk-Introspektion > Dienstkette > Kette hinzufügen** aus.
- 3 Geben Sie den Namen der Dienstkette ein.
- 4 Wählen Sie im Feld „Dienstsegmente“ das Dienstsegment aus, auf das die Dienstkette angewendet werden soll. Bei einem Dienstsegment handelt es sich um ein Segment der Dienstebene, das mehrere Dienst-VMs einer Overlay-Transportzone verbindet. Jede Dienst-VM in der Dienstkette ist von anderen Dienst-VMs und L2- und L3-Netzwerksegmenten getrennt, die von NSX-T Data Center ausgeführt werden. Die Dienstebene steuert den Zugriff auf Dienst-VMs.
- 5 Klicken Sie zum Festlegen des Weiterleitungspfads auf das Feld **Weiterleitungspfad festlegen** und dann auf **Profil nacheinander hinzufügen**.
- 6 Fügen Sie das erste Profil in der Dienstkette hinzu und klicken Sie auf **Hinzufügen**.
- 7 Klicken Sie zur Angabe des nächsten Dienstprofils auf **Profil nacheinander hinzufügen** und geben Sie Details ein. Sie können die Reihenfolge der Profile auch mithilfe der nach oben und nach unten weisenden Pfeile neu anordnen.
- 8 Klicken Sie auf **Speichern**, um das Hinzufügen eines Weiterleitungspfads für die Dienstkette abzuschließen.
- 9 Wählen Sie in der Spalte „Reverse Path“ die Option **Weiterleitungspfad umkehren** aus, um den Weiterleitungspfad auf der Dienstebene in umgekehrter Reihenfolge zu verwenden. Klicken Sie zum Festlegen eines neuen Reverse Path auf **Reverse Path festlegen** und fügen Sie einen neuen Reverse Path hinzu.
- 10 Klicken Sie auf **Speichern**, um das Hinzufügen eines Reverse Path für die Dienstkette abzuschließen.
- 11 Wählen Sie im Feld „Fehlerrichtlinie“
  - die Option **Zulassen** aus, um bei einem Ausfall der Dienst-VM Datenverkehr an die Ziel-VM zu senden. Der Ausfall der Dienst-VM wird vom Mechanismus zur Aktivitätserkennung erkannt, der nur von Partnern aktiviert werden kann.
  - Wählen Sie **Blockieren** aus, um bei einem Ausfall der Dienst-VM keinen Datenverkehr an die Ziel-VM zu senden.
- 12 Klicken Sie auf **Speichern**.

## Ergebnisse

Nach dem Hinzufügen einer Dienstkette wird der Partner Service Manager über das Update informiert.

## Nächste Schritte

Erstellen Sie eine Umleitungsregel, um eine Selbstprüfung des Ost-West-Netzwerkdatenverkehrs durchzuführen. Siehe [Hinzufügen von Umleitungsregeln für Ost-West-Datenverkehr](#).

## Hinzufügen von Umleitungsregeln für Ost-West-Datenverkehr

Fügen Sie Regeln hinzu, um Ost-West-Datenverkehr an die Netzwerkselbstprüfung umzuleiten.

Regeln werden in einer Richtlinie definiert. Richtlinien als Konzept ähneln dem Konzept der Abschnitte in Firewalls. Wenn Sie eine Richtlinie hinzufügen, wählen Sie die Dienstkette aus, um den Datenverkehr für die Introspektion nach den Dienstprofilen der Dienstkette umzuleiten.

Eine Regeldefinition besteht aus der Quelle und dem Ziel des Datenverkehrs, einem Selbstprüfungsdienst, dem NSX-Objekt, auf das die Regel angewendet werden soll, und einer Richtlinie zum Umleiten von Datenverkehr. Nach dem Veröffentlichen der Regel löst NSX Manager die Regel aus, wenn ein passendes Datenverkehrsmuster gefunden wird. Die Regel beginnt mit der Selbstprüfung des Datenverkehrs. Beispiel: Wenn NSX Manager einen Datenverkehrsfluss klassifiziert, für den eine Selbstprüfung durchgeführt werden muss, erfolgt keine Umleitung an die reguläre verteilte Firewall. Stattdessen wird dieser Datenverkehr entlang der angegebenen Dienstkette in der Richtlinie umgeleitet. Die in der Dienstkette definierten Dienstprofile führen eine Selbstprüfung des Datenverkehrs für vom Partner angebotene Netzwerkdienste durch. Wenn ein Dienstprofil die Selbstprüfung ohne Erkennung von Sicherheitsproblemen im Datenverkehr abschließt, wird der Datenverkehr zum nächsten Dienstprofil in der Dienstkette weitergeleitet. Am Ende der Dienstkette wird der Datenverkehr an das Ziel weitergeleitet.

Alle Benachrichtigungen werden an den Partner Service Manager und NSX-T Data Center gesendet.

### Voraussetzungen

Zum Umleiten des Datenverkehrs für eine Netzwerkselbstprüfung steht eine Dienstkette zur Verfügung.

### Verfahren

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

- 2 **Sicherheit > Horizontale Sicherheit > Netzwerk-Introspektion > Regeln > Richtlinie hinzufügen.**


Ein Richtlinienabschnitt gleicht einem Firewallabschnitt, in dem Regeln definiert werden, die die Flussrichtung des Datenverkehrs bestimmen.

- 3 (Optional) Klicken Sie auf die Standarddomäne, um eine andere Domäne auszuwählen.

Beachten Sie, dass das Domänenobjekt eine experimentelle Funktion in NSX-T Data Center 2.4 ist, aber in NSX-T Data Center 2.4.1 nicht verfügbar ist.

- 4 Wählen Sie eine Dienstkette aus.

- 5 Klicken Sie zum Hinzufügen einer Richtlinie auf **Veröffentlichen**.

- 6 Klicken Sie auf die vertikalen Auslassungspunkte  in einem Abschnitt und dann auf **Regel hinzufügen**.

- 7 Bearbeiten Sie das Feld **Quelle**, um eine Gruppe hinzuzufügen, indem Sie Mitgliedschaftskriterien, statische Mitglieder, IP-/MAC-Adressen oder Active Directory-Gruppen festlegen. Mitgliedschaftskriterien können anhand eines der folgenden Typen definiert werden: virtuelle Maschine, logischer Switch, logischer Port, IP Set. Sie können statische Mitglieder aus einer der folgenden Kategorien auswählen: Gruppe, Segment, Segment-Port, virtuelle Netzwerkschnittstelle oder virtuelle Maschine.
- 8 Klicken Sie auf **Speichern**.
- 9 Bearbeiten Sie zum Hinzufügen einer Zielgruppe das Feld **Ziel**.
- 10 Im Feld „Angewendet auf“ können Sie einen der folgenden Schritte ausführen:
  - Wählen Sie **DFW** aus, um die Regel auf alle virtuellen Netzwerkkarten anzuwenden, die an den logischen Switch angehängt sind.
  - Wählen Sie **VM-Gruppen** aus, um die Regel auf virtuelle Netzwerkkarten von Mitglieds-VMs der Gruppe anzuwenden. Mitglieder können aus einer statischen Liste oder basierend auf dynamischen Kriterien ausgewählt werden. Zu den unterstützten NSX-T Data Center-Objekten gehören: virtuelle Maschine, logischer Switch, logischer Port, IP Set usw.
- 11 Wählen Sie im Feld „Aktion“ die Option **Umleiten** aus, um Datenverkehr entlang der Dienstkette umzuleiten, oder die Option **Nicht umleiten**, um keine Netzwerkselbstprüfung auf den Datenverkehr anzuwenden.
- 12 Klicken Sie auf **Veröffentlichen**.
- 13 Klicken Sie zum Wiederherstellen einer veröffentlichten Regel auf **Wiederherstellen**.
- 14 Klicken Sie zum Hinzufügen einer Richtlinie auf **+ Richtlinie hinzufügen**.
- 15 Wählen Sie eine zu klonende Richtlinie oder Regel aus und klicken Sie auf **Klonen**.
- 16 Verwenden Sie zum Aktivieren einer Regel das Symbol „Aktivieren/Deaktivieren“ oder wählen Sie die Regel aus und klicken Sie im Menü auf **Aktivieren > Regel aktivieren**.
- 17 Nach dem Aktivieren bzw. Deaktivieren einer Regel klicken Sie auf **Veröffentlichen**, um die Regel durchzusetzen.

## Ergebnisse

Datenverkehr zur Quelle wird zum Zweck der Netzwerkselbstprüfung an die Dienstkette umgeleitet. Nachdem Dienstprofile in der Kette eine Selbstprüfung des Datenverkehrs vorgenommen haben, wird der Datenverkehr an das Ziel übermittelt.

Während der Bereitstellung ist es möglich, dass sich die Mitgliedschaft der VM-Gruppe für eine bestimmte Richtlinie ändert. NSX-T Data Center informiert den Partner Service Manager über diese Updates.

## Konfigurieren der Netzwerk-Introspektion (Nord-Süd)

Nachdem Partner Netzwerkdienste mit NSX-T Data Center registriert haben, können Sie als Administrator Netzwerkdienste konfigurieren, um Nord-Süd-Datenverkehr zwischen VMs in einem Datacenter und dem externen Netzwerk zu überprüfen.

### Allgemeine Aufgaben für die Nord-Süd-Netzwerksicherheit

Führen Sie die folgenden Schritte aus, um die Netzwerksicherheit für den Nord-Süd-Datenverkehr einzurichten.

Tabelle 10-5. Liste der Aufgaben zum Konfigurieren der Nord-Süd-Netzwerk-Introspektion

Workflow-Aufgaben	Persona	Implementierung
Registrieren des Diensts mit NSX-T Data Center	Partner	Nur API
<a href="#">Bereitstellen eines Diensts für die Selbstprüfung von Nord-Süd-Datenverkehr</a>	Administrator	API und NSX Manager-Benutzeroberfläche
<a href="#">Konfigurieren der Umleitung des Datenverkehrs</a>	Administrator	API und NSX Manager-Benutzeroberfläche

### Bereitstellen eines Diensts für die Selbstprüfung von Nord-Süd-Datenverkehr

Nachdem Sie einen Dienst registriert haben, müssen Sie eine Instanz des Diensts bereitstellen, damit der Dienst mit der Verarbeitung des Netzwerkdatenverkehrs beginnen kann.

Stellen Sie die Partnerdienst-VM auf dem logischen Tier-0- oder Tier-1-Router bereit, der als Gateway zwischen der physischen Welt und dem logischen Netzwerk auf dem vCenter Server fungiert. Nach der Bereitstellung der SVM als eigenständige oder Aktiv/Standby-Dienstinstanz können Sie Umleitungsregeln erstellen, um Datenverkehr zur Netzwerkselfprüfung an die SVM umzuleiten.

#### Voraussetzungen

- Alle Hosts werden von einem vCenter Server verwaltet.
- Partnerdienste werden mit NSX-T Data Center registriert und können bereitgestellt werden.
- NSX-T Data Center-Administratoren können auf Partnerdienste und Anbietervorlagen zugreifen.

Stellen Sie sicher, dass der Hochverfügbarkeitsmodus für den logischen Router auf „Aktiv/Standby“ gesetzt ist.

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Partnerdienste > Dienstinstanzen > Katalog** aus.
- 3 Auf der Registerkarte „Katalog“ werden die registrierten Dienste angezeigt.
- 4 Wählen Sie den im OVF-Formfaktor angezeigten Dienst aus und klicken Sie auf **Bereitstellen**, um mit der Bereitstellung der Dienstinstanz zu beginnen.
- 5 Klicken Sie im Fenster „Einfügung des Partnerdiensts“ auf **Fortfahren**.
- 6 Geben Sie im Fenster „Partnerdienst“ die Details ein.

Tabelle 10-6. Details des Partnerdiensts

Feld	Beschreibung
Instanzname	Geben Sie einen Namen ein, um die Dienstinstanz zu identifizieren.
Beschreibung	Beschreibung der Dienstinstanz.
Partnerdienst	Wählen Sie den mit NSX-T Data Center registrierten Partnerdienst aus.
Bereitstellungsspezifikation	Wählen Sie den bereitzustellenden Formfaktor aus.
Logischer Router	Wählen Sie den logischen Tier-0-Router aus, auf dem die Dienstinstanz bereitgestellt werden muss.

- 7 Klicken Sie auf **Weiter**.
- 8 Geben Sie im Fenster „Instanzkonfiguration“ die Details ein.

Tabelle 10-7. Details der Dienstinstanz

Feld	Beschreibung
Bereitstellungsmodus	Wählen Sie <b>Eigenständig</b> aus, um eine einzelne Dienstinstanz auf dem logischen Tier-0-Router bereitzustellen.  Wählen Sie <b>Hochverfügbarkeit</b> aus, um mehrere Dienstinstanzen im Modus „Aktiv/Standby“ auf dem logischen Tier-0-Router bereitzustellen.
Fehlerrichtlinie	Wählen Sie <b>Zulassen</b> oder <b>Blockieren</b> aus.
IP-Adresse der Dienstinstanz	Geben Sie die von der Dienstinstanz zu verwendende IP-Adresse ein.
Gateway	Geben Sie die Gateway-Adresse ein.
Subnetzmaske	Geben Sie die Subnetzmaske ein.

Tabelle 10-7. Details der Dienstinstanz (Fortsetzung)

Feld	Beschreibung
Netzwerk-ID	Geben Sie die Netzwerk-ID des logischen Switches ein, auf dem Sie das Verwaltungsnetzwerk verbinden möchten.
Berechnungsmanager	Wählen Sie den registrierten vCenter Server aus.
Ressourcenpool	Wählen Sie den Ressourcenpool aus, der Ressourcen zum Bereitstellen der Dienstinstanz zur Verfügung stellt.
Datenspeicher	Wählen Sie das Repository aus, in dem die Daten der Dienstinstanz gespeichert werden sollen.

9 Klicken Sie auf **Weiter**.

10 Geben Sie im Fenster „Erweiterte Konfiguration“ die Details ein.

Tabelle 10-8.

Feld	Beschreibung
Bereitstellungsvorlage	Wählen Sie die während der Bereitstellung der Dienstinstanz zu verwendende Vorlage aus.
Lizenz	Geben Sie die Lizenz der Vorlage ein.

11 Klicken Sie auf **Fertigstellen**.

### Ergebnisse

Auf der Registerkarte „Dienstinstanzen“ wird der Fortschritt der Bereitstellung angezeigt. Es kann einige Minuten dauern, bis die Bereitstellung abgeschlossen ist. Überprüfen Sie den Status der Bereitstellung, um sicherzustellen, dass die Dienstinstanz erfolgreich auf dem logischen Tier-0-Router bereitgestellt wurde.

Navigieren Sie alternativ zum vCenter Server und überprüfen Sie den Bereitstellungsstatus.

### Nächste Schritte

Konfigurieren Sie Regeln, um Datenverkehr an die Dienstinstanz umzuleiten, die auf dem Tier-0-Router bereitgestellt wird. Siehe [Konfigurieren der Umleitung des Datenverkehrs](#)

## Konfigurieren der Umleitung des Datenverkehrs

Nachdem Sie eine Dienstinstanz bereitgestellt haben, konfigurieren Sie, welchen Datenverkehrstyp der Router zum Dienst umleitet. Das Konfigurieren der Umleitung des Datenverkehrs ist ähnlich wie die Konfiguration einer Firewall.

Weitere Informationen zum Konfigurieren einer Firewall finden Sie unter [Firewallabschnitte und Firewallregeln](#).



## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Partnerdienste > Dienstinstanzen** aus.
- 3 Klicken Sie auf die Dienstinstanz.
- 4 Klicken Sie auf die Registerkarte **Umleitung des Datenverkehrs**.
- 5 Um einen Abschnitt hinzuzufügen, wählen Sie einen vorhandenen Abschnitt aus und klicken Sie auf **Abschnitt hinzufügen**.
  - ◆ Wählen Sie im Menü **Abschnitt oben hinzufügen** oder **Abschnitt unten hinzufügen** aus.

Es wird ein neuer Abschnitt erstellt. Der Datenverkehrstyp, der umgeleitet werden soll, ist auf **L3-Umleitung** festgelegt, der Dienst ist vom Typ **Statusfrei**, das Feld **Angewendet auf** ist mit einem logischen Tier-0 Router verknüpft, der auf dem Host konfiguriert ist. Nachdem Sie Regeln definiert haben, wird das Feld **Regeln** automatisch ausgefüllt.
- 6 Klicken Sie auf **Veröffentlichen**, um die Konfigurationsdetails des Abschnitts beizubehalten.
- 7 Um eine Regel in diesem Abschnitt hinzuzufügen, wählen Sie den Abschnitt aus und klicken Sie auf **Regel hinzufügen**.
- 8 Geben Sie in der Regelzeile die folgenden Details ein:
  - a Geben Sie den Regelnamen ein.
  - b Geben Sie die Quelle und das Ziel des L3-Datenverkehrs ein. Die Partnerdienst-VM überprüft den eingehenden Datenverkehr von der Quelle, bevor dieser an die Ziel-VM weitergeleitet wird.
  - c Wählen Sie im Feld **Angewendet auf** den Uplink des Tier-0-Routers aus.
  - d Wählen Sie im Feld **Aktion** die Option **Umleiten** aus, wenn der Datenverkehr von den Dienst-VMs geprüft werden muss, oder wählen Sie **Nicht umleiten** aus, wenn der Datenverkehr keiner Nord-Süd-Selbstprüfung unterzogen werden muss.
- 9 Jede Regel kann einzeln aktiviert werden. Nachdem Sie eine Regel aktiviert haben, wird sie auf den Datenverkehr angewendet, der mit der Regel übereinstimmt.
- 10 Klicken Sie auf „Erweiterte Einstellungen“, um die Datenverkehrsrichtung zu konfigurieren und die Protokollierung zu aktivieren.
- 11 Klicken Sie am Ende eines Abschnitts mit Regeln auf **Veröffentlichen**, um die Regeln im Abschnitt beizubehalten, oder klicken Sie auf **Wiederherstellen**, um den Vorgang abubrechen.

## Ergebnisse

Der Datenverkehr wird an Regeln zur Netzwerk-Introspektion gesendet, durch die Richtlinienregeln auf den Datenverkehr angewendet werden.

## Nächste Schritte

Siehe [Hinzufügen von Umleitungsregeln für Nord-Süd-Datenverkehr](#).

## Hinzufügen von Umleitungsregeln für Nord-Süd-Datenverkehr


Über die Benutzeroberfläche für **Netzwerk und Sicherheit – Erweitert** können Sie Umleitungsregeln für den Nord-Süd-Datenverkehr einrichten. Die Umleitung des Datenverkehrs erfolgt nur für Dienste, die auf dem Tier-0-Router eingefügt wurden.

Befolgen Sie die Anleitung unter [Konfigurieren der Umleitung des Datenverkehrs](#).

### Voraussetzungen

- Registrieren und stellen Sie Drittanbieterdienste auf NSX-T bereit.
- Konfigurieren Sie den Tier-0-Router.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 **Sicherheit > Nord-Süd-Firewall > Netzwerkselfprüfung (vertikal) > Richtlinie hinzufügen.**  
Ein Richtlinienabschnitt gleicht einem Firewallabschnitt, in dem Regeln definiert werden, die die Flussrichtung des Datenverkehrs bestimmen.
- 3 (Optional) Klicken Sie auf die Standarddomäne, um eine andere Domäne auszuwählen.  
Beachten Sie, dass das Domänenobjekt eine experimentelle Funktion in NSX-T Data Center 2.4 ist, aber in NSX-T Data Center 2.4.1 nicht verfügbar ist.
- 4 Legen Sie für **Umleiten an** die Dienstinstanz fest, die bei NSX-T registriert ist, um eine Netzwerkselfprüfung des Datenverkehrs zwischen Quell- und Zieleinheit durchzuführen.
- 5 Klicken Sie zum Hinzufügen einer Richtlinie auf **Veröffentlichen**.
- 6 Klicken Sie auf die vertikalen Auslassungspunkte  in einem Abschnitt und dann auf **Regel hinzufügen**.
- 7 Bearbeiten Sie das Feld **Quelle**, um eine Gruppe hinzuzufügen, indem Sie Mitgliedschaftskriterien, statische Mitglieder, IP-/MAC-Adressen oder Active Directory-Gruppen festlegen. Mitgliedschaftskriterien können anhand eines der folgenden Typen definiert werden: virtuelle Maschine, logischer Switch, logischer Port, IP Set. Sie können statische Mitglieder aus einer der folgenden Kategorien auswählen: Gruppe, Segment, Segment-Port, virtuelle Netzwerkschnittstelle oder virtuelle Maschine.
- 8 Klicken Sie auf **Speichern**.
- 9 Bearbeiten Sie zum Hinzufügen einer Zielgruppe das Feld **Ziel**.

**10** Im Feld „Angewendet auf“ können Sie einen der folgenden Schritte ausführen:

- Wählen Sie **DFW** aus, um die Regel auf alle virtuellen Netzwerkkarten anzuwenden, die an den logischen Switch angehängt sind.
- Wählen Sie **VM-Gruppen** aus, um die Regel auf virtuelle Netzwerkkarten von Mitglieds-VMs der Gruppe anzuwenden. Mitglieder können aus einer statischen Liste oder basierend auf dynamischen Kriterien ausgewählt werden. Zu den unterstützten NSX-T Data Center-Objekten gehören: virtuelle Maschine, logischer Switch, logischer Port, IP Set usw.

**11** Wählen Sie im Feld „Aktion“ die Option **Umleiten** aus, um den Datenverkehr der Dienstinstanz umzuleiten, oder die Option **Nicht umleiten**, um keine Netzwerkselbstprüfung auf den Datenverkehr anzuwenden.

**12** Klicken Sie auf **Veröffentlichen**.

**13** Klicken Sie zum Wiederherstellen einer veröffentlichten Regel auf **Wiederherstellen**.

**14** Klicken Sie zum Hinzufügen einer Richtlinie auf **+ Richtlinie hinzufügen**.

**15** Wählen Sie eine zu klonende Richtlinie oder Regel aus und klicken Sie auf **Klonen**.

**16** Verwenden Sie zum Aktivieren einer Regel das Symbol „Aktivieren/Deaktivieren“ oder wählen Sie die Regel aus und klicken Sie im Menü auf **Aktivieren > Regel aktivieren**.

**17** Nach dem Aktivieren bzw. Deaktivieren einer Regel klicken Sie auf **Veröffentlichen**, um die Regel durchzusetzen.

## Ergebnisse

Basierend auf den festgelegten Aktionen wird der Nord-Süd-Datenverkehr zur Netzwerkselbstprüfung an die Dienstinstanz umgeleitet.

## Überwachung der Umleitung des Datenverkehrs

Nachdem Sie eine Dienstinstanz bereitgestellt und die Umleitung des Datenverkehrs konfiguriert haben, können Sie überwachen, wie viel Datenverkehr zu der Dienstinstanz hin und aus der Dienstinstanz heraus fließt.

### Verfahren

- 1** Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2** Wählen Sie **Netzwerk und Sicherheit – Erweitert > Partnerdienste > Dienstinstanzen** aus.
- 3** Klicken Sie auf den Namen einer Dienstinstanz.

Auf der Registerkarte **Übersicht** werden die Konfiguration und der Status der Dienstinstanz angezeigt.

**4** Klicken Sie auf die Registerkarte **Statistik**.

Informationen dazu, wie viele Pakete und Daten in die Dienstinstanz und aus ihr heraus fließen, werden angezeigt.

**5** Klicken Sie auf **Aktualisieren**, um die Statistik zu aktualisieren.

## Konfigurieren von Endpoint-Schutz

Wenden Sie Richtlinien für den Endpoint-Schutz auf Gast-VM-Gruppen an, nachdem Partner die zugehörigen Dienste mit NSX-T Data Center registriert haben. Vor dem Konfigurieren von Endpoint-Schutz für Gast-VMs müssen Sie Partnerdienste als Teil des Service Insertion-Workflows bereitstellen.

## Grundlegendes zum Endpoint-Schutz

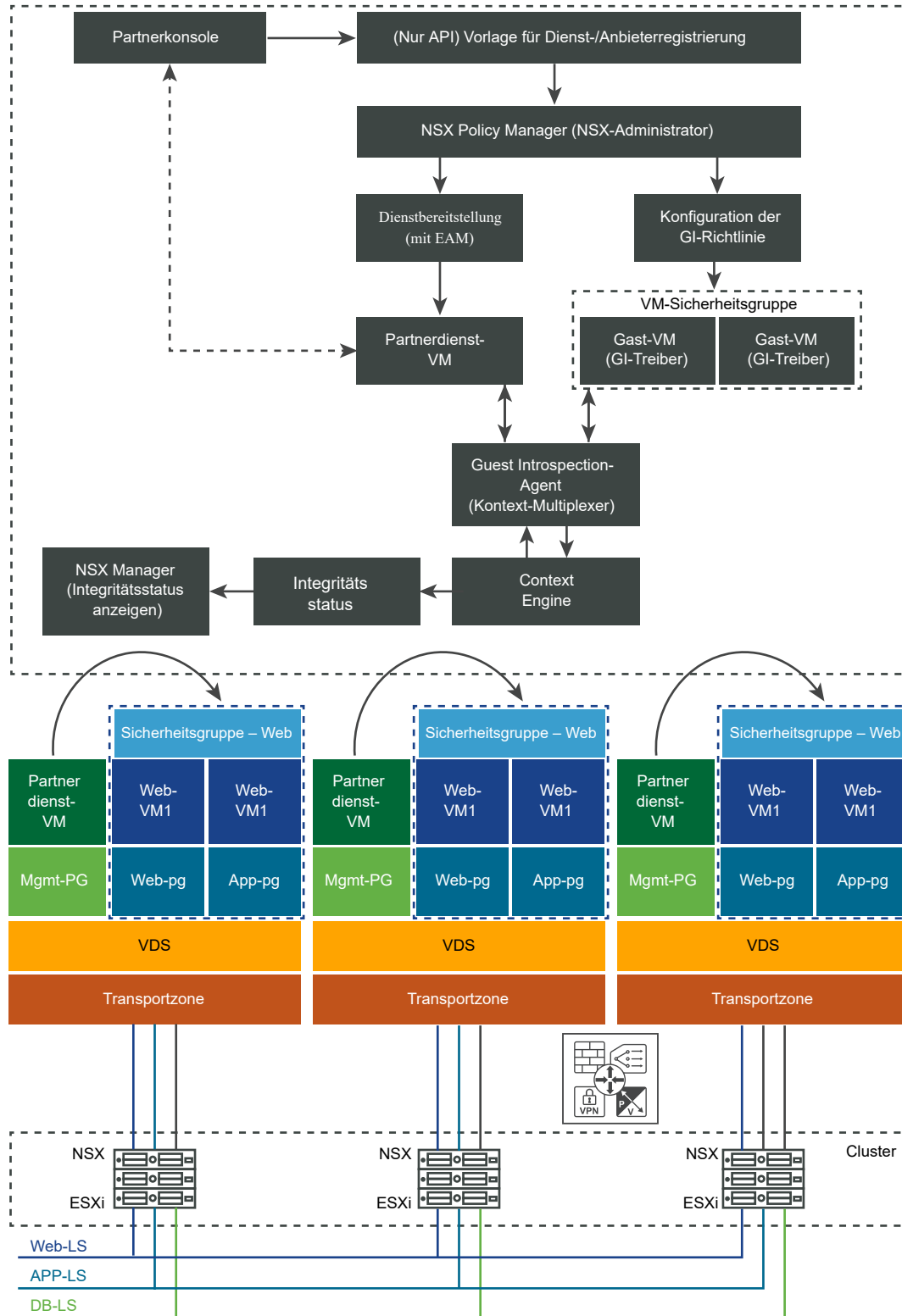
Lernen Sie den Anwendungsfall, den Workflow und die wichtigsten Konzepte des Endpoint-Schutzes kennen.

### Anwendungsfall für Endpoint-Schutz

NSX-T bietet statusbehaftete L2-L4-Firewalldienste für virtuelle Netzwerke. Wenn Ihre Umgebung Sicherheitsdienste zum Schutz vor Malware benötigt, um Gast-VMs zu schützen, bietet NSX eine leistungsstarke Möglichkeit, Gast-VMs zu prüfen, indem Dienste von Drittanbietern in Hosts zum Schutz vor Malware integriert werden.

Während der Vorbereitung des Hostknotens installiert NSX-T den Guest Introspection-Hostagent als Teil der Hostpaketinstallation auf allen Hosts eines Clusters. Daher muss der Guest Introspection-Hostagent nicht separat auf einem Hostknoten installiert werden. Die Partnerdienst-VM (SVM) wird als virtuelle Appliance auf einem Hostknoten installiert. Die SVM verwendet die Guest Introspection-API-Bibliothek (EPSec-API-Bibliothek), um Gast-VMs zu prüfen und vor Malware zu schützen.

Abbildung 10-1. Anwendungsfall für Endpoint-Schutz



Als NSX-Administrator implementieren Sie eine Lösung zum Schutz vor Malware, die als Dienst-VM (SVM) bereitgestellt wird, um eine Dateiaktivität auf einer Gast-VM zu überwachen. Wenn auf eine Datei zugegriffen wird, z. B. beim Versuch, eine Datei zu öffnen, wird die Dienst-VM für den Schutz vor Malware über das Ereignis benachrichtigt. Die Dienst-VM ermittelt dann, wie auf das Ereignis reagiert werden soll, z. B. indem die Datei auf Virensignaturen geprüft wird.

- Wenn die Dienst-VM feststellt, dass die Datei keine Viren enthält, lässt sie zu, dass die Datei geöffnet wird.
- Wenn die Dienst-VM einen Virus in der Datei erkennt, versucht sie ihn zu löschen.
  - Gelingt dies, lässt die Dienst-VM zu, dass die Datei geöffnet wird.
  - Kann die Dienst-VM die Datei nicht bereinigen, verhindert sie das Öffnen der Datei und markiert die Datei (und die VM) als infiziert. Darüber hinaus können Sie eine Regel definieren, mit der die VM automatisch in eine Sicherheitsgruppe für infizierte VMs verschoben wird.

---

**Hinweis** Wenn Gast-VMs nicht mit einem ESXi-Hostagent (MUX) oder der SVM verbunden sind oder diese nicht erreichen können, sind Dateizugriffe auf den Gast möglicherweise zulässig, ohne eine Antivirenprüfung durchlaufen zu müssen.

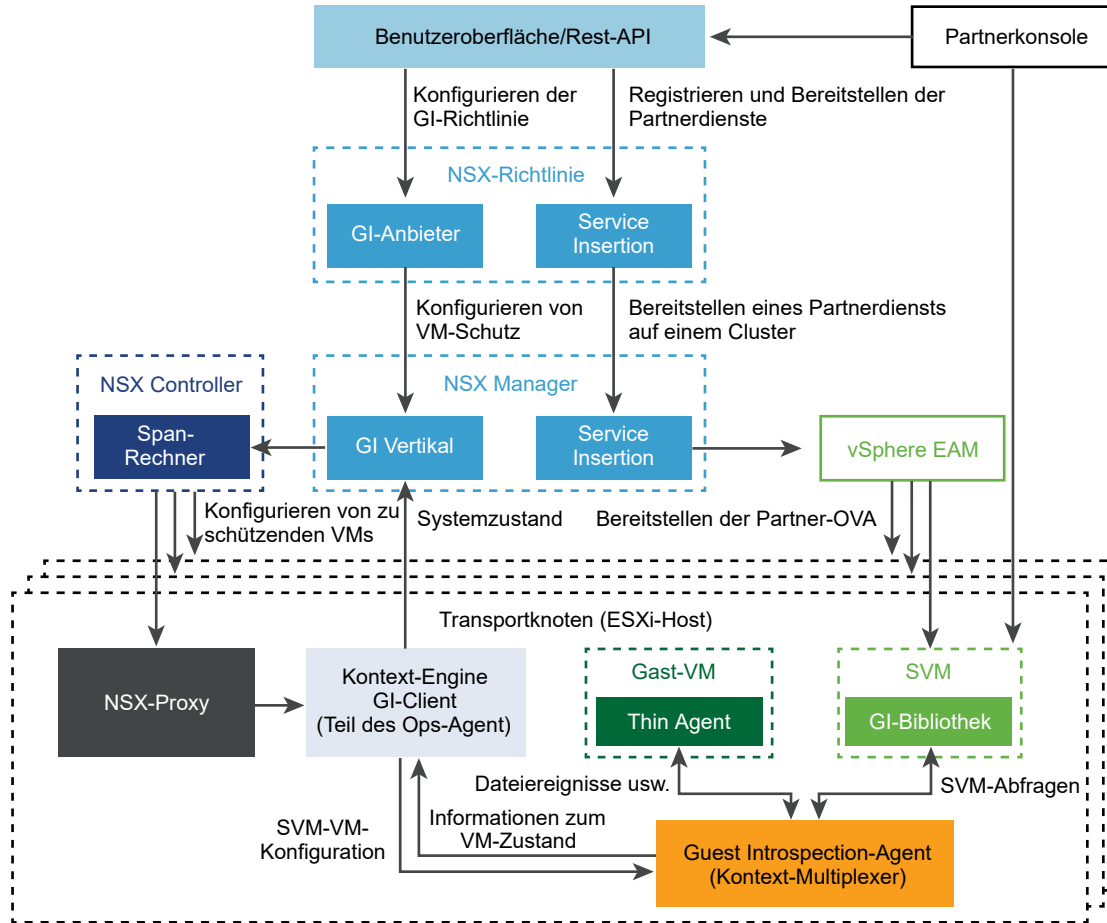
---

Im Gegensatz zu Gast-VMs, die offline geschaltet werden können, läuft eine Dienst-VM dauernd. Daher kann sie die Virensignaturen kontinuierlich aktualisieren, den virtuellen Maschinen auf dem Host einen unterbrechungsfreien Schutz bieten und den sofortigen Schutz für neue VMs gewährleisten, die online geschaltet werden. Da Dienst-VMs mit Guest Introspection befähigt werden, bestimmte Dateien auf Gast-VMs zu lesen und zu schreiben, bieten sie eine effiziente Möglichkeit, um Ressourcenengpässe zu vermeiden und die Arbeitsspeichernutzung zu optimieren.

## Guest Introspection-Architektur

Machen Sie sich mit der Architektur der Service Insertion- und Guest Introspection-Komponenten in NSX-T Data Center vertraut.

Abbildung 10-2. Guest Introspection-Architektur



#### Partnerregistrierung:

- Partner registrieren-Dienste durch Aufrufen der Guest Introspection-REST-API-Bibliothek, die von NSX Manager-APIs bereitgestellt wird.
- Wenn später im Workflow Partnerdienste (SVMs) auf einem Host bereitgestellt werden, registriert sich die Partnerkonsole bei der SVM, um Benachrichtigungen über Wartungsaktivitäten und Ereignisbenachrichtigungen über Guest-VM-Gruppen zu erhalten.

#### Dienstbereitstellung:

- Partnerdienste werden auf einem von NSX vorbereiteten Host mithilfe des Service Insertion-Frameworks bereitgestellt.
- Der vSphere Enterprise Agency Manager (EAM) stellt die VMs des Partnerdienstes auf NSX-T-Hosts bereit.
- Jeder Host des Clusters führt eine Instanz des Dienstes aus, bei der es sich um eine SVM handelt.

#### Installation des Guest Introspection-Treibers:

- Installieren Sie GI-Treiber auf Gast-VMs, bevor Sie die Kommunikation der SVM mit Gast-VMs und anderen Komponenten herstellen.
- Mithilfe von VMTools installiert der Administrator einen Thin Agent auf jeder Gast-VM.
- Thin Agents führen die folgenden Funktionen aus:
  - Sie kommunizieren mit einer Komponente namens Guest Introspection-Agent (MUX) über einen schnellen Kanal, der als Virtual Machine Communication Interface (VMCI) bezeichnet wird.
  - Sie erfassen Dateizugriffsereignisse auf Gast-VMs.
  - Sie benachrichtigen die Partner-SVM über Ereignisse auf Gast-VMs.
  - Sie implementieren die Schutzrichtlinie auf Gast-VMs. Beispiel: Zulassen oder Verweigern eines Dateizugriffs oder Quarantäne einer Datei oder VM.

#### Erstellung von Richtlinien:

Ein Administrator erstellt eine Richtlinie für den Schutz einer VM-Gruppe, indem er die VM-Gruppe Dienstprofilen zuordnet.

- NSX Policy Manager stellt die GI-Richtlinien zusammen und interagiert mit der GI-Komponente (die auf NSX Manager ausgeführt wird).
- Diese GI-Komponente ist verantwortlich für die Konfiguration von GI-Richtlinien für VM-Gruppen und für das Senden dieser Konfiguration an die Steuerungsebene, insbesondere die Komponente CCP-Bereichsberechnung.

#### Die Steuerungsebene verwaltet die VM-Konfiguration:

- Die Steuerungsebene empfängt die Konfiguration für GI-Richtlinien, die auf VM-Gruppen angewendet werden. Sie berechnet den Bereich der Transportknoten, auf denen die VMs aus einer bestimmten Gruppe gehostet werden.
- CCP-Bereichsberechnung: NSX Manager sendet Konfigurationsdetails einer Gruppe – VMs und die zugehörige Richtlinie – an das CCP. Die Bereichsberechnung ermittelt, zu welchen Transportknoten diese VMs gehören. Anschließend sendet sie die VM-ID-Liste zusammen mit der zugehörigen Richtlinie an die Transportknoten, auf denen diese VMs gehostet werden. Die lokale Steuerungskomponente (LCP) empfängt diese Informationen und speichert sie in einer Datenbank auf dem Host.
- Die Context Engine überwacht alle Aktualisierungen der Datenbank und aktualisiert die MUX-Komponente (Guest Introspection-Agent).



Herstellen der Kommunikation zwischen SVM, Gast-VM und Kontext-Multiplexer:

- SVM: Partnerdienste werden auf einer gesonderten Appliance (SVM) auf jedem Host eines Clusters ausgeführt. Partner geben beim Registrieren von Diensten den OVF-Speicherort an, an dem die SVMs bereitgestellt werden sollen. Diese kommunizieren mit den folgenden Komponenten:
  - Eine Gast-VM und der Guest Introspection-Agent kommunizieren über einen schnellen Kanal (VMCI) auf dem ESXi-Hypervisor, während Gast-VM und SVM über einen TCP/IP-Kanal kommunizieren. Der innerhalb einer Gast-VM ausgeführte Thin Agent erfasst Informationen über das Betriebssystem und Dateiaktivitäten. SVMs erfassen den Kontext, der vom Thin Agent über die EPSec-API-Bibliothek bereitgestellt wird. Die GI-Treiber senden Ereignisse an SVMs. Die jeweilige SVM ermittelt, ob es sich bei der Datei um Malware handelt oder ob sie unbedenklich ist. Die SVM liest die EPSec-API-Bibliothek, um eine Aktion aufgrund des erfassten Kontexts zu ermitteln.
  - Sobald SVMs auf jedem Host des Clusters bereitgestellt werden, sendet die Guest Introspection-Komponente in NSX Manager die SVM-Konfiguration an die Context Engine. Die Context Engine aktualisiert den Guest Introspection-Agent mit neuen SVM-Konfigurationsinformationen. Die jeweilige SVM registriert etwaige Ereignisse auf einer VM oder in einer Datei.

Der Guest Introspection-Agent stellt die Kommunikation mit der Guest Introspection-Bibliothek her. Das führt dazu, dass die SVM die Einschaltung einer VM registriert. Die SVM ist jetzt bereit für den Empfang von Dateiereignissen vom Thin Agent.

- Guest Introspection-Agent: Es ist das Guest Introspection-Hostmodul (Kontext-Multiplexer), das Nachrichten von allen geschützten Gast-VMs multiplexiert und an die SVM weiterleitet. Es wird als vSphere Installation Bundle (VIB) auf NSX-T-Hosts installiert. Der NSX Manager installiert und konfiguriert dieses Modul auf dem ESX-Host. Die Konfigurationsdatei des Guest Introspection-Agent (`/var/run/muxconfig.xml`) auf dem Host gibt Konfigurationsinformationen zur Partnerlösung an. Die `VMConfig`-Datei listet geschützte VMs und die entsprechende Lösung auf. Die `SolutionConfig`-Datei enthält eine Liste der SVM-Details wie Lösungs-ID, IP-Adresse, Listener-Port und UUID.

Funktion der Context Engine:

- Context Engine: Diese Komponente sendet Konfigurationsdetails der SVM, die VMs zugeordnet ist, an den Guest Introspection-Agent. Nach dem Empfang der Konfigurationsdetails zeichnet der Guest Introspection-Agent Aktualisierungen der SVM-Konfiguration in der `muxconfig.xml`-Datei auf. Die Konfigurationsinformationen enthalten außerdem das Dienstprofil-Tag für die SVM, um die Richtlinie abzufragen und zu identifizieren. Während der Prüfung leitet der Guest Introspection-Agent Ereignisse nur von VMs weiter, die dieser SVM zugeordnet sind. Diese Komponente ist dafür zuständig, den Integritätsstatus von Thin Agent und Guest Introspection-Agent an die GI Vertical-Komponente in NSX Manager zu senden.
- Integritätsstatus: Die GI-Komponente (die auf NSX Manager ausgeführt wird) fordert regelmäßig Integritätsinformationen von der Context Engine an.

- Die Context Engine erfasst vom Guest Introspection-Agent Informationen zum Integritätsstatus und sendet sie an die GI-Komponente (die auf NSX Manager ausgeführt wird). Der Integritätsstatus wird durch folgende Faktoren bestimmt: Status der Partnerlösung, Konnektivität zwischen Guest Introspection-Agent (Context Multiplexer) und Context Engine (Ops Agent) sowie Verfügbarkeit von Guest Introspection-Agent-Informationen, SVM-Protokollinformationen bei NSX Manager.

## Wichtige Konzepte des Endpoint-Schutzes

Gast-VMs werden vor Malware geschützt. Der Endpoint-Schutz-Workflow benötigt Partner, die ihre Dienste mit NSX-T Data Center registrieren, und einen Administrator, der diese Dienste nutzt. Es gibt einige Konzepte, die Ihnen dabei helfen, den Workflow zu verstehen.

- **Dienstdefinition:** Partner definieren Dienste mit folgenden Attributen: Name, Beschreibung, unterstützte Formfaktoren, Bereitstellungsattribute, wie z. B. Speicher, Netzwerkspeicher.
- **Diensteinfügung:** NSX bietet ein Framework, das es Partnern ermöglicht, die Dienstdefinitions-API zum Registrieren ihrer Dienste mit NSX-T zu verwenden. Die Diensteinfügung wird zum Bereitstellen von Partnerdiensten auf Hosts verwendet, die Guest Introspection gegen Malware durchführen.
- **Span-Rechner:** Die Steuerungskomponente ermittelt für eine zu schützende VM-Gruppe die Transportknoten, die die VMs dieser Gruppe hosten. Eine VM-Gruppe enthält möglicherweise VMs, die auf verschiedenen Transportknoten gehostet werden. Die Steuerungskomponente berechnet den Bereich der Transportknoten, die diese VMs hosten. Nach der Berechnung des Bereichs überträgt NSX Manager die VM-Konfiguration (eine VM und deren zugehörige Richtlinie) auf alle Transportknoten. Dies ist notwendig, da Transportknoten die mit den VMs verknüpfte Richtlinie kennen müssen. Die Steuerungskomponente überträgt darüber hinaus die Liste der VM-IDs gemeinsam mit der SVM-Richtlinie an die Transportknoten.
- **Dienstprofile und Anbietervorlagen:** Partner registrieren Anbietervorlagen, die Schutzebenen für Richtlinien darstellen. Die Schutzebenen „Gold“, „Silber“ oder „Platin“ stehen zur Verfügung. Anbietervorlagen enthalten unter Umständen auch Bereitstellungsattribute, die partnerspezifisch sind, wie z. B. Name oder Lizenzschlüssel usw. Diese Attribute sind Teil der Dienstdefinition. Diese Attribute ermöglichen einem NSX-Administrator die Anpassung der Anbietervorlage, sodass zahlreiche Dienstprofile anhand einer einzigen Anbietervorlage erstellt werden können. Wenn in der Anbietervorlage keine Bereitstellungsattribute verfügbar sind, kann der Administrator nur ein Dienstprofil anhand der Anbietervorlage erstellen.
- **Guest Introspection-Bibliothek und SVM:** Bei der Guest Introspection-Bibliothek (früher bekannt als EPSec) handelt es sich um eine Bibliothek, die auf der Partner-SVM ausgeführt wird. Sie dient auch als Schnittstelle zwischen der Partner-SVM und dem Guest Introspection Thin Agent.
- **Guest Introspection-Agent (MUX) und SVM:** Diese Komponente ist verantwortlich für die Weiterleitung von Guest Introspection Thin Agent-Ereignissen an die konfigurierten SVMs. Sie leitet auch SVM-Anfragen an den Guest Introspection Thin Agent weiter.

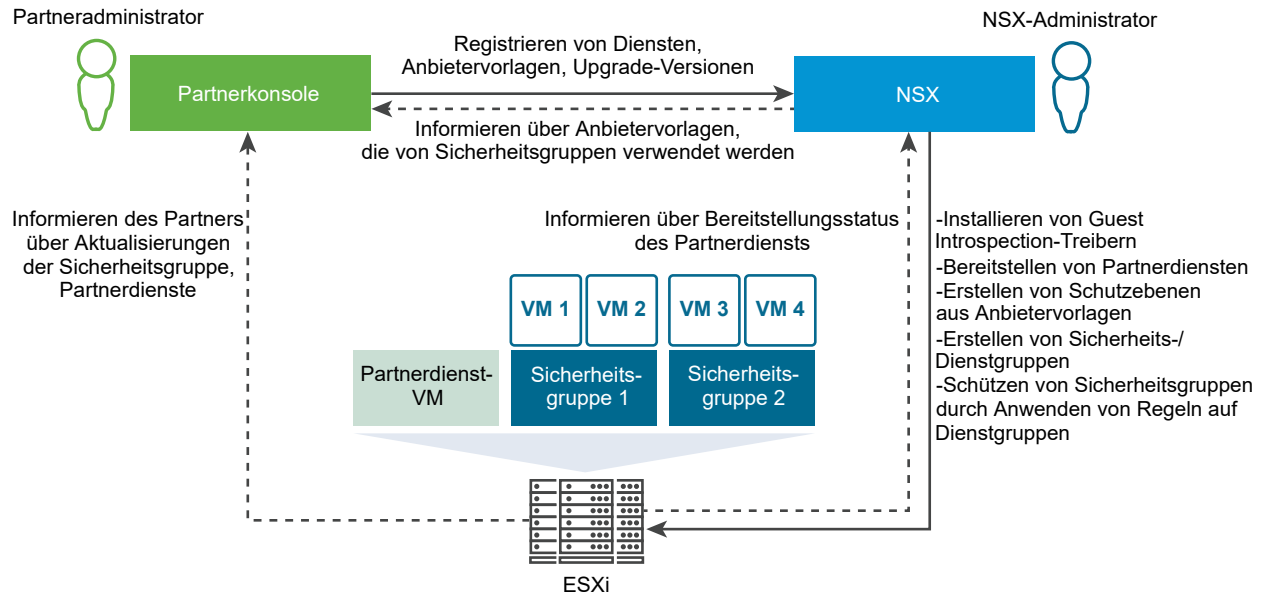
- **GI-Client der Kontext-Engine:** Diese Komponente ist verantwortlich für:
  - Senden des Systemzustands des Thin Agent und des Guest Introspection-Agent (MUX) an die GI-Komponente in NSX Manager.
  - Bereitstellen der NestDb-Konfiguration für den Guest Introspection-Agent (MUX).
- **Systemzustand:** Die Kontext-Engine sendet den Systemzustand der SVM, den VM-Status, den Status des Guest Introspection-Agent und den Status des Guest Introspection-Client an die Guest Introspection (die auf dem NSX Manager ausgeführt wird).
- **Domäne und VM-Gruppen:** Bei einer Domäne handelt es sich um eine Umgebung, die VM-Gruppen und Richtlinienregeln hostet. VM-Gruppen stellen eine Liste der VMs dar, die auf einem einzelnen oder mehreren Transportknoten gehostet werden. Der NSX-Administrator erstellt eine Gruppe von VMs in einer Domäne, bevor Schutzrichtlinien auf diese VM-Gruppe angewendet werden. Eine Domäne kann beispielsweise für eine PCI-DSS-Sicherheitsdomäne erstellt werden, die aus verschiedenen VM-Gruppen besteht, die mit den höchsten Sicherheitsstandards kompatibel sein müssen. Beachten Sie, dass das Domänenobjekt eine experimentelle Funktion in NSX-T Data Center 2.4 ist, aber in NSX-T Data Center 2.4.1 nicht verfügbar ist. In NSX-T Data Center 2.4.1 ist es nicht erforderlich, eine Domäne zu erstellen.
- **Sequenznummer:** Bestimmt die Abfolge, in der Regeln in mehreren Domänen ausgeführt werden. Wenn mehrere Domänen mit Regeln vorhanden sind, sequenziert die Guest Introspection zuerst die Regeln aus einer höherrangigen und dann aus einer niedrigerrangigen Domäne, bis alle Regeln sequenziert sind. Nach dem Veröffentlichen der Regeln werden diese sofort auf die zu schützenden VM-Gruppen angewendet und die Guest Introspection beginnt. Sequenznummern können explizit über API-Aufrufe oder über die Benutzeroberfläche definiert werden. Beachten Sie, dass das Domänenobjekt eine experimentelle Funktion in NSX-T Data Center 2.4 ist, aber in NSX-T Data Center 2.4.1 nicht verfügbar ist. In NSX-T Data Center 2.4.1 ist es nicht erforderlich, eine Domäne zu erstellen.

## Workflow für Endpoint-Schutz

Im ersten Teil des Workflows registrieren Partner Dienste bei NSX-T. Im letzten Teil des Workflows stellt der NSX-Administrator die registrierten Dienste bereit und wendet Endpunkt-Schutzrichtlinien auf VM-Gruppen an.

Der Guest Introspection-Workflow für Endpoint-Schutz sieht wie folgt aus:

Abbildung 10-3. Workflow für Endpoint-Schutz



Allgemein bereiten Partnerdienste eine Dienst-VM (SVM) vor, indem sie EPSec-API(GI)-Bibliotheken verwenden. Die Dienstregistrierung erfolgt über die Service Manager-Konsole des Partners durch Aufrufen von NSX-T-Richtlinien-APIs. Die Service Manager-Konsole wird von den Partnern verwaltet. Neben Diensten registrieren Partner auch Anbietervorlagen, die eine Konfiguration zum Schutz von Gast-VMs enthalten, wenn sie in NSX-T angewendet werden. Nach der Registrierung müssen NSX-Administratoren den Dienst mit einer bestimmten IP-Adresse und Portnummer an den Service Manager des Partners binden.

Nachdem Partner ihre Dienste registriert haben, kann ein NSX-T-Administrator alle registrierten Partnerdienste auf der Benutzeroberfläche von NSX-T Policy Manager anzeigen. Der Administrator stellt diese Dienste auf einem Cluster bereit. Wenn die Bereitstellung abgeschlossen ist, führt jeder Host des Clusters eine SVM aus, auf der das Sicherheitsmodul ausgeführt wird. SVMs kommunizieren unter Verwendung der EPSec-API-Bibliothek mit Gast-VMs, um Ereignisse abzufangen. Um Richtlinien auf Gast-VMs anzuwenden, geben Administratoren Regeln an, die VM-Gruppen Dienstprofilen (einer Instanz der Anbietervorlage) zuordnen. Auf diese Weise wird definiert, welche Schutzstufe auf die Gast-VMs angewendet wird.

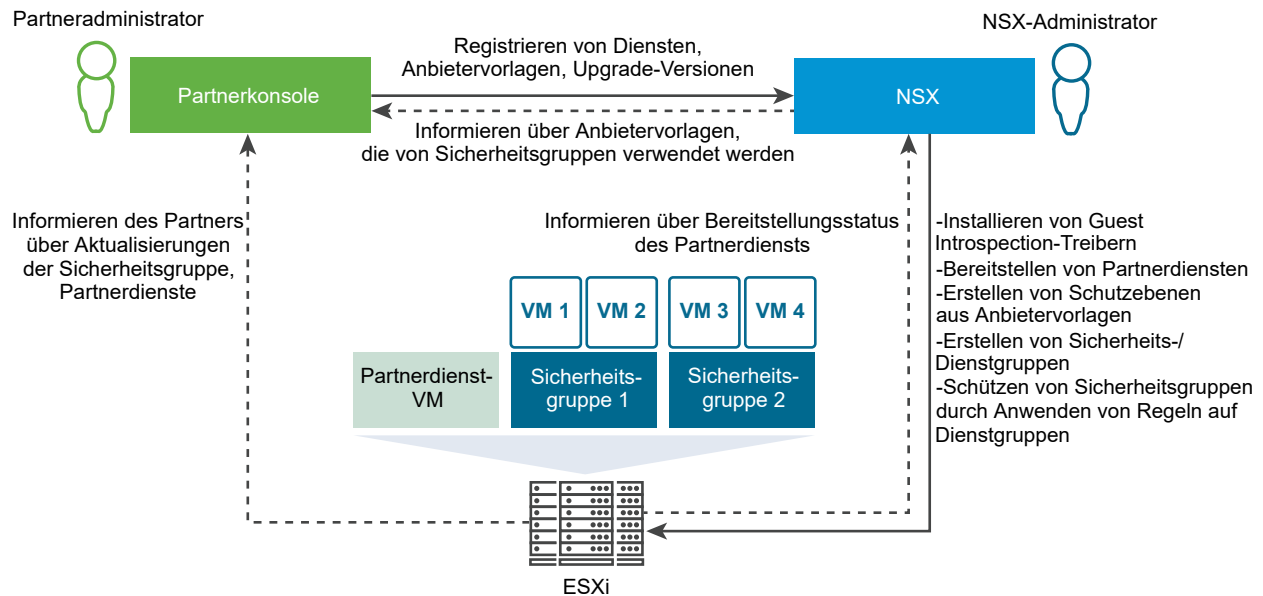
Im Anschluss an die Bereitstellung von Gast-Prüfdiensten beginnt die SVM mit der Prüfung der Gast-VMs. Tritt ein Ereignis auf einer Gast-VM auf, wird das Ereignis von der SVM erfasst und behoben. Außerdem benachrichtigt die SVM die Partnerkonsole und den NSX-T Manager.

## Workflow für Endpoint-Schutz

Im ersten Teil des Workflows registrieren Partner Dienste bei NSX-T. Im letzten Teil des Workflows stellt der NSX-Administrator die registrierten Dienste bereit und wendet Endpunkt-Schutzrichtlinien auf VM-Gruppen an.

Der Guest Introspection-Workflow für Endpoint-Schutz sieht wie folgt aus:

Abbildung 10-4. Workflow für Endpoint-Schutz



Allgemein bereiten Partnerdienste eine Dienst-VM (SVM) vor, indem sie EPSec-API(GI)-Bibliotheken verwenden. Die Dienstregistrierung erfolgt über die Service Manager-Konsole des Partners durch Aufrufen von NSX-T-Richtlinien-APIs. Die Service Manager-Konsole wird von den Partnern verwaltet. Neben Diensten registrieren Partner auch Anbietervorlagen, die eine Konfiguration zum Schutz von Gast-VMs enthalten, wenn sie in NSX-T angewendet werden. Nach der Registrierung müssen NSX-Administratoren den Dienst mit einer bestimmten IP-Adresse und Portnummer an den Service Manager des Partners binden.

Nachdem Partner ihre Dienste registriert haben, kann ein NSX-T-Administrator alle registrierten Partnerdienste auf der Benutzeroberfläche von NSX-T Policy Manager anzeigen. Der Administrator stellt diese Dienste auf einem Cluster bereit. Wenn die Bereitstellung abgeschlossen ist, führt jeder Host des Clusters eine SVM aus, auf der das Sicherheitsmodul ausgeführt wird. SVMs kommunizieren unter Verwendung der EPSec-API-Bibliothek mit Gast-VMs, um Ereignisse abzufangen. Um Richtlinien auf Gast-VMs anzuwenden, geben Administratoren Regeln an, die VM-Gruppen Dienstprofilen (einer Instanz der Anbietervorlage) zuordnen. Auf diese Weise wird definiert, welche Schutzstufe auf die Gast-VMs angewendet wird.

Im Anschluss an die Bereitstellung von Gast-Prüfdiensten beginnt die SVM mit der Prüfung der Gast-VMs. Tritt ein Ereignis auf einer Gast-VM auf, wird das Ereignis von der SVM erfasst und behoben. Außerdem benachrichtigt die SVM die Partnerkonsole und den NSX-T Manager.

## Voraussetzungen für die Konfiguration des Endpoint-Schutzes

Bevor Sie den Endpoint-Schutz für Gast-VMs konfigurieren, stellen Sie sicher, dass die Voraussetzungen erfüllt sind.

## Voraussetzungen

- NSX Manager ist auf allen Hosts installiert.
- Wenden Sie Transportknotenprofile an, um NSX-T Data Center-Cluster als Transportknoten vorzubereiten und zu konfigurieren. Nach der Konfiguration des Hosts als Transportknoten werden die Guest Introspection-Komponenten installiert. Weitere Informationen finden Sie im *NSX-T Data Center-Installationshandbuch*.
- Die Partnerkonsole ist für die Registrierung von Diensten mit NSX-T Data Center installiert und konfiguriert.
- Stellen Sie sicher, dass auf den Gast-VMs die VM-Hardwarekonfigurationsdatei der Version 9 oder höher ausgeführt wird.
- Konfigurieren Sie VMware Tools und installieren Sie Thin Agents.
  - Siehe [Installieren von Guest Introspection Thin Agent auf virtuellen Linux-Maschinen](#).
  - Siehe [Installieren von Guest Introspection Thin Agent auf virtuellen Windows-Maschinen](#).
  - Siehe [Installieren von Linux Thin Agent für die Netzwerk-Introspektion](#).

## Installieren von Guest Introspection Thin Agent auf virtuellen Windows-Maschinen

Zum Schutz von VMs, die eine Guest Introspection-Sicherheitslösung verwenden, müssen Sie den Guest Introspection Thin Agent, auch Guest Introspection-Treiber genannt, auf den virtuellen Maschinen installieren. Guest Introspection-Treiber sind im Lieferumfang der VMware Tools für Windows enthalten, aber sie sind nicht Teil der Standardinstallation. Um Guest Introspection auf einer Windows-VM zu installieren, müssen Sie eine benutzerdefinierte Installation vornehmen und die Treiber auswählen.

Virtuelle Windows-Maschinen, auf denen die Guest Introspection-Treiber installiert sind, werden automatisch geschützt, wenn sie auf einem ESXi-Host gestartet werden, auf dem die Sicherheitslösung installiert ist. Geschützte virtuelle Maschinen behalten den Sicherheitsschutz auch nach dem Herunterfahren und Neustarten und sogar nach einer vMotion-Verschiebung auf einen anderen ESXi-Host, auf dem die Sicherheitslösung installiert ist.

- Wenn Sie vSphere 6.0 verwenden, lesen Sie diese Anweisungen für die Installation von VMware Tools, siehe [Manuelles Installieren oder Aktualisieren von VMware Tools in einer virtuellen Windows-Maschine](#).
- Wenn Sie vSphere 6.5 verwenden, lesen Sie die Anweisungen zum Installieren von VMware Tools unter: <https://www.vmware.com/support/pubs/vmware-tools-pubs.html>.

## Voraussetzungen

Stellen Sie sicher, dass auf der virtuellen Gastmaschine eine unterstützte Version von Windows installiert ist. Die folgenden Windows-Betriebssysteme werden für NSX Guest Introspection unterstützt:

- Windows XP SP3 und höher (32-Bit)
- Windows Vista (32-Bit)

- Windows 7 (32/64-Bit)
- Windows 8 (32/64-Bit)
- Windows 8.1 (32/64) (vSphere 6.0 und höher)
- Windows 10
- Windows 2003 SP2 und höher (32/64-Bit)
- Windows 2003 R2 (32/64-Bit)
- Windows 2008 (32/64-Bit)
- Windows 2008 R2 (64-Bit)
- Win2012 (64)
- Win2012 R2 (64) (vSphere 6.0 und höher)

### Verfahren

- 1 Starten Sie die Installation von VMware Tools gemäß den Anweisungen für Ihre Version von vSphere. Wählen Sie **Benutzerdefinierte Installation** aus.
- 2 Erweitern Sie den VMCI-Treiberabschnitt.  
Die verfügbaren Optionen variieren je nach Version von VMware Tools.
- 3 Wählen Sie den Treiber aus, der auf der VM installiert werden soll.

Treiber	Beschreibung
vShield Endpoint-Treiber	Installiert Datei-Introspektion (vsepf1t)- und Netzwerk-Introspektion (vnetf1t)-Treiber.
Guest Introspection-Treiber	Installiert Datei-Introspektion (vsepf1t)- und Netzwerk-Introspektion (vnetf1t)-Treiber.
NSX File Introspection- und NSX Network Introspection-Treiber	Wählen Sie „NSX File Introspection-Treiber“, um vsepf1t zu installieren. Wählen Sie optional „NSX-Netzwerk-Introspektion-Treiber“ aus, um vnetf1t (vnetWFP für Windows 10 oder höher) zu installieren.  <b>Hinweis</b> Wählen Sie NSX-Netzwerk-Introspektion-Treiber nur, wenn Sie die identitätsbasierte Firewall oder Funktionen zur Endpunktüberwachung verwenden.

- 4 Wählen Sie im Dropdown-Menü neben den hinzuzufügenden Treibern die Option „Diese Funktion wird auf der lokalen Festplatte installiert“ aus.
- 5 Führen Sie die restlichen Schritte dieses Vorgangs aus.

### Nächste Schritte

Überprüfen Sie, ob der Thin Agent ausgeführt wird. Verwenden Sie dazu den `fltmc`-Befehl mit Administratorrechten. In der Spalte „Filtername“ in der Ausgabe wird der Thin Agent mit dem Eintrag `vsepf1t` aufgelistet.

## Installieren von Guest Introspection Thin Agent auf virtuellen Linux-Maschinen

Guest Introspection unterstützt Datei-Introspektion in Linux nur für den Virenschutz. Um Linux-VMs mit einer Guest Introspection-Sicherheitslösung zu schützen, müssen Sie den Guest Introspection Thin Agent installieren.

Der Linux Thin Agent ist als Bestandteil der betriebssystemspezifischen Pakete (OSPs) verfügbar. Die Pakete werden auf dem VMware-Paketportal gehostet. Der Administrator des Unternehmens oder der Sicherheitsadministrator (Nicht-NSX-Administrator) kann den Agent auf Gast-VMs außerhalb von NSX installieren.

Das Installieren von VMware Tools ist nicht erforderlich.

Führen Sie basierend auf Ihrem Linux-Betriebssystem die folgenden Schritte mit Stammrecht aus:

### Voraussetzungen

- Stellen Sie sicher, dass auf der virtuellen Gastmaschine eine unterstützte Version von Linux installiert ist:
  - Red Hat Enterprise Linux (RHEL) 7.4 (64 Bit) GA
  - SUSE Linux Enterprise Server (SLES) 12 (64 Bit) GA
  - Ubuntu 16.04.5 LTS (64 Bit) GA
  - CentOS 7.4 GA
- Stellen Sie sicher, dass GLib 2.0 auf der Linux-VM installiert ist.

### Verfahren

#### 1 Für Ubuntu-Systeme

- a Rufen Sie die öffentlichen VMware-Paketschlüssel mithilfe der folgenden Befehle ab und importieren Sie sie:

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
apt-key add VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b Erstellen Sie eine neue Datei mit dem Namen `vmware.list` unter `/etc/apt/sources.list.d`.
- c Bearbeiten Sie die Datei mit folgendem Inhalt:

```
deb [arch=amd64] https://packages.vmware.com/packages/nsx-gi/latest/ubuntu/ xenial main
```

- d Installieren Sie das Paket.

```
apt-get update
apt-get install vmware-nsx-gi-file
```



## 2 Für RHEL7-Systeme

- a Rufen Sie die öffentlichen VMware-Paketschlüssel mithilfe der folgenden Befehle ab und importieren Sie sie:

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
rpm --import VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b Erstellen Sie eine neue Datei mit dem Namen `vmware.repo` unter `/etc/yum.repos.d`.
- c Bearbeiten Sie die Datei mit folgendem Inhalt:

```
[vmware]
name = VMware
baseurl = https://packages.vmware.com/packages/nsx-gi/latest/rhel7/x86_64
enabled = 1
gpgcheck = 1
metadata_expire = 86400
ui_repoid_vars = basearch
```

## 3 Installieren Sie das Paket.

```
yum install vmware-nsx-gi-file
```

## 4 Für SLES-Systeme

- a Rufen Sie die öffentlichen VMware-Paketschlüssel mithilfe der folgenden Befehle ab und importieren Sie sie:

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
rpm --import VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b Fügen Sie das folgende Repository hinzu:

```
zypper ar -f "https://packages.vmware.com/packages/nsx-gi/latest/sle12/x86_64/" VMware
```

- c Installieren Sie das Paket.

```
zypper install vmware-nsx-gi-file
```

## 5 Für CentOS-Systeme

- a Rufen Sie die öffentlichen VMware-Paketschlüssel mithilfe der folgenden Befehle ab und importieren Sie sie:

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
rpm --import VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b Erstellen Sie eine neue Datei mit dem Namen `vmware.repo` unter `/etc/yum.repos.d`.
- c Bearbeiten Sie die Datei mit folgendem Inhalt:

```
[vmware]
name = VMware
baseurl = https://packages.vmware.com/packages/nsx-gi/latest/centos7/x86_64
enabled = 1
gpgcheck = 1
metadata_expire = 86400
ui_repoid_vars = basearch
```

### Nächste Schritte

Überprüfen Sie, ob der Thin Agent ausgeführt wird. Verwenden Sie dazu den Befehl `vsepd status` mit Administratorrechten. Der Status muss Ausführung lauten.

### Installieren von Linux Thin Agent für die Netzwerk-Introspektion

Installieren Sie Linux Thin Agent, um den Netzwerkdatenverkehr zu überprüfen.

---

**Wichtig** Zum Schützen von Gast-VMs vor Antivirus müssen Sie den Linux Thin Agent für die Netzwerk-Introspektion nicht installieren.

---

Der Linux Thin Agent-Treiber, der zur Introspektion des Netzwerkdatenverkehrs verwendet wird, hängt von einem Open-Source-Treiber ab.

### Voraussetzungen

Installieren Sie die folgenden Pakete:

- `glib2`
- `libnetfilter-conntrack3/ libnetfilter-conntrack`
- `libnetfilter-queue1/ libnetfilter-queue`
- `iptables`

## Verfahren

- 1 So installieren Sie den von Guest Introspection bereitgestellten Open-Source-Treiber.

- a Fügen Sie die folgende URL als Basis-URL für Ihr Betriebssystem hinzu.

```
deb [arch=amd64] https://packages.vmware.com/guest-introspection-for-vmware-nsx/latest/
```

- b Importieren Sie den VMware-Paketschlüssel.

```
https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- c Aktualisieren Sie das Repository und installieren Sie den Open-Source-Treiber.

```
apt-get install Guest-Introspection-for-VMware-NSX
```

- 2 So installieren Sie den Linux Thin Agent, der zur Introspektion des Datei- und/oder Netzwerkdatenverkehrs verwendet wird.

- Wählen Sie zum Installieren von Datei- und Netzwerk-Introspektionspaketen das Paket `vmware-nsx-gi` in Schritt C aus.
  - Wählen Sie zum Installieren von Netzwerk-Introspektionspaketen das Paket `vmware-nsx-gi-net` in Schritt C aus.
- a Fügen Sie die folgende URL als Basis-URL für Ihr Betriebssystem hinzu.

```
deb [arch=amd64] https://packages.vmware.com/packages/nsx-gi/latest
```

- b Importieren Sie den VMware-Paketschlüssel.

```
https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- c Installieren Sie einen der Treiber.

```
vmware-nsx-gi
vmware-nsx-gi-net
```

## Unterstützte Software

Guest Introspection ist mit bestimmten Softwareversionen kompatibel.

### VMware Tools

VMware Tool 10.3.10 wird unterstützt.

Überprüfen Sie die Interoperabilität zwischen VMware Tools und NSX-T. Siehe [VMware-Produktinteroperabilitätstabellen](#).

### Unterstütztes Betriebssystem

Nur Microsoft Windows-Betriebssystem wird unterstützt.

- Windows 7

- Windows 8/8.1
- Windows 10
- Windows 2008 Server R2
- Windows 2012 Server R2
- Windows 2016 Server

### Unterstützte Hosts

Die unterstützten ESXi-Hosts finden Sie in den [VMware-Produktinteroperabilitätstabellen](#).

## Erstellen eines Benutzers mit der Rolle „Guest Introspection-Partner-Administrator“

Weisen Sie einen Benutzer mit der Guest Introspection-Partner-Administratorrolle zu, der in NSX-T Data Center verfügbar ist.

Hinweis: Es wird empfohlen, Partnerdienste von einem Benutzer zu registrieren, dem die Administratorrolle des Guest Introspection-Partners zugeordnet ist, um Sicherheitsprobleme zu vermeiden.

### 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** → **Benutzer** → **Rollenzuweisungen** aus.
- 3 Klicken Sie auf **Hinzufügen**.
- 4 Wählen Sie den Benutzer aus und weisen Sie diesem Benutzer die Rolle **GI-Partneradministrator** zu.

### Nächste Schritte

Registrieren Sie Dienste bei NSX-T Data Center. Siehe [Registrieren eines Diensts bei NSX-T Data Center](#).

## Registrieren eines Diensts bei NSX-T Data Center

Registrieren Sie Sicherheitsdienste von Drittanbietern bei NSX-T Data Center.

### Voraussetzungen

- Stellen Sie sicher, dass die Voraussetzungen erfüllt sind. Siehe [Voraussetzungen für die Konfiguration des Endpoint-Schutzes](#).
- Stellen Sie sicher, dass einem vIDM-Benutzer die Rolle „GI-Partneradministrator“ zugewiesen ist. Diese Rolle wird zum Registrieren von Diensten mit NSX-T Data Center verwendet.

## Verfahren

- 1 Melden Sie sich mit den GI-Partneradministratorrechten bei der Partnerkonsole an.
- 2 Registrieren Sie einen Dienst und eine Anbietervorlage und konfigurieren Sie die Partnerlösung mit NSX-T Data Center. Weitere Informationen finden Sie in der Partnerdokumentation.

## Nächste Schritte

Zeigen Sie Kataloge von Partnerdiensten an. Siehe [Anzeigen der Kataloge von Partnerdiensten](#).

## Anzeigen der Kataloge von Partnerdiensten

Auf der Seite „Katalog“ werden alle Partner und deren Dienste angezeigt, die bei NSX-T Data Center registriert sind.

## Voraussetzungen

- Partner registrieren Dienste bei NSX-T Data Center.
- Dienste werden auf einem Cluster bereitgestellt.

## 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 > Dienstbereitstellungen > Katalog** aus.
- 3 Klicken Sie in einem Dienst auf **Anzeigen**. Auf der Seite „Bereitstellung“ werden die Details zum Dienst angezeigt, wie z. B. Status der Bereitstellung, Netzwerkdetails, Clusterdetails usw.

## Nächste Schritte

Bereitstellen eines Diensts. Siehe [Bereitstellen eines Diensts](#).

## Bereitstellen eines Diensts

Nachdem Sie einen Dienst registriert haben, müssen Sie eine Instanz des Diensts bereitstellen, damit der Dienst mit der Verarbeitung des Netzwerkdatenverkehrs beginnen kann.

Stellen Sie VMs des Partnerdiensts, auf denen die Sicherheits-Engine des Partners ausgeführt wird, auf allen NSX-T Data Center-Hosts in einem Cluster bereit. Der vSphere EAM-Dienst (ESX Agency Manager) wird verwendet, um die Partnerdienst-VMs auf jedem Host bereitzustellen. Nach dem Bereitstellen der SVMs können Sie Richtlinienregeln erstellen, die von SVM zum Schutz der Gast-VMs verwendet werden.

## Voraussetzungen

- Alle Hosts werden von einem vCenter Server verwaltet.
- Partnerdienste werden mit NSX-T Data Center registriert und können bereitgestellt werden.

- NSX-T Data Center-Administratoren können auf Partnerdienste und Anbietervorlagen zugreifen.
- Sowohl die Dienst-VM als auch der Partner Service Manager (Konsole) müssen auf der Ebene des Verwaltungsnetzwerks miteinander kommunizieren können.
- Bereiten Sie Hosts als NSX-T Data Center-Transportknoten vor:
  - Erstellen Sie eine Transportzone.
  - Erstellen Sie einen IP-Pool für Tunnel-Endpoint-IP-Adressen.
  - Erstellen Sie ein Uplink-Profil.
  - Fügen Sie ein Transportknotenprofil hinzu, um einen Cluster auf die automatische Bereitstellung von NSX-T Data Center-Transportknoten vorzubereiten.
  - Konfigurieren Sie einen eigenständigen oder verwalteten Host.

#### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Navigieren Sie zur Registerkarte **System** und klicken Sie auf **Dienstbereitstellung**.
- 3 Klicken Sie auf **Bereitstellung** und dann auf **Dienst bereitstellen**.
- 4 Geben Sie den Namen der Dienstbereitstellung ein.
- 5 Wählen Sie im Feld „Berechnungsmanager“ die Computing-Ressource auf dem vCenter Server aus, auf dem der Dienst bereitgestellt werden soll.
- 6 Wählen Sie im Feld „Cluster“ den Cluster aus, auf dem die Dienste bereitgestellt werden müssen.
- 7 Im Dropdown-Menü „Datenspeicher“ können Sie folgende Aktionen ausführen:
  - a Wählen Sie einen Datenspeicher als Repository für die Dienst-VM aus.
  - b Wählen Sie **Auf Host konfigurieren** aus. Mit dieser Einstellung wird festgelegt, dass in diesem Assistenten weder ein Datenspeicher noch eine Portgruppe ausgewählt werden muss. Sie können Agent-Einstellungen für EAM direkt auf dem vCenter Server konfigurieren, um auf einen bestimmten Datenspeicher oder eine bestimmte Portgruppe zu verweisen, die für die Dienstbereitstellung verwendet werden soll. Fahren Sie mit Schritt 11 fort.

Informationen zur Konfiguration von EAM finden Sie in der vSphere-Dokumentation.

- 8 Klicken Sie in der Spalte „Netzwerk“ auf **Festlegen** und geben Sie die Schnittstelle des Verwaltungsnetzwerks ein, indem Sie den DHCP- oder statischen IP-Adresstyp, das Steuerungs- und Datennetzwerk auswählen.
- 9 Wählen Sie im Feld „Bereitstellungsspezifikation“ den Dienst und den Formfaktor der Dienst-VM aus, die auf Clusterhosts bereitgestellt werden soll. Mehrere Dienste können für die Bereitstellung zur Verfügung stehen.

- 10 Wählen Sie im Feld „Bereitstellungsvorlage“ die Anbietervorlage mit Attributen zum Schutz der Arbeitslast aus, die in Gast-VM-Gruppen ausgeführt werden soll.
- 11 Klicken Sie auf **Speichern**.

### Ergebnisse

Wenn dem Cluster ein neuer Host hinzugefügt wird, stellt EAM die Dienst-VM automatisch auf dem neuen Host bereit. Der Bereitstellungsvorgang kann je nach Implementierung des Anbieters einige Zeit in Anspruch nehmen. Sie können den Status auf der Benutzeroberfläche von NSX Manager anzeigen. Der Dienst wurde erfolgreich auf dem Host bereitgestellt, wenn der Status zu **Bereitstellung erfolgreich** wechselt.

Um einen Host aus einem Cluster zu entfernen, versetzen Sie ihn zunächst in den Wartungsmodus. Wählen Sie anschließend die Option zum Migrieren der Gast-VMs auf einen anderen Host aus, um die Migration abzuschließen.

### Nächste Schritte

Informieren Sie sich über die Bereitstellungsdetails und den Systemzustand von Dienstinstanzen, die auf den Hosts bereitgestellt werden. Siehe [Anzeigen von Details der Dienstinstanz](#).

## Anzeigen von Details der Dienstinstanz

Informieren Sie sich über die Bereitstellungsdetails und den Systemzustand von Dienstinstanzen, die auf den Mitgliederhosts eines Clusters bereitgestellt werden.

### 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 > Dienstbereitstellungen > Dienstinstanzen** aus.
- 3 Wählen Sie im Dropdown-Menü „Partnerdienst“ den Partnerdienst aus, um die Details der Dienstinstanzen anzuzeigen.

**Tabelle 10-9.**

Feld	Beschreibung
Name der Dienstinstanz	Eine eindeutige ID zur Angabe der Dienstinstanz auf einem bestimmten Host.
Name der Dienstbereitstellung	Eine eindeutige ID zur Angabe der Dienstdefinition
Bereitgestellt auf	Host-IP-Adresse
Bereitstellungsmodus	Cluster oder Eigenständig

Tabelle 10-9. (Fortsetzung)

Feld	Beschreibung
Bereitstellungsstatus	Status „Aktiv“ zur Angabe einer erfolgreichen Bereitstellung
Systemzustand	<p>Systemstatus lautet „Aktiv“, wenn die folgenden Parameter von NSX-T Data Center erfolgreich umgesetzt werden.</p> <ul style="list-style-type: none"> <li>■ Lösungsstatus: Aktiv</li> <li>■ Konnektivität zwischen NSX-T Data Center Guest Introspection-Agent und NSX-T Data Center Ops-Agent: Aktiv</li> <li>■ Protokoll der Dienst-VM ist definiert</li> <li>■ Protokollkompatibilität zwischen Dienst-VM und NSX-T Data Center Guest Introspection-Agent</li> </ul>

### Nächste Schritte

Anzeigen des Katalogs der registrierte Dienste. Siehe [Anzeigen der Kataloge von Partnerdiensten](#).

## Aktivieren der Dienstinstanz

Nach der Bereitstellung der Dienstinstanz müssen bestimmte Parameter in NSX-T Data Center realisiert werden, damit der Systemzustand „Aktiv“ ist.

### 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 > Dienstbereitstellungen > Dienstinstanzen** aus.
- 3 Wählen Sie im Dropdown-Menü „Partnerdienst“ den Partnerdienst aus, um die Details der Dienstinstanzen anzuzeigen.
- 4 In der Spalte „Systemzustand“ wird der Status der Dienstinstanz als **Bereit** angezeigt. Dies deutet daraufhin, dass die Dienstinstanz mit Regeln der Endpoint-Schutzrichtlinie konfiguriert werden kann.
- 5 Die folgenden Parameter müssen in NSX-T Data Center realisiert werden, damit der Systemzustand in **Aktiv** geändert werden kann.
  - Virtuelle Gastmaschinen müssen auf dem Host verfügbar sein.
  - Die virtuellen Gastmaschinen müssen eingeschaltet sein.
  - Endpoint-Schutzregeln müssen auf die virtuellen Gastmaschinen angewendet werden.
  - Virtuelle Gastmaschinen müssen mit der unterstützten Version von VMtools und Datei-Introspektionstreibern konfiguriert werden.



## Nächste Schritte

Fügen Sie ein Dienstprofil hinzu. Siehe [Hinzufügen eines Dienstprofils für Endpoint-Schutz](#).

## Hinzufügen eines Dienstprofils für Endpoint-Schutz

Guest Introspection-Richtlinien können nur implementiert werden, wenn ein Dienstprofil in NSX-T Data Center verfügbar ist. Dienstprofile werden anhand einer vom Partner bereitgestellten Vorlage erstellt. Mithilfe von Dienstprofilen kann der Administrator Schutzebenen (Gold, Silber, Platin) für eine VM festlegen, indem er die vom Anbieter bereitgestellten Anbietervorlagen auswählt.

Beispielsweise kann ein Anbieter die Richtlinienebenen „Gold“, „Platin“ und „Silber“ bereitstellen. Jedes erstellte Profil kann einer anderen Art von Arbeitslast dienen. Ein Dienstprofil vom Typ „Gold“ bietet einer PCI-Arbeitslast vollständigen Malware-Schutz, während ein Dienstprofil vom Typ „Silber“ grundlegenden Malware-Schutz für reguläre Arbeitslasten bereitstellt.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Sicherheit > Endpoint-Schutz > Dienstprofile** aus.
- 3 Wählen Sie im Feld „Partnerdienst“ den Dienst aus, für den Sie ein Dienstprofil erstellen möchten.
- 4 Klicken Sie auf **Dienstprofil hinzufügen**.
- 5 Geben Sie den Namen des Dienstprofils ein und wählen Sie die Anbietervorlage aus. Fügen Sie optional eine Beschreibung und Tags hinzu.
- 6 Klicken Sie auf **Speichern**.

Die zum Erstellen des Dienstprofils verwendete Anbietervorlagen-ID wird an die Partnerkonsole übergeben. Partner speichern die Anbietervorlagen-ID, um die Nutzung der Gast-VMs zu verfolgen, die durch diese Anbietervorlage geschützt sind.

### Ergebnisse

Nach dem Dienstprofil erstellt ein NSX-Administrator Regeln, um einer Gruppe von VMs vor dem Veröffentlichen der Richtlinienregel ein Dienstprofil zuzuordnen.

## Nächste Schritte

Wenden Sie Regeln für den Endpoint-Schutz auf Gast-VMs an, die vor Malware geschützt werden müssen.

## Verwenden der Guest Introspection-Richtlinie

Eine Richtlinie kann in VM-Gruppen durchgesetzt werden, indem Regeln erstellt werden, die Dienstprofile mit VM-Gruppen verknüpfen. Der Schutz beginnt unmittelbar nach dem Anwenden der Regeln auf eine VM-Gruppe.

Bei der Richtlinie für Endpoint-Schutz handelt es sich um einen von Partnern angebotenen Dienst zum Schutz von Gast-VMs vor Malware, der Dienstprofile auf Gast-VMs implementiert. Mit einer auf eine VM-Gruppe angewendeten Regel werden alle Gast-VMs in dieser Gruppe vom entsprechenden Dienstprofil geschützt. Wenn ein Dateizugriffsereignis auf einer Gast-VM auftritt, sammelt der GI Thin Agent (der auf jeder Gast-VM ausgeführt wird) Kontext der Datei (Dateiattribute, Datei-Handle und andere Kontextdetails) und informiert SVM über das Ereignis. Wenn die SVM den Dateiinhalt durchsuchen möchte, fordert sie Details mithilfe der EPSec-API-Bibliothek an. Nach einer eindeutigen Bewertung von SVM ermöglicht der GI Thin Agent dem Benutzer Zugriff auf die Datei. Wird die Datei von SVM als infiziert gemeldet, verweigert der GI Thin Agent dem Benutzer den Zugriff auf diese Datei.

Zum Implementieren der Richtlinie zum Endpoint-Schutz erstellen Sie zunächst eine Domäne, die für eine bestimmte Art von Arbeitslast ausgelegt ist. Anschließend definieren Sie EPP-Regeln, indem Sie eine VM-Gruppe mit einem Dienstprofil verknüpfen, das den Dienst und die Schutzebene für VMs definiert. Beachten Sie, dass das Domänenobjekt eine experimentelle Funktion in NSX-T Data Center 2.4 ist, aber in NSX-T Data Center 2.4.1 nicht verfügbar ist. In NSX-T Data Center 2.4.1 ist es nicht erforderlich, eine Domäne zu erstellen.

Zum Ausführen eines Sicherheitsdiensts in einer VM-Gruppe müssen Sie folgende Schritte durchführen:

#### Verfahren

- 1 Definieren einer Domäne, einer Umgebung, die VM-Gruppen und Regeln hostet.  
Beachten Sie, dass das Domänenobjekt eine experimentelle Funktion in NSX-T Data Center 2.4 ist, aber in NSX-T Data Center 2.4.1 nicht verfügbar ist.
- 2 Definieren von Mitgliedschaftskriterien zum Erstellen einer VM-Gruppe.
- 3 Definieren von Regeln für VM-Gruppen.
- 4 Veröffentlichen der Regel.

### Hinzufügen und Veröffentlichen von Regeln für Endpoint-Schutz

Das Veröffentlichen von Richtlinienregeln in VM-Gruppen bedeutet, dass zu schützende VM-Gruppen mit einem bestimmten Dienstprofil verknüpft werden.

#### Verfahren

- 1 Wählen Sie im Abschnitt „Richtlinie“ eine Richtlinie aus.
- 2 Klicken Sie auf **Hinzufügen -> Regel hinzufügen**.
- 3 Geben Sie in der Spalte „Name“ einen Namen für die Regel ein.
- 4 Wählen Sie in der Spalte „Gruppe“ die VM-Gruppe aus.
- 5 Wählen Sie in der Spalte „Dienstprofile“ das Dienstprofil aus, das den Gast-VMs in der Gruppe die gewünschte Schutzebene bereitstellt.
- 6 Klicken Sie auf **Veröffentlichen**.

## Ergebnisse

Richtlinien für Endpoint-Schutz schützen VM-Gruppen.

## Nächste Schritte

Es ist möglicherweise empfehlenswert, die Reihenfolge der Regeln je nach dem für verschiedene VM-Gruppen notwendigen Schutztyp zu ändern. Siehe [So führt Guest Introspection Richtlinien zum Endpoint-Schutz aus](#)

## Überwachen des Endpoint-Schutzstatus

Überwachen Sie den Konfigurationsstatus geschützter und ungeschützter VMs, Probleme mit Hostagent- und Dienst-VMs und VMs, die mit dem Datei-Introspektionstreiber konfiguriert wurden, der als Teil der VMtools-Installation installiert wurde.

Sie können Folgendes anzeigen:

- Anzeigen des Dienstbereitstellungsstatus
- Anzeigen des Konfigurationsstatus des Endpoint-Schutzes.
- Anzeigen des Kapazitätsstatus, der für den Endpoint-Schutz festgelegt wurde.

### Anzeigen des Dienstbereitstellungsstatus

Zeigen Sie im Überwachungs-Dashboard die Dienstbereitstellungsdetails an.

Zeigen Sie den systemweiten Status der EPP-Richtlinie an.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Navigieren Sie zur **Startseite > Überwachung – Dashboards**.
- 3 Klicken Sie im Dropdown-Menü auf **Überwachung – System**.
- 4 Navigieren Sie zum Anzeigen des Bereitstellungsstatus für Cluster im System zum Widget „Endpoint-Schutz“ und klicken Sie auf das Ringdiagramm, um erfolgreiche oder nicht erfolgreiche Bereitstellungen anzuzeigen.

Auf der Seite „Dienstbereitstellungen“ werden die Bereitstellungsdetails angezeigt.

### Anzeigen des Kapazitätsstatus, der für den Endpoint-Schutz festgelegt wurde

Zeigen Sie den Kapazitätsstatus des Endpoint-Schutzdiensts an.

Zeigen Sie den Kapazitätsstatus der EPP-Richtlinie an.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Navigieren Sie zur **Startseite > Überwachung – Dashboards**.

- 3 Klicken Sie im Dropdown-Menü auf **Überwachung – Netzwerk und Sicherheit**.
- 4 Wenn Sie den Status von EPP auf Clustern anzeigen möchten, klicken Sie auf das Sicherheits-Widget.
- 5 Klicken Sie auf der Seite „Sicherheitsübersicht“ auf **Kapazität** und zeigen Sie den Kapazitätsstatus dieser Parameter an.

🔍 SICHERHEITSÜBERSICHT

Konfiguration **Kapazität**

[AKTUALISIEREN](#) | Zuletzt aktualisiert am: 29.10.2019 um 06:00:00 | [WERTE ZURÜCKSETZEN](#) | [WIEDERHERSTELLEN](#) | [SPEICHERN](#)

Grenzwert	Maximale Kapazität	Aktuelle Bestandsliste (realisiert)	Warnmeldung	Kritische Warnung
Regeln für verteilte Firewall	100.000	2	0 %	70% 100%
Systemweite Firewallabschnitte	10.000	5	0,05 %	70% 100%

- a **Systemweite Hosts mit aktiviertem Endpoint-Schutz:** Wenn die Anzahl der geschützten Hostnummern den Schwellenwert erreicht, gibt NSX Manager eine Warnmeldung oder eine kritische Warnung aus, sobald die entsprechenden Schwellenwerte erreicht sind.
- b **Systemweite virtuelle Maschinen mit aktiviertem Endpoint-Schutz:** Wenn die Anzahl der geschützten virtuellen Maschinenummern den Schwellenwert erreicht, gibt NSX Manager eine Warnmeldung oder eine kritische Warnung aus, sobald die entsprechenden Schwellenwerte erreicht sind.

**Hinweis** Sie können Schwellenwerte für diese Parameter festlegen, den Status anzeigen und Warnungen empfangen, wenn diese Parameter den festgelegten Schwellenwert erreichen.

### Anzeigen des Konfigurationsstatus des Endpoint-Schutzes

Zeigen Sie den Konfigurationsstatus des Endpoint-Schutzdienstes an.

Zeigen Sie den systemweiten Status der EPP-Richtlinie an.

#### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Navigieren Sie zu **Startseite > Sicherheit > Sicherheitsübersicht**.
- 3 Wenn Sie den Status von EPP auf Clustern anzeigen möchten, klicken Sie auf das Sicherheits-Widget.

#### 4 Klicken Sie auf der Seite „Sicherheitsübersicht“ auf **Konfiguration**.



#### 5 Zeigen Sie im Abschnitt „Endpoint-Schutz“ Folgendes an:

##### a VM-Verteilung nach Dienstprofil-Widget zeigt Folgendes an:

- 1 Anzahl VMs, die vom Top-Profil geschützt werden. Das Top-Profil stellt ein Profil dar, das die maximale Anzahl VMs in einem Cluster schützt.
- 2 Durch die verbleibenden Dienstprofile geschützte VMs, die unter „Andere Profile“ kategorisiert sind.
- 3 Nicht geschützte VMs, die unter „Kein Profil“ kategorisiert sind.

Auf der Seite „Regeln für Endpoint-Schutz“ durch Endpoint-Schutzrichtlinien geschützte VMs angezeigt.

##### b Komponenten mit angezeigtem Problem-Widget:

- 1 Host: Probleme im Zusammenhang mit dem Kontext-Multiplexer.
- 2 SVM: Probleme im Zusammenhang mit Dienst-VMs. Beispiel: der SVM-Zustand inaktiv, SVM-Verbindung mit Gast-VM ist inaktiv.

In der Spalte „Status“ auf der Seite „Bereitstellung“ werden Zustandsprobleme angezeigt.

##### c Beim Konfigurieren von VMs mit Datei-Introspektions-Widget wird Folgendes angezeigt:

- 1 VMs, die durch den Datei-Introspektionstreiber geschützt sind.
- 2 VMs, bei denen der Status des Datei-Introspektionstreibers unbekannt ist.

ESXi Agency Manager (EAM) versucht, einige Probleme im Zusammenhang mit Hosts, SVMs und Konfigurationsfehlern zu beheben. Siehe [Sicherstellen der Funktionsfähigkeit von Partnerdiensten auf allen Hosts](#).

## Hinzufügen von Domänen und VM-Gruppen

Erstellen Sie eine Domäne, die eine Umgebung darstellt, zu der die Richtlinien und VM-Sicherheitsgruppen gehören.

Beachten Sie, dass das Domänenobjekt eine experimentelle Funktion in NSX-T Data Center 2.4 ist, aber in NSX-T Data Center 2.4.1 nicht verfügbar ist. In NSX-T Data Center 2.4.1 ist es nicht erforderlich, eine Domäne zu erstellen.

## Verfahren

- 1 Wählen Sie **Sicherheit > Endpoint-Schutz > Regeln** aus.
- 2 Klicken Sie auf **Richtlinie hinzufügen**.
- 3 Geben Sie in der Spalte „Name“ einen Namen für die Richtlinie ein.
- 4 Klicken Sie im Feld „Domäne“ auf **Standard**, um eine Domäne auszuwählen oder eine neue zu erstellen.
- 5 Klicken Sie im Fenster „Domäne auswählen“ am unteren Rand des Fensters auf **NEUE DOMÄNE ERSTELLEN**.
- 6 Geben Sie in der Spalte „Name“ einen Namen für die Domäne ein.
- 7 Klicken Sie auf **Speichern**.
- 8 Klicken Sie auf **Ja**, um die Gruppen in dieser Domäne zu konfigurieren.
- 9 Klicken Sie auf **Gruppe hinzufügen**.
- 10 Geben Sie im Fenster „Gruppen hinzufügen“ den Namen für die Gruppe ein.
- 11 Wählen Sie in der Spalte „Computing-Mitglieder“ die Option „Mitglieder“ aus.
- 12 Legen Sie im Fenster „Mitglieder auswählen“ die Mitgliedschaftskriterien für VMs fest, die der Gruppe beitreten sollen, oder wählen Sie manuell VMs aus, die Teil einer Gruppe sein sollen.
- 13 Klicken Sie auf **Kriterien hinzufügen**. Mitgliedschaftskriterien können entweder durch ein Tag, einen Betriebssystemnamen oder einen Computernamen definiert werden.
- 14 Nachdem Sie die gewünschten Kriterien für den Beitritt von VMs zur Gruppe hinzugefügt haben, klicken Sie auf **Speichern**. Klicken Sie dann auf **Schließen**.
- 15 Klicken Sie auf **Speichern**.

## Nächste Schritte

Erstellen Sie Regeln und veröffentlichen Sie sie. Siehe [Hinzufügen und Veröffentlichen von Regeln für Endpoint-Schutz](#).

## So führt Guest Introspection Richtlinien zum Endpoint-Schutz aus

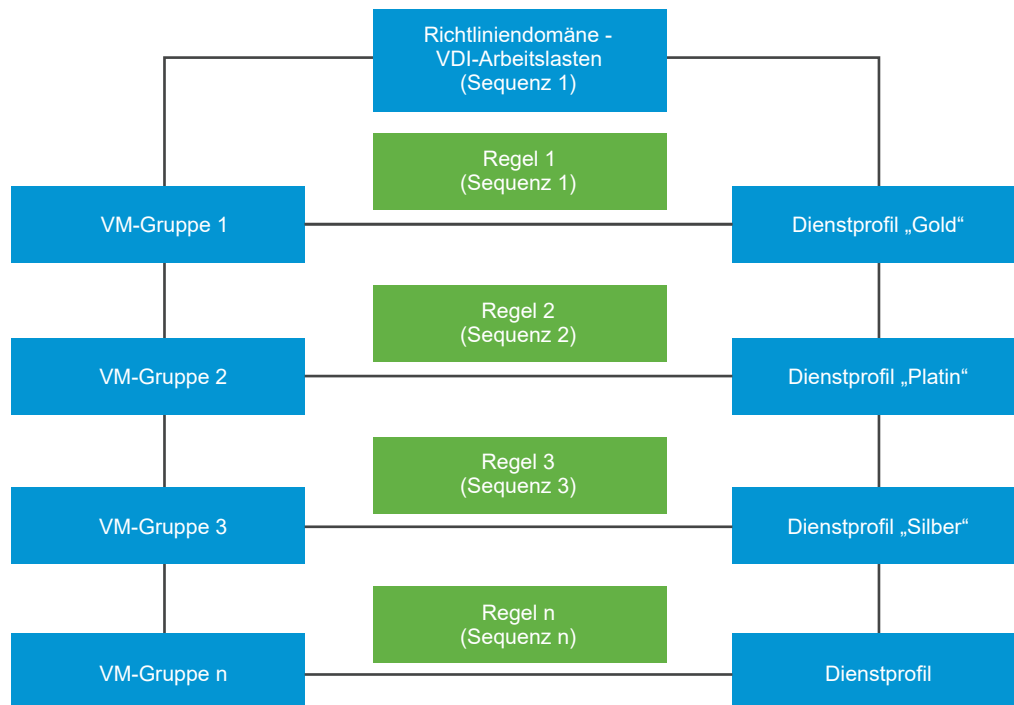
Richtlinien zum Endpoint-Schutz werden in einer bestimmten Reihenfolge durchgesetzt. Berücksichtigen Sie beim Entwurf von Richtlinien die mit Regeln verknüpfte Sequenznummer sowie die Domänen, die die Regeln hosten.

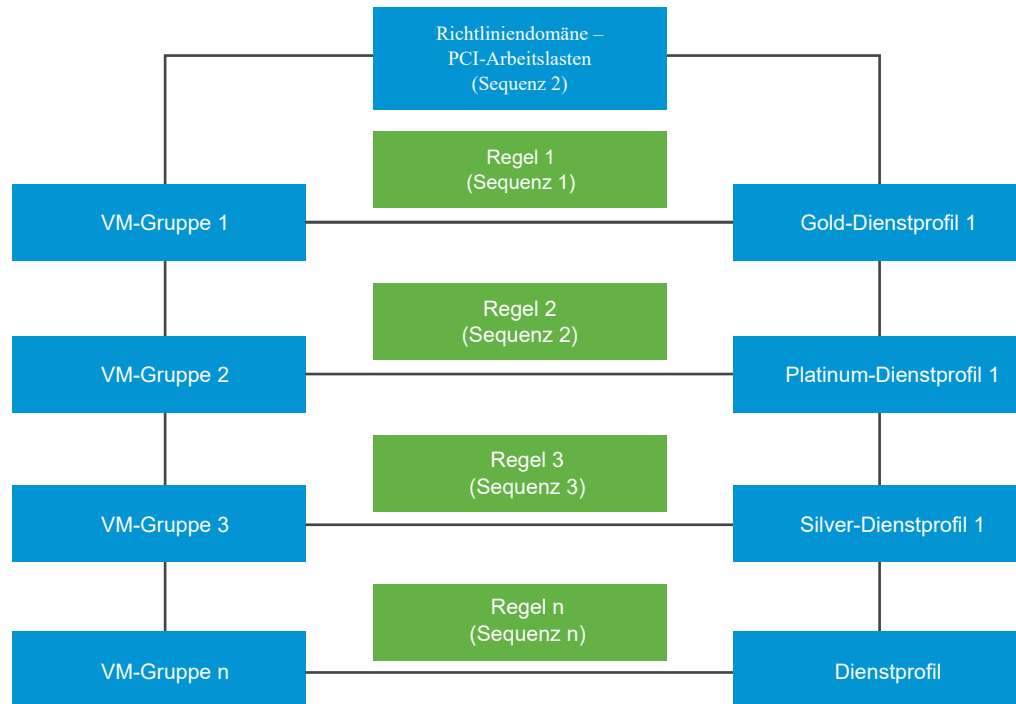
---

**Hinweis** Das Domänenobjekt ist eine experimentelle Funktion in NSX-T Data Center 2.4, die in NSX-T Data Center 2.4.1 nicht verfügbar ist. In NSX-T Data Center 2.4.1 ist es nicht erforderlich, eine Domäne zu erstellen.

---

Szenario: Von den zahlreichen Arbeitslasten, die in Ihrem Unternehmen ausgeführt werden, betrachten wir zum Zweck der Veranschaulichung zwei Arten von Arbeitslasten – VMs, auf denen VDI-Arbeitslasten (Virtual Desktop Infrastructure, Virtuelle Desktopinfrastruktur) ausgeführt werden, und VMs, auf denen PCI-DSS-Arbeitslasten (Payments Cards Industry Data Security Standards) ausgeführt werden. Ein Teil der Mitarbeiter im Unternehmen benötigt Remotedesktopzugriff, der die VDI-Arbeitslast (Virtual Desktop Infrastructure) darstellt. Diese VDI-Arbeitslasten benötigen gegebenenfalls eine Schutzebene vom Typ „Gold“, die auf den vom Unternehmen festgelegten Compliance-Regeln basiert. Eine PCI DSS-Arbeitslast hingegen benötigt die höchste Schutzebene vom Typ „Platin“.





Da es zwei Typen von Arbeitslasten gibt, erstellen Sie zwei Richtlinien: eine für VDI-Arbeitslasten und eine für Serverarbeitslasten. Definieren Sie innerhalb jeder Richtlinie bzw. jedes Abschnitts eine Domäne zur Angabe des Arbeitslasttyps und legen Sie in diesem Abschnitt Regeln für jeweilige Arbeitslast fest. Veröffentlichen Sie die Regeln zum Starten der GI-Dienste auf Gast-VMs. GI verwendet intern die folgenden beiden Sequenznummern: Richtliniensequenznummer und Regelsequenznummer zur Ermittlung der vollständigen Abfolge der auszuführenden Regeln. Jede Regel dient zwei Zwecken: Sie bestimmt die zu schützenden VMs und die Schutzrichtlinie, die zum Schutz der VMs angewendet werden muss.

Ziehen Sie zum Ändern der Reihenfolge eine Regel auf die Benutzeroberfläche von NSX-T Policy Manager. Alternativ können Sie Sequenznummern für Regeln mithilfe der API explizit zuweisen.

Führen Sie alternativ einen NSX-T Data Center-API-Aufruf durch, um manuell eine Regel zu definieren, indem Sie ein Dienstprofil mit einer VM-Gruppe verknüpfen und die Sequenznummer der Regeln deklarieren. Die API- und Parameterdetails werden ausführlich im *NSX-T Data Center - API-Handbuch* erläutert. Führen Sie API-Aufrufe der Dienstkongfiguration durch, um Profile auf Elemente anzuwenden, wie z. B. VM-Gruppen usw.



**Tabelle 10-10. NSX-T Data Center-APIs, die zum Definieren von Regeln verwendet werden, die Dienstprofile auf VM-Gruppen anwenden**

API	Details
Abrufen aller Details der Dienstkonfiguration.	<p>GET /api/v1/service-configs</p> <p>Die Dienstkonfigurations-API gibt die Details des auf eine VM-Gruppe angewendeten Dienstprofils, die geschützte VM-Gruppe sowie die Sequenz- oder Vorrangsnummer zur Bestimmung der Priorität der Regel zurück.</p>
Erstellen einer Dienstkonfiguration.	<p>POST /api/v1/service-configs</p> <p>Die Dienstkonfigurations-API verwendet Eingabeparameter eines Dienstprofils, die zu schützende VM-Gruppe sowie die Sequenz- oder Vorrangsnummer, die auf die Regel angewendet werden muss.</p>
Löschen einer Dienstkonfiguration.	<p>DELETE /api/v1/service-configs/&lt;config-set-id&gt;</p> <p>Die Dienstkonfigurations-API löscht die auf die VM-Gruppe angewendete Konfiguration.</p>
Abrufen der Details einer bestimmten Konfiguration.	<p>GET /api/v1/service-configs/&lt;config-set-id&gt;</p> <p>Abrufen der Details einer bestimmten Konfiguration</p>
Aktualisieren einer Dienstkonfiguration.	<p>PUT /api/v1/service-configs/&lt;config-set-id&gt;</p> <p>Aktualisieren einer Dienstkonfiguration.</p>
Abrufen der effektiven Profile.	<p>GET /api/v1/service-configs/effective-profiles?resource_id=&lt;resource-id&gt;&amp;resource_type=&lt;resource-type&gt;</p> <p>Die Dienstkonfigurations-API gibt nur das Profil zurück, das auf eine bestimmte VM-Gruppe angewendet wird.</p>

Beachten Sie die folgenden Empfehlungen, um Regeln effizient zu verwalten:

- Legen Sie eine höhere Sequenznummer für eine Richtlinie fest, für die Regeln zuerst ausgeführt werden müssen. Auf der Benutzeroberfläche können Sie Richtlinien ziehen, um deren Priorität zu ändern.
- Ebenso sollten Sie eine höhere Sequenznummer für Regeln innerhalb jeder Richtlinie festlegen.
- Abhängig von der Anzahl der benötigten Regeln können Sie Regeln als Vielfaches von 2, 3, 4 oder sogar 10 getrennt positionieren. Zwei aufeinanderfolgende Regeln, die 10 Positionen voneinander entfernt sind, bieten Ihnen also mehr Flexibilität bei der Neuordnung von Regeln, ohne dass die Reihenfolge aller Regeln geändert werden muss. Wenn Sie beispielsweise nicht

vorhaben, viele Regeln zu definieren, können Sie festlegen, dass die Regeln 10 Positionen voneinander entfernt positioniert werden. Auf diese Weise erhält Regel 1 die Sequenznummer 1, Regel 2 die Sequenznummer 10, Regel 3 die Sequenznummer 20 usw. Diese Empfehlung bietet Flexibilität bei der effizienten Verwaltung von Regeln, damit nicht alle Regeln neu angeordnet werden müssen.

Intern ordnet die Guest Introspection diese Richtlinienregeln folgendermaßen.

Policy 1 ↔ Sequence Number 1 (1000)

- Rule 1 : Group 1 ↔ Service Profile ↔ Sequence Number 1 (1001)
- Rule 2 : Group 1 ↔ Service Profile ↔ Sequence Number 10 (1010)
- Rule 3 : Group 1 ↔ Service Profile ↔ Sequence Number 20 (1020)
- Rule 4 : Group 1 ↔ Service Profile ↔ Sequence Number 30 (1030)

Policy 2 ↔ Sequence Number 2 (2000)

- Rule 1 : Group 1 ↔ Service Profile ↔ Sequence Number 1 (2001)
- Rule 2 : Group 1 ↔ Service Profile ↔ Sequence Number 10 (2010)
- Rule 3 : Group 1 ↔ Service Profile ↔ Sequence Number 20 (2020)
- Rule 4 : Group 1 ↔ Service Profile ↔ Sequence Number 30 (2030)

Basierend auf den oben genannten Sequenznummern führt GI die Regeln der Richtlinie 1 vor den Regeln der Richtlinie 2 aus.

Es gibt aber auch Situationen, in denen die vorgesehenen Regeln nicht auf eine VM-Gruppe oder eine VM angewendet werden. Diese Konflikte müssen behoben werden, um die gewünschten Schutzebenen für Richtlinien anzuwenden.

## Sicherstellen der Funktionsfähigkeit von Partnerdiensten auf allen Hosts

Wenn die Partnerdienst-VM nicht funktionsfähig ist, sind die Gast-VMs nicht vor Malware geschützt.

Auf jedem Host müssen die folgenden Dienste oder Prozesse ausgeführt werden:

- Der EAM-Dienst ( ESXi Agency Manager) muss ausgeführt werden. Um dies sicherzustellen, muss Zugriff auf die folgende URL bestehen.

```
https://<vCenter_Server_IP_Address>/eam/mob
```

Führen Sie den Befehl aus, um zu überprüfen, ob ESXi Agency Manager online ist.

```
root> service-control --status vmware-eam
```

- Portgruppen, die mit automatisch von NSX-T Data Center erstellten SVMs verbunden sind, werden nicht gelöscht, da durch sie sichergestellt wird, dass SVM mit dem Schutz der Gast-VMs fortfährt.

```
https://<vCenter_Server_IP_Address>/ui
```

In vCenter Server navigieren Sie zur virtuellen Maschine, klicken auf die Registerkarte **Netzwerke** und überprüfen, ob **vmervice-vshield-pg** aufgelistet ist.

- Der Kontext-Multiplexer-Dienst (MUX) wird ausgeführt. Stellen Sie sicher, dass das VIB `nsx-context-mux` auf dem Host aktiv ist und ausgeführt wird.
- Verwaltungsschnittstelle: Die SVM-Schnittstelle, auf der NSX-T Data Center mit der Partnerdienstkonsole kommuniziert.
- Steuerungsschnittstelle: Die SVM-Schnittstelle, die die Kommunikation zwischen MUX und SVM ermöglicht. Eine Portgruppe wird erstellt, die MUX mit SVM verbindet. Diese Schnittstelle und Portgruppe werden benötigt, damit der Partnerdienst funktioniert.

## Probleme bei ESXi Agency Manager

In der Tabelle werden die ESXi Agency Manager-Probleme aufgelistet, die mithilfe der Schaltfläche „Beheben“ auf der Benutzeroberfläche von NSX Manager behoben werden können. NSX Manager wird über die Fehlerdetails informiert.

**Tabelle 10-11. Probleme bei ESXi Agency Manager**

Problem	Kategorie	Beschreibung
Auf Agent-OVF kann nicht zugegriffen werden	VM nicht bereitgestellt	Eine Agent-VM soll auf einem Host bereitgestellt werden. Die Agent-VM kann aber nicht bereitgestellt werden, da der ESXi Agent Manager nicht auf das OVF-Paket für den Agent zugreifen kann. Dies liegt daran, dass der Webserver, der das OVF-Paket bereitstellt, nicht verfügbar ist. Der Webserver gehört oft zur Lösung, die die Agency erstellt hat.
Nicht kompatible Hostversion	VM nicht bereitgestellt	Eine Agent-VM soll auf einem Host bereitgestellt werden. Der Agent kann aber nicht bereitgestellt werden, da er nicht kompatibel mit dem Host ist.
Nicht genügend Ressourcen	VM nicht bereitgestellt	Eine Agent-VM soll auf einem Host bereitgestellt werden. Die Agent-VM kann aber nicht bereitgestellt werden, da auf dem Host nicht genügend freie CPU- oder Arbeitsspeicherressourcen zur Verfügung stehen.

**Tabelle 10-11. Probleme bei ESXi Agency Manager (Fortsetzung)**

Nicht genügend Speicherplatz	VM nicht bereitgestellt	Eine Agent-VM soll auf einem Host bereitgestellt werden. Die Agent-VM kann aber nicht bereitgestellt werden, da der Agent-Datenspeicher des Hosts nicht genügend freien Speicherplatz aufweist.
Kein Agent-VM-Netzwerk	VM nicht bereitgestellt	Eine Agent-VM soll auf einem Host bereitgestellt werden. Der Agent kann aber nicht bereitgestellt werden, da das Agent-Netzwerk nicht auf dem Host konfiguriert wurde.
Ungültiges OVF-Format	VM nicht bereitgestellt	Eine Agent-VM soll auf einem Host bereitgestellt werden. Die Bereitstellung schlägt jedoch fehl, da bei der Bereitstellung des OVF-Pakets ein Fehler aufgetreten ist. Die Bereitstellung kann nur dann erfolgreich ausgeführt werden, wenn die Lösung, die das OVF-Paket bereitstellt, aktualisiert oder gepatcht wurde, um ein gültiges OVF-Paket für die Agent-VM bereitzustellen.
Fehlender Agent-IP-Pool	VM ausgeschaltet	Eine Agent-VM soll eingeschaltet werden. Die Agent-VM wird jedoch ausgeschaltet, weil im VM-Netzwerk des Agents keine IP-Adressen definiert sind.
Kein Agent-VM-Datenspeicher	VM ausgeschaltet	Eine Agent-VM soll auf einem Host bereitgestellt werden. Der Agent kann aber nicht bereitgestellt werden, da der Agent-Datenspeicher nicht auf dem Host konfiguriert wurde.
Kein benutzerdefiniertes Agent-VM-Netzwerk	Kein Agent-VM-Netzwerk	Eine Agent-VM soll auf einem Host bereitgestellt werden. Der Agent kann aber nicht bereitgestellt werden, da das Agent-Netzwerk nicht auf dem Host konfiguriert wurde. Der Host muss zu einem der Netzwerke hinzugefügt werden, die im benutzerdefinierten Agent-VM-Netzwerk aufgelistet sind.
Kein benutzerdefinierter Agent-VM-Datenspeicher	Kein Agent-VM-Datenspeicher	Eine Agent-VM soll auf einem Host bereitgestellt werden. Der Agent kann aber nicht bereitgestellt werden, da der Agent-Datenspeicher nicht auf dem Host konfiguriert wurde. Der Host muss zu einem der Datenspeicher hinzugefügt werden, die im benutzerdefinierten Agent-VM-Datenspeicher aufgelistet sind.

**Tabelle 10-11. Probleme bei ESXi Agency Manager (Fortsetzung)**

Verwaiste Agency	Agency-Fehler	Die Lösung, die die Agency erstellt hat, ist nicht mehr mit dem vCenter Server registriert.
Verwaister DvFilter-Switch	Hostfehler	Auf einem Host ist ein dvFilter-Switch vorhanden, aber keine Agents auf dem Host benötigen den dvFilter. Dies ist in der Regel der Fall, wenn eine Hostverbindung bei Änderung einer Agency-Konfiguration getrennt wird.
Unbekannte Agent-VM	Hostfehler	Im vCenter Server-Bestand wurde eine Agent-VM gefunden, die zu keiner Agency in dieser vSphere ESX Agent Manager-Serverinstanz gehört.
Ungültige OVF-Eigenschaft	VM-Fehler	Eine Agent-VM muss eingeschaltet werden, aber eine OVF-Eigenschaft fehlt oder weist einen ungültigen Wert auf.
VM beschädigt	VM-Fehler	Eine Agent-VM ist beschädigt.
VM verwaist	VM-Fehler	Ein Agent-VM ist auf einem Host vorhanden, der Host gehört aber nicht mehr zum Bereich für die Agency. Dies ist in der Regel der Fall, wenn eine Hostverbindung bei Änderung der Agency-Konfiguration getrennt wird.
VM bereitgestellt	VM-Fehler	Eine Agent-VM soll von einem Host entfernt werden, wurde aber nicht entfernt. Der genaue Grund, weshalb vSphere ESX Agent Manager die Agent-VM nicht entfernen konnte, wie z. B. der Host befindet sich im Wartungs- oder Standby-Modus bzw. ist ausgeschaltet.
VM ausgeschaltet	VM-Fehler	Eine Agent-VM soll eingeschaltet werden, wurde aber ausgeschaltet.
VM eingeschaltet	VM-Fehler	Eine Agent-VM soll ausgeschaltet werden, wurde aber eingeschaltet.
VM angehalten	VM-Fehler	Eine Agent-VM soll eingeschaltet werden, wurde aber angehalten.
Falscher VM-Ordner	VM-Fehler	Eine Agent-VM soll in einem bestimmten Ordner der Agent-VM gespeichert werden, befindet sich aber in einem anderen Ordner.

**Tabelle 10-11. Probleme bei ESXi Agency Manager (Fortsetzung)**

Falscher VM-Ressourcenpool	VM-Fehler	Eine Agent-VM soll in einem bestimmten Ressourcenpool der Agent-VM gespeichert sein, befindet sich aber in einem anderen Ressourcenpool.
VM nicht bereitgestellt	Agent-Fehler	Eine Agent-VM soll auf einem Host bereitgestellt werden, wurde aber nicht bereitgestellt. Die genauen Gründe, weshalb ESXi Agent Manager den Agent nicht bereitstellen konnte, wie z. B. keine Zugriffsmöglichkeit auf das OVF-Paket für den Agent oder eine fehlende Hostkonfiguration. Dieses Problem kann auch auftreten, wenn die Agent-VM explizit vom Host gelöscht wird.

Im nächsten Schritt konfigurieren Sie Endpoint-Schutz für VM-Gruppen. Siehe [Konfigurieren von Endpoint-Schutz](#).

## Konfliktlösung bei Endpoint-Richtlinien

Stellen Sie sich ein Szenario vor, in dem zwei Richtliniendomänen vorhanden sind, die beide aus mehreren Regeln bestehen. Als Administrator wissen Sie nie genau, welche VMs letztlich Mitglieder einer Gruppe werden, da VMs basierend auf dynamischen Mitgliedschaftskriterien (z. B. Name des Betriebssystems, Name des Computers, Benutzer, Tagging) mit einer Gruppe verknüpft werden.

**Hinweis** Das Domänenobjekt ist eine experimentelle Funktion in NSX-T Data Center 2.4, die in NSX-T Data Center 2.4.1 nicht verfügbar ist. In NSX-T Data Center 2.4.1 ist es nicht erforderlich, eine Domäne zu erstellen.

Konflikte entstehen in folgenden Szenarien:

- Eine VM ist Bestandteil zweier Gruppen, wobei jede Gruppe von einem anderen Profil geschützt wird.
- Eine Partnerdienst-VM ist mit mehreren Dienstprofilen verknüpft.
- Eine unerwartete Regel wurde auf einer Gast-VM ausgeführt oder eine Regel wurde auf einer Gast-VM nicht ausgeführt.
- Richtlinienregeln oder Domänen wird keine Sequenznummer zugewiesen.

Tabelle 10-12. Lösen von Richtlinienkonflikten

Szenario	Erwarteter Ablauf für Endpoint-Schutz	Lösung
Eine VM wird Mitglied in mehreren Gruppen, wobei jede Gruppe von einem anderen Dienstprofiltyp geschützt wird. Erwarteter Schutz wurde nicht auf die VM angewendet.	<p>Eine mit einem Mitgliedschaftskriterium erstellte VM-Gruppe bedeutet, dass VMs dynamisch zur Gruppe hinzugefügt werden. In einem solchen Fall kann die gleiche VM mehreren Gruppen angehören. Es ist nicht möglich, im Voraus zu bestimmen, zu welcher Gruppe die VM gehören wird, da die VM über die Mitgliedschaftskriterien dynamisch in die Gruppe eingetragen wird. Stellen Sie sich vor, dass VM-1 zu Gruppe 1 und Gruppe 2 gehört.</p> <ul style="list-style-type: none"> <li>■ Regel 1: Auf Gruppe 1 (nach Betriebssystemname) wird „Gold“ (Dienstprofil) mit Sequenznummer 1 angewendet</li> <li>■ Regel 2: Auf Gruppe 2 (nach Tag) wird „Platin“ (Dienstprofil) mit Sequenznummer 10 angewendet</li> </ul> <p>Die Richtlinie für Endpoint-Schutz führt das Dienstprofil „Gold“, nicht aber das Dienstprofil „Platin“ auf VM 1 aus.</p>	<p>Ändern Sie die Sequenznummer von Regel 2 so, dass sie vor Regel 1 ausgeführt wird.</p> <ul style="list-style-type: none"> <li>■ Ziehen Sie auf der Benutzeroberfläche von NSX-T Policy Manager Regel 2 vor Regel 1 in der Regelliste.</li> <li>■ Fügen Sie mithilfe der NSX-T Policy Manager-API manuell eine höhere Sequenznummer für Regel 2 hinzu.</li> </ul>
Eine Regel ordnet dasselbe Dienstprofil zum Schutz von zwei VM-Gruppen zu. Der Endpoint-Schutz führt die Regel nicht in der zweiten VM-Gruppe aus.	<p>Der Endpoint-Schutz führt nur das erste Dienstprofil auf der VM aus, da dasselbe Dienstprofil nicht erneut auf alle anderen Regeln für Richtlinien oder Domänen angewendet werden kann. Stellen Sie sich vor, dass VM-1 zu Gruppe 1 und Gruppe 2 gehört.</p> <p>Regel 1: Auf Gruppe 1 (nach Betriebssystemname) wird „Gold“ (Dienstprofil) angewendet</p> <p>Regel 2: Auf Gruppe 2 (nach Tag) wird „Gold“ (Dienstprofil) angewendet</p>	<ul style="list-style-type: none"> <li>■ Fügen Sie Gruppe 2 zu Regel 1 hinzu. (Regel 1: Gruppe 1, Profil 1 wird auf Gruppe 2 angewendet)</li> </ul>

## Quarantäne-VMs

Nachdem Regeln auf der Grundlage der von Partnern festgelegten Schutzstufe und des von ihnen festgelegten Tags auf VM-Gruppen angewendet wurden, können VMs vorhanden sein, die als infiziert identifiziert wurden und die darum isoliert werden müssen.


Partner kennzeichnen infizierte VMs mithilfe der API mit dem Tag `virus_found=true`. An betroffene VMs wird das Tag `virus_found=true` angehängt.

Als Administrator können Sie eine vordefinierte Quarantänegruppe basierend auf dem Tag mit dem Wert `virus_found=true` erstellen, sodass die Gruppe mit infizierten VMs befüllt wird, sobald diese mit dem Tag gekennzeichnet werden. Als Administrator können Sie wahlweise bestimmte Firewallregeln für die Quarantänegruppe festlegen. Sie können Firewallregeln für die Quarantänegruppe festlegen. Sie können beispielsweise den gesamten eingehenden und ausgehenden Datenverkehr aus der Quarantänegruppe blockieren.

## Überprüfen des Integritätsstatus der Dienstinstanzen

Der Integritätsstatus einer Dienstinstanz wird hängt von zahlreichen Faktoren ab: dem Status der Partnerlösung, der Konnektivität zwischen Guest Introspection-Agent (Context Multiplexer) und Context Engine (Ops Agent) sowie der Verfügbarkeit von Guest Introspection-Agent-Informationen, SVM-Protokollinformationen bei 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 > Dienstbereitstellungen > Dienstinstanzen** aus.
- 3 Klicken Sie in der Spalte „Integritätsstatus“ auf , um die Integrität der Dienstinstanz zu ermitteln.

**Tabelle 10-13. Integritätsstatus der Drittanbieter-Dienstinstanz**

Parameter	Beschreibung
Integritätsstatus empfangen	Der neueste Zeitstempel, bei dem NSX Manager die Integritätsstatusdetails der Dienstinstanz empfangen hat.
Lösungsstatus	Status der Partnerlösung, die auf einer SVM ausgeführt wird. Der Status „AKTIV“ zeigt an, dass die Partnerlösung korrekt ausgeführt wird.
Konnektivität zwischen NSX-T Data Center Guest Introspection-Agent und NSX-T Data Center Ops-Agent	Der Status ist „AKTIV“, wenn der Guest Introspection-Agent (Kontext-Multiplexer) für NSX-T Data Center mit dem Ops-Agent verbunden ist (einschließlich der Context Engine). Der Kontext-Multiplexer leitet die Integritätsinformationen der SVMs an die Context Engine weiter. Sie verwenden außerdem eine gemeinsame SVM-VM-Konfiguration, um zu ermitteln, welche Gast-VMs durch die SVM geschützt werden.
Dienst-VM-Protokollversion	Intern zur Problembehandlung verwendete Transportprotokollversion.
Informationen zum NSX-T Data Center Guest Introspection-Agent	Stellt die Kompatibilität der Protokollversion zwischen NSX-T Data Center Guest Introspection-Agent und SVM dar.

- 4 Wird als Integritätsstatus Aktiv angegeben (grüne Statusanzeige) und werden in der Partnerkonsole alle Gast-VMs als geschützt angezeigt werden, lautet der Integritätsstatus der Dienstinstanz Aktiv.



- 5 Wird als Integritätsstatus zwar Aktiv angegeben (grüne Statusanzeige), doch werden die Gast-VMs in der Partnerkonsole als ungeschützt angezeigt, müssen Sie den folgenden Schritt ausführen:
  - a Wenden Sie sich an den VMware Support, um das Problem zu beheben. Der Integritätsstatus der Dienstinstanz ist möglicherweise „Inaktiv“, wird aber von der NSX Manager-Benutzeroberfläche nicht korrekt wiedergegeben.
- 6 Wenn der Integritätsstatus Inaktiv ist (rote Statusanzeige), ist mindestens ein für die Integrität der Dienstinstanz notwendiger Faktor nicht erfüllt.

Tabelle 10-14. Problembehandlung für Integritätsstatus

Integritätsstatus-Attribut	Lösung
Der Lösungsstatus ist Inaktiv oder Nicht verfügbar.	<ol style="list-style-type: none"> <li>1 Stellen Sie sicher, dass der Status der Dienstbereitstellung Aktiv ist (grüne Statusanzeige). Bei Fehlern finden Sie weiterführende Informationen unter <a href="#">Sicherstellen der Funktionsfähigkeit von Partnerdiensten auf allen Hosts</a>.</li> <li>2 Vergewissern Sie sich, dass mindestens eine Gast-VM im betroffenen Host durch eine Endpoint-Schutzrichtlinie geschützt ist.</li> <li>3 Überprüfen Sie in der Partnerkonsole, ob der Lösungsdienst auf der SVM auf dem Host ausgeführt wird. Weitere Informationen finden Sie in der Partnerdokumentation.</li> <li>4 Wenn das Problem durch keinen der oben genannten Schritte behoben wird, wenden Sie sich an den VMware Support.</li> </ol>
Konnektivität zwischen NSX-T Data Center Guest Introspection-Agent und NSX-T Data Center Ops-Agent ist Inaktiv.	<ol style="list-style-type: none"> <li>1 Stellen Sie sicher, dass der Status der Dienstbereitstellung Aktiv ist (grüne Statusanzeige). Bei Fehlern finden Sie weiterführende Informationen unter <a href="#">Sicherstellen der Funktionsfähigkeit von Partnerdiensten auf allen Hosts</a>.</li> <li>2 Vergewissern Sie sich, dass mindestens eine Gast-VM im betroffenen Host durch eine Endpoint-Schutzrichtlinie geschützt ist.</li> <li>3 Überprüfen Sie in der Partnerkonsole, ob der Lösungsdienst auf der SVM auf dem Host ausgeführt wird. Weitere Informationen finden Sie in der Partnerdokumentation.</li> <li>4 Wenn das Problem durch keinen der oben genannten Schritte behoben wird, wenden Sie sich an den VMware Support.</li> </ol>

Tabelle 10-14. Problembehandlung für Integritätsstatus (Fortsetzung)

Integritätsstatus-Attribut	Lösung
Dienst-VM-Protokollversion ist Nicht verfügbar.	<ol style="list-style-type: none"> <li>1 Stellen Sie sicher, dass der Status der Dienstbereitstellung Aktiv ist (grüne Statusanzeige). Bei Fehlern finden Sie weiterführende Informationen unter <a href="#">Sicherstellen der Funktionsfähigkeit von Partnerdiensten auf allen Hosts</a>.</li> <li>2 Vergewissern Sie sich, dass mindestens eine Gast-VM im betroffenen Host durch eine Endpoint-Schutzrichtlinie geschützt ist.</li> <li>3 Überprüfen Sie in der Partnerkonsole, ob der Lösungsdienst auf der SVM auf dem Host ausgeführt wird. Weitere Informationen finden Sie in der Partnerdokumentation.</li> <li>4 Wenn das Problem durch keinen der oben genannten Schritte behoben wird, wenden Sie sich an den VMware Support.</li> </ol>
Informationen zum NSX-T Data Center Guest Introspection-Agent sind Nicht verfügbar.	Wenden Sie sich an den VMware Support.

## Löschen von Partnerdiensten

Führen Sie zum Löschen von Partnerdiensten einen API-Aufruf durch. Bevor Sie den API-Aufruf zum Löschen von Partnerdiensten oder SVMs durchführen, die auf einem Host bereitgestellt werden, müssen Sie auf der NSX Manager-Benutzeroberfläche folgendermaßen vorgehen.

So löschen Sie Partnerdienste:

### Verfahren

- 1 Entfernen Sie EPP-Regeln, die auf VM-Gruppen angewendet werden, die auf dem Host ausgeführt werden.
- 2 Entfernen Sie den Dienstprofilschutz, der auf VM-Gruppen angewendet wird.
- 3 Zum Entfernen einer Lösung, die SVMs an den Partner Service Manager bindet, führen Sie folgenden API-Aufruf durch.

```
/DEL https://<NSX_Manager_IPaddress>/api/v1/serviceinsertion/services/{{service_id}}/solution-
configs/<solution-config-id>
```

- 4 Zum Entfernen der Dienstbereitstellung führen Sie folgenden API-Aufruf durch.

```
/DEL https://<NSX_Manager_IPaddress>/api/v1/serviceinsertion/services/<service-id>/service-
deployments/<service-deployment-id>
```

Weitere Informationen zu API-Parametern finden Sie im *Handbuch für die NSX-T Data Center-API*.

Sie können Dienste, Gruppen, Domänen und Kontextprofile für die NSX-T Data Center-Bestandsliste konfigurieren.

Beachten Sie, dass das Domänenobjekt eine experimentelle Funktion in NSX-T Data Center 2.4 ist, aber in NSX-T Data Center 2.4.1 nicht verfügbar ist.

Dieses Kapitel enthält die folgenden Themen:

- [Hinzufügen einer Domäne](#)
- [Hinzufügen eines Diensts](#)
- [Hinzufügen einer Gruppe](#)
- [Hinzufügen eines Kontextprofils](#)

## Hinzufügen einer Domäne

Eine Domäne ist eine logische Sammlung von Arbeitslasten und Objekten, die einem gemeinsamen Geschäftsziel dienen. Durch die Erstellung von Domänen wird die Verwaltung von Objekten in Ihrer Umgebung vereinfacht.

---

**Hinweis** Das Domänenobjekt ist eine experimentelle Funktion in NSX-T Data Center 2.4, die in NSX-T Data Center 2.4.1 nicht verfügbar ist.

---

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Bestand > Domänen**.
- 3 Klicken Sie auf **Domäne hinzufügen**.
- 4 Geben Sie einen Namen und optional eine Beschreibung ein.
- 5 Klicken Sie auf **Speichern** und fahren Sie mit der Konfiguration der Gruppen fort.
- 6 Klicken Sie auf **Gruppe hinzufügen**.
- 7 Geben Sie einen Namen ein.

**8** Klicken Sie auf **Mitglieder festlegen**.

Sie können Mitglieder mithilfe einer oder mehrerer der folgenden Methoden auswählen:

- Angeben von Mitgliedskriterien
- Auswählen von Mitgliedern
- Eingeben von IP- oder MAC-Adressen
- Auswählen von AD-Gruppen

**9** Klicken Sie auf **Kriterien hinzufügen**, um Mitglieder durch Angabe von Mitgliedschaftskriterien auszuwählen.**10** Klicken Sie zur Auswahl von Objekten auf die Registerkarte **Mitglieder**.**11** Klicken Sie zur Eingabe von IP- oder MAC-Adressen auf die Registerkarte **IP-/MAC-Adressen**.**12** Klicken Sie zur Auswahl von AD-Gruppen auf die Registerkarte **AD-Gruppen**.**13** Klicken Sie auf **Speichern**.

## Hinzufügen eines Diensts

Sie können einen Dienst konfigurieren und Parameter zum Abgleichen des Netzwerkdatenverkehrs angeben, z. B. eine Port- und Protokollpaarbildung.

Sie können unter Verwendung eines Diensts auch bestimmte Datenverkehrstypen in Firewallregeln zulassen oder blockieren. Nach dem Erstellen eines Diensts kann der Typ nicht mehr geändert werden. Bestimmte Dienste sind vordefiniert und können weder geändert noch gelöscht werden.

### Verfahren

- 1** Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2** Wählen Sie **Bestand > Dienste**.
- 3** Klicken Sie auf **Neuen Dienst hinzufügen**.
- 4** Geben Sie einen Namen ein.
- 5** Klicken Sie auf **Diensteinträge festlegen**. Wählen Sie einen vordefinierten Dienst in der Liste aus oder klicken Sie auf **Neuen Diensteintrag hinzufügen**.
- 6** Wählen Sie für einen neuen Dienst einen Diensttyp aus und geben Sie zusätzliche Eigenschaften an.  
  
Zu den verfügbaren Typen gehören **IP**, **IGMP**, **ICMPv4**, **ICMPv6**, **ALG**, **TCP**, **UDP** und **Ether**.
- 7** Klicken Sie auf **Speichern**.
- 8** (Optional) Geben Sie einen Geltungsbereich ein.
- 9** Klicken Sie auf **Speichern**.

## Hinzufügen einer Gruppe

Gruppen enthalten verschiedene Objekte, die sowohl statisch als auch dynamisch hinzugefügt werden und als Quell- und Zielfeld einer Firewallregel verwendet werden können.

Gruppen können so konfiguriert werden, dass sie eine Kombination aus virtuellen Maschinen, IP Sets, MAC Sets, logischen Ports, logischen Switches, AD-Benutzergruppen und anderen verschachtelten Gruppen enthalten. Gruppen können auf Basis von Tags, Maschinen-, Betriebssystem- oder Computernamen dynamisch aufgenommen werden.

Eine einzelne ID-basierte Gruppe kann innerhalb einer Firewallregel verwendet werden. Wenn IP- und ID-basierte Gruppen für die Quelle benötigt werden, erstellen Sie zwei separate Firewallregeln.

Gruppen, die nur aus IP-Adressen bestehen, MAC-Adressen oder Active Directory-Gruppen können im Textfeld **Angewendet auf** nicht verwendet werden.

---

**Hinweis** Wenn ein Host einem vCenter Server hinzugefügt oder daraus entfernt wird, ändert sich die externe ID der VMs auf dem Host. Wenn eine VM ein statisches Mitglied einer Gruppe ist und sich die externe ID der VM ändert, zeigt die NSX Manager-Benutzeroberfläche die VM nicht mehr als Mitglied der Gruppe an. Die API, die die Gruppen auflistet, zeigt die VM jedoch weiterhin mit ihrer ursprünglichen ID in der Gruppe an. Wenn Sie eine VM als statisches Mitglied einer Gruppe hinzufügen und sich die externe ID der VM ändert, müssen Sie die VM erneut mit der neuen externen ID hinzufügen. Sie können auch dynamische Mitgliedschaftskriterien verwenden, um dieses Problem zu vermeiden.

---

### Verfahren

- 1 Wählen Sie im Navigationsbereich die Option **Bestand > Gruppen** aus.
- 2 Klicken Sie auf **GRUPPE HINZUFÜGEN**.
- 3 Geben Sie einen Gruppennamen ein.
- 4 (Erforderlich) Wählen Sie eine Domäne im Dropdown-Menü aus oder verwenden Sie die Standarddomäne. Bei einer Domäne handelt es sich um ein logisches Konstrukt, das aus einer Sicherheitszone und allen Regeln und Gruppen besteht. Die Standarddomäne stellt die gesamte NSX-Umgebung dar.

Beachten Sie, dass das Domänenobjekt eine experimentelle Funktion in NSX-T Data Center 2.4 ist, die in NSX-T Data Center 2.4.1 nicht verfügbar ist. In NSX-T Data Center 2.4.1 ist es nicht erforderlich, eine Domäne zu erstellen.

- 5 (Optional) Klicken Sie auf **Mitglieder festlegen**.

Für jedes Mitgliedschaftskriterium können Sie bis zu fünf Regeln angeben, die mit dem logischen Operator AND kombiniert werden. Das verfügbare Mitgliedskriterium kann auf Folgendes angewendet werden:

- **Logischer Port** – kann ein Tag und optional den Geltungsbereich angeben.
- **Logischer Switch** – kann ein Tag und optional den Geltungsbereich angeben.

- **Virtuelle Maschine** – kann einen Namen, ein Tag, den Namen des Computerbetriebssystems oder einen Computernamen angeben, der bzw. das einer bestimmten Zeichenfolge entspricht, diese enthält, mit ihr beginnt oder endet bzw. nicht mit ihr übereinstimmt.
  - **Transportknoten** – kann einen Knotentyp angeben, der einem Edge-Knoten oder einem Hostknoten entspricht.
- 6 (Optional) Klicken Sie auf **Mitglieder**, um Mitglieder auszuwählen.
- Die verfügbaren Mitgliedstypen sind:
- **Gruppe**
  - **Segment**
  - **Segment-Port**
  - **Virtuelle Netzwerkschnittstelle**
  - **Virtuelle Maschine**
- 7 Klicken Sie auf **IP-/MAC-Adressen**, um IP- und MAC-Adressen als Gruppenmitglieder hinzuzufügen.
- 8 Klicken Sie auf **AD-Gruppen**, um Active Directory-Gruppen hinzuzufügen. Gruppen mit Active Directory-Mitgliedern können im Quell- und Zielfeld einer Regel für verteilte Firewalls sowie für identitätsbasierte Firewalls verwendet werden und müssen die einzigen Mitglieder in der Gruppe sein. Eine Gruppe darf beispielsweise nicht gleichzeitig die Mitglieder ADGroup und IPSet enthalten.
- 9 Klicken Sie auf **Anwenden**.
- Gruppen werden mit einer Option zum Anzeigen der Mitglieder und einer Angabe zu deren Verwendungsort aufgeführt.

## Hinzufügen eines Kontextprofils

Kontextprofile verwenden APP-ID-Attribute der Schicht 7 für die Verwendung in Regeln für eine verteilte Firewall. Nach der Definition eines Kontextprofils kann es in einer oder mehreren Regeln für verteilte Firewalls verwendet werden.

Es gibt zwei Attribute für die Verwendung in Kontextprofilen: APP-ID und Domänenname (FQDN). Ausgewählte APP-IDs weisen darüber hinaus die Unterattribute TLS\_Version und CIPHER\_SUITE auf. Sowohl die APP-ID als auch der Domänenname können in einem einzelnen Kontextprofil verwendet werden. Mehrere APP-IDs können im selben Profil verwendet werden. Eine APP-ID mit Unterattributen kann verwendet werden. Unterattribute werden gelöscht, wenn mehrere APP-ID-Attribute in einem einzelnen Profil verwendet werden.

### Verfahren

- 1 Wählen Sie **Bestand > Kontextprofile**.

- 2 Klicken Sie auf **Neues Kontextprofil hinzufügen**.
- 3 Geben Sie einen **Profilnamen** ein.
- 4 Klicken Sie in der Spalte „Attribute“ auf **Festlegen**.
- 5 Wählen Sie ein Attribut aus oder klicken Sie auf **Attribut hinzufügen** und wählen Sie **App-ID** oder **Domänenname (FQDN)** aus.
- 6 Wählen Sie ein oder mehrere Attribute aus.
- 7 (Optional) Wenn Sie ein Attribut mit Unterattributen, wie z. B. SSL oder CIFS, ausgewählt haben, klicken Sie in der Spalte „Unterattribute/Werte“ auf **Festlegen**.
  - a Klicken Sie auf **Unterattribut hinzufügen** und wählen Sie im Dropdown-Menü eine Kategorie für das Unterattribut aus.
  - b Wählen Sie ein oder mehrere Unterattribute aus.
  - c Klicken Sie auf **Hinzufügen**. Ein weiteres Unterattribut kann hinzugefügt werden, indem Sie auf **Unterattribut hinzufügen** klicken.
  - d Klicken Sie auf **Übernehmen**.
- 8 Klicken Sie auf **Hinzufügen**.
- 9 (Optional) Zum Hinzufügen eines weiteren Attributtyps klicken Sie erneut auf **Attribut hinzufügen**.
- 10 Klicken Sie auf **Übernehmen**.
- 11 (Optional) Geben Sie eine Beschreibung ein.
- 12 (Optional) Geben Sie ein Tag ein.
- 13 Klicken Sie auf **Speichern**.

#### Nächste Schritte

Wenden Sie dieses Kontextprofil auf eine Layer 7-Regel für verteilte Firewalls an.

In den Themen in diesem Abschnitt wird gezeigt, wie Sie die Überwachung mithilfe von IPFIX-Profilen (Internet Protocol Flow Information Export) für die Firewall und Switches konfigurieren und wie Sie einen IPFIX-Collector konfigurieren.

Dieses Kapitel enthält die folgenden Themen:

- [Hinzufügen eines Firewall-IPFIX-Profiles](#)
- [Hinzufügen eines Switch-IPFIX-Profiles](#)
- [Hinzufügen eines IPFIX-Collectors](#)
- [Hinzufügen eines Port-Mirroring-Profiles](#)
- [Erweiterte Überwachungstools](#)

## Hinzufügen eines Firewall-IPFIX-Profiles

Sie können IPFIX-Profile für Firewalls konfigurieren.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Tools > Überwachungsprofile > IPFIX**.
- 3 Klicken Sie auf die Registerkarte **Firewall-IPFIX-Profil**.
- 4 Klicken Sie auf **Firewall-IPFIX-Profil hinzufügen**.
- 5 Geben Sie die folgenden Details ein.

Einstellung	Beschreibung
Name und Beschreibung	<p>Geben Sie einen Namen und optional eine Beschreibung ein.</p> <p><b>Hinweis</b> Wenn Sie ein globales Profil erstellen möchten, nennen Sie das Profil <b>Global</b>. Ein globales Profil kann nicht in der Benutzeroberfläche bearbeitet oder gelöscht werden, aber Sie können dies mit NSX-T Data Center-APIs tun.</p>
Zeitüberschreitung bei aktivem Flow-Export (Minuten)	<p>Die Zeitspanne, nach der eine Zeitüberschreitung bei einem Flow auftritt, selbst wenn weitere mit dem Flow verknüpfte Pakete eingeht. Der Standardwert beträgt 1.</p>



Einstellung	Beschreibung
Beobachtungsdomänen-ID	Dieser Parameter gibt an, aus welcher Beobachtungsdomäne die Netzwerk-Flows stammen. Die Standardeinstellung ist 0 und verweist auf keine bestimmte Beobachtungsdomäne.
Collector-Konfiguration	Wählen Sie in der Dropdown-Liste einen Collector aus.
Priorität	Dieser Parameter dient zur Behebung von Konflikten, wenn mehrere Profile anwendbar sind. IPFIX-Exporter verwendet nur das Profil mit der höchsten Priorität. Ein niedrigerer Wert bedeutet eine höhere Priorität.

6 Klicken Sie auf **Speichern** und dann auf **Ja**, um das Profil weiter zu konfigurieren.

7 Klicken Sie auf **Angewendet auf**, um das Profil auf Objekte anzuwenden.

Wählen Sie mindestens eines der Objekte aus.

8 Klicken Sie auf **Speichern**.

## Hinzufügen eines Switch-IPFIX-Profiles

Sie können IPFIX-Profile für Switches (auch als „Segmente“ bezeichnet) konfigurieren.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Tools > Überwachungsprofile > IPFIX**.
- 3 Klicken Sie auf die Registerkarte **Switch-IPFIX-Profil**.
- 4 Klicken Sie auf **Switch-IPFIX-Profil hinzufügen**.
- 5 Geben Sie die folgenden Details ein.

Einstellung	Beschreibung
Name und Beschreibung	Geben Sie einen Namen und optional eine Beschreibung ein.  <b>Hinweis</b> Wenn Sie ein globales Profil erstellen möchten, nennen Sie das Profil <b>Global</b> . Ein globales Profil kann nicht in der Benutzeroberfläche bearbeitet oder gelöscht werden, aber Sie können dies mit NSX-T Data Center-APIs tun.
Aktive Zeitüberschreitung (Sekunden)	Die Zeitspanne, nach der eine Zeitüberschreitung bei einem Flow auftritt, selbst wenn weitere mit dem Flow verknüpfte Pakete eingehen. Der Standardwert beträgt 300.
Überschreitung Leerlaufzeit (Sekunden)	Die Zeitspanne, nach der eine Zeitüberschreitung bei einem Flow auftritt, wenn keine weiteren mit dem Flow verknüpften Pakete eingehen (nur ESXi, KVM bestimmt die Zeitüberschreitung für alle Flows basierend auf der aktiven Zeitüberschreitung) Der Standardwert beträgt 300.

Einstellung	Beschreibung
Paket-Sampling-Wahrscheinlichkeit (%)	Der Prozentsatz der Pakete, die abgetastet werden (ungefähr). Wenn Sie diese Einstellung erhöhen, kann sich dies auf die Leistung der Hypervisors und Collectors auswirken. Wenn alle Hypervisors mehr IPFIX-Pakete an den Collector senden, kann der Collector möglicherweise nicht alle Pakete erfassen. Indem Sie die Wahrscheinlichkeit auf dem Standardwert von 0,1 % belassen, bleibt die Auswirkung auf die Leistung gering.
Collector-Konfiguration	Wählen Sie in der Dropdown-Liste einen Collector aus.
Priorität	Dieser Parameter dient zur Behebung von Konflikten, wenn mehrere Profile anwendbar sind. IPFIX-Exporter verwendet nur das Profil mit der höchsten Priorität. Ein niedrigerer Wert bedeutet eine höhere Priorität.
Max. Flows	Die maximale Anzahl der in einer Bridge zwischengespeicherten Flows (nur KVM, unter ESXi nicht konfigurierbar). Der Standardwert beträgt 16384.
Beobachtungsdomänen-ID	Mit der Beobachtungsdomänen-ID wird festgelegt, aus welcher Beobachtungsdomäne die Netzwerk-Flows stammen. Geben Sie 0 ein, um keine bestimmte Beobachtungsdomäne anzugeben.

6 Klicken Sie auf **Speichern** und dann auf **Ja**, um das Profil weiter zu konfigurieren.

7 Klicken Sie auf **Angewendet auf**, um das Profil auf Objekte anzuwenden.

Wählen Sie mindestens eines der Objekte aus.

8 Klicken Sie auf **Speichern**.

## Hinzufügen eines IPFIX-Collectors

Sie können IPFIX-Collectors für Firewalls und Switches konfigurieren.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Tools > Überwachungsprofile > IPFIX**.
- 3 Klicken Sie auf die Registerkarte **Collectors**.
- 4 Wählen Sie **Neuen Collector hinzufügen > IPFIX-Switch** oder **Neuen Collector hinzufügen > IPFIX-Firewall** aus.
- 5 Geben Sie einen Namen ein.
- 6 Geben Sie die IP-Adressen und Ports von bis zu vier Collectors ein. Sowohl IPv4- als auch IPv6-Adressen werden unterstützt.
- 7 Klicken Sie auf **Speichern**.

## Hinzufügen eines Port-Mirroring-Profiles

Sie können Port-Mirroring-Profile für Port-Mirroring-Sitzungen konfigurieren.

Beachten Sie, dass die logische SPAN nur für Overlay-Segmente und nicht für VLAN-Segmente unterstützt wird.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Tools > Port-Mirroring**.
- 3 Wählen Sie **Profil hinzufügen > Remote-L3 Span** oder **Profil hinzufügen > Logische Span** aus.
- 4 Geben Sie einen Namen und optional eine Beschreibung ein.
- 5 Vervollständigen Sie die folgenden Profildetails.

Sitzungstyp	Parameter
Remote-L3 SPAN	<ul style="list-style-type: none"> <li>■ <b>Richtung</b> – wählen Sie <b>Bidirektional</b>, <b>Ingress</b> oder <b>Egress</b> aus.</li> <li>■ <b>Snap-Länge</b> – geben Sie die Anzahl der Byte zur Erfassung aus einem Paket an.</li> <li>■ <b>Kapselungstyp</b> – wählen Sie <b>GRE</b>, <b>ERSPAN TWO</b> oder <b>ERSPAN THREE</b> aus.</li> <li>■ <b>GRE-Schlüssel</b> – geben Sie einen GRE-Schlüssel an, wenn Sie für den Kapselungstyp die Option <b>GRE</b> ausgewählt haben.</li> <li>■ <b>ERSPAN-ID</b> – geben Sie eine ERSPAN-ID an, wenn Sie für den Kapselungstyp <b>ERSPAN TWO</b> oder <b>ERSPAN THREE</b> ausgewählt haben.</li> </ul>
Logische SPAN	<ul style="list-style-type: none"> <li>■ <b>Richtung</b> – wählen Sie <b>Bidirektional</b>, <b>Ingress</b> oder <b>Egress</b> aus.</li> <li>■ <b>Snap-Länge</b> – geben Sie die Anzahl der Byte zur Erfassung aus einem Paket an.</li> </ul>

- 6 Klicken Sie auf **Festlegen** in der Spalte **Ziel**, um ein Ziel festzulegen.
- 7 Klicken Sie auf **Speichern** und dann auf **Ja**, um das Profil weiter zu konfigurieren.
- 8 Klicken Sie auf **Quellen** und dann auf **Festlegen**, um Quellen festlegen.

Für „Logische SPAN“ lauten die verfügbaren Quellen **Segment-Port**, **Gruppe mit virtuellen Maschinen** und **Gruppe mit virtuellen Netzwerkschnittstellen**.

Für „Remote-L3 SPAN“ lauten die verfügbaren Quellen **Segment**, **Segment-Port**, **Gruppe mit virtuellen Maschinen** und **Gruppe mit virtuellen Netzwerkschnittstellen**.

- 9 Klicken Sie auf **Speichern**.

## Erweiterte Überwachungstools

NSX-T unterstützt erweiterte Überwachungsmethoden, einschließlich der Anzeige von Portverbindungen, Traceflow, Portspiegelung, Aktivitätsüberwachung usw.

### Anzeigen der Portverbindungsinformationen

Mithilfe des Tools für die Portverbindung können Sie auf schnelle Weise die Verbindung zwischen zwei VMs visualisieren und eventuelle Fehler beheben.

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk und Sicherheit – Erweitert > Tools > Portverbindung** aus.
- 3 Wählen Sie eine VM aus dem Dropdown-Menü **Virtuelle Quellmaschine** aus.
- 4 Wählen Sie eine VM aus dem Dropdown-Menü **Virtuelle Zielmaschine** aus.
- 5 Klicken Sie auf **Gehe zu**.

Es wird ein Schema der Portverbindungstopologie angezeigt. Sie können durch Klicken auf eine beliebige Komponente in der visuellen Ausgabe Informationen über diese Komponente darzustellen.

## Traceflow

Mit Traceflow können Sie ein Paket in das Netzwerk einfügen und beobachten, wie es das Netzwerk durchläuft. Dadurch können Sie Ihr Netzwerk überwachen und Probleme wie z. B. Engpässe oder Unterbrechungen feststellen.

Mit Traceflow können Sie identifizieren, welchen Pfad (bzw. welche Pfade) ein Paket zu seinem Ziel nimmt, oder im umgekehrten Fall, wo ein Paket auf dem Weg abgelegt wird. Jede Entität meldet die Verarbeitung des Pakets an der Eingabe und Ausgabe, damit Sie ermitteln können, ob Probleme beim Empfang oder bei der Weiterleitung des Pakets auftreten.

Traceflow unterscheidet sich von einer Ping-Anforderung/-Antwort, die von Gast-VM-Stack zu Gast-VM-Stack verläuft. Traceflow beobachtet jedes markierte Paket, während es das Overlay-Netzwerk durchläuft, bis es an die Ziel-Gast-VM übermittelt wird. Das eingefügte markierte Paket wird nie tatsächlich an die Ziel-Gast-VM übermittelt, wodurch Traceflow auch dann erfolgreich ausgeführt werden kann, wenn die Gast-VM ausgeschaltet ist.

Traceflow kann auf Transportknoten verwendet werden und unterstützt sowohl IPv4- als auch IPv6-Protokolle, einschließlich: ICMP, TCP, UDP, DHCP, DNS und ARP/NDP.

Traceflow unterstützt die folgenden Arten des Datenverkehrs:

- Schicht 2-Unicast
- Schicht 3-Unicast
- Schicht 2-Broadcast
- Schicht 2-Multicast

Sie können Pakete mit benutzerdefinierten Kopfzeilen und Paketgrößen erstellen. Die Quelle oder das Ziel von Traceflow kann ein logischer Switch-Port, der Uplink-Port eines logischen Routers, ein CSP- oder ein DHCP-Port sein. Der Zielendpunkt kann ein beliebiges Gerät im NSX Overlay oder Underlay sein. Sie dürfen jedoch kein Ziel auswählen, das sich im Norden eines NSX Edge-Knotens befindet. Das Ziel muss sich in demselben Subnetz befinden oder durch die NSX Distributed Logical Router erreichbar sein.

Der Traceflow-Vorgang wird als Schicht 2 betrachtet, wenn sich Quelle und Ziel in derselben Schicht 2-Domäne befinden. In NSX bedeutet dies, dass sie sich auf demselben VXLAN-Netzwerkbezeichner (VNI oder Segment-ID) befinden. Dies geschieht beispielsweise, wenn zwei VMs mit demselben logischen Switch verbunden sind.

Wenn das NSX-Bridging konfiguriert ist, werden unbekannte Schicht 2-Pakete immer zur Bridge gesendet. Normalerweise leitet die Bridge diese Pakete an ein VLAN weiter und meldet das Traceflow-Paket als zugestellt. Wenn ein Paket als zugestellt gemeldet wird, bedeutet dies nicht zwangsläufig, dass das Traceflow-Paket an das angegebene Ziel übermittelt wurde.

Für Schicht 3-Traceflow-Unicast-Datenverkehr befinden sich die beiden Endpunkte auf unterschiedlichen logischen Switches und haben unterschiedliche VNIs, die mit einem verteilten logischen Router (Distributed Logical Switch, DLR) verbunden sind.

Für Multicast-Datenverkehr ist die Quelle eine vNIC oder ein logischer Port einer VM und das Ziel ist eine Multicast-Gruppenadresse.

Traceflow-Beobachtungen können auch Beobachtungen von gesendeten Traceflow-Paketen beinhalten. Der ESXi-Host sendet ein Traceflow-Paket, wenn er die MAC-Adresse des Ziel-Hosts nicht kennt. Für den Broadcast-Datenverkehr ist die Quelle die vNIC einer VM. Die Schicht 2-MAC-Zieladresse für Broadcast-Datenverkehr lautet FF:FF:FF:FF:FF:FF. Der Broadcast-Traceflow-Vorgang benötigt für die Erstellung eines gültigen Pakets für eine Firewallinspektion die Länge eines Subpräfixes. Die Subnetzmaske ermöglicht NSX die Berechnung einer IP-Netzwerkadresse für das Paket.

## Nachverfolgen des Pfads eines Pakets mit Traceflow

Verwenden Sie Traceflow, um den Pfad eines Pakets zu überprüfen. Traceflow verfolgt den Pfad eines Pakets auf der Ebene des Transportknotens. Das nachverfolgte Paket durchläuft den Overlay des logischen Switch, ist aber für Schnittstellen, die an den logischen Switch angefügt wurden, nicht sichtbar. Mit anderen Worten: Kein Paket wird tatsächlich an die vorgesehenen Empfänger des Testpakets übermittelt.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Tools > Traceflow**.
- 3 Wählen Sie einen IPv4- oder IPv6-Adresstyp aus.
- 4 Wählen Sie einen Datenverkehrstyp aus.

Für IPv4-Adressen können Sie zwischen den Datenverkehrstypen „Unicast“, „Multicast“ und „Broadcast“ auswählen. Für IPv6-Adressen können Sie zwischen den Datenverkehrstypen „Unicast“ und „Multicast“ auswählen.

## 5 Geben Sie die Quell- und Zielinformationen gemäß dem Datenverkehrstyp an.

Datenverkehrstyp	Quelle	Ziel
Unicast	<p>Wählen Sie eine virtuelle Maschine oder einen logischen Port aus. Für eine VM:</p> <ul style="list-style-type: none"> <li>■ Wählen Sie in der Dropdown-Liste eine VM aus.</li> <li>■ Wählen Sie eine virtuelle Schnittstelle aus.</li> <li>■ Die IP-Adresse und die MAC-Adresse werden angezeigt, wenn VMTools in der VM installiert ist oder wenn die VM mithilfe des OpenStack-Plug-Ins bereitgestellt wurde (in diesem Fall werden Adressbindungen verwendet). Wenn die VM über mehrere IP-Adressen verfügt, wählen Sie eine Adresse in der Dropdown-Liste aus.</li> <li>■ Wenn die IP-Adresse und die MAC-Adresse nicht angezeigt werden, geben Sie die IP-Adresse und die MAC-Adresse in die Textfelder ein.</li> </ul> <p>Für einen logischen Port:</p> <ul style="list-style-type: none"> <li>■ Wählen Sie einen Anhangstyp aus: <b>VIF</b>, <b>DHCP</b>, <b>Edge-Uplink</b> oder <b>Zentraler Edge-Dienst</b>.</li> <li>■ Wählen Sie einen Port aus.</li> </ul>	<p>Wählen Sie eine virtuelle Maschine, einen logischen Port oder eine IP-/MAC-Adresse aus. Für eine VM:</p> <ul style="list-style-type: none"> <li>■ Wählen Sie in der Dropdown-Liste eine VM aus.</li> <li>■ Wählen Sie eine virtuelle Schnittstelle aus.</li> <li>■ Die IP-Adresse und die MAC-Adresse werden angezeigt, wenn VMTools in der VM installiert ist oder wenn die VM mithilfe des OpenStack-Plug-Ins bereitgestellt wurde (in diesem Fall werden Adressbindungen verwendet). Wenn die VM über mehrere IP-Adressen verfügt, wählen Sie eine Adresse in der Dropdown-Liste aus.</li> <li>■ Wenn die IP-Adresse und die MAC-Adresse nicht angezeigt werden, geben Sie die IP-Adresse und die MAC-Adresse in die Textfelder ein.</li> </ul> <p>Für einen logischen Port:</p> <ul style="list-style-type: none"> <li>■ Wählen Sie einen Anhangstyp aus: <b>VIF</b>, <b>DHCP</b>, <b>Edge-Uplink</b> oder <b>Zentraler Edge-Dienst</b>.</li> <li>■ Wählen Sie einen Port aus.</li> </ul> <p>Für IP-MAC:</p> <ul style="list-style-type: none"> <li>■ Wählen Sie den Nachverfolgungstyp aus (Schicht 2 oder Schicht 3). Geben Sie für „Schicht 2“ eine IP-Adresse und eine MAC-Adresse ein. Geben Sie für „Schicht 3“ eine IP-Adresse ein.</li> </ul>
Multicast	Siehe „Unicast“.	Geben Sie eine IP-Adresse ein. Es muss sich um eine Multicast-Adresse von 224.0.0.0 bis 239.255.255.255 handeln.
Broadcast	Siehe „Unicast“.	Geben Sie die Länge des Subnetzpräfixes ein.

## 6 (Optional) Klicken Sie auf **Erweitert**, um die erweiterten Optionen einzublenden.

## 7 (Optional) Geben Sie in die linke Spalte die gewünschten Werte oder Angaben für die folgenden Felder ein:

Option	Beschreibung
<b>Frame-Größe</b>	Die Standardeinstellung ist 128.
<b>TTL</b>	Die Standardeinstellung ist 64.
<b>Zeitüberschreitung (ms)</b>	Die Standardeinstellung ist 10000.
<b>Ethernet-Typ</b>	Die Standardeinstellung ist 2048.

Option	Beschreibung
<b>Nutzlasttyp</b>	Wählen Sie <b>Base64</b> , <b>Hex</b> , <b>Klartext</b> , <b>Binär</b> oder <b>Dezimal</b> aus.
<b>Nutzlastdaten</b>	Formatierte Nutzlast auf Basis des ausgewählten Typs.

- 8 (Optional) Wählen Sie ein Protokoll aus und stellen Sie verwandte Informationen bereit.

Protokoll	Schritt 1
TCP	Geben Sie einen Quellport, Zielport und TCP-Flags an.
UDP	Geben Sie einen Quellport und einen Zielport an.
ICMP	Geben Sie eine ICMP-ID und eine Sequenz an.
DHCPv6	Wählen Sie einen DHCP-Nachrichtentyp aus: <b>Anfordern</b> , <b>Ankündigen</b> , <b>Anfordern</b> oder <b>Antworten</b> .
DHCP	Wählen Sie einen DHCP-OP-Code aus: <b>Startanforderung</b> oder <b>Startantwort</b> .
DNS	Geben Sie eine Adresse an und wählen Sie einen Nachrichtentyp aus: <b>Abfrage</b> oder <b>Antwort</b> .

- 9 Klicken Sie auf **Ablaufverfolgung**.

Es werden Informationen zu Verbindungen, Komponenten und Schichten angezeigt. Zur Ausgabe gehört eine Tabelle mit dem Beobachtungstyp (Übermittelt, Verworfen, Erhalten, Weitergeleitet), dem Transportknoten, Komponenten und einem grafischen Schema der Topologie, wenn „Unicast“ und „Logischer Switch“ als Ziel ausgewählt wurden. Sie können einen Filter (**Alle**, **Übermittelt**, **Verworfen**) für die angezeigten Beobachtungen anwenden. Wenn verworfene Beobachtungen vorhanden sind, wird der Filter **Verworfen** automatisch angewendet. Andernfalls gilt der Filter **Alle**. Das grafische Schema zeigt die Backplane und die Router-Links. Beachten Sie, dass keine Bridging-Informationen angezeigt werden.

## Überwachen von Port-Mirroring-Sitzungen

Sie können Port-Mirroring-Sitzungen für die Fehlerbehebung und für andere Zwecke überwachen.

Beachten Sie, dass die logische SPAN nur für logische Overlay-Switches und nicht für logische VLAN-Switches unterstützt wird.

**NSX Cloud-Hinweis** Wenn Sie NSX Cloud verwenden, finden Sie unter [Verwendung von NSX-T Data Center-Funktionen mit der Public Cloud](#) eine Liste der automatisch generierten logischen Einheiten, unterstützten Funktionen und Konfigurationen, die für NSX Cloud erforderlich sind.

Für diese Funktion gelten folgende Einschränkungen:

- Ein Quellspiegelport kann nur in einer Spiegelungssitzung vorhanden sein.
- Mit KVM lassen sich mehrere NICs an einen OVS-Port anfügen. Die Spiegelung wird am OVS-Uplink-Port durchgeführt, d. h., der Datenverkehr auf allen PNICs wird gespiegelt, die an den OVS-Port angefügt wurden.

- Bei einer lokalen SPAN-Sitzung müssen sich die Quell- und Zielports der Spiegelungssitzung auf demselben Host-vSwitch befinden. Deshalb kann, wenn Sie einen vMotion-Vorgang für eine VM durchführen, deren Quell- oder Zielport sich auf einem anderen Host befindet, der Datenverkehr auf diesem Port nicht mehr gespiegelt werden.
- Auf ESXi werden TCP-Rohpakete zur Produktion bei aktivierter Spiegelung auf dem Uplink mithilfe des Geneve-Protokolls von VDL2 in UDP-Pakete gekapselt. Eine physische NIC mit TSO-Unterstützung (TCP-Segmentierungs-Offload) kann die Pakete verändern und sie mit der MUST\_TSO-Flag versehen. Auf einer Überwachungs-VM mit VMXNET3- oder E1000-vNICs werden die Pakete vom Treiber wie herkömmliche UDP-Pakete behandelt. Er kann die MUST\_TSO-Flag nicht verarbeiten und verwirft die Pakete.

Wenn Datenverkehr in großem Umfang auf eine Überwachungs-VM gespiegelt wird, kann es vorkommen, dass der Ringpuffer des Treibers voll wird und Pakete verworfen werden. Zur Behebung dieses Problems führen Sie eine oder mehrere der folgenden Aktionen durch:

- Erhöhen Sie die Größe des rx-Ringpuffers.
- Weisen Sie der VM mehr CPU-Ressourcen zu.
- Verwenden Sie das Entwicklungs-Kit für die Datenebene (DPDK, Data Plane Development Kit) zur Verbesserung der Leistung der Paketverarbeitung.

---

**Hinweis** Stellen Sie sicher, dass die MTU-Einstellung der Überwachungs-VM (bei KVM auch die MTU-Einstellung des virtuellen NIC-Gerätes des Hypervisors) für die Verarbeitung des Pakets ausreichend groß ist. Dies ist speziell für gekapselte Pakete wichtig, da die Kapselung die Größe der Pakete erhöht. Andernfalls kann es vorkommen, dass Pakete verworfen werden. Dieses Problem tritt nicht bei ESXi-VMs mit VMXNET3-NICs auf, aber potenziell mit anderen NIC-Typen sowohl bei ESXi- wie bei KVM-VMs.

---

**Hinweis** Bei einer L3-Port-Mirroring-Sitzung mit VMs auf KVM-Hosts muss die MTU-Größe hoch genug eingestellt sein, um die zusätzlichen Bytes für die Kapselung verarbeiten zu können. Der Spiegelungsdatenverkehr fließt durch eine OVS-Schnittstelle und einen OVS-Uplink. Die MTU der OVS-Schnittstelle muss mindestens um 100 Byte größer sein als die Originalpaketgröße (vor Kapselung und Spiegelung). Wenn Ihnen verworfene Pakete auffallen, erhöhen Sie den Wert der MTU-Einstellung für die virtuelle NIC des Hosts und die OVS-Schnittstelle. Legen Sie die MTU für eine OVS-Schnittstelle mit folgendem Befehl fest:

```
ovs-vsctl -- set interface <ovs_Interface> mtu_request=<MTU>
```

---

**Hinweis** Wenn Sie den logischen Port einer VM und den Uplink-Port eines Hosts, auf dem sich die VM befindet, überwachen, treten je nachdem, ob es sich bei dem Host um ESXi oder KVM handelt, unterschiedliche Verhaltensweisen auf. Bei ESXi werden die Spiegelungspakete des logischen Ports und die Uplink-Spiegelungspakete mit derselben VLAN-ID markiert und werden auf der Überwachungs-VM gleich angezeigt. Bei KVM werden die Spiegelungspakete des logischen Ports nicht mit einer VLAN-ID markiert, die Uplink-Spiegelungspakete hingegen werden markiert, und beide werden auf der Überwachungs-VM unterschiedlich angezeigt.

---



## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 3 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Tools > Port-Mirroring-Sitzung** aus.
- 4 Klicken Sie auf **Hinzufügen** und wählen Sie einen Sitzungstyp aus.

Folgende Typen sind verfügbar: **Lokale SPAN**, **Remote-SPAN**, **Remote-L3 SPAN** und **Logische SPAN**.

- 5 Geben Sie einen Namen und optional eine Beschreibung für die Sitzung ein.
- 6 Geben Sie zusätzliche Parameter an.

Sitzungstyp	Parameter
Lokale SPAN	<ul style="list-style-type: none"> <li>■ <b>Transportknoten</b> – wählen Sie einen Transportknoten aus.</li> <li>■ <b>Richtung</b> – wählen Sie <b>Bidirektional</b>, <b>Ingress</b> oder <b>Egress</b> aus.</li> <li>■ <b>Paketkürzung</b> – wählen Sie einen Wert für die Paketkürzung aus.</li> </ul>
Remote-SPAN	<ul style="list-style-type: none"> <li>■ <b>Sitzungstyp</b> – wählen Sie <b>RSPAN-Quellsitzung</b> oder <b>RSPAN-Zielsitzung</b> aus.</li> <li>■ <b>Transportknoten</b> – wählen Sie einen Transportknoten aus.</li> <li>■ <b>Richtung</b> – wählen Sie <b>Bidirektional</b>, <b>Ingress</b> oder <b>Egress</b> aus.</li> <li>■ <b>Paketkürzung</b> – wählen Sie einen Wert für die Paketkürzung aus.</li> <li>■ <b>Gekapselte VLAN-ID VLAN-ID</b> – geben Sie eine gekapselte VLAN-ID an.</li> <li>■ <b>Ursprungs-VLAN beibehalten</b> – Legen Sie fest, ob die ursprüngliche VLAN-ID beibehalten werden soll.</li> </ul>
Remote-L3 SPAN	<ul style="list-style-type: none"> <li>■ <b>Kapselung</b> – wählen Sie <b>GRE</b>, <b>ERSPAN TWO</b> oder <b>ERSPAN THREE</b> aus.</li> <li>■ <b>GRE-Schlüssel</b> – geben Sie einen GRE-Schlüssel an, wenn Sie für „Kapselung“ die Option <b>GRE</b> ausgewählt haben. <b>ERSPAN-ID</b> – geben Sie eine ERSPAN-ID an, wenn Sie für „Kapselung“ eine der Optionen <b>ERSPAN TWO</b> oder <b>ERSPAN THREE</b> ausgewählt haben.</li> <li>■ <b>Richtung</b> – wählen Sie <b>Bidirektional</b>, <b>Ingress</b> oder <b>Egress</b> aus.</li> <li>■ <b>Paketkürzung</b> – wählen Sie einen Wert für die Paketkürzung aus.</li> </ul>
Logische SPAN	<ul style="list-style-type: none"> <li>■ <b>Logischer Switch</b> – wählen Sie einen logischen Switch aus.</li> <li>■ <b>Richtung</b> – wählen Sie <b>Bidirektional</b>, <b>Ingress</b> oder <b>Egress</b> aus.</li> <li>■ <b>Paketkürzung</b> – wählen Sie einen Wert für die Paketkürzung aus.</li> </ul>

- 7 Klicken Sie auf **Weiter**.

**8** Geben Sie Quellinformationen an.

Sitzungstyp	Parameter
Lokale SPAN	<ul style="list-style-type: none"> <li>■ Wählen Sie einen N-VDS aus.</li> <li>■ Wählen Sie physische Schnittstellen aus.</li> <li>■ Aktivieren oder deaktivieren Sie die Kapselung von Paketen.</li> <li>■ Wählen Sie virtuelle Maschinen aus.</li> <li>■ Wählen Sie virtuelle Schnittstellen aus.</li> </ul>
Remote-SPAN	<ul style="list-style-type: none"> <li>■ Wählen Sie virtuelle Maschinen aus.</li> <li>■ Wählen Sie virtuelle Schnittstellen aus.</li> </ul>
Remote-L3 SPAN	<ul style="list-style-type: none"> <li>■ Wählen Sie virtuelle Maschinen aus.</li> <li>■ Wählen Sie virtuelle Schnittstellen aus.</li> <li>■ Wählen Sie einen logischen Switch aus.</li> </ul>
Logische SPAN	<ul style="list-style-type: none"> <li>■ Wählen Sie logische Ports aus.</li> </ul>

**9** Klicken Sie auf **Weiter**.**10** Geben Sie Zielinformationen an.

Sitzungstyp	Parameter
Lokale SPAN	<ul style="list-style-type: none"> <li>■ Wählen Sie virtuelle Maschinen aus.</li> <li>■ Wählen Sie virtuelle Schnittstellen aus.</li> </ul>
Remote-SPAN	<ul style="list-style-type: none"> <li>■ Wählen Sie einen N-VDS aus.</li> <li>■ Wählen Sie physische Schnittstellen aus.</li> </ul>
Remote-L3 SPAN	<ul style="list-style-type: none"> <li>■ Geben Sie eine IPv4-Adresse an.</li> </ul>
Logische SPAN	<ul style="list-style-type: none"> <li>■ Wählen Sie logische Ports aus.</li> </ul>

**11** Klicken Sie auf **Speichern**.

Die Quelle und das Ziel können nach dem Speichern der Port-Mirroring-Sitzung nicht mehr geändert werden.

## Konfigurieren von Filtern für eine Port-Mirroring-Sitzung

Sie können Filter für Port-Mirroring-Sitzungen konfigurieren, um die Menge der gespiegelten Daten zu begrenzen.

Für diese Funktion gelten folgende Möglichkeiten und Einschränkungen:

- Nur ESXi- und KVM-Host-Transportknoten werden unterstützt.
- IP-Adresse, IP-Präfix und IP-Bereiche werden für Quelle und Ziel unterstützt.
- IPSet für Quelle oder Ziel wird nicht unterstützt.
- Spiegelstatistiken unter ESXi oder KVM werden nicht unterstützt.

Sie müssen Filter mithilfe der API konfigurieren. Die Verwendung der NSX Manager-Benutzeroberfläche wird nicht unterstützt. Weitere Informationen zur Port-Mirroring-API und zum PortMirroringFilter-Schema finden Sie in der *Referenz zur NSX-T Data Center-API*.

## Verfahren

- 1 Konfigurieren Sie eine Port-mirroring-sitzung mithilfe der NSX Manager-Benutzeroberfläche oder der API.
- 2 Rufen Sie die GET `/api/v1/mirror-sessions-API` auf, um Informationen über die Port-Mirroring-Sitzung abzurufen.
- 3 Rufen Sie die GET `/api/v1/mirror-sessions/<mirror-session-id>-API` auf, um Filter hinzuzufügen. Beispiel:

```
PUT https://<nsx-mgr>/api/v1/mirror-sessions/e57e8b2d-3047-4550-b230-dd1ee0e10b49
{
  "resource_type": "PortMirroringSession",
  "id": "e57e8b2d-3047-4550-b230-dd1ee0e10b49",
  "display_name": "port-mirror-session-1",
  "description": "Pnic port mirror session 1",
  "mirror_sources": [
    {
      "resource_type": "LogicalPortMirrorSource",
      "port_ids": [
        "6a361832-43e4-430d-a48a-b84a6cba73c3"
      ]
    }
  ],
  "mirror_destination": {
    "resource_type": "LogicalPortMirrorDestination",
    "port_ids": [
      "3e42e8b2d-3047-4550-b230-dd1ee0e10b34"
    ]
  },
  "port_mirroring_filters": [
    {
      "filter_action": "MIRROR",
      "src_ips": {
        "ip-addresses": [
          "192.168.175.250",
          "2001:bd6::c:2957:160:126"
        ]
      },
      "dst_ips": {
        "ip-addresses": [
          "192.168.160.126",
          "2001:bd6::c:2957:175:250"
        ]
      }
    }
  ],
  "session_type": "LogicalPortMirrorSession",
}
```

```
"preserve_original_vlan": false,
"direction": "BIDIRECTIONAL",
"_revision": 0
}
```

- 4 (Optional) Sie können den `get mirroring-session <session-number>` CLI-Befehl aufrufen, um die Eigenschaften der Port-Mirroring-Sitzung einschließlich der Filter anzuzeigen.

## Konfigurieren von IPFIX

IPFIX (Internet Protocol Flow Information Export) ist ein Standard für das Format und den Export von Netzwerk-Flow-Informationen. Sie können IPFIX für Switches und Firewalls konfigurieren. Der Netzwerk-Flow auf VIFs (virtuellen Schnittstellen) und pNICs (physischen Netzwerkkarten) wird für Switches exportiert. Für Firewalls wird der durch die verteilte Firewallkomponente verwaltete Netzwerk-Flow exportiert.

---

**NSX Cloud-Hinweis** Wenn Sie NSX Cloud verwenden, finden Sie unter [Verwendung von NSX-T Data Center-Funktionen mit der Public Cloud](#) eine Liste der automatisch generierten logischen Einheiten, unterstützten Funktionen und Konfigurationen, die für NSX Cloud erforderlich sind.

---

Diese Funktion ist mit den in RFC 7011 und RFC 7012 angegebenen Standards konform.

Wenn Sie IPFIX aktivieren, senden alle konfigurierten Hosttransportknoten IPFIX-Nachrichten an die IPFIX-Collectors über Port 4739. Bei ESXi öffnet NSX-T Data Center Port 4739 automatisch. Bei KVM ist Port 4739 geöffnet, wenn die Firewall nicht aktiviert ist. Sollte die Firewall aber aktiviert sein, müssen Sie sicherstellen, dass der Port geöffnet ist, da NSX-T Data Center den Port nicht automatisch öffnet.

IPFIX tastet Tunnelpakete auf ESXi und KVM auf unterschiedliche Weise ab. Auf ESXi werden Tunnelpakete als zwei Einträge abgetastet:

- Äußerer Paketeintrag mit einigen Informationen zum inneren Paket
  - SrcAddr, DstAddr, SrcPort, DstPort und Protocol beziehen sich auf das äußere Paket.
  - Beinhaltet einige Unternehmenseinträge zur Beschreibung des inneren Pakets.
- Innerer Paketeintrag
  - SrcAddr, DstAddr, SrcPort, DstPort und Protocol beziehen sich auf das innere Paket.

Auf KVM werden Tunnelpakete als ein Eintrag abgetastet:

- Innerer Paketeintrag mit einigen Informationen zum äußeren Tunnel
  - SrcAddr, DstAddr, SrcPort, DstPort und Protocol beziehen sich auf das innere Paket.
  - Beinhaltet einige Unternehmenseinträge zur Beschreibung des äußeren Pakets.

## Konfigurieren von Switch-IPFIX-Collectors

Sie können IPFIX-Collectors für Switches konfigurieren.

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Tools > IPFIX** aus.
- 3 Klicken Sie auf die Registerkarte **Switch-IPFIX-Collectors**.
- 4 Klicken Sie auf **Hinzufügen**, um einen Collector hinzuzufügen.
- 5 Geben Sie einen Namen und optional eine Beschreibung ein.
- 6 Klicken Sie auf **Hinzufügen** und geben Sie die IP-Adresse und den Port eines Collectors ein.  
Sie können bis zu 4 Collectors hinzufügen.
- 7 Klicken Sie auf **Hinzufügen**.

## Konfigurieren von Switch-IPFIX-Profilen

Sie können IPFIX-Profile für Switches konfigurieren.

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Tools > IPFIX** aus.
- 3 Klicken Sie auf die Registerkarte **Switch-IPFIX-Profile**.
- 4 Klicken Sie auf **Hinzufügen**, um ein Profil hinzuzufügen.

Einstellung	Beschreibung
Name und Beschreibung	Geben Sie einen Namen und optional eine Beschreibung ein.  <b>Hinweis</b> Wenn Sie ein globales Profil erstellen möchten, nennen Sie das Profil <b>Global</b> . Ein globales Profil kann nicht in der Benutzeroberfläche bearbeitet oder gelöscht werden, aber Sie können dies mit NSX-T Data Center-APIs tun.
Aktive Zeitüberschreitung (Sekunden)	Die Zeitspanne, nach der eine Zeitüberschreitung bei einem Flow auftritt, selbst wenn weitere mit dem Flow verknüpfte Pakete eingehen. Der Standardwert beträgt 300.
Überschreitung Leerlaufzeit (Sekunden)	Die Zeitspanne, nach der eine Zeitüberschreitung bei einem Flow auftritt, wenn keine weiteren mit dem Flow verknüpften Pakete eingehen (nur ESXi, KVM bestimmt die Zeitüberschreitung für alle Flows basierend auf der aktiven Zeitüberschreitung) Der Standardwert beträgt 300.
Max. Flows	Die maximale Anzahl der in einer Bridge zwischengespeicherten Flows (nur KVM, unter ESXi nicht konfigurierbar) Der Standardwert beträgt 16384.

Einstellung	Beschreibung
Sampling-Wahrscheinlichkeit (%)	Der Prozentsatz der Pakete, die abgetastet werden (ungefähr). Wenn Sie diese Einstellung erhöhen, kann sich dies auf die Leistung der Hypervisors und Collectors auswirken. Wenn alle Hypervisors mehr IPFIX-Pakete an den Collector senden, kann der Collector möglicherweise nicht alle Pakete erfassen. Indem Sie die Wahrscheinlichkeit auf dem Standardwert von 0,1 % belassen, bleibt die Auswirkung auf die Leistung gering.
Beobachtungsdomänen-ID	Mit der Beobachtungsdomänen-ID wird festgelegt, aus welcher Beobachtungsdomäne die Netzwerk-Flows stammen. Geben Sie 0 ein, um keine bestimmte Beobachtungsdomäne anzugeben.
Collector-Profil	Wählen Sie einen Switch-IPFIX-Collector aus, den Sie im vorherigen Schritt konfiguriert haben.
Priorität	Dieser Parameter dient zur Behebung von Konflikten, wenn mehrere Profile anwendbar sind. IPFIX-Exporter verwendet nur das Profil mit der höchsten Priorität. Ein niedrigerer Wert bedeutet eine höhere Priorität.

- 5 Klicken Sie auf **Angewendet auf**, um das Profil auf ein oder mehrere Objekte anzuwenden.

Die Objekttypen sind logische Ports, logische Switches und NS-Gruppen. Wenn Sie eine NS-Gruppe auswählen, muss sie einen oder mehrere logische Switches oder logische Ports enthalten. Wenn die NS-Gruppe nur IP Sets oder MAC Sets enthält, wird sie ignoriert.

- 6 Klicken Sie auf **Speichern**.

## Konfigurieren von Firewall-IPFIX-Collectors

Sie können IPFIX-Collectors für Firewalls konfigurieren.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Tools > IPFIX** aus.
- 3 Klicken Sie auf die Registerkarte **Firewall-IPFIX-Collectors**.
- 4 Klicken Sie auf **Hinzufügen**, um einen Collector hinzuzufügen.
- 5 Geben Sie einen Namen und optional eine Beschreibung ein.
- 6 Klicken Sie auf **Hinzufügen** und geben Sie die IP-Adresse und den Port eines Collectors ein.  
Sie können bis zu 4 Collectors hinzufügen.
- 7 Klicken Sie auf **Hinzufügen**.

## Konfigurieren von Firewall-IPFIX-Profilen

Sie können IPFIX-Profile für Firewalls konfigurieren.

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Tools > IPFIX** aus.
- 3 Klicken Sie auf die Registerkarte **Firewall-IPFIX-Profile**.
- 4 Klicken Sie auf **Hinzufügen**, um ein Profil hinzuzufügen.

Einstellung	Beschreibung
Name und Beschreibung	Geben Sie einen Namen und optional eine Beschreibung ein.  <b>Hinweis</b> Wenn Sie ein globales Profil erstellen möchten, nennen Sie das Profil <b>Global</b> . Ein globales Profil kann nicht in der Benutzeroberfläche bearbeitet oder gelöscht werden, aber Sie können dies mit NSX-T Data Center-APIs tun.
Collector-Konfiguration	Wählen Sie in der Dropdown-Liste einen Collector aus.
Zeitüberschreitung bei aktivem Flow-Export (Minuten)	Die Zeitspanne, nach der eine Zeitüberschreitung bei einem Flow auftritt, selbst wenn weitere mit dem Flow verknüpfte Pakete eingehen. Der Standardwert beträgt 1.
Priorität	Dieser Parameter dient zur Behebung von Konflikten, wenn mehrere Profile anwendbar sind. IPFIX-Exporter verwendet nur das Profil mit der höchsten Priorität. Ein niedrigerer Wert bedeutet eine höhere Priorität.
Beobachtungsdomänen-ID	Dieser Parameter gibt an, aus welcher Beobachtungsdomäne die Netzwerk-Flows stammen. Die Standardeinstellung ist 0 und verweist auf keine bestimmte Beobachtungsdomäne.

- 5 Klicken Sie auf **Hinzufügen**.

## ESXi-IPFIX-Vorlagen

Ein ESXi-Host-Transportknoten unterstützt acht IPFIX-Flow-Vorlagen für einen logischen Switch und zwei IPFIX-Flow-Vorlagen für eine verteilte Firewall.

In der folgenden Tabelle sind die VMware-spezifischen Elemente in den IPFIX-Paketen des logischen Switches aufgeführt.

Element-ID	Parametername	Datentyp	Einheit
880	tenantProtocol	unsigned8	1 Byte
881	tenantSourceIPv4	ipv4Address	4 Byte
882	tenantDestIPv4	ipv4Address	4 Byte
883	tenantSourceIPv6	ipv6Address	16 Byte
884	tenantDestIPv6	ipv6Address	16 Byte
886	tenantSourcePort	unsigned16	2 Byte
887	tenantDestPort	unsigned16	2 Byte

Element-ID	Parametername	Datentyp	Einheit
888	egressInterfaceAttr	unsigned16	2 Byte
889	vxlanExportRole	unsigned8	1 Byte
890	ingressInterfaceAttr	unsigned16	2 Byte
898	virtualObsID	string	Variable Länge

In der folgenden Tabelle sind die VMware-spezifischen Elemente in den IPFIX-Paketen der verteilten Firewall aufgeführt.

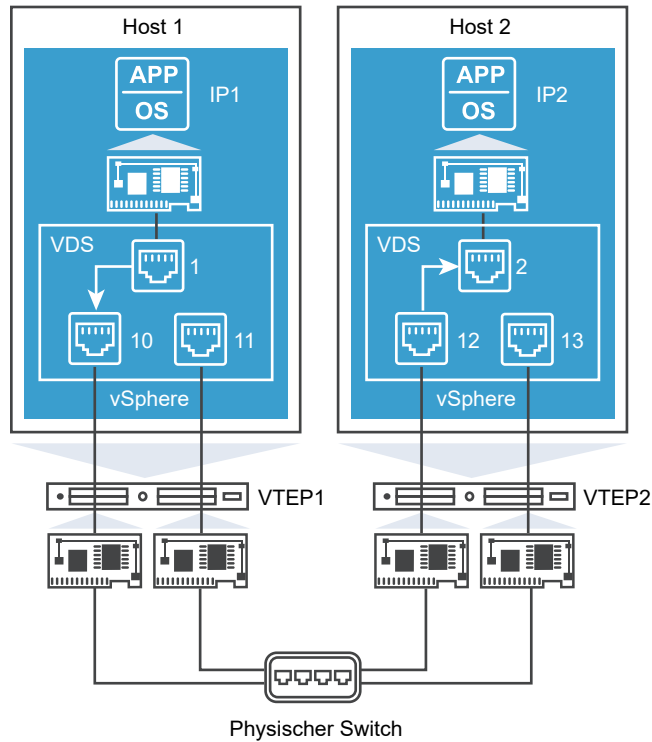
Element-ID	Parametername	Datentyp	Einheit
950	ruleId	unsigned32	4 Byte
951	vmUuid	string	16 Byte
952	vnicIndex	unsigned32	4 Byte
953	sessionFlags	unsigned8	1 Byte
954	flowDirection	unsigned8	1 Byte
955	algControlFlowId	unsigned64	8 Byte
956	algType	unsigned8	1 Byte
957	algFlowType	unsigned8	1 Byte
958	averageLatency	unsigned32	4 Byte
959	retransmissionCount	unsigned32	4 Byte
960	vifUuid	octetArray	16 Byte
961	vifId	string	Variable Länge

### IPFIX-Vorlagen für logische ESXi-Switches

Ein ESXi-Host-Transportknoten unterstützt acht IPFIX-Flow-Vorlagen für logische Switches.

Das folgende Diagramm zeigt den Datenverkehrsfluss zwischen VMs, die an die von der IPFIX-Funktion überwachten ESXi-Hosts angehängt sind:





Die IPv4-gekapselte Vorlage weist die folgenden Elemente auf:

- Standardelemente
- SrcAddr: VTEP1
- DstAddr: VTEP2
- tenantSourceIPv4: IP1
- tenantDestIPv4: IP2
- tenantSourcePort: 10000
- tenantDestPort: 80
- tenantProtocol: TCP
- ingressInterfaceAttr: 0x03 (Tunnel-Port)
- egressInterfaceAttr: 0x01
- encapExportRole: 01
- virtualObsID: 89fd5032-2dc9-4fc3-993a-9bb4b616de54 (ID des logischen Ports)

### IPv4-Vorlage

Vorlagen-ID: 256

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
```

```

IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
// Specify the Interface port- Uplink Port, Access port,N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()

```

## IPv4-Encapsulated-Vorlage

Vorlagen-ID: 257

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourcePort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port - Uplink Port, Access port, N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)

```

```
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_END()
```

## IPv4-ICMP-Vorlage

Vorlagen-ID: 258

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ICMP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
// Specify the Interface port – Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 2)
IPFIX_TEMPLATE_END()
```

## IPv4-ICMP-Encapsulated-Vorlage

Vorlagen-ID: 259

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ICMP_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
```

```
// Specify the Interface port- Uplink Port, Access port,N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()
```

## IPv6-Vorlage

Vorlagen-ID: 260

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6)
IPFIX_TEMPLATE_FIELD(sourceIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS,1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
// Specify the Interface port - Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()
```

## IPv6-Encapsulated-Vorlage

Vorlagen-ID: 261

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
```

```

IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
//ENCAP specific
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourcePort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port – Uplink Port, Access Port, or NA
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_END()

```

## IPv6-ICMP-Vorlage

Vorlagen-ID: 262

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ICMP)
IPFIX_TEMPLATE_FIELD(sourceIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
// Specify the Interface port – Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 2)
IPFIX_TEMPLATE_END()

```

## IPv6-ICMP-Encapsulated-Vorlage

Vorlagen-ID: 263

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ICMP_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)

```

```

IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_VMW_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
//ENCAP Specific
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port – Uplink Port, Access Port, or NA
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()

```

## ESXi-Vorlagen für verteilte Firewall-IPFIX

Ein ESXi-Host-Transportknoten unterstützt zwei verteilte Firewall-IPFIX-Flow-Vorlagen.

### IPv4-Vorlage

Vorlagen-ID: 288

```

IPFIX_TEMPLATE_FIELD(sourceIPv4Address,4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address,4)
IPFIX_TEMPLATE_FIELD(sourceTransportPort,2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort,2)
IPFIX_TEMPLATE_FIELD(protocolIdentifier,1)
IPFIX_TEMPLATE_FIELD(icmpTypeIPv4,1)
IPFIX_TEMPLATE_FIELD(icmpCodeIPv4,1)
IPFIX_TEMPLATE_FIELD(flowStartSeconds,4)
IPFIX_TEMPLATE_FIELD(flowEndSeconds,4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount,8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount,8)
IPFIX_TEMPLATE_FIELD(firewallEvent,1)
IPFIX_TEMPLATE_FIELD(direction,1)
IPFIX_TEMPLATE_FIELD(ruleId,4)
IPFIX_TEMPLATE_FIELD(vifUuid,16)
IPFIX_TEMPLATE_FIELD(sessionFlags,1)
IPFIX_TEMPLATE_FIELD(flowDirection,1)
IPFIX_TEMPLATE_FIELD(flowId,8)
IPFIX_TEMPLATE_FIELD(algControlFlowId,8)
IPFIX_TEMPLATE_FIELD(algType,1)
IPFIX_TEMPLATE_FIELD(algFlowType,1)
IPFIX_TEMPLATE_FIELD(averageLatency,4)
IPFIX_TEMPLATE_FIELD(retransmissionCount,4)

```

## IPv6-Vorlage

Vorlagen-ID: 289

```
IPFIX_TEMPLATE_FIELD(sourceIPv6Address,16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address,16)
IPFIX_TEMPLATE_FIELD(sourceTransportPort,2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort,2)
IPFIX_TEMPLATE_FIELD(protocolIdentifier,1)
IPFIX_TEMPLATE_FIELD(icmpTypeIPv6,1)
IPFIX_TEMPLATE_FIELD(icmpCodeIPv6,1)
IPFIX_TEMPLATE_FIELD(flowStartSeconds,4)
IPFIX_TEMPLATE_FIELD(flowEndSeconds,4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount,8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount,8)
IPFIX_TEMPLATE_FIELD(firewallEvent,1)
IPFIX_TEMPLATE_FIELD(direction,1)
IPFIX_TEMPLATE_FIELD(ruleId,4)
IPFIX_TEMPLATE_FIELD(vifUuid,16)
IPFIX_TEMPLATE_FIELD(sessionFlags,1)
IPFIX_TEMPLATE_FIELD(flowDirection,1)
IPFIX_TEMPLATE_FIELD(flowId,8)
IPFIX_TEMPLATE_FIELD(algControlFlowId,8)
IPFIX_TEMPLATE_FIELD(algType,1)
IPFIX_TEMPLATE_FIELD(algFlowType,1)
IPFIX_TEMPLATE_FIELD(averageLatency,4)
IPFIX_TEMPLATE_FIELD(retransmissionCount,4)
```

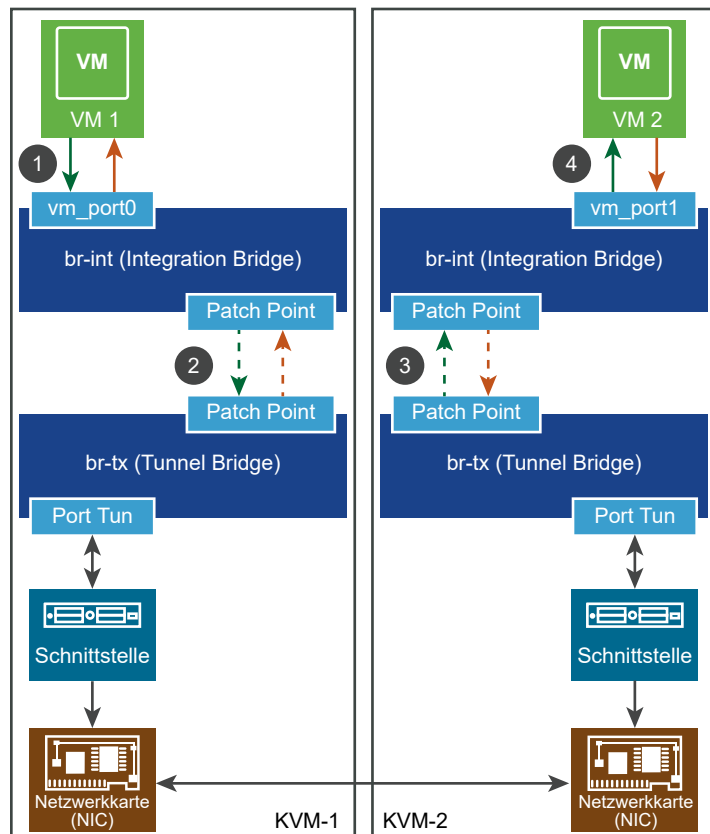
## IPFIX-Vorlagen für KVM

Ein KVM-Hosttransportknoten unterstützt 88 IPFIX-Flow-Vorlagen und eine Vorlage für Optionen.

In der folgenden Tabelle sind die VMware-spezifischen Elemente in den KVM-IPFIX-Paketen aufgeführt.

Element-ID	Parametername	Datentyp	Einheit
891	tunnelType	unsigned8	1 Byte
892	tunnelKey	Byte	Variable Länge
893	tunnelSourceIPv4Address	unsigned32	4 Byte
894	tunnelDestinationIPv4Address	unsigned32	4 Byte
895	tunnelProtocolIdentifier	unsigned8	1 Byte
896	tunnelSourceTransportPort	unsigned16	2 Byte
897	tunnelDestinationTransportPort	unsigned16	2 Byte
898	virtualObsID	string	Variable Länge

Das folgende Diagramm zeigt den Datenverkehr zwischen VMs, die mit den von der IPFIX-Funktion überwachten KVM-Hosts verbunden sind:



Die KVM-IPv4-IPFIX-Ingress-Vorlage weist die folgenden Elemente auf:

- Standardelemente
- virtualObsID: 6d876a1c-e0ac-4bcf-85ee-bdd42fa7ba34 (ID des logischen Ports)

### Ethernet-IPFIX-Vorlagen für KVM

Es gibt vier Ethernet-IPFIX-Vorlagen für KVM: Ingress (eingehender Flow), Egress (ausgehender Flow), Ingress mit Tunnel und Egress mit Tunnel.

#### Ethernet-Ingress

Vorlagen-ID: 256 Anzahl der Felder: 27

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)



- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)

### **Ethernet-Egress**

Vorlagen-ID: 257 Anzahl der Felder: 31

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)

- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 8)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMcastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)

### **Ethernet-Ingress mit Tunnel**

Vorlagen-ID: 258 Anzahl der Felder: 34

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)

- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)

### **Ethernet-Egress mit Tunnel**

Vorlagen-ID: 259 Anzahl der Felder: 38

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)

- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 8)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)

- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)

### IPv4-IPFIX-Vorlagen für KVM

Es gibt vier IPv4-IPFIX-Vorlagen für KVM: Ingress (eingehender Flow), Egress (ausgehender Flow), Ingress mit Tunnel und Egress mit Tunnel.

#### IPv4-Ingress

Vorlagen-ID: 276 Anzahl der Felder: 45

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)

- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMcastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMcastOctetTotalCount (Länge: 8)

#### IPv4-Egress

Vorlagen-ID: 277 Anzahl der Felder: 49

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)

- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)

- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMcastOctetTotalCount (Länge: 8)

#### **IPv4-Ingress mit Tunnel**

Vorlagen-ID: 278 Anzahl der Felder: 52

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)



- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)

- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

#### IPv4-Egress mit Tunnel

Vorlagen-ID: 279 Anzahl der Felder: 56

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))

- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### **TCP over IPv4-IPFIX-Vorlagen für KVM**

Es gibt vier TCP over IPv4-IPFIX-Vorlagen für KVM: Ingress (eingehender Flow), Egress (ausgehender Flow), Ingress mit Tunnel und Egress mit Tunnel.

## TCP over IPv4-Ingress

Vorlagen-ID: 280 Anzahl der Felder: 53

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)

- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)
- tcpAckTotalCount (Länge: 8)
- tcpFinTotalCount (Länge: 8)
- tcpPshTotalCount (Länge: 8)
- tcpRstTotalCount (Länge: 8)
- tcpSynTotalCount (Länge: 8)
- tcpUrgTotalCount (Länge: 8)

### **TCP over IPv4-Egress**

Vorlagen-ID: 281 Anzahl der Felder: 57

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)

- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)

- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)
- tcpAckTotalCount (Länge: 8)
- tcpFinTotalCount (Länge: 8)
- tcpPshTotalCount (Länge: 8)
- tcpRstTotalCount (Länge: 8)
- tcpSynTotalCount (Länge: 8)
- tcpUrgTotalCount (Länge: 8)

### **TCP over IPv4-Ingress mit Tunnel**

Vorlagen-ID: 282 Anzahl der Felder: 60

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)

- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)



- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMcastOctetTotalCount (Länge: 8)
- tcpAckTotalCount (Länge: 8)
- tcpFinTotalCount (Länge: 8)
- tcpPshTotalCount (Länge: 8)
- tcpRstTotalCount (Länge: 8)
- tcpSynTotalCount (Länge: 8)
- tcpUrgTotalCount (Länge: 8)

#### **TCP over IPv4-Egress mit Tunnel**

Vorlagen-ID: 283 Anzahl der Felder: 64

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)

- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)

- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)
- tcpAckTotalCount (Länge: 8)
- tcpFinTotalCount (Länge: 8)
- tcpPshTotalCount (Länge: 8)
- tcpRstTotalCount (Länge: 8)
- tcpSynTotalCount (Länge: 8)
- tcpUrgTotalCount (Länge: 8)

#### **UDP over IPv4-IPFIX-Vorlagen für KVM**

Es gibt vier UDP over IPv4-IPFIX-Vorlagen für KVM: Ingress (eingehender Flow), Egress (ausgehender Flow), Ingress mit Tunnel und Egress mit Tunnel.

#### **UDP over IPv4-Ingress**

Vorlagen-ID: 284 Anzahl der Felder: 47

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)

- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)

- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMcastOctetTotalCount (Länge: 8)

#### **UDP over IPv4-Egress**

Vorlagen-ID: 285 Anzahl der Felder: 51

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)

- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)

- postMCastOctetTotalCount (Länge: 8)

### UDP over IPv4-Ingress mit Tunnel

Vorlagen-ID: 286 Anzahl der Felder: 54

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))

- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

#### **UDP over IPv4-Egress mit Tunnel**

Vorlagen-ID: 287 Anzahl der Felder: 58

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)



- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)

- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMcastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMcastOctetTotalCount (Länge: 8)

### **SCTP over IPv4-IPFIX-Vorlagen für KVM**

Es gibt vier SCTP over IPv4-IPFIX-Vorlagen für KVM: Ingress (eingehender Flow), Egress (ausgehender Flow), Ingress mit Tunnel und Egress mit Tunnel.

#### **SCTP over IPv4-Ingress**

Vorlagen-ID: 288 Anzahl der Felder: 47

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)

- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)

- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### **SCTP over IPv4-Egress**

Vorlagen-ID: 289 Anzahl der Felder: 51

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)

- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMcastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)

- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### **SCTP over IPv4-Ingress mit Tunnel**

Vorlagen-ID: 290 Anzahl der Felder: 54

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))

- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMcastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMcastOctetTotalCount (Länge: 8)

### **SCTP over IPv4-Egress mit Tunnel**

Vorlagen-ID: 291 Anzahl der Felder: 58

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)

- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)



- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMcastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMcastOctetTotalCount (Länge: 8)

### ICMPv4-IPFIX-Vorlagen für KVM

Es gibt vier ICMPv4-IPFIX-Vorlagen für KVM: Ingress (eingehender Flow), Egress (ausgehender Flow), Ingress mit Tunnel und Egress mit Tunnel.

#### ICMPv4-Ingress

Vorlagen-ID: 292 Anzahl der Felder: 47

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)

- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- ICMP\_IPv4\_TYPE (Länge: 1)
- ICMP\_IPv4\_CODE (Länge: 1)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)

- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

#### **ICMPv4-Egress**

Vorlagen-ID: 293 Anzahl der Felder: 51

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)

- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- ICMP\_IPv4\_TYPE (Länge: 1)
- ICMP\_IPv4\_CODE (Länge: 1)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)

- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### ICMPv4-Ingress mit Tunnel

Vorlagen-ID: 294 Anzahl der Felder: 54

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- ICMP\_IPv4\_TYPE (Länge: 1)
- ICMP\_IPv4\_CODE (Länge: 1)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))

- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

#### **ICMPv4-Egress mit Tunnel**

Vorlagen-ID: 295 Anzahl der Felder: 58

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)

- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- ICMP\_IPv4\_TYPE (Länge: 1)
- ICMP\_IPv4\_CODE (Länge: 1)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)

- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### IPv6-IPFIX-Vorlagen für KVM

Es gibt vier IPv6-IPFIX-Vorlagen für KVM: Ingress (eingehender Flow), Egress (ausgehender Flow), Ingress mit Tunnel und Egress mit Tunnel.

#### IPv6-Ingress

Vorlagen-ID: 296 Anzahl der Felder: 46

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)



- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)

- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### IPv6-Egress

Vorlagen-ID: 297 Anzahl der Felder: 50

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)

- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMcastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)

- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### IPv6-Ingress mit Tunnel

Vorlagen-ID: 298 Anzahl der Felder: 53

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))

- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### IPv6-Egress mit Tunnel

Vorlagen-ID: 299 Anzahl der Felder: 57

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)

- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)

- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### **TCP over IPv6-IPFIX-Vorlagen für KVM**

Es gibt vier TCP over IPv6-IPFIX-Vorlagen für KVM Ingress (eingehender Flow), Egress (ausgehender Flow), Ingress mit Tunnel und Egress mit Tunnel.

#### **TCP over IPv6-Ingress**

Vorlagen-ID: 300 Anzahl der Felder: 54

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)

- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)



- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)
- tcpAckTotalCount (Länge: 8)
- tcpFinTotalCount (Länge: 8)
- tcpPshTotalCount (Länge: 8)
- tcpRstTotalCount (Länge: 8)
- tcpSynTotalCount (Länge: 8)
- tcpUrgTotalCount (Länge: 8)

### **TCP over IPv6-Egress**

Vorlagen-ID: 301 Anzahl der Felder: 58

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)

- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)

- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)
- tcpAckTotalCount (Länge: 8)
- tcpFinTotalCount (Länge: 8)
- tcpPshTotalCount (Länge: 8)
- tcpRstTotalCount (Länge: 8)
- tcpSynTotalCount (Länge: 8)
- tcpUrgTotalCount (Länge: 8)

#### **TCP over IPv6-Ingress mit Tunnel**

Vorlagen-ID: 302 Anzahl der Felder: 61

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)

- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)

- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)
- tcpAckTotalCount (Länge: 8)
- tcpFinTotalCount (Länge: 8)
- tcpPshTotalCount (Länge: 8)
- tcpRstTotalCount (Länge: 8)
- tcpSynTotalCount (Länge: 8)
- tcpUrgTotalCount (Länge: 8)

#### **TCP over IPv6-Egress mit Tunnel**

Vorlagen-ID: 303 Anzahl der Felder: 65

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)

- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)

- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)
- tcpAckTotalCount (Länge: 8)
- tcpFinTotalCount (Länge: 8)
- tcpPshTotalCount (Länge: 8)
- tcpRstTotalCount (Länge: 8)
- tcpSynTotalCount (Länge: 8)
- tcpUrgTotalCount (Länge: 8)

#### **UDP over IPv6-IPFIX-Vorlagen für KVM**

Es gibt vier UDP over IPv6-IPFIX-Vorlagen für KVM: Ingress (eingehender Flow), Egress (ausgehender Flow), Ingress mit Tunnel und Egress mit Tunnel.

#### **UDP over IPv6-Ingress**

Vorlagen-ID: 304 Anzahl der Felder: 48

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)

- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)



- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### UDP over IPv6-Egress

Vorlagen-ID: 305 Anzahl der Felder: 52

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)

- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

## UDP over IPv6-Ingress mit Tunnel

Vorlagen-ID: 306 Anzahl der Felder: 55

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))

- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

#### **UDP over IPv6-Egress mit Tunnel**

Vorlagen-ID: 307 Anzahl der Felder: 59

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)

- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)

- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### **SCTP over IPv6-IPFIX-Vorlagen für KVM**

Es gibt vier SCTP over IPv6-IPFIX-Vorlagen für KVM: Ingress (eingehender Flow), Egress (ausgehender Flow), Ingress mit Tunnel und Egress mit Tunnel.

### **SCTP over IPv6-Ingress**

Vorlagen-ID: 308 Anzahl der Felder: 48

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)

- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)

- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### **SCTP over IPv6-Egress**

Vorlagen-ID: 309 Anzahl der Felder: 52

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)



- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)

- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### **SCTP over IPv6-Ingress mit Tunnel**

Vorlagen-ID: 310 Anzahl der Felder: 55

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))

- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMcastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMcastOctetTotalCount (Länge: 8)

## SCTP over IPv6-Egress mit Tunnel

Vorlagen-ID: 311 Anzahl der Felder: 59

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))

- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

## ICMPv6-IPFIX-Vorlagen für KVM

Es gibt vier ICMPv6-IPFIX-Vorlagen für KVM: Ingress (eingehender Flow), Egress (ausgehender Flow), Ingress mit Tunnel und Egress mit Tunnel.

### ICMPv6-Ingress

Vorlagen-ID: 312 Anzahl der Felder: 48

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- ICMP\_IPv6\_TYPE (Länge: 1)
- ICMP\_IPv6\_CODE (Länge: 1)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)

- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### ICMPv6-Egress

Vorlagen-ID: 313 Anzahl der Felder: 52

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)

- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- ICMP\_IPv6\_TYPE (Länge: 1)
- ICMP\_IPv6\_CODE (Länge: 1)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)



- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

#### **ICMPv6-Ingress mit Tunnel**

Vorlagen-ID: 314 Anzahl der Felder: 55

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)

- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- ICMP\_IPv6\_TYPE (Länge: 1)
- ICMP\_IPv6\_CODE (Länge: 1)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMcastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)

- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### ICMPv6-Egress mit Tunnel

Vorlagen-ID: 315 Anzahl der Felder: 59

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)

- FLOW\_LABEL (Länge: 4)
- ICMP\_IPv6\_TYPE (Länge: 1)
- ICMP\_IPv6\_CODE (Länge: 1)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)

- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### **Ethernet-VLAN-IPFIX-Vorlagen für KVM**

Es gibt vier Ethernet-VLAN-IPFIX-Vorlagen für KVM: Ingress (eingehender Flow), Egress (ausgehender Flow), Ingress mit Tunnel und Egress mit Tunnel.

#### **Ethernet-VLAN-Ingress**

Vorlagen-ID: 316 Anzahl der Felder: 30

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)

- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)

### **Ethernet-VLAN-Egress**

Vorlagen-ID: 317 Anzahl der Felder: 34

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 8)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)

- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)

#### **Ethernet-VLAN-Ingress mit Tunnel**

Vorlagen-ID: 318 Anzahl der Felder: 37

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))

- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)

### **Ethernet-VLAN-Egress mit Tunnel**

Vorlagen-ID: 319 Anzahl der Felder: 41

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)



- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 8)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)

- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)

### IPv4-VLAN-IPFIX-Vorlagen für KVM

Es gibt vier IPv4-VLAN-IPFIX-Vorlagen für KVM: Ingress (eingehender Flow), Egress (ausgehender Flow), Ingress mit Tunnel und Egress mit Tunnel.

### IPv4-VLAN-Ingress

Vorlagen-ID: 336 Anzahl der Felder: 48

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)

- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMcastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMcastOctetTotalCount (Länge: 8)

#### **IPv4-VLAN-Egress**

Vorlagen-ID: 337 Anzahl der Felder: 52

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)

- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)

- MUL\_DPKTS (Länge: 8)
- postMcastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMcastOctetTotalCount (Länge: 8)

#### **IPv4-VLAN-Ingress mit Tunnel**

Vorlagen-ID: 338 Anzahl der Felder: 55

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)

- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)

- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### **IPv4-VLAN-Egress mit Tunnel**

Vorlagen-ID: 339 Anzahl der Felder: 59

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)

- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)



- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### **TCP over IPv4-VLAN-IPFIX-Vorlagen für KVM**

Es gibt vier TCP over IPv4-VLAN-IPFIX-Vorlagen für KVM: Ingress (eingehender Flow), Egress (ausgehender Flow), Ingress mit Tunnel und Egress mit Tunnel.

### **TCP over IPv4-VLAN-Ingress**

Vorlagen-ID: 340 Anzahl der Felder: 56

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)

- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)
- tcpAckTotalCount (Länge: 8)

- tcpFinTotalCount (Länge: 8)
- tcpPshTotalCount (Länge: 8)
- tcpRstTotalCount (Länge: 8)
- tcpSynTotalCount (Länge: 8)
- tcpUrgTotalCount (Länge: 8)

### **TCP over IPv4-VLAN-Egress**

Vorlagen-ID: 341 Anzahl der Felder: 60

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)

- IP\_DST\_ADDR (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)
- tcpAckTotalCount (Länge: 8)
- tcpFinTotalCount (Länge: 8)

- tcpPshTotalCount (Länge: 8)
- tcpRstTotalCount (Länge: 8)
- tcpSynTotalCount (Länge: 8)
- tcpUrgTotalCount (Länge: 8)

### **TCP over IPv4-VLAN-Ingress mit Tunnel**

Vorlagen-ID: 342 Anzahl der Felder: 63

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))

- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

- tcpAckTotalCount (Länge: 8)
- tcpFinTotalCount (Länge: 8)
- tcpPshTotalCount (Länge: 8)
- tcpRstTotalCount (Länge: 8)
- tcpSynTotalCount (Länge: 8)
- tcpUrgTotalCount (Länge: 8)

### **TCP over IPv4-VLAN-Egress mit Tunnel**

Vorlagen-ID: 343 Anzahl der Felder: 67

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)

- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)



- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)
- tcpAckTotalCount (Länge: 8)
- tcpFinTotalCount (Länge: 8)
- tcpPshTotalCount (Länge: 8)
- tcpRstTotalCount (Länge: 8)
- tcpSynTotalCount (Länge: 8)
- tcpUrgTotalCount (Länge: 8)

#### **UDP over IPv4-VLAN-IPFIX-Vorlagen für KVM**

Es gibt vier UDP over IPv4-VLAN-IPFIX-Vorlagen für KVM: Ingress (eingehender Flow), Egress (ausgehender Flow), Ingress mit Tunnel und Egress mit Tunnel.

#### **UDP over IPv4-VLAN-Ingress**

Vorlagen-ID: 344 Anzahl der Felder: 50

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)

- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMcastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)

- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### **UDP over IPv4-VLAN-Egress**

Vorlagen-ID: 345 Anzahl der Felder: 54

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)

- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

#### UDP over IPv4-VLAN-Ingress mit Tunnel

Vorlagen-ID: 346 Anzahl der Felder: 57

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))

- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

#### **UDP over IPv4-VLAN-Egress mit Tunnel**

Vorlagen-ID: 347 Anzahl der Felder: 61

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)

- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))

- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### **SCTP over IPv4-VLAN-IPFIX-Vorlagen für KVM**

Es gibt vier SCTP over IPv4-VLAN-IPFIX-Vorlagen für KVM: Ingress (eingehender Flow), Egress (ausgehender Flow), Ingress mit Tunnel und Egress mit Tunnel.

### **SCTP over IPv4-VLAN-Ingress**

Vorlagen-ID: 348 Anzahl der Felder: 50



Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)

- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

#### **SCTP over IPv4-VLAN-Egress**

Vorlagen-ID: 349 Anzahl der Felder: 54

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)

- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)

- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### **SCTP over IPv4-VLAN-Ingress mit Tunnel**

Vorlagen-ID: 350 Anzahl der Felder: 57

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)

- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)

- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### **SCTP over IPv4-VLAN-Egress mit Tunnel**

Vorlagen-ID: 351 Anzahl der Felder: 61

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)

- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)

- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### ICMPv4-VLAN-IPFIX-Vorlagen für KVM

Es gibt vier ICMPv4-VLAN-IPFIX-Vorlagen für KVM: Ingress (eingehender Flow), Egress (ausgehender Flow), Ingress mit Tunnel und Egress mit Tunnel.

#### ICMPv4-VLAN-Ingress

Vorlagen-ID: 352 Anzahl der Felder: 50

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)



- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- ICMP\_IPv4\_TYPE (Länge: 1)
- ICMP\_IPv4\_CODE (Länge: 1)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

## ICMPv4-VLAN-Egress

Vorlagen-ID: 353 Anzahl der Felder: 54

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- ICMP\_IPv4\_TYPE (Länge: 1)
- ICMP\_IPv4\_CODE (Länge: 1)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)

- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

#### **ICMPv4-VLAN-Ingress mit Tunnel**

Vorlagen-ID: 354 Anzahl der Felder: 57

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)

- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- ICMP\_IPv4\_TYPE (Länge: 1)
- ICMP\_IPv4\_CODE (Länge: 1)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)

- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

#### **ICMPv4-VLAN-Egress mit Tunnel**

Vorlagen-ID: 355 Anzahl der Felder: 61

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)

- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IP\_SRC\_ADDR (Länge: 4)
- IP\_DST\_ADDR (Länge: 4)
- ICMP\_IPv4\_TYPE (Länge: 1)
- ICMP\_IPv4\_CODE (Länge: 1)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)

- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### IPv6-VLAN-IPFIX-Vorlagen für KVM

Es gibt vier IPv6-VLAN-IPFIX-Vorlagen für KVM: Ingress (eingehender Flow), Egress (ausgehender Flow), Ingress mit Tunnel und Egress mit Tunnel.

#### IPv6-VLAN-Ingress

Vorlagen-ID: 356 Anzahl der Felder: 49

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)

- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)



- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### IPv6-VLAN-Egress

Vorlagen-ID: 357 Anzahl der Felder: 53

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)

- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMcastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)

- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### IPv6-VLAN-Ingress mit Tunnel

Vorlagen-ID: 358 Anzahl der Felder: 56

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))

- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMcastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMcastOctetTotalCount (Länge: 8)

## IPv6-VLAN-Egress mit Tunnel

Vorlagen-ID: 359 Anzahl der Felder: 60

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))

- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

## TCP over IPv6-VLAN-IPFIX-Vorlagen für KVM

Es gibt vier TCP over IPv6-VLAN-IPFIX-Vorlagen für KVM: Ingress (eingehender Flow), Egress (ausgehender Flow), Ingress mit Tunnel und Egress mit Tunnel.

### TCP over IPv6-VLAN-Ingress

Vorlagen-ID: 360 Anzahl der Felder: 57

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)

- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)
- tcpAckTotalCount (Länge: 8)
- tcpFinTotalCount (Länge: 8)
- tcpPshTotalCount (Länge: 8)
- tcpRstTotalCount (Länge: 8)
- tcpSynTotalCount (Länge: 8)
- tcpUrgTotalCount (Länge: 8)



## TCP over IPv6-VLAN-Egress

Vorlagen-ID: 361 Anzahl der Felder: 61

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))

- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)
- tcpAckTotalCount (Länge: 8)
- tcpFinTotalCount (Länge: 8)
- tcpPshTotalCount (Länge: 8)
- tcpRstTotalCount (Länge: 8)
- tcpSynTotalCount (Länge: 8)
- tcpUrgTotalCount (Länge: 8)

## TCP over IPv6-VLAN-Ingress mit Tunnel

Vorlagen-ID: 362 Anzahl der Felder: 64

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))

- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)
- tcpAckTotalCount (Länge: 8)
- tcpFinTotalCount (Länge: 8)
- tcpPshTotalCount (Länge: 8)

- tcpRstTotalCount (Länge: 8)
- tcpSynTotalCount (Länge: 8)
- tcpUrgTotalCount (Länge: 8)

### **TCP over IPv6-VLAN-Egress mit Tunnel**

Vorlagen-ID: 363 Anzahl der Felder: 68

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)

- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMcastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)

- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)
- tcpAckTotalCount (Länge: 8)
- tcpFinTotalCount (Länge: 8)
- tcpPshTotalCount (Länge: 8)
- tcpRstTotalCount (Länge: 8)
- tcpSynTotalCount (Länge: 8)
- tcpUrgTotalCount (Länge: 8)

### UDP over IPv6-VLAN-IPFIX-Vorlagen für KVM

Es gibt vier UDP over IPv6-VLAN-IPFIX-Vorlagen für KVM: Ingress (eingehender Flow), Egress (ausgehender Flow), Ingress mit Tunnel und Egress mit Tunnel.

### UDP over IPv6-VLAN-Ingress

Vorlagen-ID: 364 Anzahl der Felder: 51

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)

- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)



- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### UDP over IPv6-VLAN-Egress

Vorlagen-ID: 365 Anzahl der Felder: 55

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)

- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

#### **UDP over IPv6-VLAN-Ingress mit Tunnel**

Vorlagen-ID: 366 Anzahl der Felder: 58

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))

- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

#### **UDP over IPv6-VLAN-Egress mit Tunnel**

Vorlagen-ID: 367 Anzahl der Felder: 62

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)

- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))

- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMcastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMcastOctetTotalCount (Länge: 8)

### **SCTP over IPv6-VLAN-IPFIX-Vorlagen für KVM**

Es gibt vier SCTP over IPv6-VLAN-IPFIX-Vorlagen für KVM: Ingress (eingehender Flow), Egress (ausgehender Flow), Ingress mit Tunnel und Egress mit Tunnel.

## SCTP over IPv6-VLAN-Ingress

Vorlagen-ID: 368 Anzahl der Felder: 51

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)

- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### **SCTP over IPv6-VLAN-Egress**

Vorlagen-ID: 369 Anzahl der Felder: 55

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)



- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)

- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### **SCTP over IPv6-VLAN-Ingress mit Tunnel**

Vorlagen-ID: 370 Anzahl der Felder: 58

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)

- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)

- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

#### **SCTP over IPv6-VLAN-Egress mit Tunnel**

Vorlagen-ID: 371 Anzahl der Felder: 62

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)

- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- L4\_SRC\_PORT (Länge: 2)
- L4\_DST\_PORT (Länge: 2)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)

- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### ICMPv6-VLAN-IPFIX-Vorlagen für KVM

Es gibt vier ICMPv6-IPFIX-Vorlagen für KVM: Ingress (eingehender Flow), Egress (ausgehender Flow), Ingress mit Tunnel und Egress mit Tunnel.

#### ICMPv6-Ingress

Vorlagen-ID: 372 Anzahl der Felder: 51

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)

- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- ICMP\_IPv6\_TYPE (Länge: 1)
- ICMP\_IPv6\_CODE (Länge: 1)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)

- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMcastOctetTotalCount (Länge: 8)

### ICMPv6-Egress

Vorlagen-ID: 373 Anzahl der Felder: 55

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)



- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- ICMP\_IPv6\_TYPE (Länge: 1)
- ICMP\_IPv6\_CODE (Länge: 1)
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP\_LENGTH\_MINIMUM (Länge: 8)
- IP\_LENGTH\_MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)

- postMCastOctetTotalCount (Länge: 8)

### ICMPv6-Ingress mit Tunnel

Vorlagen-ID: 374 Anzahl der Felder: 58

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- ICMP\_IPv6\_TYPE (Länge: 1)
- ICMP\_IPv6\_CODE (Länge: 1)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))
- 896 (Länge: 2, PEN: VMware Inc. (6876))

- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

### ICMPv6-Egress mit Tunnel

Vorlagen-ID: 375 Anzahl der Felder: 62

Die Vorlage umfasst folgende Felder:

- observationPointId (Länge: 4)
- DIRECTION (Länge:1)
- SRC\_MAC (Länge: 6)
- DESTINATION\_MAC (Länge: 6)
- ethernetType (Länge: 2)
- ethernetHeaderLength (Länge: 1)
- INPUT\_SNMP (Länge: 4)
- Unknown(368) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- OUTPUT\_SNMP (Länge: 4)
- Unknown(369) (Länge: 4)
- IF\_NAME (Länge: variabel)
- IF\_DESC (Länge: variabel)
- SRC\_VLAN (Länge: 2)
- dot1qVlanId (Länge: 2)
- dot1qPriority (Länge: 1)
- IP\_PROTOCOL\_VERSION (Länge: 1)
- IP\_TTL (Länge: 1)
- PROTOCOL (Länge: 1)
- IP\_DSCP (Länge: 1)
- IP\_PRECEDENCE (Länge: 1)
- IP\_TOS (Länge: 1)
- IPV6\_SRC\_ADDR (Länge: 4)
- IPV6\_DST\_ADDR (Länge: 4)
- FLOW\_LABEL (Länge: 4)
- ICMP\_IPv6\_TYPE (Länge: 1)
- ICMP\_IPv6\_CODE (Länge: 1)
- 893 (Länge: 4, PEN: VMware Inc. (6876))
- 894 (Länge: 4, PEN: VMware Inc. (6876))
- 895 (Länge: 1, PEN: VMware Inc. (6876))

- 896 (Länge: 2, PEN: VMware Inc. (6876))
- 897 (Länge: 2, PEN: VMware Inc. (6876))
- 891 (Länge: 1, PEN: VMware Inc. (6876))
- 892 (Länge: variabel, PEN: VMware Inc. (6876))
- 898 (Länge: variabel, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (Länge: 4)
- flowEndDeltaMicroseconds (Länge: 4)
- DROPPED\_PACKETS (Länge: 8)
- DROPPED\_PACKETS\_TOTAL (Länge: 8)
- PKTS (Länge: 8)
- PACKETS\_TOTAL (Länge: 8)
- Unknown(354) (Länge: 8)
- Unknown(355) (Länge: 8)
- Unknown(356) (Länge: 8)
- Unknown(357) (Länge: 8)
- Unknown(358) (Länge: 8)
- MUL\_DPKTS (Länge: 8)
- postMCastPacketTotalCount (Länge: 8)
- Unknown(352) (Länge: 8)
- Unknown(353) (Länge: 8)
- flowEndReason (Länge: 1)
- DROPPED\_BYTES (Länge: 8)
- DROPPED\_BYTES\_TOTAL (Länge: 8)
- BYTES (Länge: 8)
- BYTES\_TOTAL (Länge: 8)
- BYTES\_SQUARED (Länge: 8)
- BYTES\_SQUARED\_PERMANENT (Länge: 8)
- IP LENGTH MINIMUM (Länge: 8)
- IP LENGTH MAXIMUM (Länge: 8)
- MUL\_DOCTETS (Länge: 8)
- postMCastOctetTotalCount (Länge: 8)

## IPFIX-Optionsvorlagen für KVM

Es gibt eine Optionsvorlage für KVM, basierend auf IETF RFC 7011 Abschnitt 3.4.2.

### Optionsvorlage

Vorlagen-ID: 462 Scope Count: 1. Data Count: 1.

## Überwachen einer Logischer Switch Port-Aktivität

Sie haben die Möglichkeit, die Aktivität eines logischen Ports zu überwachen, z. B. für die Fehlerbehebung bei einer Netzwerküberlastung oder bei verworfenen Paketen.

### Voraussetzungen

Stellen Sie sicher, dass ein logischer Switch Port konfiguriert ist. Siehe [Verbinden einer VM mit einem logischen Switch](#).

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 **Netzwerk und Sicherheit – Erweitert > Netzwerk > Switching > Ports** auswählen
- 3 Klicken Sie auf den Namen eines Ports.
- 4 Klicken Sie auf die Registerkarte **Überwachen**.  
Der Portstatus und Statistiken werden angezeigt.
- 5 Um eine CSV-Datei von den MAC-Adressen herunterzuladen, die vom Host abgerufen wurden, klicken Sie auf **MAC-Tabelle herunterladen**.
- 6 Um die Aktivität am Port zu überwachen, klicken Sie auf **Nachverfolgung starten**.  
Eine Seite für die Portnachverfolgung wird geöffnet. Sie können den bidirektionalen Portdatenverkehr einsehen und verworfene Pakete ermitteln. Die Seite für die Portnachverfolgung enthält auch die Switching-Profile, die an den logischen Switch Port angefügt wurden.

### Ergebnisse

Wenn Sie feststellen, dass Pakete wegen einer Netzwerküberlastung verworfen wurden, können Sie ein QoS-Switching-Profil für den logischen Switch Port konfigurieren, um einen Datenverlust bei bevorzugten Paketen zu vermeiden. Siehe [Grundlegendes zum QoS-Switching-Profil](#).

## Überwachen von Fabric-Knoten

Sie können Fabric-Knoten wie Hosts, Edges, NSX Edge-Cluster, Bridges und Transportknoten mithilfe der Benutzeroberfläche von NSX Manager überwachen.

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie im Navigationsbereich die Option **Fabric > Knoten** aus.
- 3 Wählen Sie eine der nachfolgend aufgeführten Registerkarten aus.
  - Hosts
  - Edges
  - Edge-Cluster
  - Bridges
  - Transportknoten

## Ergebnisse

---

**Hinweis** Sie können den LCP-Konnektivitätsstatus im Bildschirm „Hosts“ ignorieren, wenn für den MPA-Konnektivitätsstatus eines Hosts „Nicht vorhanden“ oder „Unbekannt“ angegeben wird, da dieser möglicherweise fehlerhaft ist.


---

# Logische Switches

# 13

Sie können logische Switches und verwandte Objekte über die Registerkarte **Netzwerk und Sicherheit – Erweitert** konfigurieren. Ein logischer Switch bildet die Switching-Funktionalität, Broadcast-, unbekannten Unicast- und Multicast (BUM)-Datenverkehr in einer virtuellen Umgebung ab, die von der zugrunde liegenden Hardware entkoppelt ist.

---

**Hinweis** Wenn Sie die Benutzeroberfläche **Netzwerk und Sicherheit – Erweitert** verwenden, um in der Richtlinienschnittstelle erstellte Objekte zu ändern, sind einige Einstellungen möglicherweise nicht konfigurierbar. Neben diesen schreibgeschützten Einstellungen wird dieses Symbol angezeigt: . Weitere Informationen hierzu finden Sie unter [Kapitel 1 Übersicht über NSX Manager](#).

---

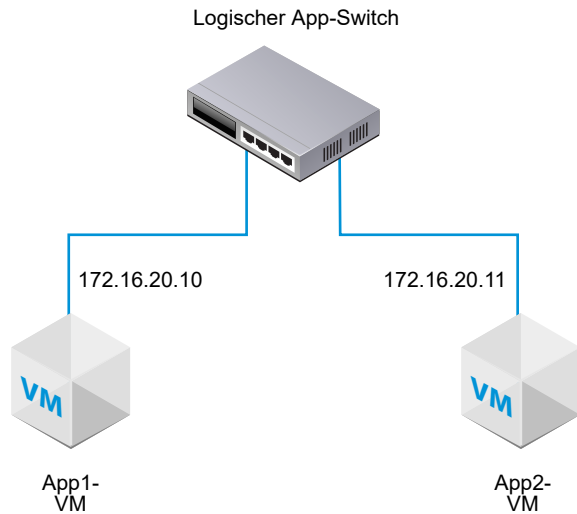
Logische Switches sind mit VLANs insofern vergleichbar, da sie Netzwerkverbindungen bereitstellen, an die virtuelle Maschinen angefügt werden können. Die VMs können dann über Tunnel zwischen Hypervisoren miteinander kommunizieren, wenn sie mit demselben logischen Switch verbunden sind. Jeder logische Switch verfügt über einen VNI (Virtueller Network Identifier, Virtueller Netzwerkbezeichner) wie eine VLAN-ID. Anders als bei VLAN lassen sich VNIs über die Beschränkungen von VLAN-IDs hinaus gut skalieren.

Um den VNI-Wertepool anzuzeigen und zu bearbeiten, melden Sie sich bei NSX Manager an, navigieren Sie zu **Fabric > Profile**, und klicken Sie auf die Registerkarte **Konfiguration**. Beachten Sie, dass die Erstellung eines logischen Switches bei einem zu kleinen Pool fehlschlägt, falls sämtliche VNI-Werte verwendet werden. Wenn Sie einen logischen Switch löschen, wird der VNI-Wert erneut verwendet, allerdings erst nach Ablauf von sechs Stunden.

Wenn Sie logische Switches hinzufügen, müssen Sie zuerst die Topologie entwickeln, die aufgebaut werden soll.



Abbildung 13-1. Topologie für einen logischen Switch



Beispielsweise enthält die Topologie oben einen einzelnen logischen Switch, der mit zwei VMs verbunden ist. Die beiden VMs können sich auf verschiedenen Hosts oder auf demselben Host, in verschiedenen Hostclustern oder im selben Hostcluster befinden. Da sich die VMs im Beispiel im selben virtuellen Netzwerk befinden, müssen die in den VMs konfigurierten zugrunde liegenden IP-Adressen im selben Subnetz enthalten sein.

---

**NSX Cloud-Hinweis** Wenn Sie NSX Cloud verwenden, finden Sie unter [Verwendung von NSX-T Data Center-Funktionen mit der Public Cloud](#) eine Liste der automatisch generierten logischen Einheiten, unterstützten Funktionen und Konfigurationen, die für NSX Cloud erforderlich sind.

---

Dieses Kapitel enthält die folgenden Themen:

- [Grundlegendes zu den BUM-Frame-Replizierungsmodi](#)
- [Erstellen eines logischen Switches](#)
- [Verbinden einer VM mit einem logischen Switch](#)
- [Erstellen eines logischen Switch Ports](#)
- [Testen der Schicht-2-Konnektivität](#)
- [Erstellen eines logischen VLAN-Switch für den NSX Edge-Uplink](#)
- [Switching-Profil für logische Switches und logische Ports](#)
- [Schicht 2-Bridging](#)

## Grundlegendes zu den BUM-Frame-Replizierungsmodi

Jeder Hosttransportknoten ist ein Tunnel-Endpoint. Jeder Tunnel-Endpoint verfügt über eine IP-Adresse. Diese IP-Adressen können sich im selben Subnetz oder in unterschiedlichen Subnetzen befinden, je nachdem, wie Sie die IP-Pools oder DHCP für Ihre Transportknoten konfiguriert haben.

Wenn zwei VMs auf unterschiedlichen Hosts direkt kommunizieren, wird der Unicast-gekapselte Datenverkehr zwischen den beiden Tunnel-Endpoint-IP-Adressen, die den beiden Hypervisoren zugeordnet sind, ausgetauscht und es ist kein Fluten nötig.

Wie bei jedem Schicht-2-Netzwerk muss allerdings manchmal der von einer VM generierte Datenverkehr weitergeleitet, also geflutet werden. Damit ist gemeint, dass dieser an alle anderen VMs gesendet werden muss, die zum selben logischen Switch gehören. Dies ist bei einem Schicht-2-Datenverkehr von Typ „Broadcast“, „Unbekannter Unicast“ und „Multicast“ (BUM-Datenverkehr) der Fall. Denken Sie daran, dass ein einzelner logischer NSX-T Data Center-Switch für mehrere Hypervisoren zuständig sein kann. Von einer VM generierter BUM-Datenverkehr auf einem bestimmten Hypervisor muss auf Remote-Hypervisoren repliziert werden, die andere VMs hosten, die mit demselben logischen Switch verbunden sind. Für die Aktivierung dieser Überflutung unterstützt NSX-T Data Center zwei unterschiedliche Replizierungsmodi:

- Hierarchischer Zwei-Ebenen-Modus (manchmal als MTEP bezeichnet)
- Head-Modus (manchmal als „Quellmodus“ bezeichnet)

Der hierarchische Zwei-Ebenen-Replizierungsmodus soll durch das nachfolgend dargestellte Beispiel veranschaulicht werden. Angenommen, Sie verfügen über einen Host A mit VMs, die mit den virtuellen Netzwerkbezeichnern (VNIs) 5000, 5001 und 5002 verbunden sind. Sie können sich VNIs wie VLANs vorstellen, wobei jeder logische Switch über einen einzelnen ihm zugeordneten VNI verfügt. Aus diesem Grund werden die Begriffe „VNI“ und „Logischer Switch“ manchmal synonym verwendet. Wenn wir davon sprechen, dass sich ein Host auf einem VNI befindet, ist damit gemeint, dass er über VMs verfügt, die mit einem logischen Switch mit diesem VNI verbunden sind.

Eine Tabelle der Tunnel-Endpoints zeigt die Host-VNI-Verbindungen an. Host A wertet die Tunnel-Endpoint-Tabelle für den VNI 5000 aus und ermittelt die Tunnel-Endpoint-IP-Adressen für die anderen Hosts auf dem VNI 5000.

Einige dieser VNI-Verbindungen befinden sich im selben IP-Subnetz (auch als „IP-Segment“ bezeichnet) wie der Tunnel-Endpoint auf Host A. Für jede dieser Verbindungen erstellt Host A eine separate Kopie jedes BUM-Frames und sendet diese direkt an jeden Host.

Andere Tunnel-Endpoints von Hosts befinden sich auf unterschiedlichen Subnetzen bzw. in unterschiedlichen IP-Segmenten. Für jedes Segment mit mehr als einem Tunnel-Endpoint benennt Host A einen dieser Tunnel-Endpoints als Replikator.

Der Replikator empfängt von Host A eine Kopie jedes BUM-Frames für VNI 5000. Diese Kopie wird in der Kapselungskopfzeile als „Lokal repliziert“ gekennzeichnet. Host A sendet keine Kopien an andere Hosts im selben IP-Segment wie der Replikator. Es obliegt nun dem Replikator, eine Kopie des BUM-Frames für jeden bekannten Host auf dem VNI 5000 und im selben IP-Segment wie dieser Replikatorhost zu erstellen.

Der Vorgang wird für VNI 5001 und 5002 repliziert. Die Liste der Tunnel-Endpoints und der sich ergebenden Replikatoren kann sich für verschiedene VNIs unterscheiden.

Bei der Head-Replizierung (auch als „Headend-Replizierung“ bezeichnet) sind keine Replikatoren notwendig. Host A erstellt einfach eine Kopie jedes BUM-Frames für jeden bekannten Tunnel-Endpoint auf dem VNI 5000 und sendet diesen.

Wenn sich alle Hosttunnel-Endpoints auf demselben Subnetz befinden, spielt die Auswahl des Replizierungsmodus keine Rolle, da sich das Replizierungsverhalten dann nicht unterscheidet. Wenn sich die Hosttunnel-Endpoints auf unterschiedlichen Subnetzen befinden, unterstützt der hierarchische Zwei-Ebenen-Replizierungsmodus die Verteilung der Arbeitslast auf mehrere Hosts. Der hierarchische Zwei-Ebenen-Modus ist der Standardmodus.

## Erstellen eines logischen Switches

Logische Switches werden an einzelne oder mehrere VMs im Netzwerk angefügt. Die mit einem logischen Switch verbundenen VMs können mithilfe der Tunnel zwischen Hypervisoren miteinander kommunizieren.

### Voraussetzungen

- Stellen Sie sicher, dass eine Transportzone konfiguriert ist. Siehe *Installationshandbuch für NSX-T Data Center*.
- Stellen Sie sicher, dass Fabric-Knoten erfolgreich mit dem NSX-T Data Center-Verwaltungskomponenten (MPA)-Agenten und der lokalen NSX-T Data Center-Steuerungskomponente (LCP) verbunden wurden.

Im GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/state`-API-Aufruf muss state auf success eingestellt sein. Siehe *Installationshandbuch für NSX-T Data Center*.

- Stellen Sie sicher, dass zur Transportzone Transportknoten hinzugefügt wurden. Siehe *Installationshandbuch für NSX-T Data Center*.
- Stellen Sie sicher, dass die Hypervisoren dem NSX-T Data Center-Fabric hinzugefügt wurden und die VMs auf diesen Hypervisoren gehostet werden.
- Machen Sie sich mit der Topologie des logischen Switch und mit den Konzepten der BUM-Frame-Replizierung vertraut. Siehe [Kapitel 13 Logische Switches](#) und [Grundlegendes zu den BUM-Frame-Replizierungsmodi](#).

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > Switching > Switches > Hinzufügen** aus.
- 3 Geben Sie für den logischen Switch einen Namen und optional eine Beschreibung ein.
- 4 Wählen Sie eine Transportzone für den logischen Switch aus.

VMs, die an logische Switches angefügt wurden, die sich in derselben Transportzone befinden, können miteinander kommunizieren.

- 5 Geben Sie den Namen einer Uplink-Teaming-Richtlinie ein.
- 6 Legen Sie den **Administrativen Status** auf **Aktiv** oder **Inaktiv** fest.
- 7 Wählen Sie einen Replizierungsmodus für den logischen Switch aus.

Der Replizierungsmodus (hierarchischer Zwei-Tier- oder Head-Modus) ist für logische Overlay-Switches, aber nicht für VLAN-basierte logische Switches erforderlich.

Replizierungsmodus	Beschreibung
<b>Hierarchischer Zwei-Tier-Modus</b>	Der Replikator ist ein Host, der die Replizierung des BUM-Datenverkehrs auf andere Hosts innerhalb des gleichen VNI durchführt. Jeder Host benennt einen Hosttunnel-Endpoint in jedem VNI als Replikator. Dies wird für jeden VNI durchgeführt.
<b>HEAD</b>	Hosts erstellen eine Kopie jedes BUM-Frames und senden diese an jeden bekannten Tunnel-Endpoint für jeden VNI.

- 8 (Optional) Geben Sie eine VLAN-ID oder Bereiche von VLAN-IDs für das VLAN-Tagging an.

Um das Gast-VLAN-Tagging für an diesen Switch angeschlossene VMs zu unterstützen, müssen Sie VLAN-ID-Bereiche, auch Trunk-VLAN-ID-Bereiche genannt, angeben. Der logische Port filtert dann Pakete nach den Trunk-VLAN-ID-Bereichen, und eine Gast-VM kann ihre Pakete mit der eigenen VLAN-ID basierend auf den Trunk-VLAN-ID-Bereichen kennzeichnen.

- 9 (Optional) Klicken Sie auf die Registerkarte **Switching-Profile** und wählen Sie Switching-Profile aus.
- 10 Klicken Sie auf **Speichern**.

Der neue logische Switch wird in der NSX Manager-Benutzeroberfläche als anklickbarer Link zur Verfügung gestellt.

#### Nächste Schritte

Fügen Sie VMs an Ihren logischen Switch an. Siehe [Verbinden einer VM mit einem logischen Switch](#).

## Verbinden einer VM mit einem logischen Switch

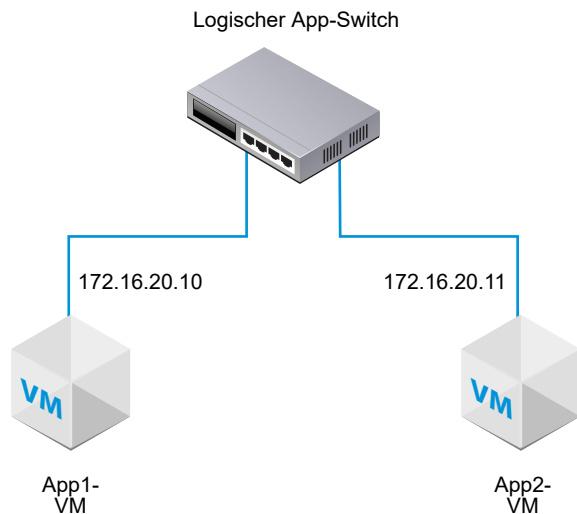
Die Konfiguration zum Verbinden einer VM mit einem logischen Switch ist vom jeweiligen Host abhängig.

Die folgenden Hosts können mit einem logischen Switch verbunden werden: ein ESXi-Host, der in vCenter Server verwaltet wird, ein eigenständiger ESXi-Host und ein KVM-Host.

## Anfügen einer auf vCenter Server gehosteten VM an einen logischen NSX-T Data Center-Switch

Wenn Sie über einen ESXi-Host verfügen, der in vCenter Server verwaltet wird, können Sie auf die Host-VMs über den webbasierten vSphere Web Client zugreifen. In diesem Fall haben Sie die Möglichkeit, mit diesem Vorgang VMs an logische NSX-T Data Center-Switches anzufügen.

Das in diesem Verfahren gezeigte Beispiel veranschaulicht das Verknüpfen einer VM namens app-vm mit einem logischen Switch namens app-switch.



Die installationsbasierte vSphere Client-Anwendung unterstützt nicht das Anfügen einer VM an einen logischen NSX-T Data Center-Switch. Wenn Sie nicht über einen (webbasierten) vSphere Web Client verfügen, finden Sie Informationen unter [Verknüpfen einer auf eigenständigem ESXi gehosteten VM mit einem logischen NSX-T Data Center-Switch](#).

### Voraussetzungen

- Die VMs müssen auf Hypervisoren gehostet werden, die der NSX-T Data Center-Fabric hinzugefügt wurden.
- Die Fabric-Knoten müssen über eine NSX-T Data Center-MPA (Management Plane)- und eine NSX-T Data Center-LCP (Control Plane)-Konnektivität verfügen.
- Die Fabric-Knoten müssen einer Transportzone hinzugefügt werden.
- Ein logischer Switch muss erstellt werden.

### Verfahren

- 1 Bearbeiten Sie im vSphere Web Client die VM-Einstellungen und fügen Sie die VM an den logischen NSX-T Data Center-Switch an.

Beispiel:



2 Klicken Sie auf **OK**.

### Ergebnisse

Nach dem Anfügen einer VM an einen logischen Switch werden dem logischen Switch Ports für logische Switches hinzugefügt. Im NSX Manager unter **Netzwerk und Sicherheit – Erweitert > Netzwerk > Switching > Ports** können Sie logische Switch-Ports anzeigen.

In der NSX-T Data Center-API haben Sie die Möglichkeit, NSX-T Data Center-angefügte VMs mit dem GET <https://<nsx-mgr>/api/v1/fabric/virtual-machines-API-Aufruf> einzusehen.

Die VIF-Anhang-ID unter **Netzwerk und Sicherheit – Erweitert > Netzwerk > Switching > Ports** in der NSX-T Data Center Manager-Benutzeroberfläche entspricht der externen ID (ExternalID) im API-Aufruf. Suchen Sie nach der VIF-Anhang-ID, die der externen VM-ID (ExternalID) entspricht, und stellen Sie sicher, dass der Verwaltungsstatus sowie der Betriebsstatus aktiviert sind.

Wenn zwei VMs mit demselben logischen Switch verknüpft sind und in demselben Subnetz konfigurierte IP-Adressen aufweisen, sollten Sie sich gegenseitig Ping-Befehle senden können.

### Nächste Schritte

Fügen Sie einen logischen Router hinzu.

Sie können die Aktivität am logischen Switch-Port überwachen, um Probleme zu beheben. Siehe „Überwachen der Aktivität eines Ports für einen logischen Switch“ im *Administratorhandbuch für NSX-T Data Center*.

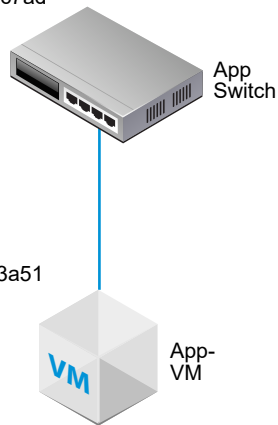
## Verknüpfen einer auf eigenständigem ESXi gehosteten VM mit einem logischen NSX-T Data Center-Switch

Wenn Sie mit einem eigenständigen ESXi-Host arbeiten, können Sie nicht über den webbasierten vSphere Web Client auf die Host-VMs zugreifen. In diesem Fall haben Sie die Möglichkeit, mit diesem Vorgang VMs an logische NSX-T Data Center-Switches anzufügen.

Das in diesem Verfahren gezeigte Beispiel veranschaulicht das Verknüpfen einer VM namens app-vm mit einem logischen Switch namens app-switch.

Nicht transparente Switch-Netzwerk-ID:  
22b22448-38bc-419b-bea8-b51126bec7ad

Externe VM-ID:  
50066bae-0f8a-386b-e62e-b0b9c6013a51



### Voraussetzungen

- Die VM muss auf Hypervisoren gehostet werden, die dem NSX-T Data Center-Fabric hinzugefügt wurden.
- Die Fabric-Knoten müssen über eine NSX-T Data Center-MPA (Verwaltungskomponenten)- und eine NSX-T Data Center-LCP (Steuerungskomponenten)-Konnektivität verfügen.
- Die Fabric-Knoten müssen einer Transportzone hinzugefügt werden.
- Ein logischer Switch muss erstellt werden.
- Sie müssen auf die NSX Manager-API zugreifen können.
- Sie benötigen Schreibzugriff für die VMX-Datei der VM.

## Verfahren

- 1 Verwenden Sie die (installationsbasierte) vSphere Client-Anwendung oder ein anderes VM-Managementtool, um die VM zu bearbeiten und einen VMXNET 3-Ethernet-Adapter hinzuzufügen.

Wählen Sie ein beliebiges benanntes Netzwerk. Sie ändern die Netzwerkverbindung in einem späteren Schritt.

### Hardware anpassen

Hardware der virtuellen Maschine konfigurieren

The screenshot shows the 'Virtuelle Hardware' tab in the vSphere Client. The 'Neues Netzwerk' (New Network) section is highlighted in yellow. It shows a configuration for a VM Network, VMXNET 3 adapter, and 'Beim Einschalten verbinden' (Connect at power on) checked. Below the main configuration, there are buttons for 'Neues Gerät' (New Device) and 'Hinzufügen' (Add).

- 2 Geben Sie über die NSX-T Data Center-API den API-Aufruf GET `https://<nsx-mgr>/api/v1/fabric/virtual-machines/<VM-ID>` aus.

Suchen Sie die externalId der VM in den Ergebnissen.

Beispiel:

```
GET https://<nsx-mgr>/api/v1/fabric/virtual-machines/60a5a5d5-ea2b-407e-a806-4fdc8468f735
```

```
{
  "resource_type": "VirtualMachine",
  "id": "60a5a5d5-ea2b-407e-a806-4fdc8468f735",
  "display_name": "app-vm",
  "compute_ids": [
    "instanceUuid:50066bae-0f8a-386b-e62e-b0b9c6013a51",
    "moIdOnHost:5",
    "externalId:50066bae-0f8a-386b-e62e-b0b9c6013a51",
    "hostLocalId:5",
    "locationId:564dc020-1565-e3f4-f591-ee3953eef3ff",
    "biosUuid:4206f47d-fe7-08c5-5bf7-ea26a4c6b18d"
  ],
}
```



```

"external_id": "50066bae-0f8a-386b-e62e-b0b9c6013a51",
"type": "REGULAR",
"host_id": "cb82b0fa-a8f1-11e5-92a9-6b7d1f8661fa",
"local_id_on_host": "5"
}

```

- 3** Schalten Sie die VM aus und heben Sie ihre Registrierung beim Host auf.

Dazu können Sie das VM-Managementtool oder die ESXi-CLI verwenden, wie hier dargestellt.

```

[user@host:~] vim-cmd /vmsvc/getallvms
Vmid    Name      File           Guest OS      Version  Annotation
5       app-vm    [ds2] app-vm/app-vm.vmx  ubuntuGuest   vmx-08
8       web-vm    [ds2] web-vm/web-vm.vmx  ubuntu64Guest vmx-08

[user@host:~] vim-cmd /vmsvc/power.off 5
Powering off VM:

[user@host:~] vim-cmd /vmsvc/unregister 5

```

- 4** Rufen Sie über die NSX Manager-Benutzeroberfläche die ID des logischen Switches ab.

Beispiel:

app-switch	
Übersicht   Überwachen   Verwalten ▾   Zugehörig ▾	
<div> <div>▾ Übersicht</div> <div>BEARBEITEN</div> </div>	
Name	app-switch
ID	b68e7ac3-877a-420e-af47-53e974c17915
Speicherort	
Beschreibung	lswitch202 (created through automation)
Administrativer Status	● Aktiv
Replizierungsmodus	Head-Replikation
VLAN	Nicht verfügbar
VNI	71681
Logische Ports	1
Datenverkehrstyp	Overlay
Transportzone	transportzone1
Name der Uplink-Teamingrich...	[Use Default]
N-VDS-Modus	STANDARD
Erstellt	9/10/2018, 12:20:46 PM von admin
Zuletzt aktualisiert	9/26/2018, 2:01:14 PM von admin

## 5 Ändern Sie die VMX-Datei der VM.

Löschen Sie das Feld **ethernet1.networkName = "<Name>"** und fügen Sie die folgenden Felder hinzu:

- ethernet1.opaqueNetwork.id = "<ID des logischen Switches>"
- ethernet1.opaqueNetwork.type = "nsx.LogicalSwitch"
- ethernet1.externalId = "<externalId der VM>"
- ethernet1.connected = "TRUE"
- ethernet1.startConnected = "TRUE"

Beispiel:

### ALT

```
ethernet1.pciSlotNumber = "224"
ethernet1.virtualDev = "vmxnet3"
ethernet1.networkName = "VM Network"
ethernet1.addressType = "vpx"
```

```

ethernet1.generatedAddress = "00:50:56:86:7b:d7"
ethernet1.uptCompatibility = "true"
ethernet1.present = "TRUE"

```

**NEU**

```

ethernet1.pciSlotNumber = "224"
ethernet1.virtualDev = "vmxnet3"
ethernet1.addressType = "vpx"
ethernet1.generatedAddress = "00:50:56:86:7b:d7"
ethernet1.uptCompatibility = "true"
ethernet1.present = "TRUE"
ethernet1.opaqueNetwork.id = "22b22448-38bc-419b-bea8-b51126bec7ad"
ethernet1.opaqueNetwork.type = "nsx.LogicalSwitch"
ethernet1.externalId = "50066bae-0f8a-386b-e62e-b0b9c6013a51"
ethernet1.connected = "TRUE"
ethernet1.startConnected = "TRUE"

```

- 6 Fügen Sie in der NSX Manager-Benutzeroberfläche einen logischen Switch Port hinzu und verwenden Sie die externalId der VM als VIF-Anhang.
- 7 Registrieren Sie die VM erneut und schalten Sie sie ein.

Dazu können Sie das VM-Managementtool oder die ESXi-CLI verwenden, wie hier dargestellt.

```
[user@host:~] vim-cmd /solo/register /path/to/file.vmx
```

For example:

```
[user@host:~] vim-cmd solo/registervm /vmfs/volumes/355f2049-6c704347/app-vm/app-vm.vmx
9
```

```
[user@host:~] vim-cmd /vmsvc/power.on 9
```

Powering on VM:

**Ergebnisse**

Suchen Sie auf der NSX Manager-Benutzeroberfläche unter **Netzwerk und Sicherheit – Erweitert > Netzwerk > Switching > Ports** nach der ID des VIF-Anhangs, die der externen ID der VM entspricht, und stellen Sie sicher, dass der Status für den administrativen und Betriebsstatus „Aktiv“ lautet.

Wenn zwei VMs mit demselben logischen Switch verknüpft sind und in demselben Subnetz konfigurierte IP-Adressen aufweisen, sollten Sie sich gegenseitig Ping-Befehle senden können.

**Nächste Schritte**

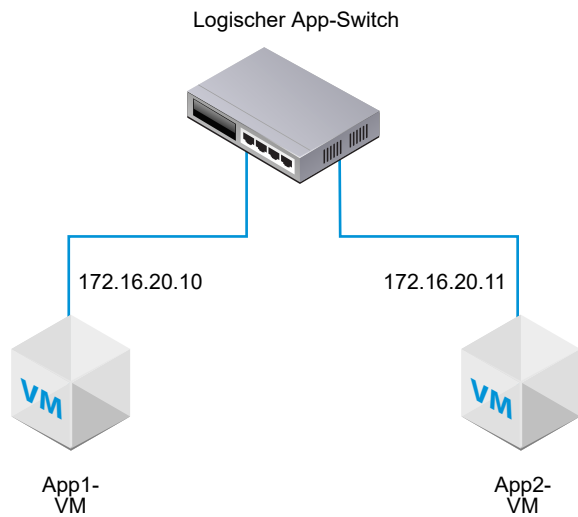
Fügen Sie einen logischen Router hinzu.

Sie können die Aktivität am logischen Switch-Port überwachen, um Probleme zu beheben. Siehe „Überwachen der Aktivität eines Ports für einen logischen Switch“ im *Administratorhandbuch für NSX-T Data Center*.

## Anfügen einer auf KVM-Hosts gehosteten VM an einen logischen NSX-T Data Center-Switch

Wenn Sie über einen KVM-Host verfügen, haben Sie die Möglichkeit, mit diesem Vorgang VMs an logische NSX-T Data Center-Switches anzufügen.

Das in diesem Verfahren gezeigte Beispiel veranschaulicht das Verknüpfen einer VM namens app-vm mit einem logischen Switch namens app-switch.



### Voraussetzungen

- Die VM muss auf Hypervisoren gehostet werden, die dem NSX-T Data Center-Fabric hinzugefügt wurden.
- Die Fabric-Knoten müssen über eine NSX-T Data Center-MPA (Verwaltungskomponenten)- und eine NSX-T Data Center-LCP (Steuerungskomponenten)-Konnektivität verfügen.
- Die Fabric-Knoten müssen einer Transportzone hinzugefügt werden.
- Ein logischer Switch muss erstellt werden.

### Verfahren

- 1 Rufen Sie von der KVM-CLI (Befehlszeilenschnittstelle) aus den Befehl `virsh dumpxml <your vm> | grep interfaceid` auf.
- 2 Fügen Sie mit der NSX Manager-Benutzeroberfläche einen logischen Switch Port hinzu und verwenden Sie die Schnittstellen-ID der VM für die VIF-Anfügung.

## Ergebnisse

Suchen Sie auf der NSX Manager-Benutzeroberfläche unter **Netzwerk und Sicherheit – Erweitert > Netzwerk > Switching > Ports** nach der ID des VIF-Anhangs und stellen Sie sicher, dass der Status für den administrativen und Betriebsstatus „Aktiv“ lautet.

Wenn zwei VMs mit demselben logischen Switch verknüpft sind und in demselben Subnetz konfigurierte IP-Adressen aufweisen, sollten Sie sich gegenseitig Ping-Befehle senden können.

## Nächste Schritte

Fügen Sie einen logischen Router hinzu.

Sie können die Aktivität am logischen Switch-Port überwachen, um Probleme zu beheben. Siehe „Überwachen der Aktivität eines Ports für einen logischen Switch“ im *Administratorhandbuch für NSX-T Data Center*.

# Erstellen eines logischen Switch Ports

Ein Logischer Switch hat mehrere Switch-Ports. Ein logischer Switch Port verbindet eine andere Netzwerkkomponente, eine virtuelle Maschine oder einen Container mit einem logischen Switch.

Wenn Sie eine VM mit einem logischen Switch auf einem ESXi-Host verbinden, der von vCenter Server verwaltet wird, wird automatisch ein logischer Switch Port erstellt. Weitere Informationen zum Verbinden einer virtuellen Maschine mit einem logischen Switch finden Sie unter [Verbinden einer VM mit einem logischen Switch](#).

Weitere Informationen zum Verbinden eines Containers mit einem logischen Switch finden Sie in *NSX-T Container Plug-in für Kubernetes – Installations- und Administratorhandbuch*.

---

**Hinweis** Die IP-Adresse und die MAC-Adresse, die an einen logischen Switch Port für einen Container gebunden sind, werden von NSX Manager zugeteilt. Ändern Sie die Adressbindung nicht manuell.

---

Informationen zum Überwachen der Aktivität auf einem logischen Switch Port finden Sie unter [Überwachen einer Logischer Switch Port-Aktivität](#).

## Voraussetzungen

Stellen Sie sicher, dass ein logischer Switch erstellt wurde. Siehe [Kapitel 13 Logische Switches](#).

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > Switching > Ports > Hinzufügen** aus.

- 3 Vervollständigen Sie auf der Registerkarte **Allgemein** die Details zum Port.

Option	Beschreibung
<b>Name und Beschreibung</b>	Geben Sie einen Namen und optional eine Beschreibung ein.
<b>Logischer Switch</b>	Wählen Sie im Dropdown-Menü einen logischen Switch aus.
<b>Administrativer Status</b>	Wählen Sie <b>Aktiv</b> oder <b>Inaktiv</b> aus.
<b>Anhangstyp</b>	Wählen Sie <b>Keine</b> oder <b>VIF</b> aus.
<b>Anhangs-ID</b>	Wenn der Anhangstyp VIF lautet, geben Sie die Anhangs-ID ein.

Mithilfe der API können Sie den Anhangstyp auf zusätzliche Werte festlegen (LOGICALROUTER, BRIDGEENDPOINT, DHCP\_SERVICE, METADATA\_PROXY, L2VPN\_SESSION). Wenn es sich beim Anhangstyp um einen DHCP-Dienst, einen Metadaten-Proxy oder eine L2-VPN-Sitzung handelt, müssen die Switching-Profile für den Port die Standardeinstellungen sein. Sie können kein benutzerdefiniertes Profil verwenden.

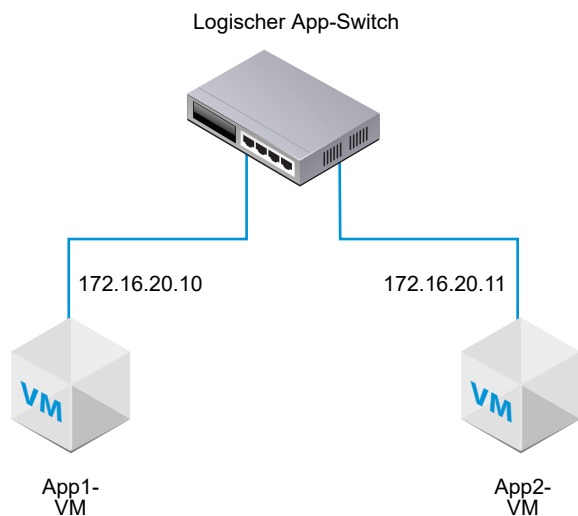
- 4 (Optional) Wählen Sie auf der Registerkarte **Switching-Profile** Switching-Profile aus.
- 5 Klicken Sie auf **Speichern**.

## Testen der Schicht-2-Konnektivität

Nach dem erfolgreichen Einrichten Ihres logischen Switch und nach dem Anfügen von VMs an diesen logischen Switch können Sie die Netzwerkkonnektivität der angefügten VMs prüfen.

Wenn Ihre Netzwerkkonfiguration korrekt konfiguriert ist, kann auf der Basis der Topologie die App2-VM einen Ping-Befehl an die App1-VM senden.

Abbildung 13-2. Topologie für einen logischen Switch



## Verfahren

- 1 Melden Sie sich mithilfe von SSH oder der VM-Konsole bei einer der VMs an, die an den logischen Switch angefügt wurden.

Beispiel: App2 VM 172.16.20.11.

- 2 Senden Sie an die zweite an den logischen Switch angefügte VM einen Ping-Befehl, um die Konnektivität zu testen.

```
$ ping -c 2 172.16.20.10
PING 172.16.20.10 (172.16.20.10) 56(84) bytes of data.
64 bytes from 172.16.20.10: icmp_seq=1 ttl=63 time=0.982 ms
64 bytes from 172.16.20.10: icmp_seq=2 ttl=63 time=0.654 ms
64 bytes from 172.16.20.10: icmp_seq=3 ttl=63 time=0.791 ms

--- 172.16.20.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1990ms
rtt min/avg/max/mdev = 0.654/0.809/0.902/0.104 ms
```

- 3 (Optional) Ermitteln Sie das Problem, das zum Scheitern des Ping-Befehls führt.
  - a Stellen Sie sicher, dass die VM-Netzwerkeinstellungen korrekt sind.
  - b Stellen Sie sicher, dass der VM-Netzwerkadapter mit dem richtigen logischen Switch verbunden ist.
  - c Stellen Sie sicher, dass der administrative Status des logischen Switch „UP“ (Aktiv) ist.
  - d Wählen Sie im NSX Manager die Option **Netzwerk und Sicherheit – Erweitert > Netzwerk > Switching > Switches** aus.

- e Klicken Sie auf den logischen Switch und notieren Sie die UUID- bzw. VNI-Informationen.
- f Führen Sie die folgenden Befehle aus, um den Fehler zu beheben.

Befehl	Beschreibung
<b>get logical-switch &lt;vni-oder-uuid&gt; arp-table</b>	<p>Zeigt die ARP-Tabelle für den angegebenen logischen Switch an. Beispielausgabe.</p> <pre>nsx-manager1&gt; get logical-switch 41866 arp-table VNI      IP              MAC              Connection-ID 41866 172.16.20.11 00:50:56:b1:70:5e 295422</pre>
<b>get logical-switch &lt;vni-oder-uuid&gt; connection-table</b>	<p>Zeigt die Verbindungen für den angegebenen logischen Switch an. Beispielausgabe.</p> <pre>nsx-manager1&gt; get logical-switch 41866 connection-table Host-IP      Port  ID 192.168.110.37 36923 295420 192.168.210.53 37883 295421 192.168.210.54 57278 295422</pre>
<b>get logical-switch &lt;vni-oder-uuid&gt; mac-table</b>	<p>Zeigt die MAC-Tabelle für den angegebenen logischen Switch an. Beispielausgabe.</p> <pre>nsx-manager1&gt; get logical-switch 41866 mac-table VNI      MAC              VTEP-IP      Connection-ID 41866 00:50:56:86:f2:b2 192.168.250.102 295421 41866 00:50:56:b1:70:5e 192.168.250.101 295422</pre>
<b>get logical-switch &lt;vni-oder-uuid&gt; stats</b>	<p>Zeigt statistische Informationen zum angegebenen logischen Switch an. Beispielausgabe.</p> <pre>nsx-manager1&gt; get logical-switch 41866 stats update.member 11 update.vtep 11 update.mac 4 update.mac.invalidate 0 update.arp 7 update.arp.duplicate 0 query.mac 2 query.mac.miss 0 query.arp 9 query.arp.miss 6</pre>
<b>get logical-switch &lt;vni-oder-uuid&gt; stats-sample</b>	<p>Zeigt eine Übersicht aller im Zeitablauf erstellten Statistiken des logischen Switch an. Beispielausgabe.</p> <pre>nsx-manager1&gt; get logical-switch 41866 stats-sample 21:00:00 21:10:00 21:20:00 21:30:00 21:40:00 update.member 0 0 0 0 0 update.vtep 0 0 0 0 0 update.mac 0 0 0 0 0 update.mac.invalidate 0 0 0 0 0 update.arp 0 0 0 0 0 update.arp.duplicate 0 0 0 0 0</pre>



Befehl	Beschreibung
	<pre>query.mac 0 0 0 0 0 query.mac.miss 0 0 0 0 0 query.arp 0 0 0 0 0 query.arp.miss 0 0 0 0 0</pre>
<b>get logical-switch &lt;vni-oder-uuid&gt; vtep</b>	<p>Zeigt alle virtuellen Tunnel-Endpoints an, die zum angegebenen logischen Switch gehören.</p> <p>Beispielausgabe.</p> <pre>nsx-manager1&gt; get logical-switch 41866 vtep VNI      IP          LABEL      Segment MAC      Connection-ID 41866 192.168.250.102 0x8801 192.168.250.0 00:50:56:65:f5:fc 295421 41866 192.168.250.100 0x1F801 192.168.250.0 02:50:56:00:00:00 295420 41866 192.168.250.101 0x16001 192.168.250.0 00:50:56:64:7c:28 295422</pre>

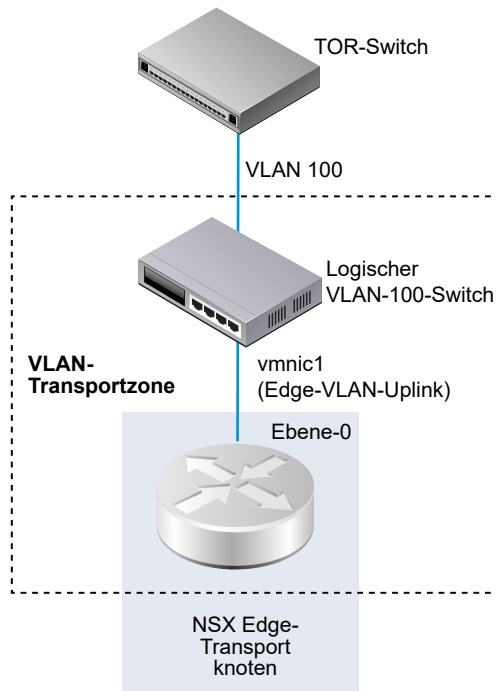
## Ergebnisse

Die erste an den logischen Switch angefügte VM kann Pakete an die zweite VM senden.

## Erstellen eines logischen VLAN-Switch für den NSX Edge-Uplink

Der ausgehende Datenfluss von Edge-Uplinks erfolgt über logische VLAN-Switches.

Wenn Sie einen logischen VLAN-Switch erstellen, ist es wichtig, dies vor dem Hintergrund der speziellen Topologie durchzuführen, die aufgebaut werden soll. Beispielsweise enthält die nachfolgend dargestellte vereinfachte Topologie einen einzelnen logischen VLAN-Switch innerhalb einer VLAN-Transportzone. Der logische VLAN-Switch verfügt über die VLAN-ID 100. Diese entspricht der VLAN-ID auf dem TOR-Port, der mit dem Hypervisor-Hostport verbunden ist, der für den VLAN-Uplink des Edge verwendet wird.



## Voraussetzungen

- Für die Erstellung eines logischen VLAN-Switch müssen Sie zuerst eine VLAN-Transportzone anlegen.
- Dem NSX Edge muss ein NSX-T Data Center-vSwitch hinzugefügt werden. Um diesen für ein Edge zu bestätigen, führen Sie den Befehl `get host-switches` aus. Beispiel:

```
nsx-edge1> get host-switches

Host Switch      : c0a78378-1c20-432a-9e23-ddb34f1c80c9
Switch Name      : hs1
Transport Zone   : c46dcd72-808a-423d-b4cc-8752c33f6b2c
Transport Zone   : 73def985-d122-4b7b-ab6a-a58176dfc32d
Physical Port    : fp-eth0
Uplink Name      : uplink-1
Transport VLAN   : 4096
Default Gateway  : 192.168.150.1
Subnet Mask      : 255.255.255.0
Local VTEP Device : fp-eth0
Local VTEP IP    : 192.168.150.102
```

- Stellen Sie sicher, dass Fabric-Knoten erfolgreich mit dem NSX-T Data Center-Verwaltungskomponenten (MPA)-Agenten und der lokalen NSX-T Data Center-Steuerungskomponente (LCP) verbunden wurden.

Im GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/state`-API-Aufruf muss `state` auf `success` eingestellt sein. Siehe *Installationshandbuch für NSX-T Data Center*.

## Verfahren

- 1 Melden Sie sich in einem Browser bei NSX Manager unter `https://<nsx-mgr>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > Switching > Switches > Hinzufügen** aus.
- 3 Geben Sie für den logischen Switch einen Namen ein.
- 4 Wählen Sie eine Transportzone für den logischen Switch aus.
- 5 Wählen Sie eine Uplink-Teaming-Richtlinie.
- 6 Wählen Sie für den administrativen Status die Option **Aktiv** oder **Inaktiv**.
- 7 Geben Sie eine VLAN-ID ein.

Geben Sie in das Feld „VLAN-ID“ 0 ein, wenn keine VLAN-ID für den Uplink zum physischen TOR vorhanden ist.

- 8 (Optional) Klicken Sie auf die Registerkarte **Switching-Profile** und wählen Sie Switching-Profile aus.

## Ergebnisse

---

**Hinweis** Bei Vorhandensein von zwei logischen VLAN-Switches, die dieselbe VLAN-ID aufweisen, können diese nicht an denselben Edge-N-VDS (vormals Host-Switch) angeschlossen werden. Liegen ein logischer VLAN-Switch und ein logischer Overlay-Switch vor und entspricht die VLAN-ID des logischen VLAN-Switches der Transport-VLAN-ID des logischen Overlay-Switches, können diese ebenfalls nicht an denselben Edge-N-VDS angeschlossen werden.

---

## Nächste Schritte

Fügen Sie einen logischen Router hinzu.

# Switching-Profile für logische Switches und logische Ports

Switching-Profile umfassen Konfigurationsdetails für das Schicht-2-Networking für logische Switches und logische Ports. NSX Manager unterstützt mehrere Typen von Switching-Profilen und bietet mindestens ein systemdefiniertes Standard-Switching-Profil für jeden Profiltyp.

Die folgenden Typen von Switching-Profilen sind verfügbar.

- QoS (Quality of Service; Dienstqualität)
- Port-Mirroring
- IP Discovery
- SpoofGuard
- Switch-Sicherheit

## ■ MAC-Verwaltung

---

**Hinweis** Sie können die Standard-Switching-Profile in NSX Manager nicht bearbeiten oder löschen. Stattdessen können Sie benutzerdefinierte Switching-Profile erstellen.

Stellen Sie vor der Verwendung eines Standardprofils sicher, dass die Einstellungen Ihren Anforderungen entsprechen. Wenn Sie ein benutzerdefiniertes Profil erstellen, weisen einige Einstellungen Standardwerte auf. Gehen Sie nicht davon aus, dass diese Einstellungen im Standardprofil die Standardwerte aufweisen.

---

Jedes standardmäßige oder benutzerdefinierte Switching-Profil weist einen eindeutigen reservierten Bezeichner auf. Anhand dieses Bezeichners können Sie das Switching-Profil einem logischen Switch oder einem logischen Port zuordnen. Beispiel: Die ID des Standard-Switching-Profils für QoS lautet f313290b-eba8-4262-bd93-fab5026e9495.

Ein logischer Switch oder logischer Port kann einem Switching-Profil jedes Typs zugeordnet werden. Sie können beispielsweise nicht zwei unterschiedliche Switching-Profile einem logischen Switch oder logischen Port zuordnen.

Wenn Sie beim Erstellen oder Aktualisieren eines logischen Switches kein Switching-Profil zuordnen, ordnet NSX Manager ein entsprechendes systemdefiniertes Standard-Switching-Profil zu. Die untergeordneten logischen Ports übernehmen das systemdefinierte Standard-Switching-Profil vom übergeordneten logischen Switch.

Beim Erstellen oder Aktualisieren eines logischen Switches oder logischen Ports können Sie entweder ein standardmäßiges oder ein benutzerdefiniertes Switching-Profil zuordnen. Wenn Sie das Switching-Profil einem logischen Switch zuordnen bzw. diese Zuordnung aufheben, wird das Switching-Profil für die untergeordneten logischen Ports basierend auf den folgenden Kriterien angewendet.

- Wenn dem übergeordneten logischen Switch ein Profil zugeordnet ist, übernehmen die untergeordneten logischen Ports das Switching-Profil vom übergeordneten Element.
- Wenn dem übergeordneten logischen Switch kein Switching-Profil zugeordnet ist, wird dem logischen Switch ein Standard-Switching-Profil zugewiesen und der logische Port übernimmt dieses Standard-Switching-Profil.
- Wenn Sie einem logischen Port explizit ein benutzerdefiniertes Profil zuordnen, setzt dieses benutzerdefinierte Profil das vorhandene Switching-Profil außer Kraft.

---

**Hinweis** Wenn Sie ein benutzerdefiniertes Switching-Profil einem logischen Switch zugeordnet haben, aber das Standard-Switching-Profil für einen der untergeordneten logischen Ports beibehalten möchten, müssen Sie eine Kopie des Standard-Switching-Profils erstellen und diese dem jeweiligen logischen Port zuordnen.

---

Sie können keine benutzerdefinierten Switching-Profil löschen, die einem logischen Switch oder logischen Port zugeordnet sind. Um zu ermitteln, ob logische Switches und logische Ports dem benutzerdefinierten Switching-Profil zugeordnet sind, gehen Sie zum Abschnitt „Zugewiesen zu“ der Übersichtsansicht und klicken Sie auf die aufgeführten logischen Switches und logischen Ports.

## Grundlegendes zum QoS-Switching-Profil

QoS stellt eine qualitativ hochstehende und dedizierte Netzwerkleistung für einen bevorzugten Datenverkehr zur Verfügung, der eine hohe Bandbreite erfordert. Der QoS-Mechanismus ermöglicht dies durch Reservierung von ausreichend Bandbreite, Kontrolle von Latenz und Jitter sowie Reduzierung des Datenverlustes für bevorzugte Pakete, auch bei Netzwerküberlastung. Dieses Netzwerkdienstniveau wird durch eine effiziente Nutzung der Netzwerkressourcen erreicht.

In dieser Version werden CoS (Class of Service, Dienstklasse) und DSCP (Differentiated Services Code Point) für das Shaping des Datenverkehrs und dessen namentliche Kennzeichnung unterstützt. Die Schicht-2-CoS ermöglicht die Festlegung einer Priorität für Datenpakete, wenn der Datenverkehr im logischen Switch wegen Überlastung gepuffert wird. Der Schicht-3-DSCP ermittelt Pakete auf der Basis ihrer DSCP-Werte. CoS wird immer auf das Datenpaket angewendet, unabhängig vom vertrauenswürdigen Modus.

NSX-T Data Center stuft die von einer virtuellen Maschine übernommene DSCP-Einstellung oder den auf der Ebene des logischen Switch geänderten oder festgelegten DSCP-Wert als vertrauenswürdig ein. In beiden Fällen wird der DSCP-Wert an die äußere IP-Kopfzeile der gekapselten -Frames weitergegeben. Dies bietet dem externen physischen Netzwerk die Möglichkeit, dem Datenverkehr auf der Basis dieser DSCP-Einstellung in der äußeren Kopfzeile Priorität einzuräumen. Wenn für DSCP der Modus „Vertrauenswürdig“ eingestellt ist, wird der DSCP-Wert von der inneren Kopfzeile kopiert. Ist für DSCP der Modus „Nicht vertrauenswürdig“ eingestellt, wird der DSCP-Wert nicht für die innere Kopfzeile beibehalten.

---

**Hinweis** DSCP-Einstellungen sind nur für getunnelten Datenverkehr wirksam. Diese Einstellungen haben keine Auswirkungen auf den Datenverkehr innerhalb desselben Hypervisors.

---

Sie können mit dem QoS-Switching-Profil die durchschnittliche Bandbreite für den Ingress und Egress konfigurieren und so den Grenzwert für die Übertragungsrate festlegen. Die höchste Bandbreitenrate dient der Unterstützung des Burstdatenverkehrs, der für einen logischen Switch zulässig ist, um eine Überlastung auf vertikalen Netzwerkverbindungen zu vermeiden. Diese Einstellungen gewährleisten nicht die Bandbreite, tragen jedoch zur Begrenzung der Netzwerkbandbreitennutzung bei. Die tatsächlich beobachtbare Bandbreite wird durch die Link-Geschwindigkeit des Ports oder die Werte im Switching-Profil bestimmt, je nachdem, welcher davon niedriger ist.

Die Einstellungen für das QoS-Switching-Profil gelten für den logischen Switch und werden vom untergeordneten logischen Switch Port übernommen.

## Konfigurieren eines benutzerdefinierten QoS-Switching-Profils

Sie können den DSCP-Wert definieren und die Ingress- und Egress-Einstellungen zum Erstellen eines benutzerdefinierten QoS-Switching-Profils konfigurieren.

### Voraussetzungen

- Machen Sie sich mit dem Konzept des QoS-Switching-Profils vertraut. Siehe [Grundlegendes zum QoS-Switching-Profil](#).
- Ermitteln Sie den Netzwerkdatenverkehr, der Priorität haben soll.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 **Netzwerk und Sicherheit – Erweitert > Netzwerk > Switching > Switching-Profile > Hinzufügen** auswählen
- 3 Wählen Sie **QoS** aus und ergänzen Sie die Details des QoS-Switching-Profils.

Option	Beschreibung
<b>Name und Beschreibung</b>	Weisen Sie dem QoS-Switching-Profil einen Namen zu. Optional können Sie für die im Profil geänderte Einstellung eine Beschreibung eingeben.
<b>Modus</b>	<p>Wählen Sie die Option <b>Vertrauenswürdig</b> oder <b>Nicht vertrauenswürdig</b> aus dem Dropdown-Menü „Modus“ aus.</p> <p>Bei der Auswahl des Modus „Vertrauenswürdig“ wird der innere DSCP-Kopfzeilenwert von der äußeren IP-Kopfzeile für den IP-/IPv6-Datenverkehr übernommen. Für den Nicht-IP-/IPv6-Datenverkehr gilt für die äußere IP-Kopfzeile der Standardwert. Der Modus „Vertrauenswürdig“ wird auf einem Overlay-basierten logischen Port unterstützt. Der Standardwert ist 0.</p> <p>Der Modus „Nicht vertrauenswürdig“ wird auf einem Overlay-basierten und auf einem VLAN-basierten logischen Port unterstützt. Für den Overlay-basierten logischen Port wird der DSCP-Wert der äußeren IP-Kopfzeile auf den konfigurierten Wert festgelegt, unabhängig vom inneren Pakettyp für den logischen Port. Für den VLAN-basierten logischen Port wird der DSCP-Wert des IP-/IPv6-Pakets auf den konfigurierten Wert festgelegt. Der Bereich der DSCP-Werte für den Modus „Nicht vertrauenswürdig“ liegt zwischen 0 und 63.</p> <p><b>Hinweis</b> DSCP-Einstellungen sind nur für getunnelten Datenverkehr wirksam. Diese Einstellungen haben keine Auswirkungen auf den Datenverkehr innerhalb desselben Hypervisors.</p>
<b>Priorität</b>	<p>Legen Sie den DSCP-Wert fest.</p> <p>Die Prioritätswerte liegen zwischen 0 und 63.</p>

Option	Beschreibung
<b>Dienstklasse</b>	<p>Legen Sie den CoS-Wert fest.</p> <p>CoS wird auf VLAN-basierten logischen Ports unterstützt. CoS fasst ähnliche Datenverkehrstypen im Netzwerk in Gruppen zusammen. Jeder Datenverkehrstyp wird als eine Klasse mit einer eigenen Stufe der Dienstpriorität behandelt. Der Datenverkehr mit geringerer Priorität wird verlangsamt bzw. in manchen Fällen sogar verworfen, um einen besseren Durchsatz für den Datenverkehr mit höherer Priorität zu gewährleisten. CoS kann für die VLAN-ID auch mit „Null-Paket“ konfiguriert werden.</p> <p>Die CoS-Werte reichen von 0 bis 7, wobei 0 für den maximalen Dienst steht.</p>
<b>Ingress</b>	<p>Legen Sie benutzerdefinierte Werte für den ausgehenden Netzwerkdatenverkehr von der VM zum logischen Netzwerk fest.</p> <p>Sie können mit der durchschnittlichen Bandbreite die Netzwerküberlastung reduzieren. Mit der Spitzenbandbreite wird der Burstdatenverkehr unterstützt. Die Burstgröße basiert auf der Dauer mit Spitzenbandbreite. Sie können die Burstdauer in der Einstellung für die Burstgröße festlegen. Sie können die Bandbreite nicht dauerhaft gewährleisten. Sie können jedoch die Einstellungen für Durchschnitt, Spitzenbandbreite und Burstgröße verwenden, um die Netzwerkbandbreite zu begrenzen.</p> <p>Wenn beispielsweise die durchschnittliche Bandbreite 30 Mbit/s, die Spitzenbandbreite 60 Mbit/s und die zulässige Dauer 0,1 Sekunden beträgt, beträgt die Burstgröße <math>60 \times 1000000 \times 0,1/8 = 750000</math> Byte.</p> <p>Der Standardwert 0 deaktiviert die Ratenbegrenzung für den Ingress-Datenverkehr.</p>
<b>Ingress Broadcast</b>	<p>Legen Sie benutzerdefinierte Werte für den eingehenden Netzwerkdatenverkehr von der VM zum logischen Netzwerk auf Broadcast-Basis fest.</p> <p>Legen Sie benutzerdefinierte Werte für den eingehenden Netzwerkdatenverkehr von der VM zum logischen Netzwerk auf Broadcast-Basis fest. Wenn Sie beispielsweise die durchschnittliche Bandbreite für einen logischen Switch auf 3000 Kbit/s festlegen, die Spitzenbandbreite 6000 Kbit/s und die zulässige Dauer 0,1 Sekunden beträgt, beträgt die Burstgröße <math>6000 \times 1000 \times 0,1/8 = 75000</math> Byte.</p> <p>Der Standardwert 0 deaktiviert die Ratenbegrenzung für den Ingress Broadcast-Datenverkehr.</p>
<b>Egress</b>	<p>Legen Sie benutzerdefinierte Werte für den eingehenden Netzwerkdatenverkehr vom logischen Netzwerk zur VM fest.</p> <p>Der Standardwert 0 deaktiviert die Ratenbegrenzung für den ausgehenden Datenverkehr.</p>

Wenn die Ingress-, Ingress-Broadcast- und Egress-Optionen nicht konfiguriert sind, werden die Standardwerte verwendet.

#### 4 Klicken Sie auf **Speichern**.

#### Ergebnisse

Ein benutzerdefiniertes QoS-Switching-Profil wird als Link angezeigt.

## Nächste Schritte

Hängen Sie dieses benutzerdefinierte QoS-Switching-Profil an einen logischen Switch oder logischen Port an, damit die im Switching-Profil geänderten Parameter auf den Netzwerkdatenverkehr angewendet werden. Siehe [Zuordnen eines benutzerdefinierten Profils zu einem logischen Switch](#) oder [Zuordnen eines benutzerdefinierten Profils zu einem logischen Port](#).

## Grundlegendes zum Switching-Profil für Port-Mirroring

Durch das Mirroring eines logischen Ports können Sie den gesamten Datenverkehr, der von einem an einen VM-VIF-Port angefügten logischen Switch Port ein- oder ausgeht, replizieren und umleiten. Der gespiegelte Datenverkehr wird gekapselt innerhalb eines GRE (Generic Routing Encapsulation)-Tunnels an einen Collector gesendet, sodass die gesamten Informationen des ursprünglichen Pakets beim Durchlauf durch das Netzwerk zu einem Remote-Ziel erhalten bleiben.

In der Regel wird die Portspiegelung in folgenden Fällen verwendet:

- Fehlerbehebung – Analyse des Datenverkehrs zur Ermittlung von Eindringversuchen und zum Debugging bzw. zur Diagnose von Netzwerkfehlern.
- Übereinstimmung und Überwachung – Weiterleitung des gesamten überwachten Datenverkehrs an eine Netzwerk-Appliance zur Analyse und Wartung.

Im Unterschied zur physischen Portspiegelung wird mit der logischen Portspiegelung der gesamte VM-Netzwerkdatenverkehr erfasst. Wenn Sie die Portspiegelung nur in einem physischen Netzwerk implementieren, wird nicht der gesamte VM-Netzwerkdatenverkehr gespiegelt. Dies liegt daran, dass die Kommunikation zwischen VMs, die sich auf demselben Host befinden, nicht über das physische Netzwerk verläuft und deshalb auch nicht gespiegelt werden kann. Mit der Spiegelung logischer Ports können Sie weiterhin VM-Datenverkehr spiegeln, auch wenn die betreffende VM auf einen anderen Host migriert wurde.

Der Vorgang der Portspiegelung ist für beide VM-Ports in der NSX-T Data Center-Domäne und für Ports physischer Anwendungen vergleichbar. Sie können den Datenverkehr, der von einer Arbeitslast erfasst wird, die mit einem logischen Netzwerk verbunden ist, weiterleiten und diesen Datenverkehr auf einen Collector spiegeln. Die IP-Adresse muss von der Gast-IP-Adresse aus, auf der die VM gehostet wird, erreichbar sein. Dieser Vorgang gilt auch für physische Anwendungen, die mit Gateway-Knoten verbunden sind.

## Konfigurieren eines benutzerdefinierten Switching-Profiles für die Portspiegelung

Sie können ein benutzerdefiniertes Switching-Profil für die Portspiegelung mit unterschiedlichem Ziel und Schlüsselwert erstellen.

### Voraussetzungen

- Machen Sie sich mit dem Konzept des Switching-Profiles für die Portspiegelung vertraut. Siehe [Grundlegendes zum Switching-Profil für Port-Mirroring](#).
- Ermitteln Sie die IP-Adresse der ID des logischen Zielports, an den Sie den Netzwerkdatenverkehr umleiten möchten.



## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 **Netzwerk und Sicherheit – Erweitert > Netzwerk > Switching > Switching-Profile > Hinzufügen** auswählen
- 3 Wählen Sie **Port Mirroring** aus und ergänzen Sie die Details des Switching-Profiles der Portspiegelung.

Option	Beschreibung
<b>Name und Beschreibung</b>	Weisen Sie dem Switching-Profil für die Portspiegelung einen Namen zu. Optional können Sie für die Einstellung, die Sie zur Anpassung dieses Profils geändert haben, eine Beschreibung eingeben.
<b>Richtung</b>	Wählen Sie im Dropdown-Menü eine Option für den Datenverkehr aus, für den diese Quelle verwendet werden soll: <b>Eingehend</b> , <b>Ausgehend</b> oder <b>Bidirektional</b> .  Der eingehende Netzwerkdatenverkehr verläuft von der VM zum logischen Netzwerk.  Der ausgehende Netzwerkdatenverkehr verläuft vom logischen Netzwerk zur VM.  Der bidirektionale Datenverkehr verläuft in beide Richtungen, von der VM zum logischen Netzwerk und vom logischen Netzwerk zur VM. Dies ist die Standardoption.
<b>Paketkürzung</b>	Optional Der Bereich liegt zwischen 60 und 65535.
<b>Schlüssel</b>	Geben Sie einen zufälligen 32-Bit-Wert zur Ermittlung gespiegelter Pakete vom logischen Port ein.  Der Schlüsselwert wird in das Schlüsselfeld der GRE-Kopfzeile jedes gespiegelten Pakets kopiert. Wenn für den Schlüsselwert 0 festgelegt ist, wird die Standarddefinition in das Schlüsselfeld der GRE-Kopfzeile kopiert.  Der standardmäßige 32-Bit-Wert besteht aus den im Folgenden aufgeführten Werten. <ul style="list-style-type: none"> <li>■ Der erste 24-Bit-Wert ist ein VNI-Wert. VNI ist Bestandteil der IP-Kopfzeile gekapselter Frames.</li> <li>■ Das 25. Bit gibt an, ob der erste 24-Bit-Wert ein gültiger VNI-Wert ist. „Eins“ steht für einen gültigen Wert und „Null“ für einen ungültigen Wert.</li> <li>■ Das 26. Bit gibt die Richtung des gespiegelten Datenverkehrs an. „Eins“ steht für eine eingehende Richtung und „Null“ für eine ausgehende Richtung.</li> <li>■ Die verbleibenden sechs Bits werden nicht verwendet.</li> </ul>
<b>Ziele</b>	Geben Sie die Ziel-ID des Collector für die zu spiegelnde Sitzung ein.  Die Ziel-IP-Adresse-ID kann nur eine IPv4-Adresse innerhalb des Netzwerks oder eine Remote-IPv4-Adresse sein, die nicht von NSX-T Data Center verwaltet wird. Sie können bis zu drei Ziel-IP-Adressen, durch Kommas getrennt, hinzufügen.

- 4 Klicken Sie auf **Speichern**.

## Ergebnisse

Ein benutzerdefiniertes Switching-Profil für die Portspiegelung wird als Link angezeigt.

## Nächste Schritte

Hängen Sie das Switching-Profil an einen logischen Switch oder logischen Port an. Siehe [Zuordnen eines benutzerdefinierten Profils zu einem logischen Switch](#) oder [Zuordnen eines benutzerdefinierten Profils zu einem logischen Port](#).

Überprüfen Sie, ob das benutzerdefinierte Switching-Profil für die Portspiegelung funktioniert. Siehe [Überprüfen eines benutzerdefinierten Switching-Profiles für die Portspiegelung](#).

## Überprüfen eines benutzerdefinierten Switching-Profiles für die Portspiegelung

Bevor Sie das benutzerdefinierte Switching-Profil für die Portspiegelung verwenden, müssen Sie prüfen, ob die Anpassung korrekt funktioniert.

### Voraussetzungen

- Stellen Sie sicher, dass das benutzerdefinierte Switching-Profil für die Portspiegelung konfiguriert ist. Siehe [Konfigurieren eines benutzerdefinierten Switching-Profiles für die Portspiegelung](#).
- Stellen Sie sicher, dass das benutzerdefinierte Switching-Profil für die Portspiegelung an einen logischen Switch angefügt wurde. Siehe [Zuordnen eines benutzerdefinierten Profils zu einem logischen Switch](#).

### Verfahren

- 1 Suchen Sie zwei VMs mit VIF-Anfügungen an den logischen Port, der für die Portspiegelung konfiguriert ist.

Beispielsweise verfügen VM1 10.70.1.1 und VM2 10.70.1.2 über VIF-Anfügungen. Beide sind im selben logischen Netzwerk enthalten.

- 2 Führen Sie den Befehl `tcpdump` auf einer Ziel-IP-Adresse aus.

**`sudo tcpdump -n -i eth0 dst host Ziel_IP_Adresse and proto gre`**

Die Ziel-IP-Adresse kann z. B. 10.24.123.196 lauten.

- 3 Melden Sie sich bei der ersten VM an und senden Sie einen Ping-Befehl an die zweite VM, um sicherzustellen, dass die zugehörigen ECHO-Anforderungen und -Antworten an der Zieladresse empfangen werden.

## Nächste Schritte

Fügen Sie dieses benutzerdefinierte Switching-Profil für die Portspiegelung an den logischen Switch an, damit die im Switching-Profil geänderten Parameter für den Netzwerkdatenverkehr angewendet werden. Siehe [Zuordnen eines benutzerdefinierten Profils zu einem logischen Switch](#).

## Grundlegendes zum Switching-Profil für die IP Discovery

Die IP Discovery ruft MAC- und IP-Adressen mithilfe von DHCP- und DHCPv6-Snooping, ARP-Snooping (Address Resolution Protocol), ND-Snooping (Neighbor Discovery) und VM-Tools ab.

Die ermittelten MAC- und IP-Adressen werden zur ARP/ND-Unterdrückung verwendet. Dadurch wird der Datenverkehr zwischen VMs minimiert, die mit demselben logischen Switch verbunden sind. Die Adressen werden auch von den SpoofGuard-Komponenten und Komponenten der verteilten Firewall (DFW) verwendet. Anhand der Adressbindungen ermittelt DFW die IP-Adresse von Objekten in Firewallregeln.

Das DHCP/DHCPv6-Snooping prüft die DHCP/DHCPv6-Pakete, die zwischen dem DHCP/DHCPv6-Client und dem DHCP/DHCPv6-Server ausgetauscht werden, um die IP- und MAC-Adressen abzurufen.

Das ARP-Snooping überprüft die ausgehenden ARP- und GARP- (Gratuitous ARP-)Pakete der VM, um die IP- und MAC-Adressen abzurufen.

VM Tools ist eine Software, die auf einer ESXi-gehosteten virtuellen Maschine ausgeführt wird und die Konfigurationsdaten der virtuellen Maschine, einschließlich MAC- und IP- oder IPv6-Adressen, bereitstellen kann. Diese IP Discovery-Methode ist nur für VMs verfügbar, die auf ESXi-Hosts ausgeführt werden.

ND-Snooping ist das IPv6-Äquivalent zum ARP-Snooping. Es prüft Neighbor Solicitation (NS)- und Neighbor Advertisement (NA)-Nachrichten, um die IP- und MAC-Adressen zu ermitteln.

Die Erkennung von doppelten Adressen überprüft, ob eine neu ermittelte IP-Adresse bereits in der realisierten Bindungsliste für einen anderen Port vorhanden ist. Diese Überprüfung wird für Ports auf demselben logischen Switch durchgeführt. Wenn eine doppelte Adresse erkannt wird, wird die neu ermittelte Adresse nicht zur realisierten Bindungsliste, sondern zur ermittelten Liste hinzugefügt. Allen doppelten IPs ist ein Ermittlungszeitstempel zugeordnet. Wenn die IP, die sich in der realisierten Bindungsliste befindet, entweder durch Hinzufügen zur Ignorieren-Bindungsliste (siehe unten) oder durch Deaktivieren des Snooping entfernt wird, wird die doppelte IP mit dem ältesten Zeitstempel in die realisierte Bindungsliste verschoben. Die doppelten Adressinformationen sind über einen API-Aufruf verfügbar.

Standardmäßig arbeiten die Ermittlungsmethoden ARP-Snooping und ND-Snooping in einem Modus namens „Trust on First Use“ (TOFU). Wenn im TOFU-Modus eine Adresse ermittelt und zur realisierten Bindungsliste hinzugefügt wird, bleibt diese Bindung für immer in der realisierten Liste. TOFU gilt für die ersten „n“ eindeutigen <IP-, MAC-, VLAN->Bindungen, die mithilfe von ARP/ND-Snooping erkannt werden, wobei „n“ der Bindungsgrenzwert ist, den Sie konfigurieren können. Sie können TOFU für ARP-/ND-Snooping deaktivieren. Die Methoden werden dann im

TOEU-Modus als vertrauenswürdig eingestuft. Wenn eine Adresse im TOEU-Modus ermittelt wird, wird Sie zur realisierten Bindungsliste hinzugefügt, und wenn sie gelöscht oder abgelaufen ist, wird sie aus der realisierten Bindungsliste entfernt. DHCP-Snooping und VM-Tools funktionieren immer im TOEU-Modus.

**Hinweis** TOFU ist nicht identisch mit SpoofGuard und blockiert nicht den Datenverkehr, wie dies bei SpoofGuard der Fall ist. Weitere Informationen zu SpoofGuard finden Sie unter [Grundlegendes zu SpoofGuard](#).

NSX Manager verwaltet für jeden Port eine Ignorieren-Bindungsliste, die IP-Adressen enthält, die nicht an den Port gebunden werden können. Sie können diese Liste nur über die API aktualisieren. Sie können diese Methode auch verwenden, um eine zuvor ermittelte IP für einen bestimmten Port zu löschen. Weitere Informationen finden Sie in der Referenz zur NSX-T-API unter `ignore_address_bindings`.

**Hinweis** Für Linux-VMs kann das ARP-Flux-Problem möglicherweise dazu führen, dass das ARP-Snooping inkorrekte Informationen erhält. Das Problem kann durch einen ARP-Filter verhindert werden. Weitere Informationen finden Sie unter <http://linux-ip.net/html/ether-arp.html#ether-arp-flux>.

## Konfigurieren eines Switching-Profiles für die IP-Ermittlung

NSX-T Data Center weist mehrere standardmäßige Switching-Profile für die IP-Ermittlung auf. Sie können auch weitere Profile erstellen.

### Voraussetzungen

Machen Sie sich mit dem Konzept des Switching-Profiles für die IP-Ermittlung vertraut. Siehe [Grundlegendes zum Switching-Profil für die IP Discovery](#)

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > Switching > Switching-Profil > Hinzufügen** aus.
- 3 Wählen Sie **IP-Ermittlung** aus und geben Sie die Details der Switching-Profile für die IP-Ermittlung ein.

Option	Beschreibung
<b>Name und Beschreibung</b>	Geben Sie einen Namen und optional eine Beschreibung ein.
<b>ARP-Snooping</b>	Für eine IPv4-Umgebung. Anwendbar, wenn VMs statische IP-Adressen aufweisen.
<b>ARP-Bindungsgrenzwert</b>	Die maximale Anzahl von IPv4-IP-Adressen, die an einen Port gebunden werden können.

Option	Beschreibung
<b>Zeitüberschreitung bei ARP-ND-Bindungsgrenzwert</b>	Der Zeitüberschreitungswert in Minuten für IP-Adressen in der ARP-/ND-Bindungstabelle, wenn TOFU deaktiviert ist. Wenn für eine Adresse eine Zeitüberschreitung auftritt, wird sie durch eine neu erkannte Adresse ersetzt.
<b>DHCP-Snooping</b>	Für eine IPv4-Umgebung. Anwendbar, wenn VMs IPv4-Adressen aufweisen.
<b>DHCP-Snooping-V6</b>	Für eine IPv6-Umgebung. Anwendbar, wenn VMs IPv6-Adressen aufweisen.
<b>VM Tools</b>	Nur für ESXi-gehostete VMs verfügbar.
<b>VM-Tools für IPv6</b>	Nur für ESXi-gehostete VMs verfügbar.
<b>Überwachung (Snooping) der Nachbarermittlung</b>	Für eine IPv6-Umgebung. Anwendbar, wenn VMs statische IP-Adressen aufweisen.
<b>Bindungsgrenzwert für Nachbarermittlung</b>	Die maximale Anzahl an IPv6-Adressen, die an einen Port gebunden werden können.
<b>Vertrauen bei erster Nutzung</b>	Anwendbar auf ARP- und ND-Snooping.
<b>Doppelte IP-Erkennung</b>	Für alle Snooping-Methoden sowie für IPv4- und IPv6-Umgebungen.

#### 4 Klicken Sie auf **Hinzufügen**.

##### Nächste Schritte

Fügen Sie dieses benutzerdefinierte Switching-Profil für die IP-Ermittlung an einen logischen Switch oder logischen Port an, damit die im Switching-Profil geänderten Parameter für den Netzwerkdatenverkehr angewendet werden. Siehe [Zuordnen eines benutzerdefinierten Profils zu einem logischen Switch](#) oder [Zuordnen eines benutzerdefinierten Profils zu einem logischen Port](#).

## Grundlegendes zu SpoofGuard

Mit SpoofGuard unterstützt die Abwehr von bestimmten Angriffen wie „Web-Spoofing“ und „Phishing“. Eine SpoofGuard-Richtlinie blockiert Datenverkehr, der als manipuliert erkannt wird.

SpoofGuard ist ein Tool, das virtuelle Maschinen in Ihrer Umgebung daran hindert, Datenverkehr von einer nicht für das Senden berechtigten IP-Adresse zu senden. Wenn die IP-Adresse einer virtuellen Maschine nicht mit der IP-Adresse des zugehörigen logischen Ports und der Switch-Adressbindung in SpoofGuard übereinstimmt, wird die vNIC der virtuellen Maschine komplett am Zugriff auf das Netzwerk gehindert. SpoofGuard lässt sich auf Port- oder Switch-Ebene konfigurieren. SpoofGuard kann aus verschiedenen Gründen in Ihrer Umgebung verwendet werden:

- Zur Verhinderung der Erkennung der IP-Adresse einer vorhandenen VM durch eine nicht berechnete virtuelle Maschine.
- Zur Sicherstellung, dass sich die IP-Adressen von virtuellen Maschinen nicht ohne Eingriff verändern lassen. In einigen Umgebungen ist es wünschenswert, dass virtuelle Maschinen ihre IP-Adressen ohne ordnungsgemäße Änderungskontrolle nicht ändern können. Mit SpoofGuard lässt sich dies vereinfachen. Damit wird sichergestellt, dass der Besitzer der virtuellen Maschine die IP-Adresse nicht einfach ändern und seine Arbeit ungehindert fortsetzen kann.
- Zur Sicherstellung, dass Regeln der die verteilte Firewall nicht irrtümlich (oder absichtlich) umgangen werden. Bei Regeln für die verteilte Firewall, die unter Verwendung von IP Sets als Quelle oder Ziele erstellt wurden, besteht immer die Gefahr, dass die IP-Adresse einer virtuellen Maschine in der Paketkopfzeile gefälscht ist und so die betreffenden Regeln umgangen werden.

Die Konfiguration von NSX-T Data Center SpoofGuard umfasst die folgenden Elemente:

- MAC SpoofGuard – authentifiziert die MAC-Adresse des Pakets
- IP SpoofGuard – authentifiziert die MAC- und die IP-Adresse des Pakets
- Dynamische ARP (Address Resolution Protocol)-Untersuchung, d. h., es wird eine ARP-, GARP (Gratuitous Address Resolution Protocol)- und ND (Neighbor Discovery)-SpoofGuard-Überprüfung der Zuordnung der MAC-, IP- und IP-MAC-Quelle in der ARP-/GARP-/ND-Nutzlast durchgeführt.

Auf Portebene wird die Positivliste zulässiger MAC/VLAN/IP-Werte über die Adressbindungseigenschaft des Ports zur Verfügung gestellt. Wenn die virtuelle Maschine Datenverkehr sendet, wird dieser verworfen, wenn ihre IP-/MAC-/VLAN-Werte nicht mit den IP-/MAC-/VLAN-Eigenschaften des Ports übereinstimmen. SpoofGuard auf Portebene ist für die Authentifizierung des Datenverkehrs zuständig, d. h. für die Überprüfung, ob der Datenverkehr mit der VIF-Konfiguration in Einklang steht.

Auf Switch-Ebene wird die Positivliste zulässiger MAC/VLAN/IP-Werte über die Adressbindungseigenschaft des Switch zur Verfügung gestellt. Dabei handelt es sich in der Regel um einen zulässigen IP-Bereich bzw. um ein zulässiges Subnetz für den Switch. SpoofGuard auf Switch-Ebene ist für die Authentifizierung des Datenverkehrs zuständig.

Der Datenverkehr muss durch SpoofGuard auf Port- UND auf Switch-Ebene gestattet werden, bevor er für den Switch zugelassen wird. Die Aktivierung/Deaktivierung von SpoofGuard auf Port- und Switch-Ebene kann mithilfe des SpoofGuard-Switch-Profiles gesteuert werden.

## Konfigurieren von Port-Adressbindungen

Adressbindungen geben die IP- und MAC-Adresse eines logischen Ports an. Damit wird die Positivliste für Ports in SpoofGuard festgelegt.

Mit Port-Adressbindungen geben Sie die IP- und MAC-Adresse sowie das VLAN (sofern zutreffend) des logischen Ports an. Wenn SpoofGuard aktiviert ist, wird damit sichergestellt, dass die angegebenen Adressbindungen in den Datenpfad aufgenommen werden. Port-Adressbindungen werden nicht nur für SpoofGuard, sondern auch für DFW-Regelübersetzungen verwendet.

### Verfahren

- 1 Wählen Sie in NSX Manager die Option **Netzwerk und Sicherheit – Erweitert > Netzwerk > Switching > Ports** aus.
- 2 Klicken Sie auf den logischen Port, für den eine Adressbindung verwendet werden soll.  
Die Übersicht für den logischen Port wird eingeblendet.
- 3 Erweitern Sie in der Registerkarte **Übersicht** die Option **Adressbindungen**.
- 4 Klicken Sie auf **Hinzufügen**.  
Das Dialogfeld „Adressbindungen hinzufügen“ wird angezeigt.
- 5 Geben Sie die IP- und MAC-Adresse des logischen Ports an, für den eine Adressbindung angewendet werden soll. Sie können auch eine VLAN-ID angeben.
- 6 Klicken Sie auf **Hinzufügen**.

### Nächste Schritte

Die Port-Adressbindungen können Sie für die Konfiguration eines SpoofGuard-Switching-Profiles verwenden. Erläuterungen dazu finden Sie unter [Konfigurieren eines SpoofGuard-Switching-Profiles](#).

## Konfigurieren eines SpoofGuard-Switching-Profiles

Wenn sich bei konfiguriertem SpoofGuard die IP-Adresse einer virtuellen Maschine ändert, kann der Datenverkehr von einer virtuellen Maschine blockiert sein, solange die zugehörigen konfigurierten Port-/Switch-Adressbindungen nicht mit der neuen IP-Adresse aktualisiert wurden.

Aktivieren Sie SpoofGuard für die Portgruppen, die die Gastbetriebssysteme enthalten. Wenn SpoofGuard für jeden Netzwerkadapter aktiviert ist, untersucht es Pakete für die vorgegebene MAC-Adresse und die zugehörige IP-Adresse.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > Switching > Switching-Profile > Hinzufügen** aus.

- 3 Wählen Sie **Spoof Guard** aus.
- 4 Geben Sie einen Namen und optional eine Beschreibung ein.
- 5 Um SpoofGuard auf Portebene zu aktivieren, setzen Sie **Portbindungen** auf **Aktiviert**.
- 6 Klicken Sie auf **Hinzufügen**.

#### Ergebnisse

Es wurde ein neues Switching-Profil mit einem SpoofGuard-Profil erstellt.

#### Nächste Schritte

Ordnen Sie das SpoofGuard-Profil einem logischen Switch oder logischen Port zu. Siehe [Zuordnen eines benutzerdefinierten Profils zu einem logischen Switch](#) oder [Zuordnen eines benutzerdefinierten Profils zu einem logischen Port](#).

## Grundlegendes zum Switching-Profil für die Switch-Sicherheit

Die Switch-Sicherheit bietet eine zustandsfreie Schicht-2- und Schicht-3-Sicherheit durch Überprüfung des eingehenden Datenverkehrs zum logischen Switch und durch Verwerfung unberechtigter Pakete, die von VMs gesendet wurden. Dazu werden die IP- und die MAC-Adresse sowie die Protokolle mit einem Satz zulässiger Adressen und Protokolle verglichen. Sie können mit der Switch-Sicherheit die Integrität des logischen Switch durch Herausfiltern von Angriffen aus den VMs im Netzwerk schützen.

Sie haben die Möglichkeit, Filter für die BPDUs (Bridge Protocol Data Unit), DHCP-Snooping, DHCP-Serverblockierungen und Optionen zur Begrenzung der Übertragungsrate zu konfigurieren, um das Switching-Profil für die Switch-Sicherheit auf einem logischen Switch anzupassen.

### Konfigurieren eines benutzerdefinierten Switching-Profiles für die Switch-Sicherheit

Sie können ein benutzerdefiniertes Switching-Profil für die Switch-Sicherheit mit MAC-Ziel-Adressen aus der BPDUs-Liste zulässiger Adressen anlegen und die Beschränkung der Rate konfigurieren.

#### Voraussetzungen

Machen Sie sich mit dem Konzept des Switching-Profiles für die Switch-Sicherheit vertraut. Siehe [Grundlegendes zum Switching-Profil für die Switch-Sicherheit](#).

#### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > Switching**.
- 3 Klicken Sie auf die Registerkarte **Switching-Profile**.



- 4 Klicken Sie auf **Hinzufügen**, und wählen Sie **Switch-Sicherheit** aus.
- 5 Vervollständigen Sie die Details des Switching-Profiles für die Switch-Sicherheit.

Option	Beschreibung
<b>Name und Beschreibung</b>	Weisen Sie dem Switching-Profil für die Switch-Sicherheit einen Namen zu. Optional können Sie für die im Profil geänderte Einstellung eine Beschreibung eingeben.
<b>BPDU-Filter</b>	Schalten Sie die Schaltfläche <b>BPDU-Filter</b> zur Aktivierung der BPDU-Filterung um. Standardmäßig deaktiviert. Wenn der BPDU-Filter aktiviert ist, wird der gesamte Datenverkehr zur BPDU-Ziel-MAC-Adresse blockiert. Dabei wird auch STP auf den logischen Switch-Ports deaktiviert, da davon ausgegangen wird, dass diese Ports nicht Bestandteil von STP sind.
<b>Positivliste für den BPDU-Filter</b>	Klicken Sie auf die Ziel-MAC-Adresse aus der Liste der BPDU-Ziel-MAC-Adressen, um den Datenverkehr zum zugelassenen Ziel zu ermöglichen. Sie müssen <b>BPDU-Filter</b> aktivieren, um aus dieser Liste auswählen zu können.
<b>DHCP-Filter</b>	Schalten Sie die Schaltflächen <b>Serverblock</b> und <b>Clientblock</b> zur Aktivierung der DHCP-Filterung um. Beide sind standardmäßig deaktiviert. Die DHCP-Serverblockierung blockiert Datenverkehr von einem DHCP-Server an einen DHCP-Client. Dabei wird kein Datenverkehr von einem DHCP-Server an einen DHCP-Relay-Agent blockiert. Die DHCP-Clientblockierung verhindert, dass eine VM eine DHCP-IP-Adresse erhält, indem DHCP-Anforderungen blockiert werden.
<b>DHCPv6-Filter</b>	Schalten Sie die Schaltflächen <b>V6-Serverblock</b> und <b>V6-Clientblock</b> zur Aktivierung der DHCP-Filterung um. Beide sind standardmäßig deaktiviert. Die DHCPv6-Serverblockierung blockiert Datenverkehr von einem DHCPv6-Server an einen DHCPv6-Client. Dabei wird kein Datenverkehr von einem DHCP-Server an einen DHCP-Relay-Agent blockiert. Pakete, deren UDP-Quellportnummer 547 beträgt, werden gefiltert. Die DHCPv6-Clientblockierung verhindert, dass eine VM eine DHCP-IP-Adresse erhält, indem DHCP-Anforderungen blockiert werden. Pakete, deren UDP-Quellportnummer 546 beträgt, werden gefiltert.
<b>Nicht-IP-Datenverkehr blockieren</b>	Schalten Sie die Schaltfläche <b>Nicht-IP-Datenverkehr blockieren</b> um, um nur IPv4-, IPv6-, ARP- und BPDU-Datenverkehr zuzulassen. Der übrige Nicht-IP-Datenverkehr wird blockiert. Der zugelassene IPv4-, IPv6-, ARP-, GARP- und BPDU-Datenverkehr basiert auf anderen Richtlinien, die in der Konfiguration der Adressbindung und von SpoofGuard festgelegt sind. Standardmäßig ist diese Option deaktiviert, d. h. der Nicht-IP-Datenverkehr wird als regulärer Datenverkehr behandelt.

Option	Beschreibung
<b>RA-Guard</b>	Schalten Sie die Schaltfläche <b>RA-Guard</b> um, um Ingress-IPv6-Routerankündigungen herauszufiltern. ICMPv6-Pakete vom Typ 134 werden herausgefiltert. Diese Option ist standardmäßig aktiviert.
<b>Ratenbegrenzungen</b>	Legen Sie eine Ratenbegrenzung für Broadcast-und Multicast-Datenverkehr fest. Diese Option ist standardmäßig aktiviert.  Ratenbegrenzungen können verwendet werden, um den logischen Switch oder VMs vor Ereignissen wie Broadcast-Stürmen zu schützen.  Um Konnektivitätsprobleme zu vermeiden, muss die Mindestrate größer oder gleich 10 PPS sein.

## 6 Klicken Sie auf **Hinzufügen**.

### Ergebnisse

Ein benutzerdefiniertes Switching-Profil für die Switch-Sicherheit wird als Link angezeigt.

### Nächste Schritte

Hängen Sie dieses benutzerdefinierte Switching-Profil für die Switch-Sicherheit an einen logischen Switch oder logischen Port an, damit die im Switching-Profil geänderten Parameter auf den Netzwerkdatenverkehr angewendet werden. Siehe [Zuordnen eines benutzerdefinierten Profils zu einem logischen Switch](#) oder [Zuordnen eines benutzerdefinierten Profils zu einem logischen Port](#).

## Grundlegendes zum Switching-Profil für die MAC-Verwaltung

Das Switching-Profil für die MAC-Verwaltung unterstützt zwei Funktionen: MAC Learning und MAC-Adressänderung.

Die Änderungsfunktion für die MAC-Adresse ermöglicht einem VM die Änderung der zugehörigen MAC-Adresse. Eine mit einem Port verbundene VM kann einen administrativen Befehl zur Änderung der MAC-Adresse ihrer vNIC ausführen, und es kann weiterhin Datenverkehr an diese vNIC gesendet bzw. von ihr empfangen werden. Diese Funktion wird nur für ESXi- und nicht für KVM-VMs unterstützt. Diese Eigenschaft ist standardmäßig deaktiviert, es sei denn, die Gast-VM wird mithilfe von VMware Integrated OpenStack bereitgestellt. In diesem Fall ist die Eigenschaft standardmäßig aktiviert.

MAC Learning bietet eine Netzwerkkonnektivität für Bereitstellungen, in denen mehrere MAC-Adressen hinter einer vNIC konfiguriert sind. Ein Beispiel ist eine geschachtelte Hypervisor-Bereitstellung, in der eine ESXi-VM auf einem ESXi-Host ausgeführt wird und mehrere VMs innerhalb der ESXi-VM ausgeführt werden. Ohne MAC Learning ist die MAC-Adresse, wenn die vNIC der ESXi-VM eine Verbindung mit einem Switch-Port herstellt, statisch. VMs, die innerhalb der ESXi-VM ausgeführt werden, verfügen über keine Netzwerkkonnektivität, da ihre Pakete über unterschiedliche MAC-Quelladressen verfügen. Beim MAC Learning überprüft vSwitch die MAC-Quelladresse jedes Pakets von der vNIC, ruft die MAC-Adresse ab und gestattet dem Paket die Weiterleitung. Wird eine erlernte MAC-Adresse eine bestimmte Zeit lang nicht verwendet, wird sie entfernt. Diese zeitliche Festlegung ist nicht konfigurierbar.

MAC Learning unterstützt auch unbekanntes Unicast Flooding. Im Normalfall wird ein Paket, das von einem Port empfangen wird und über eine unbekannte Ziel-MAC-Adresse verfügt, verworfen. Bei aktiviertem Flooding des Datenverkehrs vom Typ „Unbekannter Unicast“ leitet der Port diesen Datenverkehr an jeden Port auf dem Switch weiter, für den MAC Learning und unbekanntes Unicast-Flooding aktiviert wurden. Diese Eigenschaft ist standardmäßig aktiviert, wenn MAC Learning aktiviert ist.

Die Anzahl erlernbarer MAC-Adressen ist konfigurierbar. Der Maximalwert ist 4096. Dies ist die Standardeinstellung. Sie können auch die Richtlinie für den Fall festlegen, dass der Grenzwert erreicht wird. Folgende Optionen stehen zur Verfügung:

- **Verwerfen** – Pakete von einer unbekannten MAC-Quelladresse werden verworfen. Pakete, die bei dieser MAC-Adresse eingehen, werden als unbekannte Unicast-Objekte behandelt. Der Port empfängt die Pakete nur dann, wenn unbekanntes Unicast-Flooding aktiviert ist.
- **Zulassen** – Pakete von einer unbekannten MAC-Quelladresse werden weitergeleitet, obwohl die Adresse nicht erlernt wird. Pakete, die bei dieser MAC-Adresse eingehen, werden als unbekannte Unicast-Objekte behandelt. Der Port empfängt die Pakete nur dann, wenn unbekanntes Unicast-Flooding aktiviert ist.

Wenn Sie MAC Learning und die MAC-Adressänderung aktiviert haben, müssen Sie zur Verbesserung der Sicherheit zusätzlich SpoofGuard konfigurieren.

## Konfigurieren des Switching-Profiles für die MAC-Verwaltung

Sie können ein Switching-Profil für die MAC-Verwaltung erstellen, um MAC-Adressen zu verwalten.

### Voraussetzungen

Machen Sie sich mit dem Konzept des Switching-Profiles für die MAC-Verwaltung vertraut. Siehe [Grundlegendes zum Switching-Profil für die MAC-Verwaltung](#).

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > Switching > Switching-Profil > Hinzufügen** aus.
- 3 Wählen Sie **MAC-Verwaltung** aus und ergänzen Sie die Details des MAC-Verwaltungsprofils.

Option	Beschreibung
<b>Name und Beschreibung</b>	Weisen Sie dem MAC-Verwaltungsprofil einen Namen zu. Optional können Sie für die im Profil geänderte Einstellung eine Beschreibung eingeben.
<b>MAC-Änderung</b>	Aktivieren oder deaktivieren Sie die Funktion zum Ändern der MAC-Adresse. Standardmäßig ist sie deaktiviert.

Option	Beschreibung
<b>Status</b>	Aktivieren oder deaktivieren Sie MAC Learning. Standardmäßig ist sie deaktiviert.
<b>Unbekannte Unicast-Überflutung</b>	Aktivieren oder deaktivieren Sie die unbekannte Unicast Flooding-Funktion. Standardmäßig ist sie aktiviert. Diese Option ist verfügbar, wenn Sie Mac Learning aktivieren.
<b>MAC-Grenzwert</b>	Legen Sie die maximale Anzahl an MAC-Adressen fest. Die Standardeinstellung ist 4096. Diese Option ist verfügbar, wenn Sie Mac Learning aktivieren.
<b>MAC-Grenzwertrichtlinie</b>	Wählen Sie <b>Zulassen</b> oder <b>Verwerfen</b> aus. Die Standardeinstellung ist <b>Zulassen</b> . Diese Option ist verfügbar, wenn Sie Mac Learning aktivieren.

#### 4 Klicken Sie auf **Hinzufügen**.

#### Nächste Schritte

Hängen Sie das Switching-Profil an einen logischen Switch oder logischen Port an. Siehe [Zuordnen eines benutzerdefinierten Profils zu einem logischen Switch](#) oder [Zuordnen eines benutzerdefinierten Profils zu einem logischen Port](#).

## Zuordnen eines benutzerdefinierten Profils zu einem logischen Switch

Sie können einem logischen Switch ein benutzerdefiniertes Switching-Profil zuordnen, sodass das Profil auf alle Ports auf dem Switch angewendet wird.

Wenn benutzerdefinierte Switching-Profile einem logischen Switch zugeordnet werden, setzen sie vorhandene Standard-Switching-Profile außer Kraft. Das benutzerdefinierte Switching-Profil wird von untergeordneten logischen Switch-Ports übernommen.

**Hinweis** Wenn Sie ein benutzerdefiniertes Switching-Profil einem logischen Switch zugeordnet haben, aber das Standard-Switching-Profil für einen der untergeordneten logischen Switch Ports beibehalten möchten, müssen Sie eine Kopie des Standard-Switching-Profiles erstellen und diese dem jeweiligen logischen Switch Port zuordnen.

#### Voraussetzungen

- Stellen Sie sicher, dass ein logischer Switch konfiguriert ist. Siehe [Erstellen eines logischen Switches](#).
- Stellen Sie sicher, dass ein benutzerdefiniertes Switching-Profil konfiguriert ist. Siehe [Switching-Profile für logische Switches und logische Ports](#).

#### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > Switching > Switches** aus.

- 3 Klicken Sie auf den logischen Switch, um das benutzerdefinierte Switching-Profil anzuwenden.
- 4 Klicken Sie auf die Registerkarte **Verwalten**.
- 5 Wählen Sie das benutzerdefinierte Switching-Profil im Dropdown-Menü aus.
  - **QoS**
  - **Port Mirroring**
  - **IP-Ermittlung**
  - **SpoofGuard**
  - **Switch-Sicherheit**
  - **MAC-Verwaltung**
- 6 Klicken Sie auf **Ändern**.
- 7 Wählen Sie das zuvor erstellte benutzerdefinierte Switching-Profil im Dropdown-Menü aus.
- 8 Klicken Sie auf **Speichern**.  
Der logische Switch ist nun dem benutzerdefinierten Switching-Profil zugeordnet.
- 9 Stellen Sie sicher, dass das neue benutzerdefinierte Switching-Profil mit der geänderten Konfiguration auf der Registerkarte **Verwalten** angezeigt wird.
- 10 (Optional) Klicken Sie auf die Registerkarte **Zugehörig** und wählen Sie **Ports** im Dropdown-Menü aus, um sicherzustellen, dass das benutzerdefinierte Switching-Profil für die untergeordneten logischen Ports übernommen wurde.

#### Nächste Schritte

Wenn Sie das übernommene Switching-Profil von einem logischen Switch nicht verwenden möchten, können Sie ein benutzerdefiniertes Switching-Profil auf den untergeordneten logischen Switch Port anwenden. Siehe [Zuordnen eines benutzerdefinierten Profils zu einem logischen Port](#).

## Zuordnen eines benutzerdefinierten Profils zu einem logischen Port

Ein logischer Port stellt einen logischen Verbindungspunkt für ein VIF, eine Patch-Verbindung mit einem Router oder eine Gateway-Verbindung der Ebene 2 mit einem externen Netzwerk bereit. Logische Ports stellen zudem Switching-Profile, Portstatistikzähler und einen Status für logische Links bereit.

Sie haben die Möglichkeit, das vom logischen Switch übernommene Switching-Profil in ein anderes, benutzerdefiniertes Switching-Profil für den untergeordneten logischen Port zu ändern.

#### Voraussetzungen

- Stellen Sie sicher, dass ein logischer Port konfiguriert ist. Siehe [Verbinden einer VM mit einem logischen Switch](#).
- Stellen Sie sicher, dass ein benutzerdefiniertes Switching-Profil konfiguriert ist. Siehe [Switching-Profile für logische Switches und logische Ports](#).

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > Switching > Ports** aus.
- 3 Klicken Sie auf den logischen Port, um das benutzerdefinierte Switching-Profil anzuwenden.
- 4 Klicken Sie auf die Registerkarte **Verwalten**.
- 5 Wählen Sie das benutzerdefinierte Switching-Profil im Dropdown-Menü aus.
  - **QoS**
  - **Port Mirroring**
  - **IP-Ermittlung**
  - **SpoofGuard**
  - **Switch-Sicherheit**
  - **MAC-Verwaltung**
- 6 Klicken Sie auf **Ändern**.
- 7 Wählen Sie das zuvor erstellte benutzerdefinierte Switching-Profil im Dropdown-Menü aus.
- 8 Klicken Sie auf **Speichern**.  
Der logische Port ist nun dem benutzerdefinierten Switching-Profil zugeordnet.
- 9 Stellen Sie sicher, dass das neue benutzerdefinierte Switching-Profil mit der geänderten Konfiguration auf der Registerkarte **Verwalten** angezeigt wird.

## Nächste Schritte

Sie können die Aktivität am logischen Switch-Port überwachen, um Probleme zu beheben. Siehe „Überwachen der Aktivität eines Ports für einen logischen Switch“ im *Administratorhandbuch für NSX-T Data Center*.

## Schicht 2-Bridging

Wenn ein logischer NSX-T Data Center-Switch eine Schicht-2-Verbindung mit einer VLAN-gestützten Portgruppe benötigt oder ein anderes Gerät, z. B. ein Gateway, erreichen muss, das sich außerhalb einer NSX-T Data Center-Bereitstellung befindet, können Sie dafür eine NSX-T Data Center-Schicht-2-Bridge verwenden. Diese Schicht 2-Bridge ist besonders in einem Migrationsszenario hilfreich, wenn Sie ein Subnetz auf physische und virtuelle Arbeitslasten aufteilen müssen.

Die NSX-T Data Center-Konzepte beim Schicht 2-Bridging sind Edge-Cluster- und Edge-Bridge-Profile. Sie können das Schicht-2-Bridging mithilfe von NSX Edge-Transportknoten konfigurieren. Um NSX Edge-Transportknoten für das Bridging zu verwenden, erstellen Sie ein Edge-Bridge-Profil. Ein Edge-Bridge-Profil gibt an, welcher Edge-Cluster für das Bridging verwendet werden soll und welcher Edge-Transportknoten als primäre Bridge und Sicherungs-Bridge fungiert.

Das Edge-Bridge-Profil ist an einen logischen Switch angehängt und die Zuordnung gibt den physischen Uplink auf dem Edge an, der für das Bridging verwendet wird. Zudem gibt sie die VLAN-ID an, die dem logischen Switch zugeordnet werden soll. Ein logischer Switch kann an mehrere Bridge-Profile angehängt werden.

## Erstellen eines ESXi-Bridge-Clusters

Ein ESXi-Bridge-Cluster ist eine Sammlung von ESXi-Host-Transportknoten, die einem logischen Switch Bridging auf der Ebene von Schicht 2 ermöglichen.

Ein ESXi-Bridge-Cluster kann maximal zwei ESXi-Host-Transportknoten als Bridge-Knoten umfassen. Ein ESXi-Bridge-Cluster mit zwei Bridge-Knoten ermöglicht Hochverfügbarkeit im Aktiv/Standby-Modus. Selbst wenn Sie für das Bridging nur einen Bridge-Knoten verwenden möchten, müssen Sie dennoch einen Bridge-Cluster erstellen. Nach dem Erstellen des Bridge-Clusters können Sie später einen weiteren Bridge-Knoten hinzufügen.

### Voraussetzungen

- Erstellen Sie mindestens einen NSX-T Data Center-Transportknoten für die Verwendung als Bridge-Knoten.
- Der als Bridge-Knoten verwendete Transportknoten muss ein ESXi-Host sein. KVM-Hosts werden für Bridge-Knoten nicht unterstützt.
- Es wird empfohlen, auf Bridge-Knoten keine VMs zu hosten.
- Ein Transportknoten kann nur einem Bridge-Cluster hinzugefügt werden. Ein bestimmter Transportknoten lässt sich nicht zu mehreren Bridge-Clustern hinzufügen.

### Verfahren

- 1 Wählen Sie **System > Fabric > Knoten > ESXi-Bridge-Cluster > Hinzufügen** aus.
- 2 Geben Sie einen Namen für den Bridge-Cluster und optional eine Beschreibung ein.
- 3 Wählen Sie eine Transportzone für den Bridge-Cluster aus.
- 4 Wählen Sie in der Spalte **Verfügbar** die Transportknoten aus und klicken Sie auf den Pfeil nach rechts, um diese in die Spalte **Ausgewählt** zu übertragen.
- 5 Klicken Sie auf die Schaltfläche **Hinzufügen**.

### Nächste Schritte

Sie können jetzt den Bridge-Cluster einem logischen Switch zuordnen.

## Erstellen eines Edge-Bridge-Profils

Ein Edge-Bridge-Profil ermöglicht es einem NSX Edge-Cluster, Schicht-2-Bridging für einen logischen Switch bereitzustellen.

### Voraussetzungen

- Stellen Sie sicher, dass Sie über einen NSX Edge-Cluster mit zwei NSX Edge-Transportknoten verfügen.

### Verfahren

- 1 Wählen Sie **System > Fabric > Profile > Edge-Bridge-Profile > Hinzufügen** aus.
- 2 Geben Sie einen Namen für das Edge-Bridge-Profil und optional eine Beschreibung ein.
- 3 Wählen Sie einen NSX Edge-Cluster aus.
- 4 Wählen Sie einen Primärknoten aus.
- 5 Wählen Sie einen Sicherungsknoten aus.
- 6 Wählen Sie einen Failover-Modus aus.

Die Optionen sind **Vorbeugend** und **Nicht vorbeugend**.

- 7 Klicken Sie auf die Schaltfläche **Hinzufügen**.

### Nächste Schritte

Sie können jetzt das Bridge-Profil einem logischen Switch zuordnen.

## Konfigurieren von Edge-basiertem Bridging

Wenn Sie Edge-basiertes Bridging konfigurieren, sind nach dem Erstellen eines Edge-Bridge-Profils für einen Edge-Cluster einige zusätzliche Konfigurationen erforderlich.

Beachten Sie, dass das zweimalige Bridging eines logischen Switches auf demselben Edge-Knoten nicht unterstützt wird. Sie können jedoch zwei VLANs auf denselben logischen Switch auf zwei unterschiedlichen Edge-Knoten überbrücken.

Es stehen drei Konfigurationsoptionen zur Verfügung.

### Option 1: Promiskuitiven Modus konfigurieren

- Legen Sie den promiskuitiven Modus für die Portgruppe fest.
- Lassen Sie gefälschte Übertragungen für die Portgruppe zu.
- Führen Sie den folgenden Befehl aus, um den umgekehrten Filter auf dem ESXi-Host zu aktivieren, auf dem die Edge-VM ausgeführt wird:

```
esxcli system settings advanced set -o /Net/ReversePathFwdCheckPromisc -i 1
```



Deaktivieren und aktivieren Sie dann mit folgenden Schritten den promiskuitiven Modus für die Portgruppe:

- Bearbeiten Sie die Portgruppeneinstellungen.
- Deaktivieren Sie den promiskuitiven Modus und speichern Sie die Einstellungen.
- Bearbeiten Sie die Einstellungen der Portgruppe erneut.
- Aktivieren Sie den promiskuitiven Modus und speichern Sie die Einstellungen.
- Sie sollten auf demselben Host keine anderen Portgruppen im promiskuitiven Modus betreiben, die denselben Satz von VLANs verwenden.
- Zudem sollten sich die aktiven und die Standby-Edge-VMs auf verschiedenen Hosts befinden. Wenn sie sich auf demselben Host befinden, kann der Durchsatz sinken, da der VLAN-Datenverkehr im promiskuitiven Modus an beide VMs weitergeleitet werden muss.

## Option 2: MAC Learning konfigurieren

Wenn der Edge auf einem Host bereitgestellt wird, auf dem NSX-T installiert ist, kann er eine Verbindung zu einem logischen VLAN-Switch oder -Segment herstellen. Der logische Switch muss über ein MAC-Verwaltungsprofil mit aktiviertem MAC Learning verfügen. Gleichermäßen muss das Segment über ein MAC Discovery-Profil mit aktiviertem MAC Learning verfügen.

## Option 3: Sink-Port konfigurieren

- 1 Rufen Sie die Portnummer für die Trunk-vNIC ab, die Sie als Sink-Port konfigurieren möchten.
  - a Melden Sie sich beim vSphere Web Client an und navigieren Sie zu **Startseite > Netzwerk**.
  - b Klicken Sie auf die verteilte Portgruppe, mit der die NSX Edge-Trunk-Schnittstelle verbunden ist, und klicken Sie dann auf **Ports**, um die Ports und verbundenen VMs anzuzeigen. Beachten Sie die Portnummer, die der Trunk-Schnittstelle zugeordnet ist. Verwenden Sie diese Portnummer, wenn Sie Opaque-Daten abrufen und aktualisieren.
- 2 Rufen Sie den dvsUuid-Wert für den vSphere Distributed Switch ab.
  - a Melden Sie sich bei der vCenter Mob-Benutzeroberfläche unter `https://<vc-ip>/mob` an.
  - b Klicken Sie auf **Inhalt**.
  - c Klicken Sie auf den Link für den **rootFolder** (Beispiel: *group-d1 [Datacenter]*).
  - d Klicken Sie auf den Link für das **childEntity** (Beispiel: *Datacenter-1*).
  - e Klicken Sie auf den Link für den **networkFolder** (Beispiel: *Gruppe-n6*).
  - f Klicken Sie auf den DVS-Namens-Link für den vSphere Distributed Switch, der NSX Edges zugeordnet ist (Beispiel: *dvs-1 [Mgmt\_VDS]*).
  - g Kopieren Sie den Wert der UUID-Zeichenfolge. Verwenden Sie diesen Wert für dvsUuid, wenn Sie Opaque-Daten abrufen und aktualisieren.

### 3 Überprüfen Sie, ob Opaque-Daten für den angegebenen Port vorhanden sind.

- Wechseln Sie zu `https://<vc-ip>/mob/?moid=DVSManager&vmodl=1`.
- Klicken Sie auf **fetchOpaqueDataEx**.
- Fügen Sie die folgende XML-Eingabe in das Feld für den **selectionSet** ein:

```
<selectionSet xsi:type="DVPortSelection">
  <dvsUuid>c2 1d 11 50 6a 7c 77 68-e6 ba ce 6a 1d 96 2a 15</dvsUuid> <!-- example dvsUuid --
>
  <portKey>393</portKey> <!-- example port number -->
</selectionSet>
```

Verwenden Sie die abgerufene Port-Nummer und den dvsUuid-Wert für die NSX Edge-Trunk-Schnittstelle.

- Legen Sie `isRuntime` auf `false` fest.
  - Klicken Sie auf **Methode aufrufen**. Wenn das Ergebnis Werte für `vim.dvs.OpaqueData.ConfigInfo` anzeigt, ist bereits ein Opaque-Datensatz vorhanden. Verwenden Sie in diesem Fall den Vorgang `edit`, wenn Sie den Sink-Port festlegen. Wenn kein Wert für `vim.dvs.OpaqueData.ConfigInfo` angezeigt wird, verwenden Sie die Operation `add`, wenn Sie den Sink-Port festlegen.
- ### 4 Konfigurieren Sie den Sink-Port im Browser für verwaltete Objekte (Managed Object Browser, MOB) von vCenter.

- Wechseln Sie zu `https://<vc-ip>/mob/?moid=DVSManager&vmodl=1`.
- Klicken Sie auf **updateOpaqueDataEx**.
- Fügen Sie die folgende XML-Eingabe in das Feld für den **selectionSet** ein. Beispiel:

```
<selectionSet xsi:type="DVPortSelection">
  <dvsUuid>c2 1d 11 50 6a 7c 77 68-e6 ba ce 6a 1d 96 2a 15</dvsUuid> <!-- example dvsUuid --
>
  <portKey>393</portKey> <!-- example port number -->
</selectionSet>
```

Verwenden Sie den dvsUuid-Wert, den Sie von vCenter MOB abgerufen haben.

- Fügen Sie eine der folgenden XML-Eingaben in das Feld für die „opaqueDataSpec“ ein.

Verwenden Sie diese Eingabe, um einen SINK-Port zu aktivieren, wenn keine Opaque-Daten festgelegt sind (wenn operation auf `add` festgelegt ist):

```
<opaqueDataSpec>
  <operation>add</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData
xsi:type="vmodl.Binary">AAABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA=
```

Verwenden Sie diese Eingabe, um einen SINK-Port zu aktivieren, wenn bereits Opaque-Daten festgelegt sind (wenn operation auf edit festgelegt ist):

```

<opaqueDataSpec>
  <operation>edit</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData
xsi:type="vmidl.Binary">AAABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA=
```

Verwenden Sie diese Eingabe, um einen SINK-Port zu deaktivieren:

```

<opaqueDataSpec>
  <operation>edit</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData
xsi:type="vmidl.Binary">AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA=
```

- e Legen Sie isRuntime auf false fest.
- f Klicken Sie auf **Methode aufrufen**.

## Erstellen eines Bridge-gestützten logischen Schicht-2-Switches

Wenn Sie über VMs verfügen, die mit dem NSX-T Data Center-Overlay verbunden sind, können Sie einen Bridge-gestützten logischen Switch konfigurieren, um Schicht-2-Konnektivität mit anderen Geräten oder VMs, die sich außerhalb Ihrer NSX-T Data Center-Bereitstellung befinden, zu ermöglichen.

### Voraussetzungen

- Stellen Sie sicher, dass Sie über einen Bridge-Cluster oder ein Bridge-Profil verfügen.
- Mindestens ein ESXi- oder KVM-Host als regulärer Transportknoten. Dieser Knoten verfügt über gehostete VMs, für die eine Konnektivität mit Geräten außerhalb einer NSX-T Data Center-Bereitstellung erforderlich ist.

- Eine VM oder ein anderes Endgerät außerhalb der NSX-T Data Center-Bereitstellung. Dieses Endgerät muss an einen VLAN-Port angefügt sein, der der VLAN-ID des Bridge-gestützter logischer Switch entspricht.
- Ein logischer Switch in einer Overlay-Transportzone als Bridge-gestützter logischer Switch.

## Verfahren

- 1 Melden Sie sich in einem Browser bei NSX Manager unter `https://<nsx-mgr>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > Switching**.
- 3 Klicken Sie auf den Namen eines Overlay-Switches (Datenverkehrstyp: Overlay).
- 4 Klicken Sie auf **Zugehörig > ESXi-Bridge-Cluster** oder auf **Zugehörig > Edge-Bridge-Profile**.
- 5 Klicken Sie auf **Anhängen**.
- 6 Um den Switch an einen Bridge-Cluster anzuhängen, verfahren Sie wie folgt:
  - a Wählen Sie einen Bridge-Cluster aus.
  - b Geben Sie eine VLAN-ID ein.
  - c Aktivieren oder deaktivieren Sie **HA auf VLAN**.
  - d Klicken Sie auf **Anhängen**.
- 7 Um den Switch an ein Bridge-Profil anzuhängen, verfahren Sie wie folgt:
  - a Wählen Sie ein Bridge-Profil aus.
  - b Wählen Sie eine Transportzone aus.
  - c Geben Sie eine VLAN-ID ein.
  - d Klicken Sie auf **Speichern**.
- 8 Verbinden Sie VMs mit dem logischen Switch, wenn diese noch nicht verbunden sind.  
Die VMs müssen sich auf Transportknoten in derselben Transportzone wie der Bridge-Cluster bzw. das Bridge-Profil befinden.

## Ergebnisse

Sie können das Funktionieren der Bridge durch Senden eines Ping-Befehls von der NSX-T Data Center-internen VM an einen für NSX-T Data Center externen Knoten überprüfen.

Sie können den Datenverkehr auf dem Bridge-gestützten Switch überwachen, indem Sie auf die Registerkarte **Überwachen** klicken.

Der Bridge-Datenverkehr lässt sich auch mit dem API-Aufruf GET `https://192.168.110.31/api/v1/bridge-endpoints/<endpoint-id>/statistics` anzeigen:

```
{
  "tx_packets": {
    "total": 134416,
```


```
    "dropped": 0,  
    "multicast_broadcast": 0  
  },  
  "rx_bytes": {  
    "total": 22164,  
    "multicast_broadcast": 0  
  },  
  "tx_bytes": {  
    "total": 8610134,  
    "multicast_broadcast": 0  
  },  
  "rx_packets": {  
    "total": 230,  
    "dropped": 0,  
    "multicast_broadcast": 0  
  },  
  "last_update_timestamp": 1454979822860,  
  "endpoint_id": "ba5ba59d-22f1-4a02-b6a0-18ef0e37ef31"  
}
```

NSX-T Data Center unterstützt ein Routing-Modell mit 2 Ebenen.

In der obersten Ebene befindet sich der logische Tier-0 Router. In Northbound-Richtung stellt der logische Tier-0 Router eine Verbindung mit einem oder mehreren physischen Routern oder Layer-3-Switches her und dient als Gateway zur physischen Infrastruktur. In Southbound-Richtung verbindet sich der logische Tier-0 Router mit einem oder mehreren logischen Tier-1 Routern oder direkt mit einem oder mehreren logischen Switches.

In der untersten Ebene befindet sich der logische Tier-1-Router. In Northbound-Richtung stellt der logische Tier-1 Router eine Verbindung mit einem logischen Tier-0 Router her. In Southbound-Richtung wird eine Verbindung mit einem oder mehreren logischen Switches hergestellt.

---

**Hinweis** Wenn Sie die Benutzeroberfläche **Netzwerk und Sicherheit – Erweitert** verwenden, um in der Richtlinienschnittstelle erstellte Objekte zu ändern, sind einige Einstellungen möglicherweise nicht konfigurierbar. Neben diesen schreibgeschützten Einstellungen wird dieses Symbol angezeigt: . Weitere Informationen hierzu finden Sie unter [Kapitel 1 Übersicht über NSX Manager](#).

---

Dieses Kapitel enthält die folgenden Themen:

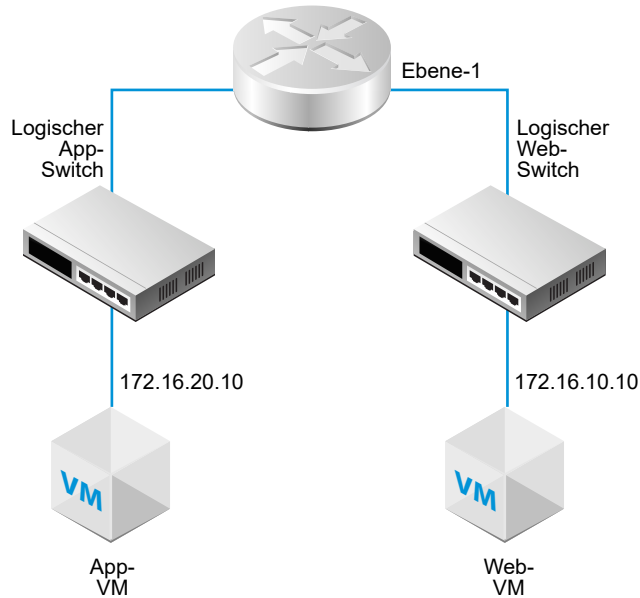
- [Logischer Tier-1-Router](#)
- [Logischer Tier-0 Router](#)

## Logischer Tier-1-Router

Logische Tier-1 Router verfügen über Downlink-Ports, mit denen Sie eine Verbindung mit logischen -Switches, und über Uplink-Ports, mit denen Sie eine Verbindung mit logischen -Tier-0 Routern herstellen können.

Wenn Sie einen logischen Router hinzufügen, müssen Sie zuerst die Netzwerktopologie konzipieren, die aufgebaut werden soll.

Abbildung 14-1. Topologie eines logischen Tier-1-Routers



Beispiel: Die folgende einfache Topologie enthält zwei logische Switches, die mit einem logischen Tier-1 Router verbunden sind. Jeder logische Switch ist mit einer einzelnen VM verbunden. Die beiden VMs können sich auf verschiedenen Hosts oder auf demselben Host, in verschiedenen Hostclustern oder im selben Hostcluster befinden. Wenn ein logischer Router die VMs nicht trennt, müssen sich die zugrunde liegenden IP-Adressen, die in den VMs konfiguriert sind, im selben Subnetz befinden. Wenn ein logischer Router die VMs trennt, müssen sich die IP-Adressen in den VMs in verschiedenen Subnetzen befinden.

In bestimmten Szenarien senden externe Clients API-Anfragen für MAC-Adressen, die an LB VIP-Ports gebunden sind. LB VIP-Ports verfügen jedoch nicht über MAC-Adressen und können solche Anfragen nicht verarbeiten. Proxy-ARP wird auf den zentralen Dienstports eines logischen Tier-1-Routers implementiert, um ARP-Anfragen im Auftrag der LB VIP-Ports zu verarbeiten.

Wenn ein logischer Tier-1 Router mit DNAT, Edge-Firewall und Load Balancer konfiguriert ist, wird der Datenverkehr zu und von einem anderen logischen Tier-1 Router in dieser Reihenfolge verarbeitet: zuerst DNAT, dann Edge-Firewall und dann der Load Balancer. Der Datenverkehr innerhalb des logischen Tier-1 Routers wird zuerst über DNAT und dann durch den Load Balancer verarbeitet. Die Edge-Firewall-Verarbeitung wird übersprungen.

Auf einem logischen Tier-0 oder Tier-1 Router können Sie verschiedene Arten von Ports konfigurieren. Ein Typ wird als zentralisierter Dienstport (Centralized Service Port, CSP) bezeichnet. Sie müssen einen CSP auf einem logischen Tier-0 Router im Aktiv/Standby-Modus oder einem logischen Tier-1 Router konfigurieren, um eine Verbindung zu einem VLAN-gestützten logischen Switch herzustellen oder um einen eigenständigen logischen Tier-1 Router zu erstellen. Ein CSP unterstützt die folgenden Dienste auf einem logischen Tier-0 Router im Aktiv/Standby-Modus oder einem logischen Tier-1 Router:

- NAT

- Load Balancing
- Statusbehaftete Firewall
- VPN (IPSec und L2VPN)

## Erstellen eines logischen Tier-1-Routers

Der logische Tier-1 Router muss mit dem logischen Tier-0 Router verbunden sein, um Zugriff auf den physischen Northbound-Router zu erhalten.

### Voraussetzungen

- Stellen Sie sicher, dass die logischen Switches konfiguriert sind. Siehe [Erstellen eines logischen Switches](#).
- Stellen Sie sicher, dass ein NSX Edge-Cluster bereitgestellt ist, um die NAT-Konfiguration (Network Address Translation) auszuführen. Siehe *Installationshandbuch für NSX-T Data Center*.
- Machen Sie sich mit der Topologie eines logischen Tier-1-Routers vertraut. Siehe [Logischer Tier-1-Router](#).

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Router > Hinzufügen** aus.
- 3 Wählen Sie **Tier-1-Router** aus und geben Sie einen Namen für den logischen Router und optional eine Beschreibung ein.
- 4 (Optional) Wählen Sie einen logischen Tier-0 Router, der mit diesem logischen Tier-1 Router verbunden werden soll.

Wenn noch keine logischen Tier-0-Router konfiguriert sind, können Sie dieses Feld hier leer lassen und die Routerkonfiguration später bearbeiten.

- 5 (Optional) Wählen Sie einen NSX Edge-Cluster aus.

Klicken Sie zum Aufheben der Auswahl eines ausgewählten Clusters auf das Symbol **x**. Wenn der logische Tier-1-Router für die NAT-Konfiguration verwendet werden soll, muss er mit einem NSX Edge-Cluster verbunden werden. Wenn noch keine NSX Edge-Cluster konfiguriert sind, können Sie dieses Feld hier leer lassen und die Routerkonfiguration später bearbeiten.

- 6 (Optional) Klicken Sie auf den Umschalter **Standby-Verlagerung**, um die Standby-Verlagerung zu aktivieren oder zu deaktivieren.

Wenn bei der Standby-Verlagerung der Edge-Knoten, auf dem der aktive oder der logische Standby-Router ausgeführt wird, fehlschlägt, wird ein neuer logischer Standby-Router auf einem anderen Edge-Knoten erstellt, um Hochverfügbarkeit aufrechtzuerhalten. Wenn der



fehlerhafte Edge-Knoten den aktiven logischen Router ausführt, wird der ursprüngliche logische Standby-Router zum aktiven logischen Router und ein neuer logischer Standby-Router wird erstellt. Wenn der fehlerhafte Edge-Knoten den logischen Standby-Router ausführt, wird er durch den neuen logischen Standby-Router ersetzt.

- 7 (Optional) Wenn Sie einen NSX Edge-Cluster ausgewählt haben, wählen Sie einen Failover-Modus aus.

Option	Beschreibung
Vorbeugend	Wenn der bevorzugte Knoten fehlschlägt und wiederhergestellt wird, hat er Vorrang vor seinem Peer und wird zum aktiven Knoten. Der Peer ändert seinen Zustand in Standby. Dies ist die Standardoption.
Nicht vorbeugend	Wenn der bevorzugte Knoten fehlschlägt und wiederhergestellt wird, erfolgt eine Überprüfung, ob der zugehörige Peer der aktive Knoten ist. Ist dies der Fall, hat der bevorzugte Knoten keinen Vorrang vor seinem Peer, und er ist der Standby-Knoten.

- 8 (Optional) Klicken Sie auf die Registerkarte **Erweitert**, und geben Sie einen Wert für **Intra-Tier1-Transitsubnetz** ein.

- 9 Klicken Sie auf **Hinzufügen**.

### Ergebnisse

Wenn Sie nach dem Erstellen des logischen Routers den Edge-Cluster aus der Konfiguration des Routers entfernen möchten, führen Sie die folgenden Schritte aus:

- Klicken Sie auf den Namen des Routers, um die Konfigurationsdetails anzuzeigen.
- Wählen Sie **Dienste > Edge-Firewall** aus.
- Klicken Sie auf **Firewall deaktivieren**.
- Klicken Sie auf die Registerkarte **Übersicht** und anschließend auf **Bearbeiten**.
- Klicken Sie im Feld **Edge-Cluster** auf das Symbol **x**.
- Klicken Sie auf **Speichern**.

Wenn dieser logische Router mehr als 5000 VMs unterstützt, müssen Sie die folgenden Befehle auf jedem Knoten im NSX Edge-Cluster ausführen, um die ARP-Tabelle zu vergrößern.

```
set debug-mode
set dataplane neighbor max-arp-logical-router 10000
```

Sie müssen die Befehle erneut nach einem Neustart der Datenebene oder des Knotens ausführen, da die Änderung nicht persistent ist.

### Nächste Schritte

Erstellen Sie Downlink-Ports für den logischen Tier-1-Router. Siehe [Hinzufügen eines Downlink-Ports auf einem logischen Tier-1-Router](#).

## Hinzufügen eines Downlink-Ports auf einem logischen Tier-1-Router

Wenn Sie einen Downlink-Port auf einem logischen Tier-1-Router erstellen, dient der Port als Standard-Gateway für die VMs im selben Subnetz.

### Voraussetzungen

Stellen Sie sicher, dass ein logischer Tier-1-Router konfiguriert ist. Siehe [Erstellen eines logischen Tier-1-Routers](#).

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.
- 3 Klicken Sie auf den Namen eines Routers.
- 4 Klicken Sie auf die Registerkarte **Konfiguration** und wählen Sie **Router-Ports**.
- 5 Klicken Sie auf **Hinzufügen**.
- 6 Geben Sie für den Router-Port einen Namen und optional eine Beschreibung ein.
- 7 Wählen Sie im Feld **Typ** die Option **Downlink** aus.
- 8 Wählen Sie als **URPF-Modus** entweder **Streng** oder **Keine** aus.  
URPF (Unicast Reverse Path Forwarding) ist eine Sicherheitsfunktion.
- 9 (Optional) Wählen Sie einen logischen Switch aus.
- 10 Wählen Sie aus, ob diese Anfügung einen neuen Switch-Port erstellt oder einen vorhandenen Switch-Port aktualisiert.  
Bezieht sich die Anfügung auf einen vorhandenen Switch-Port, wählen Sie den betreffenden Port im Dropdown-Menü aus.
- 11 Geben Sie die IP-Adresse des Routerports in CIDR-Notation ein.  
So kann die IP-Adresse z. B. 172.16.10.1/24 lauten.
- 12 (Optional) Wählen Sie einen DHCP-Relay-Dienst aus.
- 13 Klicken Sie auf **Hinzufügen**.

### Nächste Schritte

Aktivieren Sie Routen-Advertisement für eine vertikale Konnektivität zwischen VMs und externen physischen Netzwerken oder zwischen unterschiedlichen logischen Tier-1 Routern, die mit dem gleichen logischen Tier-0 Router verbunden sind. Siehe [Konfigurieren von Routen-Advertisement auf einem logischen Tier-1 Router](#).

## Hinzufügen eines VLAN-Ports auf einem logischen Tier-0- oder Tier-1-Router

Wenn Sie nur über VLAN-basierte logische Switches verfügen, können Sie die Switches mit VLAN-Ports auf einem Tier-0- oder Tier-1-Router verbinden, sodass NSX-T Data Center Schicht-3-Dienste bereitstellen kann.

### Verfahren

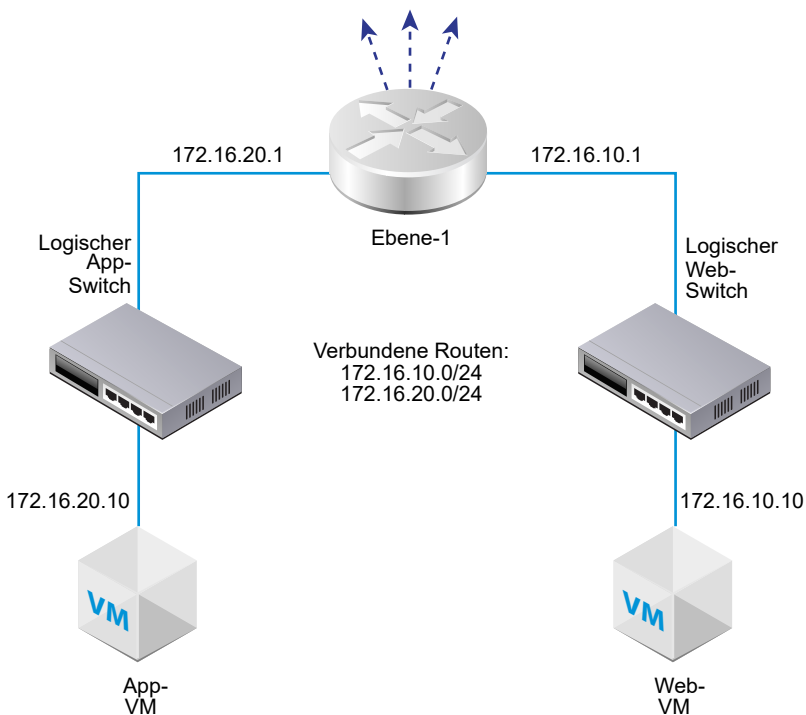
- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.
- 3 Klicken Sie auf den Namen eines Routers.
- 4 Klicken Sie auf die Registerkarte **Konfiguration** und wählen Sie **Router-Ports**.
- 5 Klicken Sie auf **Hinzufügen**.
- 6 Geben Sie für den Router-Port einen Namen und optional eine Beschreibung ein.
- 7 Wählen Sie im Feld **Typ** die Option **Zentral** aus.
- 8 Wählen Sie als **URPF-Modus** entweder **Streng** oder **Keine** aus.  
URPF (Unicast Reverse Path Forwarding) ist eine Sicherheitsfunktion.
- 9 (Erforderlich) Wählen Sie einen logischen Switch aus.
- 10 Wählen Sie aus, ob diese Anfügung einen neuen Switch-Port erstellt oder einen vorhandenen Switch-Port aktualisiert.  
  
Bezieht sich die Anfügung auf einen vorhandenen Switch-Port, wählen Sie den betreffenden Port im Dropdown-Menü aus.
- 11 Geben Sie die IP-Adresse des Routerports in CIDR-Notation ein.
- 12 Klicken Sie auf **Hinzufügen**.

## Konfigurieren von Routen-Advertisement auf einem logischen Tier-1 Router

Um eine Schicht-3-Konnektivität zwischen VMs zur Verfügung zu stellen, die mit logischen Switches verbunden sind, die an unterschiedliche logische Tier-1 Router angefügt wurden, muss Tier-1-Routen-Advertisement in Richtung Tier-0 aktiviert sein. Sie müssen kein Routing-Protokoll und keine statische Routen zwischen Tier-1- und Tier-0-Routern konfigurieren. NSX-T Data Center erstellt statische NSX-T Data Center-Routen automatisch, wenn Sie Routen-Advertisement aktivieren.

Um beispielsweise eine Konnektivität zu und von VMs über andere Peer-Router bereitzustellen, muss für den logischen Tier-1 Router Routen-Advertisement für verbundene Routen konfiguriert sein. Wenn nicht alle verbundenen Routen angekündigt werden sollen, können Sie die dafür vorgesehenen Routen einzeln festlegen.

## Ankündigen verbundener Router



### Voraussetzungen

- Stellen Sie sicher, dass VMs an logische Switches angefügt sind. Siehe [Kapitel 13 Logische Switches](#).
- Stellen Sie sicher, dass Downlink-Ports für den logischen Tier-1-Router konfiguriert sind. Siehe [Hinzufügen eines Downlink-Ports auf einem logischen Tier-1-Router](#).

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.
- 3 Klicken Sie auf den Namen eines Tier-1-Routers.
- 4 Wählen Sie im Dropdown-Menü **Routing** die Option **Routen-Advertisement** aus.
- 5 Klicken Sie auf **Bearbeiten**, um die Konfiguration von Routen-Advertisement zu bearbeiten.

Sie können die folgenden Switches umschalten:

- **Status**
- **Alle mit NSX verbundenen Routen ankündigen**
- **Alle NAT-Routen ankündigen**
- **Alle statischen Routen ankündigen**

- **Alle LB VIP-Routen ankündigen**
- **Alle LB SNAT-IP-Routen ankündigen**
- **Alle DNS-Weiterleitungsrouten ankündigen**

a Klicken Sie auf **Speichern**.

6 Klicken Sie auf **Hinzufügen**, um Routen anzukündigen.

- a Geben Sie einen Namen und optional eine Beschreibung ein.
- b Geben Sie ein Routen-Präfix im CIDR-Format ein.
- c Klicken Sie auf **Filter anwenden**, um die folgenden Optionen festzulegen:

Aktion	Geben Sie <b>Zulassen</b> oder <b>Verweigern</b> an.
<b>Routentypen abgleichen</b>	Wählen Sie mindestens eine der folgenden Optionen aus: <ul style="list-style-type: none"> <li>■ <b>Alle</b></li> <li>■ <b>NSX verbunden</b></li> <li>■ <b>Tier-1-LB-VIP</b></li> <li>■ <b>Statisch</b></li> <li>■ <b>Tier-1 NAT</b></li> <li>■ <b>Tier-1-LB-SNAT</b></li> </ul>
<b>Präfix-Operator</b>	Wählen Sie <b>GE</b> oder <b>EQ</b> aus.

- d Klicken Sie auf **Hinzufügen**.

#### Nächste Schritte

Machen Sie sich mit der Topologie des logischen Tier-0 Routers vertraut und erstellen Sie den logischen Tier-0 Router. Siehe [Logischer Tier-0 Router](#).

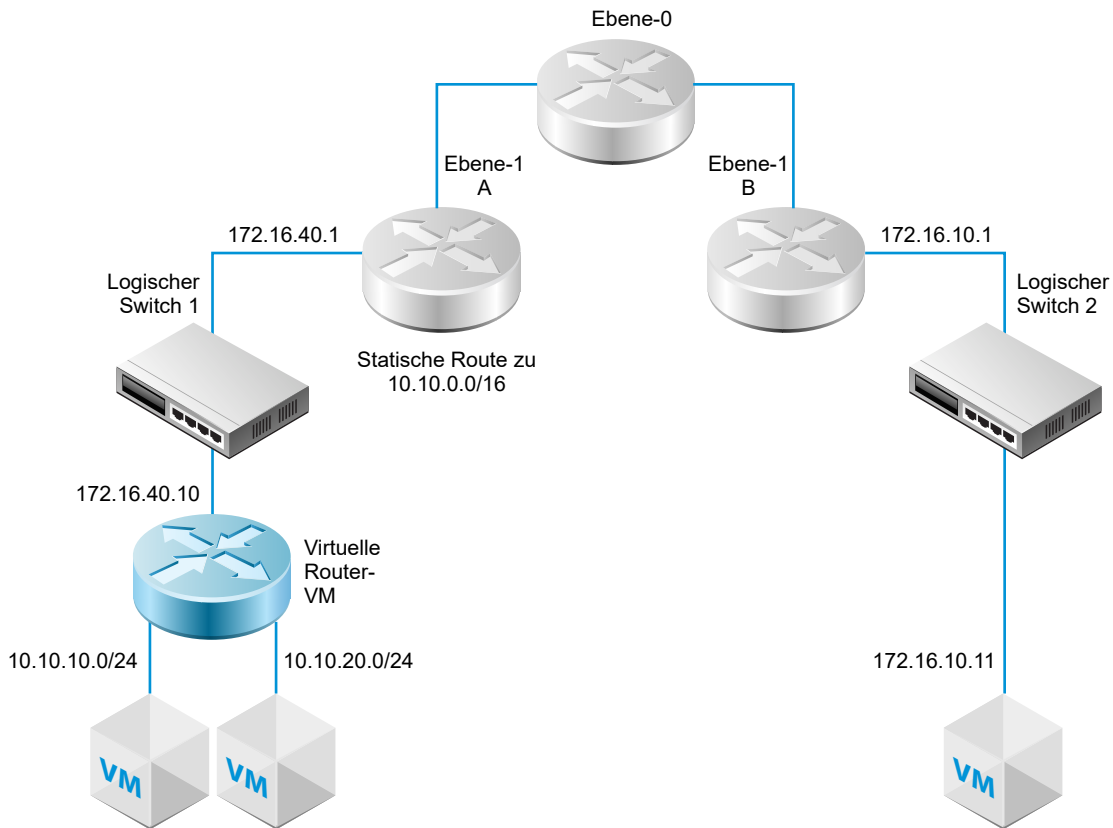
Wenn bereits ein logischer Tier-0 Router mit dem logischen Tier-1 Router verbunden ist, müssen Sie sicherstellen, dass der Tier-0 Router die Informationen über die mit dem Tier-1 Router verbundenen Routen abrufen. Siehe [Überprüfen des Abrufs von Routen von einem Tier-1-Router für einen Tier-0-Router](#).

## Konfigurieren einer statischen Route auf einem logischen Tier-1-Router

Sie können eine statische Route auf einem logischen Tier-1-Router konfigurieren, um Konnektivität von NSX-T Data Center zu einer Gruppe aus Netzwerken bereitzustellen, auf die über einen virtuellen Router zugegriffen werden kann.

Im folgenden Diagramm verfügt beispielsweise der logische Tier-1 A-Router über einen Downlink-Port zu einem logischen NSX-T Data Center-Switch. Dieser Downlink-Port (172.16.40.1) bedient das Standard-Gateway für die virtuelle Router-VM. Die virtuelle Router-VM und Tier-1 A sind über denselben logischen NSX-T Data Center-Switch verbunden. Der logische Tier-1-Router hat die statische Route 10.10.0.0/16, die die über den virtuellen Router verfügbaren Netzwerke zusammenfasst. Bei Tier-1 A wird dann Routen-Advertisement konfiguriert, um die statische Route zu Tier-1 B anzukündigen.

Abbildung 14-2. Topologie einer statischen Route auf einem logischen Tier-1-Router



Rekursive statische Routen werden unterstützt.

#### Voraussetzungen

Stellen Sie sicher, dass ein Downlink-Port konfiguriert ist. Siehe [Hinzufügen eines Downlink-Ports auf einem logischen Tier-1-Router](#).

#### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.
- 3 Klicken Sie auf den Namen eines Tier-1-Routers.
- 4 Klicken Sie auf die Registerkarte **Routing**, und wählen Sie im Dropdown-Menü den Eintrag **Statische Routen** aus.
- 5 Klicken Sie auf **Hinzufügen**.
- 6 Geben Sie eine Netzwerkadresse im CIDR-Format ein.

Auf IPv6 basierende statische Route wird unterstützt. IPv6-Präfixe können nur einen nächsten IPv6-Hop aufweisen.

Beispielsweise 10.10.10.0/16 oder eine IPv6-Adresse.

- 7 Klicken Sie auf **Hinzufügen**, um eine IP-Adresse für den nächsten Hop hinzuzufügen.

Beispiel: 172.16.40.10. Sie können auch eine Null-Route angeben, indem Sie auf das Bleistiftsymbol klicken und in der Dropdown-Liste **NULL** auswählen. Um weitere Adressen für den nächsten Hop hinzuzufügen, klicken Sie erneut auf **Hinzufügen**.

- 8 Klicken Sie unten im Dialogfeld auf **Hinzufügen**.

Die neu erstellte Netzwerkadresse für die statische Route wird in der Zeile angezeigt.

- 9 Wählen Sie beim logischen Tier-1-Router die Option **Routing > Routen-Advertisement**.

- 10 Klicken Sie auf **Bearbeiten** und wählen Sie **Alle statischen Routen ankündigen**.

- 11 Klicken Sie auf **Speichern**.

Die statische Route wird über das NSX-T Data Center-Overlay weitergegeben.

## Erstellen eines eigenständigen logischen Tier-1-Routers

Ein eigenständiger logischer Tier-1-Router hat keinen Downlink und keine Verbindung zu einem Tier-0-Router. Er hat einen Dienst-Router, aber keinen verteilten Router. Der Dienst-Router kann auf einem NSX Edge-Knoten oder zwei NSX Edge-Knoten im Aktiv-Standby-Modus bereitgestellt werden.

Ein eigenständiger logischer Tier-1-Router:

- Darf keine Verbindung zu einem logischen Tier-0-Router haben.
- Darf keinen Downlink haben.
- Kann nur einen zentralen Dienstport (Centralized Service Port, CSP) haben, wenn er dazu dient, einen Load Balancer-Dienst (LB) anzuhängen.
- Kann eine Verbindung zu einem logischen Overlay-Switch oder einem logischen VLAN-Switch herstellen.
- Unterstützt eine beliebige Kombination der IPSec-, DNAT-, Firewall-, Load Balancer- und Service Insertion-Dienste. Für Ingress lautet die Verarbeitungsreihenfolge: IPSec – DNAT – Firewall – Load Balancer – Service Insertion. Für Egress lautet die Verarbeitungsreihenfolge: Service Insertion - Load Balancer - Firewall- DNAT - IPSec.

In der Regel ist ein eigenständiger logischer Tier-1-Router mit einem logischen Switch verbunden, mit dem auch ein normaler logischer Tier-1-Router verbunden ist. Der eigenständige logische Tier-1-Router kann mit anderen Geräten über den normalen logischen Tier-1-Router kommunizieren, nachdem statische Routen und Routen-Ankündigungen konfiguriert wurden.

Bevor Sie den eigenständigen logischen Tier-1-Router verwenden, beachten Sie Folgendes:

- Um das Standard-Gateway für den eigenständigen logischen Tier-1-Router anzugeben, müssen Sie eine statische Route hinzufügen. Das Subnetz sollte 0.0.0.0/0 sein, und der nächste Hop ist die IP-Adresse eines normalen Tier-1-Routers, der mit demselben Switch verbunden ist.

- ARP-Proxy auf dem eigenständigen Router wird unterstützt. Sie können eine virtuelle LB-Server-IP oder LB-SNAT-IP im Subnetz des CSP konfigurieren. Wenn beispielsweise die CSP-IP 1.1.1.1/24 lautet, kann die virtuelle IP-Adresse 1.1.1.2 sein. Es kann sich auch um eine IP in einem anderen Subnetz (z. B. 2.2.2.2) handeln, wenn das Routing ordnungsgemäß konfiguriert ist, sodass der Datenverkehr für 2.2.2.2 den eigenständigen Router erreichen kann.
- Bei einer NSX Edge-VM darf es nur einen CSP geben, der mit demselben VLAN-gestützten logischen Switch oder mit anderen VLAN-gestützten logischen Switches, die über dieselbe VLAN-ID verfügen, verbunden ist.

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Router > Hinzufügen** aus.
- 3 Wählen Sie **Tier-1-Router** aus und geben Sie einen Namen für den logischen Router und optional eine Beschreibung ein.
- 4 (Erforderlich) Wählen Sie einen NSX Edge-Cluster, der mit diesem logischen Tier-1-Router verbunden werden soll.
- 5 (Erforderlich) Wählen Sie einen Failover-Modus und Clustermitglieder aus.

Option	Beschreibung
Vorbeugend	Wenn der bevorzugte Knoten fehlschlägt und wiederhergestellt wird, hat er Vorrang vor seinem Peer und wird zum aktiven Knoten. Der Peer ändert seinen Zustand in Standby. Dies ist die Standardoption.
Nicht vorbeugend	Wenn der bevorzugte Knoten fehlschlägt und wiederhergestellt wird, erfolgt eine Überprüfung, ob der zugehörige Peer der aktive Knoten ist. Ist dies der Fall, hat der bevorzugte Knoten keinen Vorrang vor seinem Peer, und er ist der Standby-Knoten.

- 6 Klicken Sie auf **Hinzufügen**.
- 7 Klicken Sie auf den Namen des Routers, den Sie gerade erstellt haben.
- 8 Klicken Sie auf die Registerkarte **Konfiguration** und wählen Sie **Router-Ports**.
- 9 Klicken Sie auf **Hinzufügen**.
- 10 Geben Sie für den Router-Port einen Namen und optional eine Beschreibung ein.
- 11 Wählen Sie im Feld **Typ** die Option **Zentral** aus.
- 12 Wählen Sie als **URPF-Modus** entweder **Streng** oder **Keine** aus.  
URPF (Unicast Reverse Path Forwarding) ist eine Sicherheitsfunktion.
- 13 (Erforderlich) Wählen Sie einen logischen Switch aus.
- 14 Wählen Sie aus, ob diese Anfügung einen neuen Switch-Port erstellt oder einen vorhandenen Switch-Port aktualisiert.
- 15 Geben Sie die IP-Adresse des Routerports in CIDR-Notation ein.



16 Klicken Sie auf **Hinzufügen**.

## Logischer Tier-0 Router

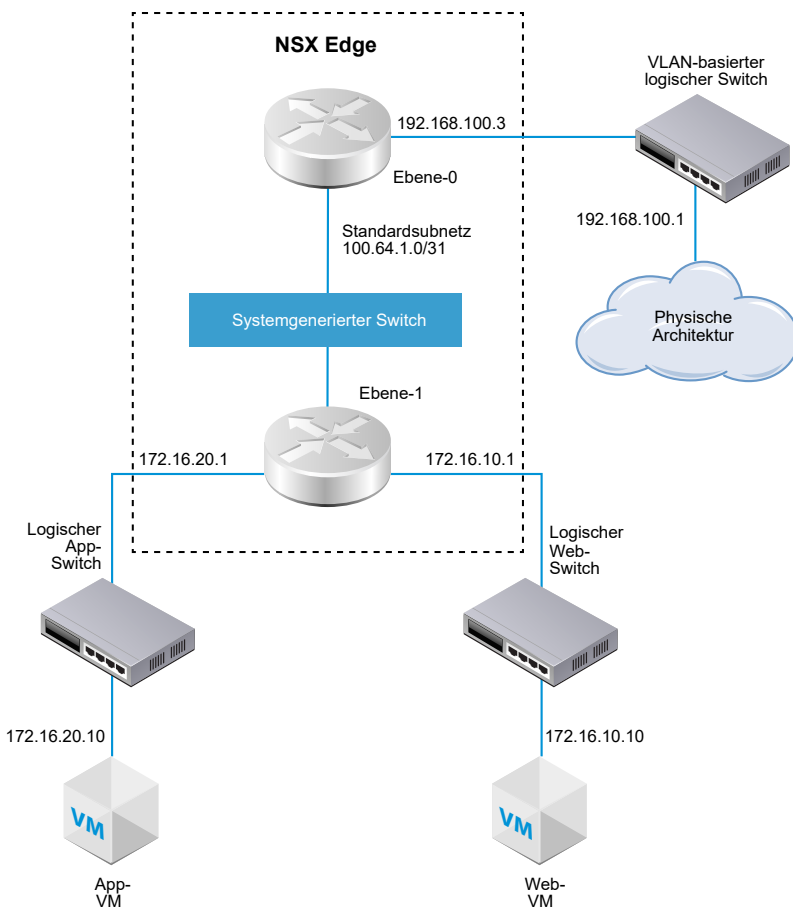
Ein logischer Tier-0 Router bietet einen Gateway-Dienst zwischen dem logischen und dem physischen Netzwerk.

**NSX Cloud-Hinweis** Wenn Sie NSX Cloud verwenden, finden Sie unter [Verwendung von NSX-T Data Center-Funktionen mit der Public Cloud](#) eine Liste der automatisch generierten logischen Einheiten, unterstützten Funktionen und Konfigurationen, die für NSX Cloud erforderlich sind.

Ein Edge-Knoten kann nur ein Tier-0-Gateway oder einen logischen Router unterstützen. Wenn Sie ein Tier-0-Gateway oder einen logischen Router erstellen, stellen Sie sicher, dass Sie nicht mehr Tier-0-Gateways oder logische Router als die Anzahl der Edge-Knoten im NSX Edge-Cluster anlegen.

Wenn Sie einen logischen Tier-0 Router hinzufügen, müssen Sie zuerst die Netzwerktopologie entwickeln, die aufgebaut werden soll.

Abbildung 14-3. Topologie des logischen Tier-0 Routers



Der Einfachheit halber stellt die Beispieltopologie einen einzelnen logischen Tier-1 Router dar, der mit einem einzelnen logischen Tier-0 Router verbunden ist, der auf einem einzelnen NSX Edge-Knoten gehostet wird. Bitte beachten Sie, dass dies keine empfohlene Topologie darstellt. Idealerweise sollten Sie über mindestens zwei NSX Edge-Knoten verfügen, um das Design des logischen Routers maximal nutzen zu können.

Der logische Tier-1 Router verfügt über einen logischen Web-Switch und über einen logischen App-Switch mit angefügten entsprechenden VMs. Der Router-Link-Switch zwischen dem Tier-1-Router und dem Tier-0-Router wird automatisch beim Anfügen des Tier-1-Routers an den Tier-0-Router erstellt. Dieser Switch wird deshalb als „systemgeneriert“ gekennzeichnet.

In einigen Szenarien senden externe Clients ARP-Abfragen für MAC-Adressen, die an Loopback- oder IKE-IP-Ports gebunden sind. Allerdings haben Loopback- und IKE-IP-Ports keine MAC-Adressen und können solche Abfragen nicht verarbeiten. Proxy ARP wird auf den Uplink- und zentralisierten Dienstports eines logischen Tier-0 Routers implementiert, um ARP-Abfragen für die Loopback- und IKE-IP-Ports zu verarbeiten.

Wenn ein logischer Tier-0 Router mit DNAT-, IPsec- und Edge-Firewall konfiguriert ist, wird der Datenverkehr in dieser Reihenfolge verarbeitet: zuerst IPsec, dann DNAT und dann die Edge-Firewall.

Auf einem logischen Tier-0 oder Tier-1 Router können Sie verschiedene Arten von Ports konfigurieren. Ein Typ wird als zentralisierter Dienstport (Centralized Service Port, CSP) bezeichnet. Sie müssen einen CSP auf einem logischen Tier-0 Router im Aktiv/Standby-Modus oder einem logischen Tier-1 Router konfigurieren, um eine Verbindung zu einem VLAN-gestützten logischen Switch herzustellen oder um einen eigenständigen logischen Tier-1 Router zu erstellen. Ein CSP unterstützt die folgenden Dienste auf einem logischen Tier-0 Router im Aktiv/Standby-Modus oder einem logischen Tier-1 Router:

- NAT
- Load Balancing
- Statusbehaftete Firewall
- VPN (IPSec und L2VPN)

## Erstellen eines logischen Tier-0-Routers

Logische Tier-0-Router verfügen über Downlink-Ports, mit denen Sie eine Verbindung mit logischen NSX-T Data Center-Tier-1-Routern, und über Uplink-Ports, mit denen Sie eine Verbindung mit externen Netzwerken herstellen können.

### Voraussetzungen

- Stellen Sie sicher, dass mindestens ein NSX Edge installiert ist. Weitere Informationen finden Sie unter *Installationshandbuch für NSX-T Data Center*.
- Stellen Sie sicher, dass ein NSX Edge-Cluster konfiguriert ist. Siehe *Installationshandbuch für NSX-T Data Center*.

- Machen Sie sich mit der Netzwerktopologie des logischen Tier-0-Routers vertraut. Siehe [Logischer Tier-0 Router](#).

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Router > Hinzufügen** aus.
- 3 Wählen Sie **Tier-0-Router** im Dropdown-Menü aus.
- 4 Weisen Sie dem logischen Tier-0-Router einen Namen zu.
- 5 Wählen Sie im Dropdown-Menü einen vorhandenen NSX Edge-Cluster zur Unterstützung dieses logischen Tier-0-Routers aus.
- 6 (Optional) Wählen Sie einen Modus für die Hochverfügbarkeit aus.

Standardmäßig wird der Aktiv/Aktiv-Modus verwendet. Im Aktiv/Aktiv-Modus findet für den Datenverkehr bezüglich aller Mitglieder ein Load Balancing statt. Im Aktiv/Standby-Modus wird der gesamte Datenverkehr von einem ausgewählten aktiven Mitglied abgewickelt. Wenn das aktive Mitglied ausfällt, wird ein anderes Mitglied als aktiv ausgewählt.

- 7 (Optional) Klicken Sie auf die Registerkarte **Erweitert**, um ein Subnetz für das Transitsubnetz innerhalb von Tier 0 einzugeben.

Dabei handelt es sich um das Subnetz, das den Tier-0-Dienstrouter mit seinem verteilten Router verbindet. Wenn Sie kein Subnetz eingeben, wird das Standard-Subnetz 169.0.0.0/28 verwendet.

- 8 (Optional) Klicken Sie auf die Registerkarte **Erweitert**, um ein Subnetz für das Transitsubnetz von Tier-0-Tier-1 einzugeben.

Dabei handelt es sich um das Subnetz, das den Tier-0-Router mit allen Tier-1-Routern verbindet, für die eine Verbindung zu diesem Tier-0-Router möglich ist. Wenn Sie kein Subnetz eingeben, lautet der Adressraum, der diesen Tier-0-zu-Tier-1-Verbindungen zugewiesen ist, 100.64.0.0/16. Jede Tier-0-zu-Tier-1-Peer-Verbindung erhält ein /31-Subnetz innerhalb des 100.64.0.0/16-Adressraums.

- 9 Klicken Sie auf **Speichern**.

Der neue logische Tier-0-Router wird als Link angezeigt.

- 10 (Optional) Klicken Sie auf den Link des logischen Tier-0-Routers, um die Übersicht zu überprüfen.

## Nächste Schritte

Fügen Sie logische Tier-1-Router an diesen logischen Tier-0-Router an.

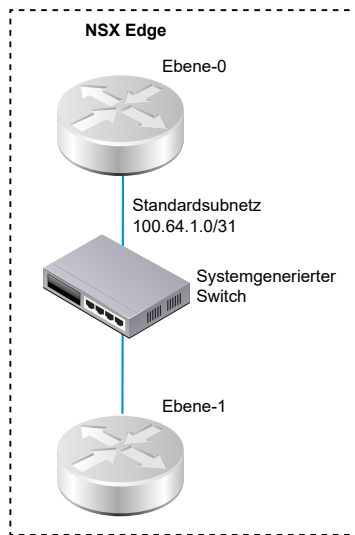
Konfigurieren Sie den logischen Tier-0-Router für dessen Verbindung mit einem logischen VLAN-Switch zum Erstellen eines Uplinks zu einem externen Netzwerk. Siehe [Verbinden eines logischen Tier-0 Routers mit einem logischen VLAN-Switch für den NSX Edge-Uplink](#).

## Anfügen von Tier-0 und Tier-1

Sie können den logischen Tier-0-Router an einen logischen Tier-1-Router anfügen, damit der logische Tier-1-Router über eine vertikale und horizontale Netzwerkkonnektivität verfügt.

Wenn Sie einen logischen Tier-1-Router an einen logischen Tier-0-Router anfügen, wird ein Router-Link-Switch zwischen den beiden Routern erstellt. Der Switch ist in der Topologie als „systemgeneriert“ gekennzeichnet. Der Standardadressraum, der diesen Tier-0-zu-Tier-1-Verbindungen zugewiesen ist, lautet 100.64.0.0/16. Jede Tier-0-zu-Tier-1-Peer-Verbindung erhält ein /31-Subnetz innerhalb des 100.64.0.0/16-Adressraums. Optional haben Sie die Möglichkeit, den Adressraum in der Tier-0-Konfiguration mit **Übersicht > Erweitert** zu konfigurieren.

Die nachfolgend dargestellte Abbildung zeigt eine Beispieltopologie.



### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.
- 3 Wählen Sie den logischen Tier-1-Router.
- 4 Klicken Sie auf der Registerkarte **Übersicht** auf **Bearbeiten**.
- 5 Wählen Sie im Dropdown-Menü den logischen Tier-0-Router aus.
- 6 (Optional) Wählen Sie einen NSX Edge-Cluster im Dropdown-Menü aus.

Der Tier-1-Router muss von einem Edge-Gerät unterstützt werden, wenn dieser für Dienste wie z. B. NAT (Network Address Translation) verwendet werden soll. Wenn Sie keinen NSX Edge-Cluster auswählen, kann der Tier-1-Router kein NAT ausführen.

- 7 Geben Sie Mitglieder und ein bevorzugtes Mitglied an.

Wenn Sie einen NSX Edge-Cluster auswählen und die Felder für die Mitglieder bzw. das bevorzugte Mitglied leer lassen, legt NSX-T Data Center das unterstützende Edge-Gerät vom angegebenen Cluster für Sie fest.

- 8 Klicken Sie auf **Speichern**.

- 9 Klicken Sie auf die Registerkarte **Konfiguration** des Tier-1-Routers, um zu prüfen, ob eine neue Punkt-zu-Punkt-IP-Adresse für den verknüpften Port erstellt wurde.

So kann die IP-Adresse des verknüpften Ports z. B. 100.64.1.1/31 lauten.

- 10 Wählen Sie aus dem Navigationsbereich den logischen Tier-0-Router aus.

- 11 Klicken Sie auf die Registerkarte **Konfiguration** des Tier-0-Routers, um zu prüfen, ob eine neue Punkt-zu-Punkt-IP-Adresse für den verknüpften Port erstellt wurde.

So kann die IP-Adresse des verknüpften Ports z. B. 100.64.1.1/31 lauten.

### Nächste Schritte

Stellen Sie sicher, dass der Tier-0-Router Informationen über Routen abrufen, die von Tier-1-Routern angekündigt werden.

## Überprüfen des Abrufs von Routen von einem Tier-1-Router für einen Tier-0-Router

Wenn ein logischer Tier-1 Router Routen für einen logischen Tier-0 Router ankündigt, werden die Routen in der Routing-Tabelle des Tier-0 Routers als statische NSX-T Data Center-Routen aufgeführt.

### Verfahren

- 1 Führen Sie den Befehl `get logical-routers` auf NSX Edge aus, um die VRF-Nummer des Tier-0-Dienstrouters abzurufen.

```
nsx-edge-1> get logical-routers
Logical Router
UUID       : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf        : 0
type       : TUNNEL

Logical Router
UUID       : 421a2d0d-f423-46f1-93a1-2f9e366176c8
vrf : 5
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : f3ce9d7d-7123-47d6-aba6-45cf1388ca7b
vrf        : 6
type       : DISTRIBUTED_ROUTER

Logical Router
```

```

UUID      : c8e64eff-02b2-4462-94ff-89f3788f1a61
vrf       : 7
type      : SERVICE_ROUTER_TIER1

```

#### Logical Router

```

UUID      : fb6c3f1f-599f-4421-af8a-99692dff3dd4
vrf       : 8
type      : DISTRIBUTED_ROUTER

```

- 2 Führen Sie den Befehl `vrf <number>` aus, um den Kontext des Tier-O-Dienstrouters einzugeben.

```

nsx-edge-1> vrf 5
nsx-edge1(tier0_sr)>

```

- 3 Führen Sie auf dem Tier-O-Dienstrouter den Befehl `get route` aus und stellen Sie sicher, dass die vorgesehenen Routen in der Routing-Tabelle enthalten sind.

Beachten Sie, dass die statischen NSX-T Data Center-Routen (ns) für den Tier-O-Router abgerufen wurden, da der Tier-1-Router Routen ankündigt.

```

nsx-edge1(tier0_sr)> get route

Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

Total number of routes: 7

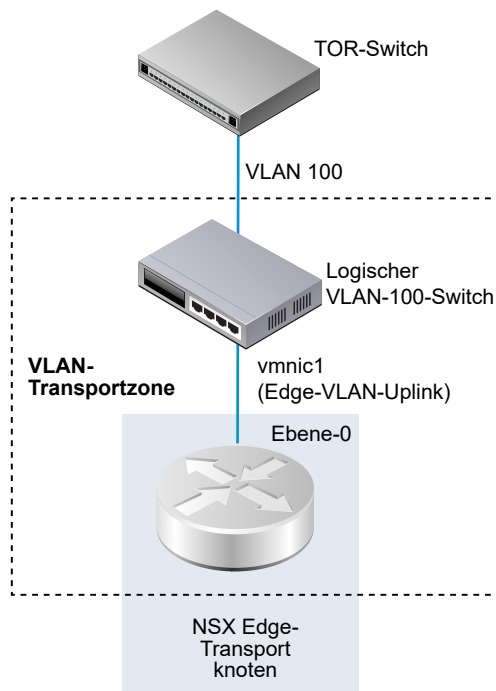
b   10.10.10.0/24      [20/0]      via 192.168.100.254
rl  100.91.176.0/31   [0/0]      via 169.254.0.1
c   169.254.0.0/28    [0/0]      via 169.254.0.2
ns  172.16.10.0/24 [3/3] über 169.254.0.1 ns 172.16.20.0/24 [3/3] über 169.254.0.1
c   192.168.100.0/24  [0/0]      via 192.168.100.2

```

## Verbinden eines logischen Tier-O Routers mit einem logischen VLAN-Switch für den NSX Edge-Uplink

Um einen NSX Edge-Uplink zu erstellen, verbinden Sie einen Tier-O-Router mit einem VLAN-Switch.

Die nachfolgend dargestellte vereinfachte Topologie enthält einen logischen VLAN-Switch innerhalb einer VLAN-Transportzone. Der logische VLAN-Switch verfügt über eine VLAN-ID, die der VLAN-ID auf dem TOR-Port für den VLAN-Uplink des Edge entspricht.



### Voraussetzungen

Erstellen Sie einen logischen VLAN-Switch. Siehe [Erstellen eines logischen VLAN-Switch für den NSX Edge-Uplink](#).

Erstellen Sie einen Tier-0-Router.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.
- 3 Wählen Sie den logischen Tier-0-Router.
- 4 Fügen Sie auf der Registerkarte **Konfiguration** einen neuen Logical Router Port hinzu.
- 5 Geben Sie einen Namen für den Port ein, z. B. „Uplink“.
- 6 Wählen Sie den Typ für den **Uplink** aus.
- 7 Wählen Sie einen Edge-Transportknoten aus.
- 8 Wählen Sie einen logischen VLAN-Switch aus.
- 9 Geben Sie eine IP-Adresse im CIDR-Format aus dem Subnetz ein, in dem sich der verbundene Port des TOR-Switch befindet.

### Ergebnisse

Ein neuer Uplink-Port wird für den Tier-0-Router hinzugefügt.

## Nächste Schritte

Konfigurieren Sie BGP oder eine statische Route.

## Überprüfen des logischen Tier-0 Routers und der TOR-Verbindung

Damit das Routing auf dem Uplink vom Tier-0-Router funktioniert, muss Konnektivität mit dem Top-of-Rack-Gerät gegeben sein.

### Voraussetzungen

- Stellen Sie sicher, dass der logische Tier-0 Router mit einem logischen VLAN-Switch verbunden ist. Siehe [Verbinden eines logischen Tier-0 Routers mit einem logischen VLAN-Switch für den NSX Edge-Uplink](#).

### Verfahren

- 1 Melden Sie sich bei der NSX Manager-Befehlszeilenschnittstelle (CLI) an.
- 2 Führen Sie den Befehl `get logical-routers` auf NSX Edge aus, um die VRF-Nummer des Tier-0-Dienstrouters abzurufen.

```
nsx-edge-1> get logical-routers
Logical Router
UUID       : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf        : 0
type       : TUNNEL

Logical Router
UUID       : 421a2d0d-f423-46f1-93a1-2f9e366176c8
vrf : 5
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : f3ce9d7d-7123-47d6-aba6-45cf1388ca7b
vrf        : 6
type       : DISTRIBUTED_ROUTER

Logical Router
UUID       : c8e64eff-02b2-4462-94ff-89f3788f1a61
vrf        : 7
type       : SERVICE_ROUTER_TIER1

Logical Router
UUID       : fb6c3f1f-599f-4421-af8a-99692dff3dd4
vrf        : 8
type       : DISTRIBUTED_ROUTER
```



- 3** Führen Sie den Befehl `vrf <number>` aus, um den Kontext des Tier-O-Dienstrouters einzugeben.

```
nsx-edge-1> vrf 5
nsx-edge1(tier0_sr)>
```

- 4** Führen Sie den Befehl `get route` auf dem Tier-O-Dienstrouter aus und stellen Sie sicher, dass die erwartete Route in der Routing-Tabelle angezeigt wird.

Beachten Sie, dass die Route zum TOR als verbunden (c) angezeigt wird.

```
nsx-edge1(tier0_sr)> get route

Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

Total number of routes: 7

b   10.10.10.0/24      [20/0]      via 192.168.100.254
rl  100.91.176.0/31    [0/0]      via 169.254.0.1
c   169.254.0.0/28     [0/0]      via 169.254.0.2
ns  172.16.10.0/24     [3/3]      via 169.254.0.1
ns  172.16.20.0/24     [3/3]      via 169.254.0.1
c  192.168.100.0/24 [0/0] via 192.168.100.2
```

- 5** Pingen Sie das TOR an.

```
nsx-edge1(tier0_sr)> ping 192.168.100.254
PING 192.168.100.254 (192.168.100.254): 56 data bytes
64 bytes from 192.168.100.254: icmp_seq=0 ttl=64 time=2.822 ms
64 bytes from 192.168.100.254: icmp_seq=1 ttl=64 time=1.393 ms
^C
nsx-edge1>
--- 192.168.100.254 ping statistics ---
3 packets transmitted, 2 packets received, 33.3% packet loss
round-trip min/avg/max/stddev = 1.393/2.107/2.822/0.715 ms
```

## Ergebnisse

Pakete werden zwischen dem logischen Tier-O Router und dem physischen Router gesendet, um die Verbindung zu prüfen.

## Nächste Schritte

Je nach Ihren Netzwerkanforderungen können Sie einen statischen Router oder BGP konfigurieren. Siehe [Konfigurieren einer statischen Route](#) oder [Konfigurieren von eBGP auf einem logischen Tier-O-Router](#).

## Hinzufügen eines Loopback-Router-Ports

Sie können einem logischen Tier-0 Router einen Loopback-Port hinzufügen.

Der Loopback-Port kann für folgende Zwecke verwendet werden:

- Router-ID für Routing-Protokolle
- NAT
- BFD
- Quelladresse für Routing-Protokolle

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.
- 3 Wählen Sie den logischen Tier-0-Router.
- 4 Wählen Sie **Konfiguration > Router-Ports** aus.
- 5 Klicken Sie auf **Hinzufügen**.
- 6 Geben Sie einen Namen und optional eine Beschreibung ein.
- 7 Wählen Sie den **Loopback**-Typ aus.
- 8 Wählen Sie einen Edge-Transportknoten aus.
- 9 Geben Sie eine IP-Adresse im CIDR-Format ein.

### Ergebnisse

Ein neuer Port wird für den Tier-0-Router hinzugefügt.

## Hinzufügen eines VLAN-Ports auf einem logischen Tier-0- oder Tier-1-Router

Wenn Sie nur über VLAN-basierte logische Switches verfügen, können Sie die Switches mit VLAN-Ports auf einem Tier-0- oder Tier-1-Router verbinden, sodass NSX-T Data Center Schicht-3-Dienste bereitstellen kann.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.
- 3 Klicken Sie auf den Namen eines Routers.
- 4 Klicken Sie auf die Registerkarte **Konfiguration** und wählen Sie **Router-Ports**.
- 5 Klicken Sie auf **Hinzufügen**.

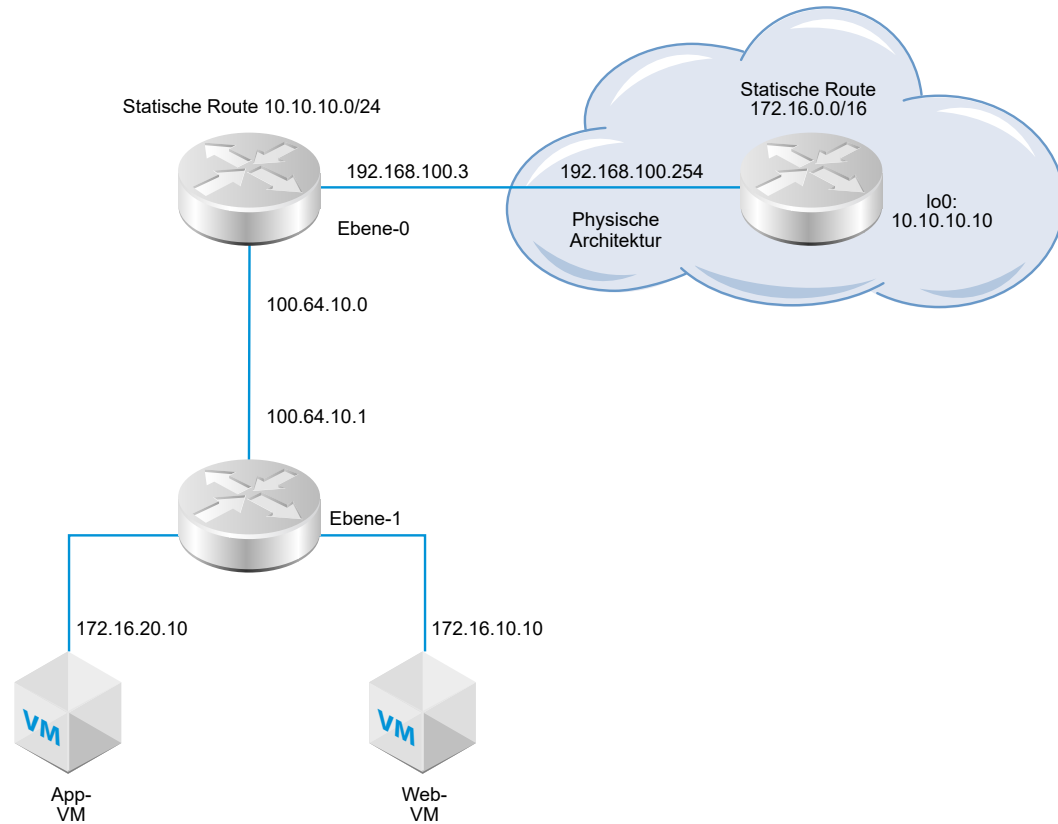
- 6** Geben Sie für den Router-Port einen Namen und optional eine Beschreibung ein.
- 7** Wählen Sie im Feld **Typ** die Option **Zentral** aus.
- 8** Wählen Sie als **URPF-Modus** entweder **Streng** oder **Keine** aus.  
URPF (Unicast Reverse Path Forwarding) ist eine Sicherheitsfunktion.
- 9** (Erforderlich) Wählen Sie einen logischen Switch aus.
- 10** Wählen Sie aus, ob diese Anfügung einen neuen Switch-Port erstellt oder einen vorhandenen Switch-Port aktualisiert.  
Bezieht sich die Anfügung auf einen vorhandenen Switch-Port, wählen Sie den betreffenden Port im Dropdown-Menü aus.
- 11** Geben Sie die IP-Adresse des Routerports in CIDR-Notation ein.
- 12** Klicken Sie auf **Hinzufügen**.

## Konfigurieren einer statischen Route

Sie können eine statische Route auf einem Tier-0-Router für externe Netzwerken konfigurieren. Nach der Konfiguration einer statischen Route müssen Sie die Route nicht von Tier-0 zu Tier-1 ankündigen, da Tier-1-Router automatisch über eine statische Standardroute in Richtung auf ihren verbundenen Tier-0-Router verfügen.

Die Topologie der statischen Route enthält einen logischen Tier-0 Router mit einer statischen Route zum 10.10.10.0/24-Präfix in der physischen Architektur. Für Testzwecke ist die Adresse 10.10.10.10/32 für die Loopback-Schnittstelle des externen Routers konfiguriert. Der externe Router verfügt über eine statische Route zum 172.16.0.0/16-Präfix, um die Anwendungs- und Web-VMs erreichen zu können.

Abbildung 14-4. Topologie der statischen Route



Rekursive statische Routen werden unterstützt.

#### Voraussetzungen

- Stellen Sie sicher, dass der physische Router und der logische Tier-0 Router verbunden sind. Siehe [Überprüfen des logischen Tier-0 Routers und der TOR-Verbindung](#).
- Stellen Sie sicher, dass der Tier-1-Router für die Ankündigung verbundener Routen konfiguriert ist. Siehe [Erstellen eines logischen Tier-1-Routers](#).

#### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.
- 3 Wählen Sie den logischen Tier-0-Router.
- 4 Klicken Sie auf die Registerkarte **Routing** und wählen Sie **Statische Route** im Dropdown-Menü aus.
- 5 Wählen Sie **Hinzufügen** aus.
- 6 Geben Sie eine Netzwerkadresse im CIDR-Format ein.  
Beispiel: 10.10.10.0/24.

- 7 Klicken Sie auf **+ Hinzufügen**, um eine IP-Adresse für den nächsten Hop hinzuzufügen.

Beispiel: 192.168.100.254. Sie können auch eine Null-Route angeben, indem Sie auf das Bleistiftsymbol klicken und in der Dropdown-Liste **NULL** auswählen.

- 8 Geben Sie die administrative Distanz an.
- 9 Wählen Sie in der Dropdown-Liste einen Logical Router Port aus.

Die Liste enthält mit IPSec gesicherte Virtual Tunnel Interface-Ports (VTI-Ports).

- 10 Klicken Sie auf die Schaltfläche **Hinzufügen**.

#### Nächste Schritte

Prüfen Sie, ob die statische Route korrekt konfiguriert ist. Siehe [Überprüfen der statischen Route](#).

### Überprüfen der statischen Route

Mit der Befehlszeilenschnittstelle (CLI) können Sie überprüfen, ob die statische Route verbunden ist. Sie müssen auch überprüfen, ob der externe Router einen Ping-Befehl an die internen VMs senden kann und ob die internen VMs einen Ping-Befehl an den externen Router senden können.

#### Voraussetzungen

Stellen Sie sicher, dass eine statische Route konfiguriert ist. Siehe [Konfigurieren einer statischen Route](#).

#### Verfahren

- 1 Melden Sie sich bei der NSX Manager-Befehlszeilenschnittstelle (CLI) an.

**2** Bestätigen Sie die statische Route.

- a Rufen Sie die UUID-Informationen des Dienstrouters ab.

```
get logical-routers
```

```
nsx-edge1> get logical-routers
Logical Router
UUID       : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf        : 2
type       : TUNNEL

Logical Router
UUID       : d40bbfa4-3e3d-4178-8615-6f42ea335037
vrf        : 4
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : d0289ba4-250e-41b4-8ffc-7cab4a46c3e4
vrf        : 5
type       : DISTRIBUTED_ROUTER

Logical Router
UUID       : a6ee6316-2212-4171-99cc-930c98bcad7f
vrf        : 6
type       : DISTRIBUTED_ROUTER
```

- b Suchen Sie die UUID-Informationen in der Ausgabe.

```
Logical Router
UUID       : d40bbfa4-3e3d-4178-8615-6f42ea335037
vrf        : 4
type       : SERVICE_ROUTER_TIER0
```

- c Stellen Sie sicher, dass die statische Route funktioniert.

```
get logical-router d40bbfa4-3e3d-4178-8615-6f42ea335037 route static
```

```
Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

s    10.10.10.0/24      [1/1]      via 192.168.100.254
rl   100.64.1.0/31      [0/0]      via 169.0.0.1
ns   172.16.10.0/24     [3/3]      via 169.0.0.1
ns   172.16.20.0/24     [3/3]      via 169.0.0.1
```

- 3** Senden Sie vom externen Router einen Ping-Befehl an die internen VMs, um sicherzustellen, dass diese über den NSX-T Data Center-Overlay erreichbar sind.

- a Stellen Sie eine Verbindung mit dem externen Router her.

```
ping 172.16.10.10
```

```
PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
64 bytes from 172.16.10.10: icmp_req=1 ttl=62 time=127 ms
64 bytes from 172.16.10.10: icmp_req=2 ttl=62 time=1.96 ms
^C
--- 172.16.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.966/64.793/127.620/62.827 ms
```

- b Testen Sie die Netzwerkkonnektivität.

```
tracert 172.16.10.10
```

```
tracert to 172.16.10.10 (172.16.10.10), 30 hops max, 60 byte packets
 1  192.168.100.3 (192.168.100.3)  0.640 ms  0.575 ms  0.696 ms
 2  100.64.1.1 (100.64.1.1)  0.656 ms  0.604 ms  0.578 ms
 3  172.16.10.10 (172.16.10.10)  3.397 ms  3.703 ms  3.790 ms
```

- 4** Senden Sie von den VMs einen Ping-Befehl an die externe IP-Adresse.

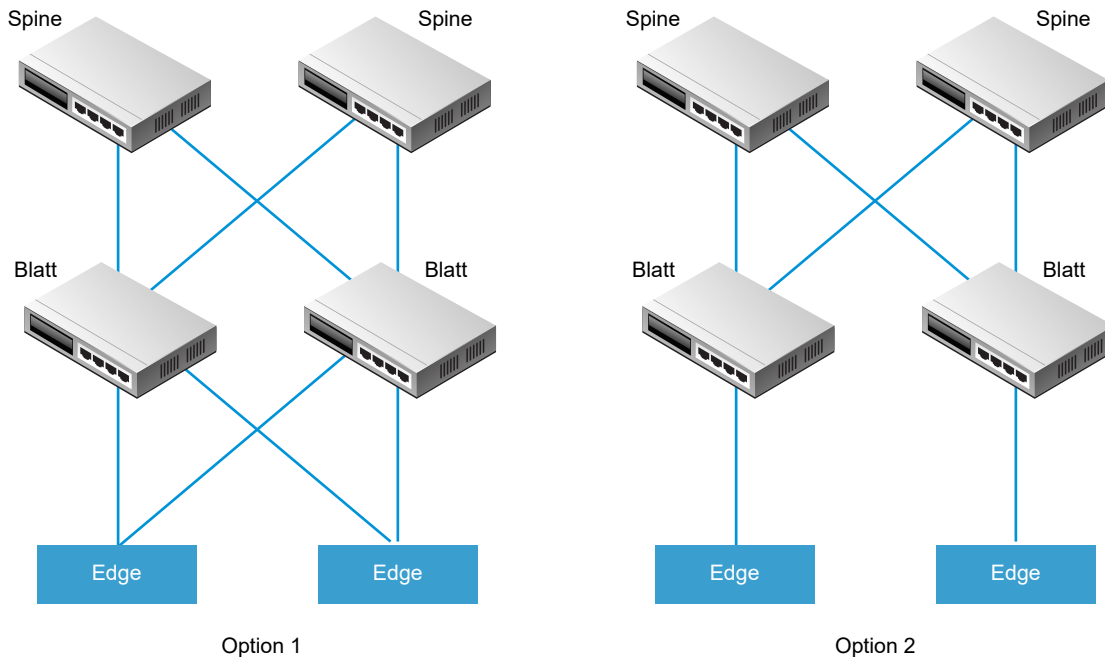
```
ping 10.10.10.10
```

```
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_req=1 ttl=62 time=119 ms
64 bytes from 10.10.10.10: icmp_req=2 ttl=62 time=1.93 ms
^C
--- 10.10.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.936/60.865/119.795/58.930 ms
```

## BGP-Konfigurationsoptionen

Um den logischen Tier-0 Router maximal nutzen zu können, muss die Topologie mit Redundanz und Symmetrie sowie mit BGP zwischen den Tier-0 Routern und den externen Top-of-Rack (TOR)-Peers konfiguriert werden. Mit diesem Design lässt sich die Konnektivität im Falle von Link- und Knotenfehlern aufrechterhalten.

Es sind zwei Arten der Konfiguration verfügbar: Aktiv/Aktiv und Aktiv-Standby. Das nachfolgend dargestellte Diagramm zeigt zwei Optionen für eine symmetrische Konfiguration. In jeder Topologie werden zwei NSX Edge-Knoten dargestellt. Wenn Sie im Falle einer Aktiv/Aktiv-Konfiguration Tier-0-Uplink-Ports erstellen, können Sie jedem Uplink-Port bis zu acht NSX Edge-Transportknoten zuweisen. Jeder NSX Edge-Knoten kann über zwei Uplinks verfügen.



Für die Option 1 muss, wenn die physischen Blattknoten-Router konfiguriert sind, eine BGP-Nachbarschaft mit den NSX Edges vorhanden sein. Die Route Redistribution muss die gleichen Netzwerkpräfixe mit identischen BGP-Metriken für alle BGP-Nachbarn enthalten. In der Konfiguration des logischen Tier-0 Routers müssen alle Blattknoten-Router als BGP-Nachbarn konfiguriert sein.

Wenn Sie bei der Konfiguration der BGP-Nachbarn des Tier-0 Routers keine lokale Adresse (die Quell-IP-Adresse) angeben, wird die Konfiguration der BGP-Nachbarn an alle NSX Edge-Knoten gesendet, die den Uplinks des logischen Tier-0 Routers zugeordnet sind. Wenn Sie aber eine lokale Adresse konfigurieren, wird die Konfiguration dem NSX Edge-Knoten mit dem Uplink übermittelt, der diese IP-Adresse besitzt.

Bei Option 1 ist es sinnvoll, auf die lokale Adresse zu verzichten, wenn sich die Uplinks auf den NSX Edge-Knoten im selben Subnetz befinden. Wenn sich die Uplinks auf den NSX Edge-Knoten in unterschiedlichen Subnetzen befinden, muss die lokale Adresse in der Konfiguration des BGP-Nachbarn des Tier-0-Routers angegeben werden. Damit wird verhindert, dass die Konfiguration für alle zugeordneten NSX Edge-Knoten aktiviert wird.

Für die Option 2 müssen Sie sicherstellen, dass die Konfiguration für den logischen Tier-0 Router die lokale IP-Adresse des Tier-0-Dienstrouters enthält. Die Blattknoten-Router werden nur mit den NSX Edges konfiguriert, mit denen sie direkt als BGP-Nachbar verbunden sind.



## Konfigurieren von eBGP auf einem logischen Tier-0-Router

Um den Zugriff zwischen Ihren VMs und der Außenwelt zu ermöglichen, können Sie eine externe oder interne BGP-Verbindung (eBGP/iBGP) zwischen einem logischen Tier-0-Router und einem Router in Ihrer physischen Infrastruktur konfigurieren.

Wenn Sie eBGP konfigurieren, müssen Sie eine lokale AS-Nummer des autonomen Systems für den logischen Tier-0-Router konfigurieren. Beispielsweise ist in der im Folgenden dargestellten Topologie die lokale AS-Nummer 64510 enthalten. Sie müssen auch die Remote-AS-Nummer des physischen Routers konfigurieren. In diesem Beispiel lautet die Remote-AS-Nummer 64511. Die Remote-Nachbar-IP-Adresse ist 192.168.100.254. Der Nachbar muss sich im selben IP-Subnetz wie der Uplink auf dem logischen Tier-0-Router befinden. BGP-Multi-Hop wird unterstützt.

Für Testzwecke ist die Adresse 10.10.10.10/32 für die Loopback-Schnittstelle des externen Routers konfiguriert.

Ein logischer Tier-0-Router im Aktiv/Aktiv-Modus unterstützt Routing zwischen verschiedenen Service-Routern (Inter-SR Routing). Wenn Router Nr. 1 nicht in der Lage ist, mit einem vertikalen physischen Router zu kommunizieren, wird der Datenverkehr im Aktiv/Aktiv-Cluster an Router Nr. 2 umgeleitet. Kann Router Nr. 2 nicht mit dem physischen Router kommunizieren, ist der Datenverkehr zwischen Router Nr. 1 und dem physischen Router nicht betroffen.

In einer Topologie mit einem logischen Tier-0-Router im Aktiv/Aktiv-Modus, der an einen logischen Tier-1-Router im Aktiv/Standby-Modus angehängt ist, müssen Sie Inter-SR-Routing aktivieren, um das asymmetrische Routing zu verarbeiten. Sie haben asymmetrisches Routing, wenn Sie eine statische Route auf einem der SR konfigurieren oder wenn ein SR den Uplink eines anderen SR erreichen muss. Beachten Sie außerdem Folgendes:

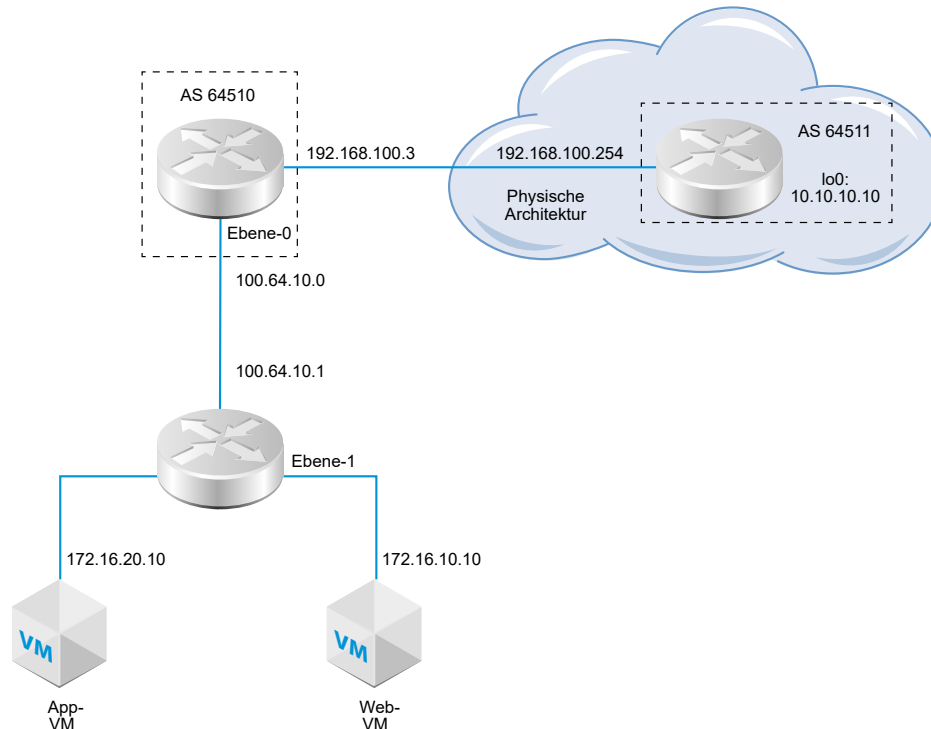
- Im Falle einer statischen Route, die auf einem SR konfiguriert ist (z. B. SR 1 auf Edge-Knoten 1), kann ein anderer SR (z. B. SR 2 auf Edge-Knoten 2) dieselbe Route von einem eBGP-Peer erlernen und die erlernte Route vor der statischen Route auf SR 1 bevorzugen, was möglicherweise effizienter ist. Um sicherzustellen, dass SR 2 die auf SR 1 konfigurierte statische Route verwendet, konfigurieren Sie den logischen Tier-1-Router im präventiven Modus und konfigurieren Sie den Edge-Knoten 1 als bevorzugten Knoten.
- Wenn der logische Tier-0-Router über einen Uplink-Port auf dem Edge-Knoten 1 und einem anderen Uplink-Port auf dem Edge-Knoten 2 verfügt, funktioniert der Ping-Datenverkehr von Mandanten-VMs zu den Uplinks, wenn sich die beiden Uplinks in unterschiedlichen Subnetzen befinden. Ping-Datenverkehr schlägt fehl, wenn sich die beiden Uplinks im selben Subnetz befinden.

---

**Hinweis** Die für die Bildung von BGP-Sitzungen auf einem Edge-Knoten verwendete Router-ID wird automatisch aus den IP-Adressen ausgewählt, die auf den Uplinks eines logischen Tier-0-Routers konfiguriert wurden. BGP-Sitzungen auf einem Edge-Knoten können fehlschlagen, wenn sich die Router-ID ändert. Dies ist der Fall, wenn die für die Router-ID automatisch ausgewählte IP-Adresse oder der Port eines logischen Routers, auf dem diese IP zugewiesen wurde, gelöscht wird.

---

Abbildung 14-5. BGP-Verbindungsstopologie



Beachten Sie die folgenden Szenarien, wenn Verbindungsfehler bezüglich BGP oder BFD vorliegen:

- Wenn nur BGP konfiguriert ist und alle BGP-Nachbarn ausfallen, ist der Status des Dienstrouters inaktiv.
- Wenn nur BFD konfiguriert ist und alle BFD-Nachbarn ausfallen, ist der Status des Dienstrouters inaktiv.
- Wenn BGP und BFD konfiguriert sind und alle BGP- und BFD-Nachbarn ausfallen, ist der Status des Dienstrouters inaktiv.
- Wenn BGP und statische Routen konfiguriert sind und alle BGP-Nachbarn ausfallen, ist der Status des Dienstrouters inaktiv.
- Wenn nur statische Routen konfiguriert sind, ist der Status des Dienstrouters immer aktiv, es sei denn, der Knoten weist einen Fehler auf oder befindet sich im Wartungsmodus.

#### Voraussetzungen

- Stellen Sie sicher, dass der Tier-1-Router für die Ankündigung verbundener Routen konfiguriert ist. Siehe [Konfigurieren von Routen-Advertisement auf einem logischen Tier-1 Router](#). Dies ist für eine BGP-Konfiguration nicht zwingend notwendig. Wenn Sie aber über eine Zwei-Tier-Topologie verfügen und Ihre Tier-1-Netzwerke in BGP neu verteilen möchten, ist dieser Schritt erforderlich.

- Stellen Sie sicher, dass ein Tier-0-Router konfiguriert ist. Siehe [Erstellen eines logischen Tier-0-Routers](#).
- Stellen Sie sicher, dass der logische Tier-0-Router die Informationen über Routen vom logischen Tier-1-Router abgerufen hat. Siehe [Überprüfen des Abrufs von Routen von einem Tier-1-Router für einen Tier-0-Router](#).

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.
- 3 Wählen Sie den logischen Tier-0-Router.
- 4 Klicken Sie auf die Registerkarte **Routing**, und wählen Sie **BGP** im Dropdown-Menü aus.
- 5 Klicken Sie auf **Bearbeiten**.
  - a Geben Sie die lokale AS-Nummer ein.  
Beispiel: 64510.
  - b Mit einem Klick auf den Schalter **Status** können Sie BGP aktivieren bzw. deaktivieren.
  - c Klicken Sie auf den Schalter **ECMP**, um ECMP zu aktivieren bzw. zu deaktivieren.
  - d Klicken Sie auf die Umschaltfläche **Graceful Restart**, um den Graceful Restart zu aktivieren oder zu deaktivieren.  
  
Graceful Restart wird nur unterstützt, wenn der dem Tier-0-Router zugeordnete NSX Edge-Cluster nur über einen Edge-Knoten verfügt.
  - e Wenn sich dieser logische Router im Aktiv/Aktiv-Modus befindet, klicken Sie auf den Schalter **Inter-SR-Routing**, um das Routing zwischen Service-Routern zu aktivieren bzw. zu deaktivieren.
  - f Konfigurieren Sie die Routenaggregation.
  - g Klicken Sie auf **Speichern**.
- 6 Klicken Sie auf **Hinzufügen**, um einen BGP-Nachbarn hinzuzufügen.
- 7 Geben Sie die IP-Adresse des Nachbarn ein.  
Beispiel: 192.168.100.254.
- 8 Geben Sie das maximale Hop-Limit an.  
Die Standardeinstellung ist 1.
- 9 Geben Sie die Remote-AS-Nummer ein.  
Beispiel: 64511.
- 10 Konfigurieren Sie die Timer (Keepalive-Timer und Hold-Down-Timer) und ein Kennwort.

- 11 Klicken Sie auf die Registerkarte **Lokale Adresse**, um eine lokale Adresse auszuwählen.
  - a (Optional) Deaktivieren Sie **Alle Uplinks**, um sowohl Loopback-Ports als auch Uplink-Ports anzuzeigen.
- 12 Klicken Sie auf die Registerkarte **Adressfamilien**, um eine Adressfamilie hinzuzufügen.
- 13 Klicken Sie auf die Registerkarte **BFD-Konfiguration**, um BFD zu aktivieren.
- 14 Klicken Sie auf **Speichern**.

#### Nächste Schritte

Überprüfen Sie, ob BGP korrekt funktioniert. Siehe [Überprüfen von BGP-Verbindungen von einem Tier-O-Dienstrouter aus](#).

## Konfigurieren von iBGP auf einem logischen Tier-O-Router

Sie können internes BGP (iBGP) für logische Tier-O Router über die API konfigurieren. Wenn iBGP konfiguriert ist, können die logischen Tier-O-Router Routing- und Erreichbarkeitsinformationen austauschen.

Für diese iBGP-Funktion gelten folgende Möglichkeiten und Einschränkungen:

- Umverteilung, Präfixlisten und Route Maps werden unterstützt.
- Routenreflektoren werden nicht unterstützt.
- BGP-Verbund wird nicht unterstützt.

Die Konfiguration von iBGP mithilfe der NSX Manager-Benutzeroberfläche wird in dieser Version nicht unterstützt.

#### Verfahren

- 1 Rufen Sie die folgende API auf, um einen BGP-Nachbarn mit dem `remote_as`-Parameter hinzuzufügen, der auf den gleichen Wert wie das lokale AS gesetzt ist. Beispiel:

```
POST https://<nsx-mgr>/api/v1/logical-routers/7a62a0c5-1ea1-4b25-9d43-dce1c0fa4b8c/routing/bgp/neighbors
{
  "display_name": "neighbor1",
  "neighbor_address": "2.2.2.2",
  "remote_as_num": "200",
  "maximum_hop_limit": 1,
  "enabled": true,
  "logical_router_id": "c831795d-dc7b-448c-92ce-21b16ec9a7ad",
  "address_families": [
    {
      "type": "IPv4_UNICAST",
      "enabled": true,
    }
  ]
}
```

```

],
"remote_as": 200,
"enable_bfd": false,
}

```

- 2** Rufen Sie die folgende API auf, um eine Route Map hinzuzufügen, bei der der Parameter `nexthop_self` auf **true** und der Parameter `local_preference` auf „200“ festgelegt ist. Beispiel:

```

POST https://<nsx-mgr>/api/v1/logical-routers/7a62a0c5-1ea1-4b25-9d43-dce1c0fa4b8c/routing/route-
maps
{
  "description": "Route Map",
  "display_name": "Route Map",
  "logical_router_id": "c831795d-dc7b-448c-92ce-21b16ec9a7ad",
  "sequences": [
    {
      "match_criteria": {
        "match_community_expression": {
          "expression": [
            {
              "match_operator": "MATCH_ALL",
              "community_list_id": "c4b2b171-661b-4059-960c-fc931a612507"
            }
          ],
          "operator": "AND"
        }
      },
      "set_criteria": {
        "as_path_prepend" : "50",
        "weight" : 50,
        "community" : "30:40",
        "multi_exit_discriminator" : 10,
        "nexthop_self" : true,
        "local_preference" : 200
      },
      "action": "PERMIT"
    }
  ]
}

```

## Überprüfen von BGP-Verbindungen von einem Tier-0-Dienstrouter aus

Mit der Befehlszeilenschnittstelle (CLI) können Sie vom Tier-0-Dienstrouter aus überprüfen, ob eine BGP-Verbindung mit einem Nachbarn eingerichtet ist.

### Voraussetzungen

Stellen Sie sicher, dass BGP konfiguriert ist. Siehe [Konfigurieren von eBGP auf einem logischen Tier-0-Router](#).

### Verfahren

- 1** Melden Sie sich bei der NSX Manager-Befehlszeilenschnittstelle (CLI) an.

- 2** Führen Sie den Befehl `get logical-routers` auf NSX Edge aus, um die VRF-Nummer des Tier-O-Dienstrouters abzurufen.

```

nsx-edge-1> get logical-routers
Logical Router
UUID       : 736a80e3-23f6-5a2d-81d6-bbafb2786666
vrf        : 0
type       : TUNNEL

Logical Router
UUID       : 421a2d0d-f423-46f1-93a1-2f9e366176c8
vrf : 5
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : f3ce9d7d-7123-47d6-aba6-45cf1388ca7b
vrf        : 6
type       : DISTRIBUTED_ROUTER

Logical Router
UUID       : c8e64eff-02b2-4462-94ff-89f3788f1a61
vrf        : 7
type       : SERVICE_ROUTER_TIER1

Logical Router
UUID       : fb6c3f1f-599f-4421-af8a-99692dff3dd4
vrf        : 8
type       : DISTRIBUTED_ROUTER

```

- 3** Führen Sie den Befehl `vrf <number>` aus, um den Kontext des Tier-O-Dienstrouters einzugeben.

```

nsx-edge-1> vrf 5
nsx-edge1(tier0_sr)>

```

- 4** Stellen Sie sicher, dass für den BGP-Zustand Eingerichtet, aktiviert gültig ist.

`get bgp neighbor`

```

BGP neighbor: 192.168.100.254   Remote AS: 64511
BGP state: Established, up
Hold Time: 180s   Keepalive Interval: 60s
Capabilities:
    Route Refresh: advertised and received
    Address Family: IPv4 Unicast:advertised and received
    Graceful Restart: none
    Restart Remaining Time: 0
Messages: 28 received, 31 sent
Minimum time between advertisements: 30s (default)
For Address Family IPv4 Unicast:advertised and received

```

```

Route Refresh: 0 received, 0 sent
Prefixes: 2 received, 2 sent, 2 advertised
1 Connections established, 2 dropped
Local host: 192.168.100.3, Local port: 179
Remote host: 192.168.100.254, Remote port: 33044

```

### Nächste Schritte

Überprüfen Sie die BGP-Verbindung vom externen Router aus. Siehe [Überprüfen der Nord-Süd-Konnektivität und Route Redistribution](#).

## Konfigurieren von BFD auf einem logischen Tier-0 Router

BFD (Bidirectional Forwarding Detection, Bidirektionale Weiterleitungserkennung) ist ein Protokoll zur Erkennung von Fehlern bei Weiterleitungspfaden.

---

**Hinweis** In dieser Version wird BFD über VTI-Ports (Virtual Tunnel Interface) nicht unterstützt.

---

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.
- 3 Wählen Sie den logischen Tier-0-Router.
- 4 Klicken Sie auf die Registerkarte **Routing** und wählen Sie **BFD** im Dropdown-Menü aus.
- 5 Klicken Sie auf **Bearbeiten** zur Konfiguration von BFD.
- 6 Klicken Sie auf die Umschaltfläche **Status**, um BFD zu aktivieren.  
 Sie können optional auch die globalen BFD-Eigenschaften **Receive interval** (Intervall empfangen), **Transmit interval** (Intervall übertragen) und **Declare dead interval** (Ausfallintervall deklarieren) ändern.
- 7 (Optional) Klicken Sie auf **Hinzufügen** unter „BFD-Peers für die nächsten Hops der statischen Route“, um einen BFD-Peer hinzuzufügen.  
 Geben Sie die Peer-IP-Adresse an und legen Sie für den administrativen Status **Aktiviert** fest. Sie können optional auch die globalen BFD-Eigenschaften **Receive interval** (Intervall empfangen), **Transmit interval** (Intervall übertragen) und **Declare dead interval** (Ausfallintervall deklarieren) überschreiben.

## Aktivieren von Route Redistribution auf dem logischen Tier-0 Router

Wenn Sie die Route Redistribution aktivieren, beginnt der logische Tier-0 Router damit, angegebene Routen mit seinem Northbound-Router zu teilen.

## Voraussetzungen

- Stellen Sie sicher, dass der logische Tier-0- und der Tier-1 Router verbunden sind, damit Sie die Netzwerke des logischen Tier-1 Routers ankündigen können, um sie auf dem logischen Tier-0 Router neu zu verteilen. Siehe [Anfügen von Tier-0 und Tier-1](#).
- Wenn Sie bestimmte IP-Adressen aus der Route Redistribution herausfiltern möchten, müssen Routenzuordnungen konfiguriert sein. Siehe [Erstellen einer Route Map](#).

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.
- 3 Wählen Sie den logischen Tier-0-Router.
- 4 Klicken Sie auf die Registerkarte **Routing** und wählen Sie **Route Redistribution** im Dropdown-Menü aus.
- 5 Klicken Sie auf **Bearbeiten**, um Route Redistribution zu aktivieren oder zu deaktivieren.
- 6 Klicken Sie auf **Hinzufügen**, um einen Satz von Route Redistribution-Kriterien hinzuzufügen.

Option	Beschreibung
<b>Name und Beschreibung</b>	Weisen Sie der Route Redistribution einen Namen zu. Sie können optional auch eine Beschreibung bereitstellen. Beispielname: advertise-to-bgp-neighbor
<b>Quellen</b>	Wählen Sie mindestens eine der folgenden Quellen aus: <ul style="list-style-type: none"> <li>■ <b>T0 Verbunden</b></li> <li>■ <b>T0 Uplink</b></li> <li>■ <b>T0 Downlink</b></li> <li>■ <b>T0 CSP</b></li> <li>■ <b>T0 Loopback</b></li> <li>■ <b>T0 Statisch</b></li> <li>■ <b>T0 NAT</b></li> <li>■ <b>T0 DNS-Weiterleitungs-IP</b></li> <li>■ <b>T0 Lokale IPSec-IP</b></li> <li>■ <b>T1 Verbunden</b></li> <li>■ <b>T1 CSP</b></li> <li>■ <b>T1 Downlink</b></li> <li>■ <b>T1 Statisch</b></li> <li>■ <b>T1 LB-SNAT</b></li> <li>■ <b>T1 NAT</b></li> <li>■ <b>T1 LB-VIP</b></li> <li>■ <b>T1 DNS-Weiterleitungs-IP</b></li> </ul>
<b>Routenzuordnung</b>	(Optional) Weisen Sie eine Route Map zu, um eine Reihe von IP-Adressen von der Route Redistribution herauszufiltern.



## Überprüfen der Nord-Süd-Konnektivität und Route Redistribution

Prüfen Sie anhand der CLI, ob die BGP-Routen abgerufen wurden. Sie können außerdem über den externen Router prüfen, ob die mit NSX-T Data Center verbundenen VMs erreichbar sind.

### Voraussetzungen

- Stellen Sie sicher, dass BGP konfiguriert ist. Siehe [Konfigurieren von eBGP auf einem logischen Tier-O-Router](#).
- Stellen Sie sicher, dass statische NSX-T Data Center-Routen für die Neuverteilung festgelegt sind. Siehe [Aktivieren von Route Redistribution auf dem logischen Tier-O Router](#).

### Verfahren

- 1 Melden Sie sich bei der NSX Manager-Befehlszeilenschnittstelle (CLI) an.
- 2 Zeigen Sie die Routen an, die vom externen BGP-Nachbarn abgerufen wurden.

```
nsx-edge1(tier0_sr)> get route bgp

Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

b    10.10.10.0/24      [20/0]      via 192.168.100.254
```

- 3** Prüfen Sie über den externen Router, ob BGP-Routen abgerufen wurden und ob die VMs über das NSX-T Data Center-Overlay erreichbar sind.

- a Listen Sie die BGP-Routen auf.

```
user@router# run show ip route bgp
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

B>* 172.16.10.0/24 [20/0] via 192.168.100.2, eth2, 00:00:48
B>* 172.16.20.0/24 [20/0] via 192.168.100.2, eth2, 00:00:48
B>* 172.16.30.0/24 [20/0] via 192.168.100.2, eth2, 00:00:48
```

- b Pingen Sie die mit NSX-T Data Center verbundenen VMs über den externen Router an.  
ping 172.16.10.10

```
PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
64 bytes from 172.16.10.10: icmp_req=1 ttl=62 time=127 ms
64 bytes from 172.16.10.10: icmp_req=2 ttl=62 time=1.96 ms
^C
--- 172.16.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.966/64.793/127.620/62.827 ms
```

- c Prüfen Sie den Pfad über das NSX-T Data Center-Overlay.  
traceroute 172.16.10.10

```
traceroute to 172.16.10.10 (172.16.10.10), 30 hops max, 60 byte packets
 1 192.168.100.3 (192.168.100.3) 0.640 ms 0.575 ms 0.696 ms
 2 100.91.176.1 (100.91.176.1) 0.656 ms 0.604 ms 0.578 ms
 3 172.16.10.10 (172.16.10.10) 3.397 ms 3.703 ms 3.790 ms
```

- 4** Pingen Sie die externe IP-Adresse über die internen VMs an.  
ping 10.10.10.10

```
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_req=1 ttl=62 time=119 ms
64 bytes from 10.10.10.10: icmp_req=2 ttl=62 time=1.93 ms
^C
--- 10.10.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.936/60.865/119.795/58.930 ms
```

## Nächste Schritte

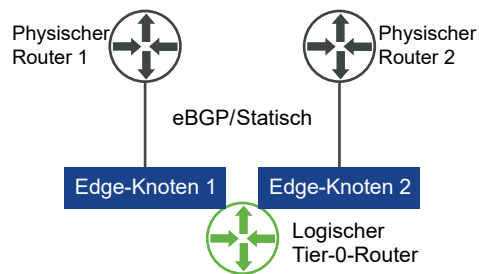
Konfigurieren Sie weitere Routing-Funktionen, wie ECMP.

## Grundlegendes zum ECMP-Routing

Das ECMP-Routing-Protokoll (Equal Cost Multi-Path) erhöht die Bandbreite für die vertikale Kommunikation durch Hinzufügen eines Uplinks zum logischen Tier-0-Router und konfiguriert diesen für jeden Edge-Knoten in einem NSX Edge-Cluster. Die ECMP-Routing-Pfade werden für das Load Balancing des Datenverkehrs verwendet und bieten eine Fault Tolerance für fehlgeschlagene Pfade.

Der logische Tier-0-Router muss sich im Aktiv/Aktiv-Modus befinden, damit ECMP verfügbar ist. Es werden maximal acht ECMP-Pfade unterstützt.

Abbildung 14-6. ECMP-Routing-Topologie



Beispielsweise zeigt die obige Topologie einen einzelnen logischen Tier-0-Router im Aktiv/Aktiv-Modus an, der in einem NSX Edge-Cluster mit zwei Knoten ausgeführt wird. Zwei Uplink-Ports werden konfiguriert, einer auf jedem Edge-Knoten.

### Hinzufügen eines Uplink-Ports für den zweiten Edge-Knoten

Bevor Sie ECMP aktivieren, müssen Sie einen Uplink konfigurieren, um den logischen Tier-0 Router mit dem logischen VLAN-Switch zu verbinden.

#### Voraussetzungen

- Stellen Sie sicher, dass eine Transportzone und zwei Transportknoten konfiguriert sind. Siehe *Installationshandbuch für NSX-T Data Center*.
- Stellen Sie sicher, dass zwei Edge-Knoten und ein Edge-Cluster konfiguriert sind. Siehe *Installationshandbuch für NSX-T Data Center*.
- Stellen Sie sicher, dass ein logischer VLAN-Switch für den Uplink verfügbar ist. Siehe [Erstellen eines logischen VLAN-Switch für den NSX Edge-Uplink](#).
- Stellen Sie sicher, dass ein logischer Tier-0 Router konfiguriert ist. Siehe [Erstellen eines logischen Tier-0-Routers](#).

#### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.

- 3 Wählen Sie den logischen Tier-O-Router.
- 4 Klicken Sie auf die Registerkarte **Konfiguration**, um einen Router-Port hinzuzufügen.
- 5 Klicken Sie auf **Hinzufügen**.
- 6 Geben Sie die Details für den Router-Port an.

Option	Beschreibung
<b>Name</b>	Weisen Sie dem Router-Port einen Namen zu.
<b>Beschreibung</b>	Geben Sie eine zusätzliche Beschreibung ein, dass der Port der ECMP-Konfiguration dient.
<b>Typ</b>	Übernehmen Sie den Standardtyp <b>Uplink</b> .
<b>MTU</b>	Wenn Sie dieses Feld leer lassen, lautet der Standardwert 1500.
<b>Transportknoten</b>	Weisen Sie den Edge-Transportknoten im Dropdown-Menü zu.
<b>URPF-Modus</b>	„Unicast Reverse Path Forwarding“ ist eine Sicherheitsfunktion. Die Einstellung <b>Keine</b> wird empfohlen, wenn Sie über mehrere Edge-Knoten mit einer Aktiv/Aktiv-Konfiguration im ECMP-Modus verfügen. Der Standardwert lautet <b>Streng</b> .
<b>Logischer Switch</b>	Weisen Sie den logischen VLAN-Switch im Dropdown-Menü zu.
<b>Logischer Switch Port</b>	Weisen Sie einen neuen Namen für den Switch-Port zu. Sie können auch einen vorhandenen Switch-Port verwenden.
<b>IP-Adresse/-Maske</b>	Geben Sie eine IP-Adresse aus dem Subnetz ein, in dem sich der verbundene Port des TOR-Switch befindet.

- 7 Klicken Sie auf **Speichern**.

## Ergebnisse

Es wird dem Tier-O-Router und dem logischen VLAN-Switch ein neuer Uplink-Port hinzugefügt. Der logische Tier-O Router wird für beide Edge-Knoten konfiguriert.

## Nächste Schritte

Erstellen Sie eine BGP-Verbindung für den zweiten Nachbarn und aktivieren Sie das ECMP-Routing. Siehe [Hinzufügen eines zweiten BGP-Nachbarn und Aktivieren des ECMP-Routings](#).

## Hinzufügen eines zweiten BGP-Nachbarn und Aktivieren des ECMP-Routings

Bevor Sie das ECMP-Routing aktivieren, müssen Sie einen BGP-Nachbarn hinzufügen und mit den Informationen des neu hinzugefügten Uplink konfigurieren.

## Voraussetzungen

Stellen Sie sicher, dass der zweite Edge-Knoten über einen konfigurierten Uplink-Port verfügt. Siehe [Hinzufügen eines Uplink-Ports für den zweiten Edge-Knoten](#).

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.
- 3 Wählen Sie den logischen Tier-O-Router.
- 4 Klicken Sie auf die Registerkarte **Routing**, und wählen Sie **BGP** im Dropdown-Menü aus.
- 5 Klicken Sie auf **Hinzufügen** im Abschnitt „Nachbarn“, um einen BGP-Nachbarn hinzuzufügen.
- 6 Geben Sie die IP-Adresse des Nachbarn ein.  
Beispiel: 192.168.200.254.
- 7 (Optional) Geben Sie das maximale Hop-Limit an.  
Die Standardeinstellung ist 1.
- 8 Geben Sie die Remote-AS-Nummer ein.  
Beispiel: 64511.
- 9 (Optional) Klicken Sie auf die Registerkarte **Lokale Adresse**, um eine lokale Adresse auszuwählen.
  - a (Optional) Deaktivieren Sie **Alle Uplinks**, um sowohl Loopback-Ports als auch Uplink-Ports anzuzeigen.
- 10 (Optional) Klicken Sie auf die Registerkarte **Adressfamilien**, um eine Adressfamilie hinzuzufügen.
- 11 (Optional) Klicken Sie auf die Registerkarte **BFD-Konfiguration**, um BFD zu aktivieren.
- 12 Klicken Sie auf **Speichern**.  
Der neu hinzugefügte BGP-Nachbar wird angezeigt.
- 13 Klicken Sie auf **Bearbeiten** neben dem Abschnitt „BGP-Konfiguration“.
- 14 Klicken Sie auf die Umschaltfläche **ECMP**, um ECMP zu aktivieren.  
Für die Statusschaltfläche muss „Aktiviert“ angezeigt werden.
- 15 Klicken Sie auf **Speichern**.

## Ergebnisse

Mehrere ECMP-Routing-Pfade verbinden die VMs, die den logischen Switches und den beiden Edge-Knoten im Edge-Cluster angefügt wurden.

## Nächste Schritte

Überprüfen Sie, ob die ECMP-Routing-Verbindungen richtig funktionieren. Siehe [Überprüfen der ECMP-Routing-Konnektivität](#).

## Überprüfen der ECMP-Routing-Konnektivität

Überprüfen Sie mit der Befehlszeilenschnittstelle (CLI), ob die ECMP-Routing-Verbindung mit dem Nachbarn eingerichtet ist.

### Voraussetzungen

Stellen Sie sicher, dass das ECMP-Routing konfiguriert ist. Siehe [Hinzufügen eines Uplink-Ports für den zweiten Edge-Knoten](#) und [Hinzufügen eines zweiten BGP-Nachbarn und Aktivieren des ECMP-Routings](#).

### Verfahren

- 1 Melden Sie sich bei der NSX Manager-Befehlszeilenschnittstelle (CLI) an.
- 2 Rufen Sie die UUID-Informationen des verteilten Routers ab.

```
get logical-routers
```

```
Logical Router
UUID       : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf        : 2
type       : TUNNEL

Logical Router
UUID       : d40bbfa4-3e3d-4178-8615-6f42ea335037
vrf        : 4
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : d0289ba4-250e-41b4-8ffc-7cab4a46c3e4
vrf        : 5
type       : DISTRIBUTED_ROUTER

Logical Router
UUID       : a6ee6316-2212-4171-99cc-930c98bcad7f
vrf        : 6
type       : DISTRIBUTED_ROUTER
```

- 3 Suchen Sie die UUID-Informationen in der Ausgabe.

```
Logical Router
UUID       : d0289ba4-250e-41b4-8ffc-7cab4a46c3e4
vrf        : 5
type       : DISTRIBUTED_ROUTER
```

- 4 Geben Sie den VRF für den verteilten Tier-O-Router ein.  

```
vrf 5
```
- 5 Stellen Sie sicher, dass der verteilte Tier-O-Router mit den Edge-Knoten verbunden ist.  

```
get forwarding
```

Beispiel: Edge-Knoten-1 und Edge-Knoten-2.

- 6 Geben Sie **exit** zum Verlassen des VRF-Kontextes ein.
- 7 Stellen Sie sicher, dass der verteilte Tier-O-Router verbunden ist.  

```
get logical-router <UUID> route
```

Für den Routentyp der UUID sollte NSX\_CONNECTED angezeigt werden.
- 8 Starten Sie eine SSH-Sitzung auf den beiden Edge-Knoten.
- 9 Starten Sie eine Sitzung zur Erfassung von Paketen.  

```
set capture session 0 interface fp-eth1 dir tx
```

```
set capture session 0 expression src net <IP_Address>
```
- 10 Verwenden Sie ein beliebiges Tool, das Datenverkehr von einer mit dem mit dem Tier-O-Router verbundenen Quell-VM zu einer Ziel-VM generieren kann.
- 11 Beobachten Sie den Datenverkehr auf den beiden Edge-Knoten.

## Erstellen einer IP-Präfix-Liste

Eine IP-Präfix-Liste enthält einzelne oder mehrere IP-Adressen, denen Zugriffsberechtigungen für Routen-Advertisement zugewiesen werden. Die IP-Adressen in dieser Liste werden nacheinander verarbeitet. Auf IP-Präfix-Listen wird mit BGP-Nachbarschaftsfiltern oder Routenzuordnungen mit ein- oder ausgehender Richtung verwiesen.

So können Sie beispielsweise der IP-Präfix-Liste die IP-Adresse 192.168.100.3/27 hinzufügen und damit verhindern, dass die Route zum vertikalen Router neu verteilt wird. Sie haben auch die Möglichkeit, eine IP-Adresse mit den Modifizierern „kleiner oder gleich“ (le) bzw. „größer oder gleich“ (ge) anzufügen, um die Route Redistribution zu ermöglichen oder zu beschränken. Beispielsweise entspricht 192.168.100.3/27 mit den Modifizierern ge 24 le 30 Subnetzmasken größer oder gleich 24 Bit oder kleiner oder gleich 30 Bit in der Länge.

---

**Hinweis** Die Standardaktion für eine Route ist **Verweigern**. Wenn Sie eine Präfixliste zum Ablehnen oder Erlauben spezifischer Routen erstellen, stellen Sie sicher, dass Sie ein IP-Präfix ohne bestimmte Netzwerkadresse erstellen (wählen Sie in der Dropdown-Liste die Option **Beliebige** aus) und die Aktion **Zulassen**, wenn Sie alle anderen Routen zulassen möchten.

---

### Voraussetzungen

Stellen Sie sicher, dass ein logischer Tier-O Router konfiguriert ist. Siehe [Erstellen eines logischen Tier-O-Routers](#).

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.

- 3 Wählen Sie den logischen Tier-O-Router.
- 4 Klicken Sie auf die Registerkarte **Routing** und wählen Sie **IP-Präfix-Listen** im Dropdown-Menü aus.
- 5 Klicken Sie auf **Hinzufügen**.
- 6 Geben Sie einen Namen für die IP-Präfix-Liste ein.
- 7 Klicken Sie auf **Hinzufügen**, um ein Präfix anzugeben.
  - a Geben Sie eine IP-Adresse im CIDR-Format ein.  
Beispiel: 192.168.100.3/27.
  - b Wählen Sie **Verweigern** oder **Zulassen** im Dropdown-Menü aus.
  - c (Optional) Legen Sie einen Bereich von IP-Adressnummern in den **le**- oder **ge**-Modifizierern fest.  
Setzen Sie beispielsweise **le** auf 30 und **ge** auf 24.
- 8 Wiederholen Sie den vorherigen Schritt, um zusätzliche Präfixe anzugeben.
- 9 Klicken Sie unten im Fenster auf **Hinzufügen**.

## Erstellen einer Community-Liste

Sie können BGP-Community-Listen erstellen, um das Konfigurieren von Routenzuordnungen anhand von Community-Listen zu ermöglichen.

### Voraussetzungen

Stellen Sie sicher, dass ein logischer Tier-O Router konfiguriert ist. Siehe [Erstellen eines logischen Tier-O-Routers](#).

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.
- 3 Wählen Sie den logischen Tier-O-Router.
- 4 Klicken Sie auf die Registerkarte **Routing** und wählen Sie im Dropdown-Menü **Community-Listen** aus.
- 5 Klicken Sie auf **Hinzufügen**.
- 6 Geben Sie einen Namen für die Community-Liste ein.



- 7 Geben Sie eine Community im Format „aa:nn“ an, z. B. 300:500 und drücken Sie die Eingabetaste. Wiederholen Sie diese Schritte, wenn Sie weitere Communitys hinzufügen möchten.

Zusätzlich können Sie auf den Dropdown-Pfeil klicken und eine oder mehrere der folgenden Optionen auswählen:

- NO\_EXPORT\_SUBCONFED – Keine Ankündigung für EBG-Peers.
- NO\_ADVERTISE – Keine Ankündigung für alle Peers.
- NO\_EXPORT – Keine Ankündigung außerhalb der BGP-Konföderation.

- 8 Klicken Sie auf **Hinzufügen**.

## Erstellen einer Route Map

Eine Route Map besteht aus einer Abfolge von IP-Präfix-Listen, BGP-Pfadattributen und einer zugeordneten Aktion. Der Router prüft die Abfolge auf eine Übereinstimmung mit der IP-Adresse. Ist die Übereinstimmung gegeben, führt der Router die vorgesehene Aktion aus und keine weitere Prüfung mehr durch.

Auf Routenzuordnungen kann auf der Ebene der BGP-Nachbarschaft und bei der Route Redistribution verwiesen werden. Wenn in Routenzuordnungen auf IP-Präfix-Listen verwiesen wird und als Route Map-Aktion das Zulassen und Verweigern angewendet wird, überschreibt die in der Abfolge der Route Map angegebene Aktion die Spezifikation in der IP-Präfix-Liste.

### Voraussetzungen

Stellen Sie sicher, dass eine IP-Präfix-Liste konfiguriert ist. Siehe [Erstellen einer IP-Präfix-Liste](#).

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.
- 3 Wählen Sie den logischen Tier-0-Router.
- 4 Wählen Sie **Routing > Route Maps** aus.
- 5 Klicken Sie auf **Hinzufügen**.
- 6 Geben Sie einen Namen und eine optionale Beschreibung für die Route Map ein.
- 7 Klicken Sie auf **Hinzufügen**, um einen Eintrag in der Route Map hinzuzufügen.
- 8 Bearbeiten Sie die Spalte **IP-Präfix-Liste/Community-Liste abgleichen**, um entweder IP-Präfix-Listen oder Community-Listen auszuwählen, aber nicht beide.

## 9 (Optional) Legen Sie BGP-Attribute fest.

BGP-Attribut	Beschreibung
AS für Pfad voranstellen	Stellen Sie einem Pfad eine oder mehrere AS-Nummern des autonomen Systems voran, um den Pfad zu verlängern und damit in der Priorität herabzustufen.
MED	Der Multi-Exit Discriminator zeigt einem externen Peer einen bevorzugten Pfad für ein autonomes System an.
Gewicht	Legen Sie eine Gewichtung für die Pfadauswahl fest. Der Bereich liegt zwischen 0 und 65535.
Community	Geben Sie eine Community im Format „aa:nn“ an, z. B. 300:500. Sie können mithilfe des Dropdown-Menüs auch eine der folgenden Optionen auswählen: <ul style="list-style-type: none"> <li>■ NO_EXPORT_SUBCONFED – Keine Ankündigung für EBGPeers.</li> <li>■ NO_ADVERTISE – Keine Ankündigung für alle Peers.</li> <li>■ NO_EXPORT – Keine Ankündigung außerhalb der BGP-Konföderation.</li> </ul>

## 10 Wählen Sie in der Spalte „Aktion“ die Option **Zulassen** oder **Verweigern** aus.

Sie können es zulassen oder verweigern, dass IP-Adressen der IP-Präfix-Liste angekündigt werden.

## 11 Klicken Sie auf **Speichern**.

## Konfigurieren des Timers für die Weiterleitung der Aktiv-Benachrichtigung

Sie können für logische Tier-0 Router einen Timer für die Weiterleitung der Aktiv-Benachrichtigung konfigurieren.

Der Timer für die Weiterleitung der Aktiv-Benachrichtigung definiert die Zeit in Sekunden, die der Router warten muss, bevor die Aktiv-Benachrichtigung nach dem Herstellen der ersten BGP-Sitzung gesendet wird. Dieser Timer (zuvor als Weiterleitungsverzögerung bezeichnet) minimiert die Ausfallzeit bei einem Failover für Aktiv/Aktiv- oder Aktiv/Standby-Konfigurationen logischer Router auf NSX Edge, die dynamisches Routing (BGP) verwenden. Er sollte auf die Anzahl Sekunden festgelegt werden, die ein externer Router (TOR) benötigt, um nach der ersten BGP/BFD-Sitzung alle Routen auf diesem Router zu veröffentlichen. Der Timer-Wert sollte direkt proportional zur Anzahl dynamischer Northbound-Routen sein, die der Router lernen muss. Dieser Timer sollte bei Konfigurationen mit einzeltem Edge-Knoten auf 0 festgelegt werden.


### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.
- 3 Wählen Sie den logischen Tier-0-Router.
- 4 Wählen Sie **Routing > Globale Konfiguration** aus.
- 5 Klicken Sie auf **Bearbeiten**.

- 6 Geben Sie einen Wert für den Timer für die Weiterleitung der Aktiv-Benachrichtigung ein.
- 7 Klicken Sie auf **Speichern**.

Sie können NAT über die Registerkarte **Netzwerk und Sicherheit – Erweitert** konfigurieren.

---

**Hinweis** Wenn Sie die Benutzeroberfläche **Netzwerk und Sicherheit – Erweitert** verwenden, um in der Richtlinienschnittstelle erstellte Objekte zu ändern, sind einige Einstellungen möglicherweise nicht konfigurierbar. Neben diesen schreibgeschützten Einstellungen wird dieses Symbol angezeigt: . Weitere Informationen hierzu finden Sie unter [Kapitel 1 Übersicht über NSX Manager](#).

---

Dieses Kapitel enthält die folgenden Themen:

- [Netzwerkadressübersetzung \(NAT\)](#)

## Netzwerkadressübersetzung (NAT)

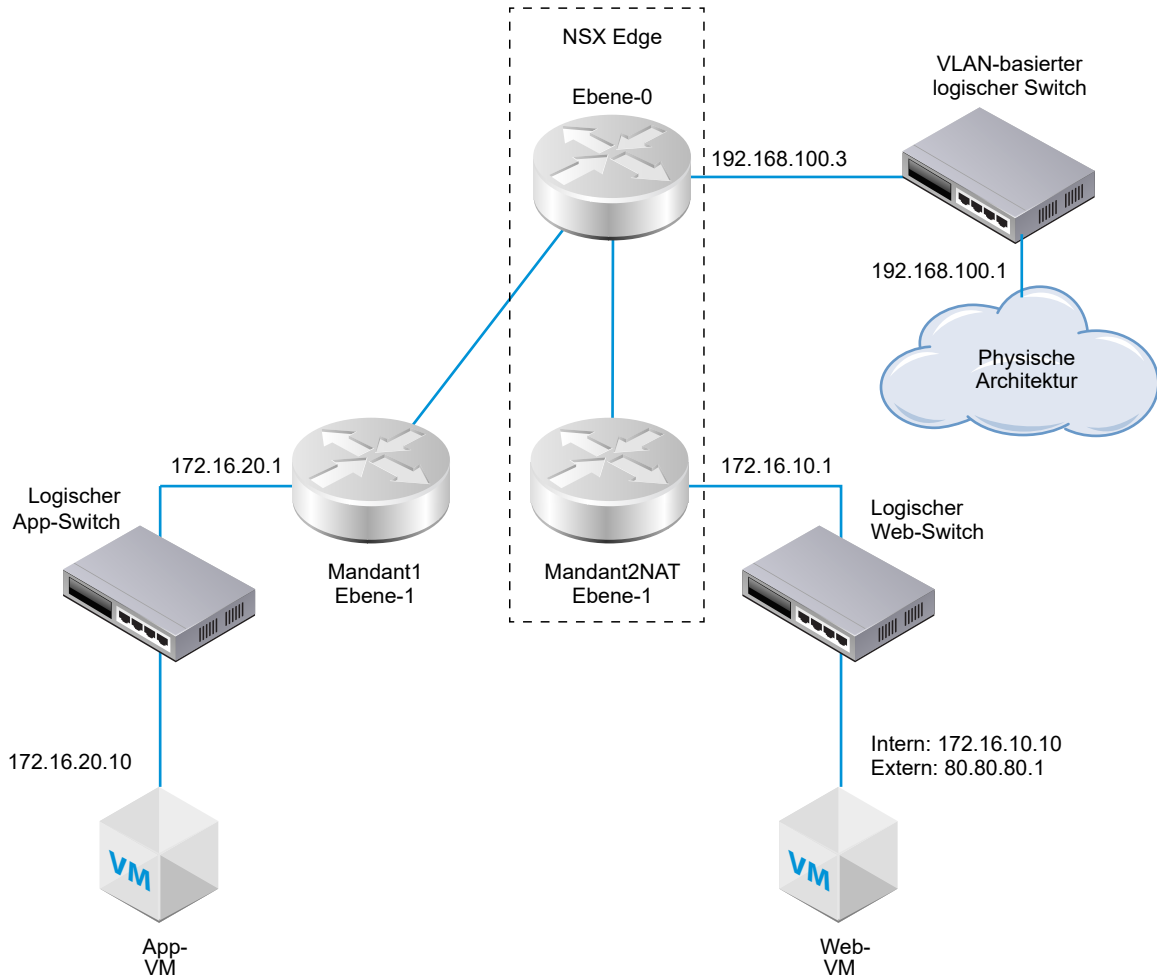
Die Netzwerkadressübersetzung (NAT, Network Address Translation) in NSX-T Data Center kann auf logischen Tier-0- und Tier-1-Routern konfiguriert werden.

Das nachfolgend dargestellte Diagramm enthält beispielhaft zwei logische Tier-1-Router mit auf Mandant2NAT konfigurierter NAT. Für die Web-VM ist vereinfacht 172.16.10.10 als IP-Adresse und 172.16.10.1 als Standard-Gateway konfiguriert.

Die NAT wird für den Uplink des logischen Routers Mandant2NAT auf seiner Verbindung mit dem logischen Tier-0-Router erzwungen.

Um die NAT-Konfiguration aktivieren zu können, muss für Mandant2NAT eine Dienstkomponente auf einem NSX Edge-Cluster vorhanden sein. Mandant2NAT wird deshalb innerhalb von NSX Edge angezeigt. Für einen Vergleich kann sich Mandant1 auch außerhalb von NSX Edge befinden, kein Edge-Dienst genutzt wird.

Abbildung 15-1. NAT-Topologie



## Tier-1-NAT

Ein logischer Tier-1-Router unterstützt Quell-NAT (SNAT), Ziel-NAT (DNAT) und reflexive NAT.

### Konfigurieren einer Quell-NAT auf einem Tier-1-Router

Eine Quell-NAT (SNAT, Source NAT) ändert die Quelladresse in der IP-Kopfzeile eines Pakets. Damit lässt sich auch der Quellport in den TCP/UDP-Kopfzeilen ändern. Typischerweise wird damit eine private Adresse (RFC 1918) bzw. ein privater Port in eine öffentliche Adresse bzw. in einen öffentlichen Port für Pakete geändert, die Ihr Netzwerk verlassen.

Sie können eine Regel zum Aktivieren oder Deaktivieren der Quell-NAT erstellen.

In diesem Beispiel, in dem Pakete von der Web-VM empfangen werden, ändert der Mandant2NAT-Tier-1-Router die Quell-IP-Adresse der Pakete von 172.16.10.10 in 80.80.80.1. Durch eine öffentliche Quelladresse können Ziele außerhalb des privaten Netzwerks Pakete zur ursprünglichen Quelle zurückleiten.

## Voraussetzungen

- Der Tier-0-Router muss einen Uplink aufweisen, der mit einem VLAN-basierten logischen Switch verbunden ist. Siehe [Verbinden eines logischen Tier-0 Routers mit einem logischen VLAN-Switch für den NSX Edge-Uplink](#).
- Beim Tier-0-Router muss Routing (statisch oder BGP) und Route Redistribution am Uplink zur physischen Architektur konfiguriert sein. Siehe [Konfigurieren einer statischen Route](#), [Konfigurieren von eBGP auf einem logischen Tier-0-Router](#) und [Aktivieren von Route Redistribution auf dem logischen Tier-0 Router](#).
- Bei den Tier-1- Routern muss jeweils ein Uplink zu einem Tier-0-Router konfiguriert sein. Mandant2NAT muss von einem NSX Edge-Cluster unterstützt werden. Siehe [Anfügen von Tier-0 und Tier-1](#).
- Bei den Tier-1 Routern müssen Downlink-Ports und Routen-Advertisement konfiguriert sein. Siehe [Hinzufügen eines Downlink-Ports auf einem logischen Tier-1-Router](#) und [Konfigurieren von Routen-Advertisement auf einem logischen Tier-1 Router](#).
- Die VMs müssen an die richtigen logischen Switches angefügt werden.

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.
- 3 Klicken Sie auf den logischen Tier-1-Router, für den Sie eine NAT konfigurieren möchten.
- 4 Wählen Sie **Dienste > NAT** aus.
- 5 Klicken Sie auf **HINZUFÜGEN**.
- 6 Geben Sie einen Prioritätswert an.  
Ein niedrigerer Wert bedeutet eine höhere Priorität für diese Regel.
- 7 Um die Quell-NAT zu aktivieren, wählen Sie für **Aktion** die Option **SNAT** aus. Mit der Option **NO\_SNAT** deaktivieren Sie die Quell-NAT.
- 8 Wählen Sie den Protokolltyp aus.  
Standardmäßig ist **Jedes Protokoll** ausgewählt.
- 9 (Optional) Geben Sie für **Quell-IP** eine IP-Adresse oder einen IP-Adressbereich im CIDR-Format an.  
Wenn Sie das Feld leer lassen, werden alle Quellen an den Downlink-Ports des Routers übersetzt. In diesem Beispiel lautet die Quell-IP-Adresse 172.16.10.10.
- 10 (Optional) Geben Sie für **Ziel-IP** eine IP-Adresse oder einen IP-Adressbereich im CIDR-Format an.  
Wenn Sie das Feld leer lassen, wird die NAT auf alle Ziele außerhalb des lokalen Subnetzes angewendet.

- 11** Wenn Sie für **Aktion** die Option **SNAT** ausgewählt haben, geben Sie für **Übersetzte IP** eine IP-Adresse oder einen IP-Adressbereich im CIDR-Format an.

In diesem Beispiel lautet die übersetzte IP-Adresse 80.80.80.1.

- 12** (Optional) Wählen Sie für **Angewendet auf** einen Router-Port aus.

- 13** (Optional) Legen Sie den Status der Regel fest.

Die Regel ist standardmäßig aktiviert.

- 14** (Optional) Ändern Sie den Status der Protokollierung.

Die Protokollierung ist standardmäßig deaktiviert.

- 15** (Optional) Ändern Sie die Einstellung für die Firewall-Umgehung.

Diese Funktion ist standardmäßig aktiviert.

## Ergebnisse

Die neue Regel wird unter „NAT“ aufgeführt. Beispiel:

Tenant2NAT

Übersicht

Konfiguration

Routing

Dienste

NAT | AKTUALISIEREN

Es wurden keine Statistiken erfasst

+ HINZUFÜGEN

BEARBEITEN

LÖSCHEN

ID	aktion	Abgleichen					Übersetzt		Angewendet auf	Statistik
		Protokoll	Quell-IP	Quellports	Ziel-IP	Zielports	IP	Ports		
Priorität: 1024										
1031	SNAT	Belie...	172.16.10.10	Beliebig	Bel...	Belie...	80.80.80.1	B...		

## Nächste Schritte

Konfigurieren Sie den Tier-1-Router für die Ankündigung von NAT-Routen.

Um die NAT-Routen vorgelagert vor dem Tier-0-Router zur physischen Architektur anzukündigen, müssen Sie den Tier-0-Router so konfigurieren, dass Tier-1-NAT-Routen angekündigt werden.

## Konfigurieren der Ziel-NAT auf einem Tier-1-Router

Mit der Ziel-NAT wird die Zieladresse in der IP-Kopfzeile eines Pakets geändert. Sie kann außerdem den Zielport in den TCP/UDP-Kopfzeilen ändern. Dies wird normalerweise eingesetzt, um eingehende Pakete mit einem öffentlichen Adress-/Portziel zu einer privaten IP-Adresse/ einem privaten Port im Netzwerk umzuleiten.

Sie können eine Regel zum Aktivieren oder Deaktivieren von Ziel-NAT erstellen

Wenn in diesem Beispiel Pakete bei der App-VM eingehen, ändert der Tier-1-Router Mandant2NAT die Ziel-IP-Adresse der Pakete von 172.16.10.10 in 80.80.80.1. Bei einer öffentlichen Zieladresse kann ein Ziel innerhalb eines privaten Netzwerks von außerhalb des privaten Netzwerks kontaktiert werden.

## Voraussetzungen

- Der Tier-0-Router muss einen Uplink aufweisen, der mit einem VLAN-basierten logischen Switch verbunden ist. Siehe [Verbinden eines logischen Tier-0 Routers mit einem logischen VLAN-Switch für den NSX Edge-Uplink](#).
- Beim Tier-0-Router muss Routing (statisch oder BGP) und Route Redistribution am Uplink zur physischen Architektur konfiguriert sein. Siehe [Konfigurieren einer statischen Route](#), [Konfigurieren von eBGP auf einem logischen Tier-0-Router](#) und [Aktivieren von Route Redistribution auf dem logischen Tier-0 Router](#).
- Bei den Tier-1- Routern muss jeweils ein Uplink zu einem Tier-0-Router konfiguriert sein. Mandant2NAT muss von einem NSX Edge-Cluster unterstützt werden. Siehe [Anfügen von Tier-0 und Tier-1](#).
- Bei den Tier-1 Routern müssen Downlink-Ports und Routen-Advertisement konfiguriert sein. Siehe [Hinzufügen eines Downlink-Ports auf einem logischen Tier-1-Router](#) und [Konfigurieren von Routen-Advertisement auf einem logischen Tier-1 Router](#).
- Die VMs müssen an die richtigen logischen Switches angefügt werden.

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.
- 3 Klicken Sie auf den logischen Tier-1-Router, für den Sie eine NAT konfigurieren möchten.
- 4 Wählen Sie **Dienste > NAT** aus.
- 5 Klicken Sie auf **HINZUFÜGEN**.
- 6 Geben Sie einen Prioritätswert an.  
Ein niedrigerer Wert bedeutet eine höhere Priorität für diese Regel.
- 7 Um die Ziel-NAT zu aktivieren, wählen Sie für **Aktion** die Option **DNAT** aus. Mit der Option **NO\_DNAT** deaktivieren Sie die Ziel-NAT.
- 8 Wählen Sie den Protokolltyp aus.  
Standardmäßig ist **Jedes Protokoll** ausgewählt.
- 9 (Optional) Geben Sie für **Quell-IP** eine IP-Adresse oder einen IP-Adressbereich im CIDR-Format an.  
Wenn Sie die Quell-IP leer lassen, wird die NAT auf alle Quellen außerhalb des lokalen Subnetzes angewendet.
- 10 Geben Sie für **Ziel-IP** eine IP-Adresse oder einen IP-Adressbereich im CIDR-Format an.  
In diesem Beispiel lautet die Ziel-IP-Adresse 80.80.80.1.



- 11** Wenn Sie für **Aktion** die Option **DNAT** ausgewählt haben, geben Sie für **Übersetzte IP** eine IP-Adresse oder einen IP-Adressbereich im CIDR-Format an.

In diesem Beispiel lautet die interne/übersetzte IP-Adresse 172.16.10.10.

- 12** (Optional) Wenn Sie für **Aktion** die Option **DNAT** ausgewählt haben, geben Sie für **Übersetzte Ports** die übersetzten Ports an.

- 13** (Optional) Wählen Sie für **Angewendet auf** einen Router-Port aus.

- 14** (Optional) Legen Sie den Status der Regel fest.

Die Regel ist standardmäßig aktiviert.

- 15** (Optional) Ändern Sie den Status der Protokollierung.

Die Protokollierung ist standardmäßig deaktiviert.

- 16** (Optional) Ändern Sie die Einstellung für die Firewall-Umgehung.

Diese Funktion ist standardmäßig aktiviert.

## Ergebnisse

Die neue Regel wird unter „NAT“ aufgeführt. Beispiel:

Tenant2NAT

Übersicht

Konfiguration

Routing

Dienste

NAT | AKTUALISIEREN

Es wurden keine Statistiken erfasst

+ HINZUFÜGEN

BEARBEITEN

LÖSCHEN

ID	aktion	Abgleichen					Übersetzt		Angewendet auf	Statistik
		Protokoll	Quell-IP	Quellports	Ziel-IP	Zielports	IP	Ports		
▼ Priorität: 1024										
✓ 1032	DNAT	Belie...	Beliebig	Beliebig	80.80.80.1	Belle...	172.16.10.10	B...		

## Nächste Schritte

Konfigurieren Sie den Tier-1-Router für die Ankündigung von NAT-Routen.

Um die NAT-Routen vorgelagert vor dem Tier-0-Router zur physischen Architektur anzukündigen, müssen Sie den Tier-0-Router so konfigurieren, dass Tier-1-NAT-Routen angekündigt werden.

## Ankündigen von Tier-1-NAT-Routen für den Upstream-Tier-0-Router

Die Ankündigung von Tier-1-NAT-Routen ermöglicht dem Upstream-Tier-0-Router, Informationen über diese Routen abzurufen.

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.

- 3 Klicken Sie auf einen logischen Tier-1-Router, für den NAT konfiguriert wurde.
- 4 Wählen Sie vom Tier-1-Router aus die Option **Routing > Routen-Advertisement** aus.
- 5 Klicken Sie auf **Bearbeiten**, um die Konfiguration von Routen-Advertisement zu bearbeiten.

Sie können die folgenden Switches umschalten:

- **Status**
- **Alle mit NSX verbundenen Routen ankündigen**
- **Alle NAT-Routen ankündigen**
- **Alle statischen Routen ankündigen**
- **Alle LB VIP-Routen ankündigen**
- **Alle LB SNAT-IP-Routen ankündigen**
- **Alle DNS-Weiterleitungsrouten ankündigen**

- 6 Klicken Sie auf **Speichern**.

#### Nächste Schritte

Kündigen Sie Tier-1-NAT-Routen des Tier-0-Routers für die physische Upstream-Architektur an.

### Ankündigen von Tier-1-NAT-Routen für die physische Architektur

Die Ankündigung von Tier-1-NAT-Routen des Tier-0-Routers ermöglicht der physischen Upstream-Architektur, Informationen über diese Routen abzurufen.

#### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Routing** aus.
- 3 Klicken Sie auf einen logischen Tier-0 Router, der mit einem Tier-1 Router verbunden ist, für den Sie NAT konfiguriert haben.
- 4 Wählen Sie vom Tier-0-Router aus die Option **Routing > Route Redistribution** aus.
- 5 Klicken Sie auf **Bearbeiten**, um Route Redistribution zu aktivieren oder zu deaktivieren.

- 6 Klicken Sie auf **Hinzufügen**, um einen Satz von Route Redistribution-Kriterien hinzuzufügen.

Option	Beschreibung
<b>Name und Beschreibung</b>	Weisen Sie der Route Redistribution einen Namen zu. Sie können optional auch eine Beschreibung bereitstellen. Beispielname: advertise-to-bgp-neighbor
<b>Quellen</b>	Wählen Sie mindestens eine der folgenden Quellen aus: <ul style="list-style-type: none"> <li>■ <b>T0 Verbunden</b></li> <li>■ <b>T0 Uplink</b></li> <li>■ <b>T0 Downlink</b></li> <li>■ <b>T0 CSP</b></li> <li>■ <b>T0 Loopback</b></li> <li>■ <b>T0 Statisch</b></li> <li>■ <b>T0 NAT</b></li> <li>■ <b>T0 DNS-Weiterleitungs-IP</b></li> <li>■ <b>T0 Lokale IPSec-IP</b></li> <li>■ <b>T1 Verbunden</b></li> <li>■ <b>T1 CSP</b></li> <li>■ <b>T1 Downlink</b></li> <li>■ <b>T1 Statisch</b></li> <li>■ <b>T1 LB-SNAT</b></li> <li>■ <b>T1 NAT</b></li> <li>■ <b>T1 LB-VIP</b></li> <li>■ <b>T1 DNS-Weiterleitungs-IP</b></li> </ul>
<b>Route Map</b>	(Optional) Weisen Sie eine Route Map zu, um eine Reihe von IP-Adressen von der Route Redistribution herauszufiltern.

## Überprüfen der Tier-1-NAT

Stellen Sie sicher, dass die SNAT- und DNAT-Regeln korrekt funktionieren.

### Verfahren

- 1 Melden Sie sich bei NSX Edge an.
- 2 Führen Sie `get logical-routers` aus, um die VRF-Nummer für den Tier-0-Dienstrouter zu ermitteln.
- 3 Führen Sie den Befehl `vrf <number>` aus, um in den Kontext des Tier-0-Dienstrouters zu gelangen.
- 4 Führen Sie den Befehl `get route` aus und stellen Sie sicher, dass die Tier-1-NAT-Adresse angezeigt wird.

```
nsx-edge(tier0_sr)> get route
```

```
Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT
```

```
Total number of routes: 8
```

```
t1n 80.80.80.1/32      [3/3]      via 169.0.0.1
...
```

- 5 Wenn Ihre Web-VM für die Unterstützung von Webseiten eingerichtet ist, stellen Sie sicher, dass Sie eine Webseite unter `http://80.80.80.1` öffnen können.
- 6 Stellen Sie sicher, dass der Upstream-Nachbar des Tier-O-Routers in der physischen Architektur einen Ping-Befehl an 80.80.80.1 senden kann.
- 7 Achten Sie während der Ausführung des Ping-Befehls auf die Statistikspalte für die DNAT-Regel.

Hier muss eine aktive Sitzung angezeigt werden.

## Tier-O-NAT

Ein logischer Tier-O-Router im Modus „Aktiv/Standby“ unterstützt Quell-NAT (SNAT), Ziel-NAT (DNAT) und reflexive NAT. Ein logischer Tier-O-Router im Modus „Aktiv/Aktiv“ unterstützt nur reflexive NAT.

### Konfigurieren der Quell- und Ziel-NAT auf einem logischen Tier-O Router

Sie können eine Quell- und Ziel-NAT auf einem logischen Tier-O Router konfigurieren, der im Aktiv-Standby-Modus ausgeführt wird.

Sie können SNAT oder DNAT auch für eine IP-Adresse oder einen Adressbereich deaktivieren. Wenn für eine Adresse mehrere NAT-Regeln gelten, wird die Regel mit der höchsten Priorität angewendet.

Auf dem Uplink eines logischen Tier-O Routers konfigurierte SNAT verarbeitet den Datenverkehr von einem logischen Tier-1 Router sowie von einem anderen Uplink auf dem logischen Tier-O-Router.

#### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.
- 3 Klicken Sie auf einen logischen Tier-O Router.
- 4 Wählen Sie **Dienste > NAT** aus.
- 5 Klicken Sie auf **HINZUFÜGEN**, um eine NAT-Regel hinzuzufügen.
- 6 Geben Sie einen Prioritätswert an.  
Ein niedrigerer Wert bedeutet eine höhere Priorität.
- 7 Wählen Sie als **Aktion** eine der Optionen **SNAT**, **DNAT**, **Reflexiv**, **NO\_SNAT** oder **NO\_DNAT** aus.

- 8 Wählen Sie den Protokolltyp aus.

Standardmäßig ist **Jedes Protokoll** ausgewählt.

- 9 (Erforderlich) Geben Sie für **Quell-IP** eine IP-Adresse oder einen IP-Adressbereich im CIDR-Format an.

Wenn Sie dieses Feld leer lassen, gilt diese NAT-Regel für alle Quellen außerhalb des lokalen Subnetzes.

- 10 Geben Sie für **Ziel-IP** eine IP-Adresse oder einen IP-Adressbereich im CIDR-Format an.

- 11 Geben Sie für **Übersetzte IP** eine IP-Adresse oder einen IP-Adressbereich im CIDR-Format an.

- 12 (Optional) Wenn Sie für **Aktion** die Option **DNAT** ausgewählt haben, geben Sie für **Übersetzte Ports** die übersetzten Ports an.

- 13 (Optional) Wählen Sie für **Angewendet auf** einen Router-Port aus.

- 14 (Optional) Legen Sie den Status der Regel fest.

Die Regel ist standardmäßig aktiviert.

- 15 (Optional) Ändern Sie den Status der Protokollierung.

Die Protokollierung ist standardmäßig deaktiviert.

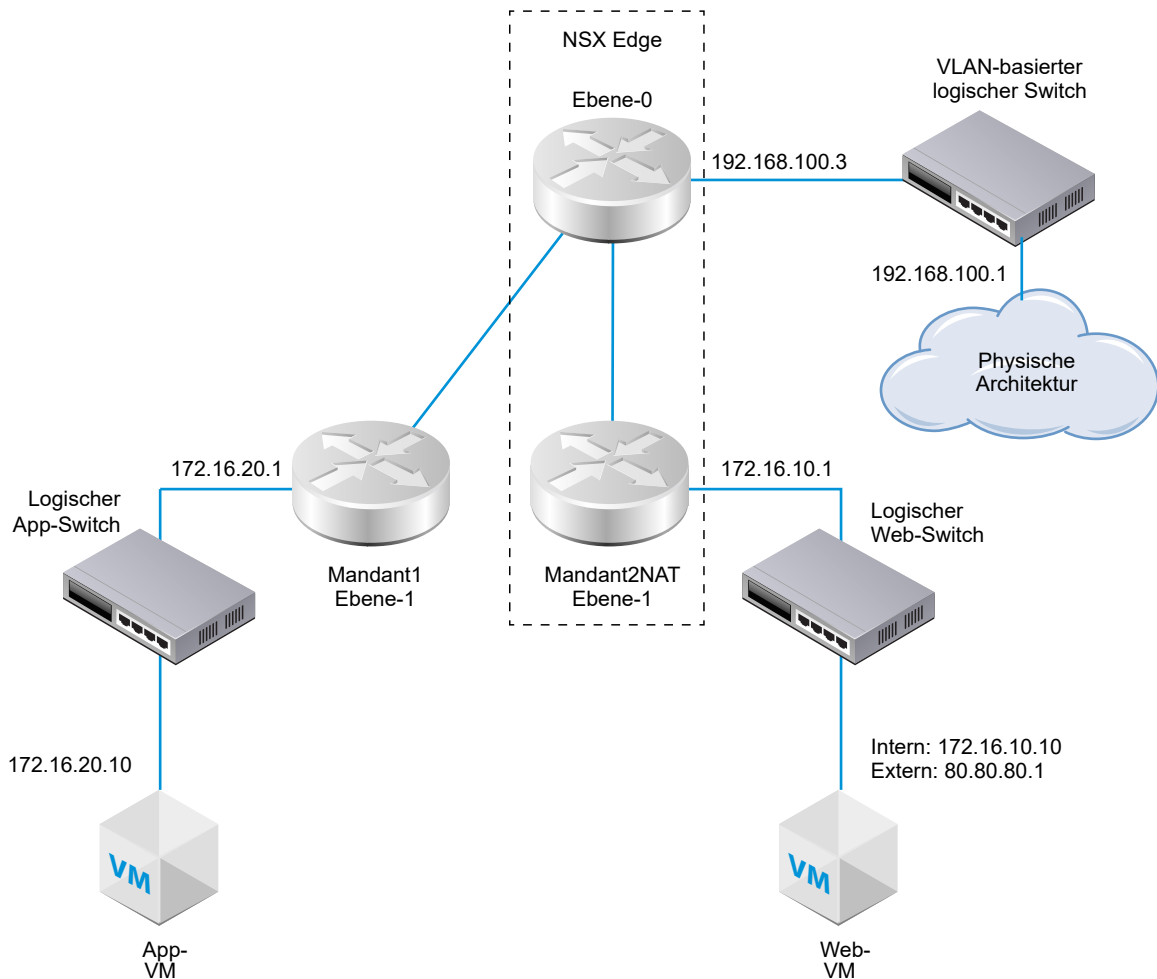
- 16 (Optional) Ändern Sie die Einstellung für die Firewall-Umgehung.

Diese Funktion ist standardmäßig aktiviert.

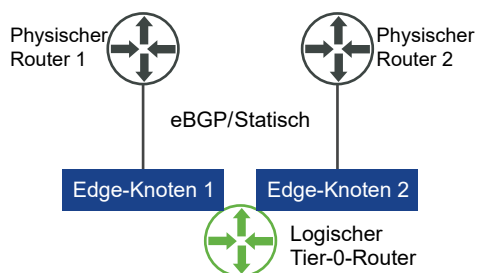
## Reflexive NAT

Wenn ein logischer Tier-0-Router im Aktiv/Aktiv-Modus ausgeführt wird, können Sie keine zustandsbehaftete NAT konfigurieren. Dabei besteht die Gefahr, dass asymmetrische Pfade zu Problemen führen. Für Aktiv/Aktiv-Router können Sie eine reflexive NAT (manchmal als statusfreie NAT bezeichnet) konfigurieren.

In diesem Beispiel, in dem Pakete von der Web-VM empfangen werden, ändert der Mandant2NAT-Tier-1-Router die Quell-IP-Adresse der Pakete von 172.16.10.10 in 80.80.80.1. Durch eine öffentliche Quelladresse können Ziele außerhalb des privaten Netzwerks Pakete zur ursprünglichen Quelle zurückleiten.



Wenn allerdings, wie hier gezeigt, zwei Aktiv/Aktiv-Tier-0-Router beteiligt sind, muss eine reflexive NAT konfiguriert werden.



## Konfigurieren einer reflexiven NAT auf einem logischen Tier-0- oder Tier-1-Router

Wenn ein logischer Tier-0- oder Tier-1-Router im Aktiv/Aktiv-Modus ausgeführt wird, können Sie keine statusbehaftete NAT konfigurieren. Bei dieser besteht die Gefahr, dass asymmetrische Pfade zu Problemen führen. Für Aktiv/Aktiv-Router steht eine reflexive NAT (manchmal als „statusfreie NAT“ bezeichnet) zur Verfügung.

Für eine reflexive NAT können Sie eine einzelne zu übersetzende Quelladresse oder einen Bereich von zu übersetzenden Quelladressen konfigurieren. Wenn Sie einen Bereich von Quelladressen konfigurieren, müssen Sie auch einen Bereich von übersetzten Adressen konfigurieren. Die Größe der beiden Bereiche muss identisch sein. Die Adressübersetzung ist deterministisch, d. h. die erste Adresse im Quelladressbereich wird in die erste Adresse im übersetzten Adressbereich übersetzt, die zweite Adresse im Quellbereich wird in die zweite Adresse im übersetzten Bereich übersetzt und so weiter.

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.
- 3 Klicken Sie auf den logischen Tier-0- oder Tier-1-Router, für den Sie eine reflexive NAT konfigurieren möchten.
- 4 Wählen Sie **Dienste > NAT** aus.
- 5 Klicken Sie auf **HINZUFÜGEN**.
- 6 Geben Sie einen Prioritätswert an.  
Ein niedrigerer Wert bedeutet eine höhere Priorität für diese Regel.
- 7 Wählen Sie für **Aktion** die Option **Reflexiv** aus.
- 8 Geben Sie für **Quell-IP** eine IP-Adresse oder einen IP-Adressbereich im CIDR-Format an.
- 9 Geben Sie für **Übersetzte IP** eine IP-Adresse oder einen IP-Adressbereich im CIDR-Format an.
- 10 (Optional) Legen Sie den Status der Regel fest.  
Die Regel ist standardmäßig aktiviert.
- 11 (Optional) Ändern Sie den Status der Protokollierung.  
Die Protokollierung ist standardmäßig deaktiviert.
- 12 (Optional) Ändern Sie die Einstellung für die Firewall-Umgehung.  
Diese Funktion ist standardmäßig aktiviert.

## Ergebnisse

Die neue Regel wird unter „NAT“ aufgeführt. Beispiel:

Tier0-LR-1

✕

[Übersicht](#) [Konfiguration](#) [Routing](#) **[Dienste](#)****NAT** | [AKTUALISIEREN](#)

Gesamte Regelstatistiken | Letzte Aktualisierung: 6. März 2019 18:15:06

0 Aktive Sitzungen

0 Paketanzahl

0 Byte Daten

[+ HINZUFÜGEN](#) [BEARBEITEN](#) [LÖSCHEN](#)

ID	Aktion	Abgleichen					Übersetzt		Angewendet auf	Statistik
		Protokoll	Quell-IP	Quellports	Ziel-IP	Zielports	IP	Ports		
▼ Priorität: 1024										
✓ 2048	Reflexiv	Beliebig	80.80.80.1	Beliebig	Beliebig	Beliebig	172.16.10.10	Beliebig		




# Erweiterte Gruppierungsobjekte

# 16

Sie können IP Sets, IP-Pools, MAC-Sätze, NSGroups und NS-Dienste erstellen. Sie können auch die Tags für die virtuellen Maschinen verwalten.

---

**Hinweis** Wenn Sie die Benutzeroberfläche **Netzwerk und Sicherheit – Erweitert** verwenden, um in der Richtlinienschnittstelle erstellte Objekte zu ändern, sind einige Einstellungen möglicherweise nicht konfigurierbar. Neben diesen schreibgeschützten Einstellungen wird dieses Symbol angezeigt: . Weitere Informationen hierzu finden Sie unter [Kapitel 1 Übersicht über NSX Manager](#).

---

Dieses Kapitel enthält die folgenden Themen:

- [Erstellen eines IP Sets](#)
- [Erstellen eines IP-Pools](#)
- [Erstellen eines MAC Set](#)
- [Erstellen einer NS-Gruppe](#)
- [Konfigurieren von Diensten und Dienstgruppen](#)
- [Verwalten von Tags für eine virtuelle Maschine](#)

## Erstellen eines IP Sets

Ein IP Set ist eine Gruppe von IP-Adressen, die als Quellen und Ziele in Firewallregeln verwendet werden können.

Ein IP Set kann aus einer Kombination von einzelnen IP-Adressen, IP-Bereichen und Subnetzen bestehen. Sie können IPv4- und/oder IPv6-Adressen festlegen. Ein IP Set kann Mitglied von NSGroups sein. IP-Sets, die mit dieser Methode erstellt werden, werden im Richtlinienmodus nicht angezeigt. Im Richtlinienmodus können wir eine Gruppe erstellen und Mitglieder als IP-Adressen, Bereiche, Netzwerkadressen oder MAC-Adressen hinzufügen. Navigieren Sie dazu zu **Bestandsliste > Gruppen > Mitglieder festlegen** und geben Sie die IP- oder MAC-Adresse an.

---

**Hinweis** IPv4- und IPv6-Adressen werden für Quell- und Zielbereiche von Firewallregeln unterstützt.

---

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Bestandsliste > Gruppen > IP Sets > Hinzufügen** aus.
- 3 Geben Sie einen Namen ein.
- 4 (Optional) Geben Sie eine Beschreibung ein.
- 5 Geben Sie unter **Mitglieder** einzelne IP-Adressen, IP-Bereiche und Subnetze in Form einer kommagetrennten Liste ein.
- 6 Klicken Sie auf **Speichern**.

## Erstellen eines IP-Pools

Sie können mit einem IP-Pool beim Erstellen von L3-Subnetzen IP-Adressen oder Subnetze zuteilen.

## Verfahren

- 1 Melden Sie sich in Ihrem 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 einen Namen für den neuen IP-Pool ein.
- 4 (Optional) Geben Sie eine Beschreibung ein.
- 5 Klicken Sie auf **Hinzufügen**.
- 6 Klicken Sie auf die Zelle „IP-Bereiche“ und geben Sie die IP-Bereiche ein.  
Setzen Sie den Mauszeiger oben rechts auf eine beliebige Zelle und klicken Sie auf das Bleistiftsymbol zur Bearbeitung.
- 7 (Optional) Geben Sie ein Gateway ein.
- 8 Geben Sie eine CIDR-IP-Adresse mit Suffix ein.
- 9 (Optional) Geben Sie DNS-Server ein.
- 10 (Optional) Geben Sie ein DNS-Suffix ein.
- 11 Klicken Sie auf **Speichern**.

## Erstellen eines MAC Set

Ein MAC Set ist eine Gruppe von MAC-Adressen, die Sie als Quellen und Ziele in Schicht-2-Firewallregeln bzw. als Mitglieder einer NS-Gruppe verwenden können.

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Bestandsliste > Gruppen > MAC Sets > Hinzufügen** aus.
- 3 Geben Sie einen Namen ein.
- 4 (Optional) Geben Sie eine Beschreibung ein.
- 5 Geben Sie die MAC-Adressen in einer kommagetrennten Liste ein.
- 6 Klicken Sie auf **HINZUFÜGEN**.

## Erstellen einer NS-Gruppe

NS-Gruppen können so konfiguriert werden, dass diese eine Kombination von IP-Sätzen, MAC Sets, logischen Ports, logischen Switches und anderen NS-Gruppen aufnehmen. Sie können NS-Gruppen mit logischen Switches, logischen Ports und VMs als Quellen und Ziele sowie im Feld **Applied To** einer Firewallregel angeben. NS-Gruppen mit IPset und MACSet werden in einem **Applied To**-Feld einer verteilten Firewall ignoriert.

---

**NSX Cloud-Hinweis** Wenn Sie NSX Cloud verwenden, finden Sie unter [Verwendung von NSX-T Data Center-Funktionen mit der Public Cloud](#) eine Liste der automatisch generierten logischen Einheiten, unterstützten Funktionen und Konfigurationen, die für NSX Cloud erforderlich sind.

---

Eine NS-Gruppe verfügt über die folgenden Merkmale:

- Eine NS-Gruppe verfügt über direkte und effektive Mitglieder. Zu den effektiven Mitgliedern gehören Mitglieder, die mithilfe von Mitgliedschaftskriterien festgelegt werden, sowie alle direkten und effektiven Mitglieder, die zu den Mitgliedern dieser NS-Gruppe gehören. Angenommen, NS-Gruppe-1 verfügt über das direkte Mitglied LogischerSwitch-1. Sie fügen NS-Gruppe-2 hinzu und Sie legen NS-Gruppe-1 sowie LogischerSwitch-2 als Mitglieder fest. Damit verfügt NS-Gruppe-2 über die direkten Mitglieder NS-Gruppe-1 und LogischerSwitch-2 sowie über ein effektives Mitglied, LogischerSwitch-1. Als Nächstes fügen Sie NS-Gruppe-3 hinzu und legen NS-Gruppe-2 als Mitglied fest. NS-Gruppe-3 verfügt damit über das direkte Mitglied NS-Gruppe-2 sowie über die effektiven Mitglieder LogischerSwitch-1 und LogischerSwitch-2. Aus der Hauptgruppentabelle würde durch Klicken auf eine Gruppe und Auswählen der Option **Zugehörig > NS-Gruppen** NS-Gruppe-1, NS-Gruppe-2 und NS-Gruppe-3 angezeigt werden, da alle drei direkt oder indirekt LogischerSwitch-1 als Mitglied haben.
- Eine NS-Gruppe kann maximal 500 direkte Mitglieder enthalten.

- Der empfohlene Grenzwert für die Anzahl der effektiven Mitglieder in einer NS-Gruppe beträgt 5000. Der NSX Manager überprüft die NS-Gruppen zweimal täglich auf diesen Grenzwert, um 7:00 Uhr und um 19:00 Uhr. Wird der Grenzwert überschritten, beeinträchtigt dies nicht die Funktionalität, aber möglicherweise die Leistung.
- Wenn die Anzahl der effektiven Mitglieder einer NS-Gruppe 80 % von 5000 überschreitet, wird die Warnmeldung **NS-Gruppe XYZ ist im Begriff, die maximale Anzahl an Mitgliedern in einer NS-Gruppe zu überschreiten. Gesamtanzahl in NS-Gruppe ist...** in der Protokolldatei angezeigt. Wenn die Anzahl 5000 überschreitet, wird die Warnmeldung **„NS-Gruppe Xyz hat das maximale Zahlenlimit erreicht“** angezeigt. Die Gesamtzahl an Mitgliedern in der NS-Gruppe = ....
- Wenn die Anzahl der übersetzten VIFs/IPs/MACs in einer NS-Gruppe 5000 überschreitet, wird die Warnmeldung **Container XYZ hat die maximale Anzahl an IP-/MAC-/VIF-Übersetzungen erreicht. Aktuelle Anzahl der Übersetzungen im Container - IPs:..., MACs:..., VIFs:...** in der Protokolldatei angezeigt.
- Die maximal unterstützte Anzahl VMs ist 10.000.
- Sie können maximal 10.000 NS-Gruppen erstellen.

Für alle Objekte, die Sie einer NS-Gruppe als Mitglieder hinzufügen können, können Sie zum Bildschirm navigieren und die Option **Zugehörig > NS-Gruppen** auswählen.

#### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Bestandsliste > Gruppen > Hinzufügen** aus.
- 3 Geben Sie einen Namen für die NS-Gruppe ein.
- 4 (Optional) Geben Sie eine Beschreibung ein.
- 5 (Optional) Klicken Sie auf **Mitgliedschaftskriterien**.

Für jedes Kriterium können Sie bis zu fünf Regeln angeben, die mit dem logischen Operator AND kombiniert werden. Das verfügbare Mitgliedskriterium kann auf Folgendes angewendet werden:

- **Logischer Port** – kann ein Tag und optional den Geltungsbereich angeben.
- **Logischer Switch** – kann ein Tag und optional den Geltungsbereich angeben.
- **Virtuelle Maschine** – kann einen Namen, ein Tag, den Namen des Computerbetriebssystems oder einen Computernamen angeben, der bzw. das einer bestimmten Zeichenfolge entspricht, diese enthält, mit ihr beginnt oder endet oder nicht mit ihr übereinstimmt
- **Transportknoten** – kann einen Knotentyp angeben, der einem Edge-Knoten oder einem Hostknoten entspricht.

## 6 (Optional) Klicken Sie auf **Mitglieder**, um Mitglieder auszuwählen.

Die verfügbaren Mitgliedstypen sind:

- **AD-Gruppe** – NS-Gruppen mit AD-Gruppen können nur im Feld „Extended\_source“ einer verteilten Firewallregel verwendet werden und müssen die einzigen Mitglieder der Gruppe sein. Beispiel: Es kann keine NS-Gruppen mit sowohl einer AD-Gruppe als auch einem IP Set zusammen als Mitglieder geben.
- **IP Set** – kann sowohl IPv4- als auch IPv6-Adressen enthalten.
- **Logischer Port** – kann sowohl IPv4- als auch IPv6-Adressen enthalten.
- **Logischer Switch** – kann sowohl IPv4- als auch IPv6-Adressen enthalten.
- **MAC Set**
- **NS-Gruppe**
- **Transportknoten**
- **VIF**
- **Virtuelle Maschine**

## 7 Klicken Sie auf **HINZUFÜGEN**.

Die Gruppe wird zur Gruppentabelle hinzugefügt. Klicken Sie auf einen Gruppennamen, um eine Übersicht über Gruppeninformationen, einschließlich den Kriterien für Mitgliedschaft, Mitglieder, Anwendungen und verwandte Gruppen, anzuzeigen und diese zu bearbeiten. Scrollen Sie zum unteren Rand der Registerkarte **Übersicht**, um Tags hinzuzufügen und zu löschen. Weitere Informationen hierzu finden Sie unter [Hinzufügen von Tags zu einem Objekt](#). Bei der Auswahl von **Zugehörig> NS-Gruppen** werden alle NS-Gruppen, die die ausgewählte NS-Gruppe als Mitglied haben, angezeigt.

# Konfigurieren von Diensten und Dienstgruppen

Sie können einen NS-Dienst konfigurieren und Parameter für die Abstimmung des Netzwerkdatenverkehrs angeben, z. B. eine Port- und Protokollpaarbildung. Sie können mit einem NS-Dienst auch bestimmte Datenverkehrstypen in Firewallregeln zulassen oder blockieren.

Ein NS-Dienst kann zu einem der folgenden Typen gehören:

- Ethernet
- IP
- IGMP
- ICMP
- ALG
- L4-Port-Satz

Ein L4-Port-Satz unterstützt die Ermittlung von Quell- und Zielports. Sie können einzelne Ports oder einen Bereich von maximal 15 Ports angeben.

Ein NS-Dienst kann auch aus einer Gruppe anderer NS-Dienste bestehen. Ein NS-Dienst ist eine Gruppe, für die folgende Typen möglich sind:

- Schicht 2
- Schicht 3 und höher

Nach dem Erstellen eines NS-Dienstes kann der Typ nicht mehr geändert werden. Es sind einige vordefinierte NS-Dienste vorhanden. Diese können nicht geändert oder gelöscht werden.

## Erstellen eines NS-Dienstes

Sie können mit einem NS-Dienst die Merkmale für die Prüfung der Netzwerkübereinstimmung angeben oder den Typ des Datenverkehrs definieren, der in Firewallregeln blockiert oder zugelassen werden kann.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Bestandsliste > Dienste > Hinzufügen** aus.
- 3 Geben Sie einen Namen ein.
- 4 (Optional) Geben Sie eine Beschreibung ein.
- 5 Wenn Sie einen einzelnen Dienst konfigurieren möchte, wählen Sie **Protokoll festlegen** aus. Um eine Gruppe von NS-Diensten zu konfigurieren, wählen Sie **Vorhandene Dienste gruppieren** aus.
- 6 Für einen einzelnen Dienst müssen Sie einen Diensttyp und ein Dienstprotokoll auswählen. Es sind folgende Typen verfügbar: **Ethernet**, **IP**, **IGMP**, **ICMP**, **ALG** und **L4-Port-Satz**.
- 7 Für eine Dienstgruppe wählen Sie einen Typ und Mitglieder für die Gruppe aus. Es sind folgende Typen verfügbar: **Schicht 2** und **Schicht 3 und höher**.
- 8 Klicken Sie auf **HINZUFÜGEN**.

## Verwalten von Tags für eine virtuelle Maschine

Sie können die Liste der VMs in der Bestandsliste einsehen. Außerdem können Sie einer VM Tags hinzufügen, um die Suche zu vereinfachen.

### Verfahren

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

- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Bestand > Virtuelle Maschinen** aus dem Navigationsbereich aus.

Die Liste der VMs weist 4 Spalten auf: Virtuelle Maschine, Externe ID, Quelle und Tag. Klicken Sie auf das Filtersymbol in den ersten drei Spaltenüberschriften, um die Liste zu filtern. Geben Sie eine Zeichenfolge ein, um nach einer teilweisen Übereinstimmung zu filtern. Falls die Zeichenfolge in der Spalte die von Ihnen eingegebene Zeichenfolge enthält, wird der Eintrag angezeigt. Geben Sie eine Zeichenfolge in doppelten Anführungszeichen ein, um nach einer genauen Entsprechung zu filtern. Falls die Zeichenfolge in der Spalte genau mit der von Ihnen eingegebenen Zeichenfolge übereinstimmt, wird der Eintrag angezeigt.

- 3 Wählen Sie im Navigationsbereich die Option **Bestand > Virtuelle Maschinen** aus.
- 4 Wählen Sie eine VM aus.
- 5 Klicken Sie auf **TAGS VERWALTEN**.
- 6 Fügen Sie Tags hinzu bzw. löschen Sie Tags.


Option	Aktion
Tag hinzufügen	Klicken Sie auf <b>HINZUFÜGEN</b> , um ein Tag und optional einen Geltungsbereich anzugeben.
Tag löschen	Wählen Sie ein vorhandenes Tag aus und klicken Sie auf <b>LÖSCHEN</b> .

Die maximale Anzahl an Tags, die von NSX Manager einer virtuellen Maschine zugewiesen werden können, beträgt 25. Die maximale Anzahl an Tags für alle anderen verwalteten Objekte, wie logische Switches oder Ports, beträgt 30.

- 7 Klicken Sie auf **Speichern**.

Sie können DHCP über die Registerkarte **Netzwerk und Sicherheit – Erweitert** konfigurieren.

---

**Hinweis** Wenn Sie die Benutzeroberfläche **Netzwerk und Sicherheit – Erweitert** verwenden, um in der Richtlinienschnittstelle erstellte Objekte zu ändern, sind einige Einstellungen möglicherweise nicht konfigurierbar. Neben diesen schreibgeschützten Einstellungen wird dieses Symbol angezeigt: . Weitere Informationen hierzu finden Sie unter [Kapitel 1 Übersicht über NSX Manager](#).

---

Dieses Kapitel enthält die folgenden Themen:

- [DHCP](#)
- [Metadaten-Proxyserver](#)

## DHCP

Mit DHCP (Dynamic Host Configuration Protocol) können Clients die Netzwerkkonfiguration, wie IP-Adresse, Subnetzmaske, Standard-Gateway und DNS-Konfiguration, automatisch von einem DHCP-Server abrufen.

Sie können DHCP-Server erstellen, um DHCP-Anforderungen zu verarbeiten, und Sie können DHCP-Relay-Dienste erstellen, um DHCP-Datenverkehr auf externe DHCP-Server weiterzuleiten. Sie sollten jedoch nicht einen DHCP-Server auf einem logischen Switch und daneben einen DHCP-Relay-Dienst auf einem Router-Port konfigurieren, mit dem derselbe logische Switch verbunden ist. In einem solchen Szenario gehen DHCP-Anforderungen ausschließlich beim DHCP-Relay-Dienst ein.

Wenn Sie DHCP-Server konfigurieren, müssen Sie für verbesserte Sicherheit eine DFW-Regel konfigurieren, um Datenverkehr auf UDP-Ports 67 und 68 nur für gültige DHCP-Server-IP-Adressen zuzulassen.

---

**Hinweis** Eine DFW-Regel mit Logical Switch/Logical Port/NSGroup als Quelle und Any als Ziel, die zum Verwerfen von DHCP-Paketen für Ports 67 und 68 konfiguriert ist, blockiert keinen DHCP-Datenverkehr. Um DHCP-Datenverkehr zu blockieren, konfigurieren Sie Any als Quelle und als Ziel.

In dieser Version unterstützt der DHCP-Server kein Gast-VLAN-Tagging.

---



## Erstellen eines DHCP-Serverprofils

Ein DHCP-Serverprofil gibt einen NSX Edge-Cluster oder Mitglieder eines NSX Edge-Clusters an. Ein DHCP-Server mit diesem Profil bedient DHCP-Anforderungen von VMs auf logischen Switches, die mit den NSX Edge-Knoten verbunden sind, die im Profil angegeben wurden.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > DHCP > Server-Profile > Hinzufügen** aus.
- 3 Geben Sie einen Namen und optional eine Beschreibung ein.
- 4 Wählen Sie einen NSX Edge-Cluster im Dropdown-Menü aus.
- 5 (Optional) Wählen Sie die Mitglieder des NSX Edge-Clusters.  
Sie können bis zu zwei Mitglieder angeben.

### Nächste Schritte

Erstellen Sie einen DHCP-Server. Siehe [Erstellen eines DHCP-Servers](#).

## Erstellen eines DHCP-Servers

Sie können DHCP-Server erstellen, um DHCP-Anforderungen von VMs zu bedienen, die mit logischen Switches verbunden sind.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > DHCP > Server > Hinzufügen** aus.
- 3 Geben Sie einen Namen und optional eine Beschreibung ein.
- 4 Geben Sie die IP-Adresse des DHCP-Servers und die zugehörige Subnetzmaske im CIDR-Format ein.  
Geben Sie beispielsweise 192.168.1.2/24 ein.
- 5 (Erforderlich) Wählen Sie ein DHCP-Profil im Dropdown-Menü aus.
- 6 (Optional) Geben Sie gängige Optionen ein, wie Domänenname, Standard-Gateway, DNS-Server und Subnetzmaske.
- 7 (Optional) Geben Sie Optionen für klassenlose statische Routen ein.
- 8 (Optional) Geben Sie andere Optionen ein.
- 9 Klicken Sie auf **Speichern**.

- 10 Wählen Sie den neu erstellten DHCP-Server.
- 11 Blenden Sie den Abschnitt „IP-Pools“ ein.
- 12 Klicken Sie auf **Hinzufügen**, um IP-Bereiche, Standard-Gateway, Lease-Dauer, Warnungsschwellenwert, Fehlerschwellenwert, Option für klassenlose statische Route und weitere Optionen hinzuzufügen.
- 13 Blenden Sie den Abschnitt „Statische Bindungen“ ein.
- 14 Klicken Sie auf **Hinzufügen**, um statische Bindungen zwischen MAC-Adressen und IP-Adressen, Standard-Gateway, Hostname, Lease-Dauer, Option für klassenlose statische Route und weitere Optionen hinzuzufügen.

#### Nächste Schritte

Fügen Sie einen DHCP-Server einem logischen Switch hinzu. Siehe [Anfügen eines DHCP-Servers an einen logischen Switch](#).

## Anfügen eines DHCP-Servers an einen logischen Switch

Sie müssen einen DHCP-Server an einen logischen Switch anfügen, bevor der DHCP-Server DHCP-Anforderungen von mit dem Switch verbundenen VMs verarbeiten kann.

#### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > Switching** aus.
  - a Klicken Sie auf das Kontrollkästchen eines logischen Switches.
  - b Klicken Sie auf **Aktionen > DHCP-Server anhängen**.
- 3 Alternativ können Sie **Netzwerk und Sicherheit – Erweitert > DHCP** auswählen.
  - a Klicken Sie auf die Registerkarte **Server**.
  - b Klicken Sie auf das Kontrollkästchen eines DHCP-Servers.
  - c Klicken Sie auf **Aktionen > An logischen Switch anhängen**.

## Trennen eines DHCP-Servers von einem logischen Switch

Sie haben die Möglichkeit, einen DHCP-Server von einem logischen Switch zu trennen, um Ihre Umgebung neu zu konfigurieren.

#### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > Switching**.
- 3 Klicken Sie auf den logischen Switch, von dem ein DHCP-Server getrennt werden soll.

- 4 Klicken Sie auf **Aktionen > DHCP-Server trennen**.

## Erstellen eines DHCP-Relay-Profiles

Ein DHCP-Relay-Profil legt einen oder mehrere externe DHCP- oder DHCPv6-Server fest. Beim Erstellen eines DHCP-/DHCPv6-Relay-Dienstes müssen Sie ein DHCP-Relay-Profil angeben.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > DHCP > Relay-Profile > Hinzufügen** aus.
- 3 Geben Sie einen Namen und optional eine Beschreibung ein.
- 4 Geben Sie eine oder mehrere externe DHCP-/DHCPv6-Serveradressen ein.

### Nächste Schritte

Erstellen Sie einen DHCP-/DHCPv6-Relay-Dienst. Siehe [Erstellen eines DHCP-Relay-Dienstes](#).

## Erstellen eines DHCP-Relay-Dienstes

Sie können einen DHCP-Relay-Dienst erstellen, mit dem sich der Datenverkehr zwischen DHCP-Clients und DHCP-Servern weiterleiten lässt, die nicht in NSX-T Data Center erstellt wurden.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > DHCP > Relay-Dienste > Hinzufügen** aus.
- 3 Geben Sie einen Namen und optional eine Beschreibung ein.
- 4 Wählen Sie ein DHCP-Relay-Profil im Dropdown-Menü aus.

### Nächste Schritte

Hinzufügen eines DHCP-Dienstes zu einem Logical Router Port Siehe [Hinzufügen eines DHCP-Relay-Dienstes zu einem Port für einen logischen Router](#).

## Hinzufügen eines DHCP-Relay-Dienstes zu einem Port für einen logischen Router

Sie können einen DHCP-Relay-Dienst zu einem Port für einen logischen Router hinzufügen. VMs auf dem logischen Switch, der mit diesem Port verbunden ist, können mit den DHCP-Servern kommunizieren, die im Relay-Dienst konfiguriert sind.

## Voraussetzungen

- Stellen Sie sicher, dass Sie über einen konfigurierten DHCP-Relay-Dienst verfügen. Siehe [Erstellen eines DHCP-Relay-Dienstes](#).
- Stellen Sie sicher, dass der Router-Port den Typ **Downlink** aufweist.

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.
- 3 Wählen Sie den entsprechenden Router aus, um weitere Informationen und Konfigurationsoptionen anzuzeigen.
- 4 Wählen Sie **Konfiguration > Router-Ports** aus.
- 5 Wählen Sie den Router-Port aus, der mit dem gewünschten logischen Switch eine Verbindung herstellt, und klicken Sie auf **Bearbeiten**.
- 6 Wählen Sie einen DHCP-Relay-Dienst aus der Dropdown-Liste **Relay-Dienst** aus und klicken Sie auf **Speichern**.

Sie haben auch die Möglichkeit, einen DHCP-Relay-Dienst beim Hinzufügen eines neuen Ports für einen logischen Router auszuwählen.

## Löschen einer DHCP-Lease

In einigen Situationen möchten Sie möglicherweise eine DHCP-Lease löschen. Beispielsweise, wenn ein DHCP-Client eine andere IP-Adresse erhalten soll oder wenn ein Client heruntergefahren wird, ohne seine IP-Adresse freizugeben, und Sie möchten, dass die Adresse anderen Clients zur Verfügung steht.

Sie können die folgende API verwenden, um eine DHCP-Lease zu löschen:

```
DELETE /api/v1/dhcp/servers/<server-id>/leases?ip=<ip>&mac=<mac>
```

Um sicherzustellen, dass die richtige Lease gelöscht wird, rufen Sie die folgende API vor und nach der DELETE-API auf:

```
GET /api/v1/dhcp/servers/<server-id>/leases
```

Stellen Sie nach dem Aufruf der DELETE-API sicher, dass die Ausgabe der GET-API nicht die Lease anzeigt, die gelöscht wurde.

Weitere Informationen finden Sie in der *Referenz zur NSX-T Data Center-API*.

## Metadaten-Proxyserver

Mit einem Metadaten-Proxyserver können VM-Instanzen instanzenspezifische Metadaten von einem OpenStack Nova-API-Server abrufen.

Die folgenden Schritte beschreiben die Funktionsweise eines Proxy-Servers:

- 1 Eine VM sendet einen HTTP GET-Befehl an `http://169.254.169.254:80` zur Anforderung einiger Metadaten.
- 2 Der Metadaten-Proxyserver, der mit demselben logischen Switch verbunden ist wie die VM, liest die Anforderung, führt die erforderlichen Änderungen an den Kopfzeilen durch und leitet die Anforderung an den Nova-API-Server weiter.
- 3 Der Nova-API-Server fordert Informationen über die VM vom Neutron-Server an und erhält diese vom Neutron-Server.
- 4 Der Nova-API-Server übernimmt die Metadaten und sendet diese an den Metadaten-Proxyserver.
- 5 Der Metadaten-Proxyserver leitet die Metadaten an die VM weiter.

Ein Metadaten-Proxyserver wird auf einem NSX Edge-Knoten ausgeführt. Für eine Hochverfügbarkeit können Sie den Metadaten-Proxy-Server zur Ausführung auf zwei oder mehr NSX Edge-Knoten in einem NSX Edge-Cluster konfigurieren.

## Hinzufügen eines Metadaten-Proxyservers

Über einen Metadaten-Proxyserver können VMs Metadaten aus einem OpenStack Nova-API-Server abrufen.

### Voraussetzungen

Stellen Sie sicher, dass Sie einen NSX Edge-Cluster erstellt haben. Weitere Informationen finden Sie unter *Installationshandbuch für NSX-T Data Center*.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > DHCP > Metadaten-Proxys > Hinzufügen** aus.
- 3 Geben Sie einen Namen für den Metadaten-Proxyserver ein.
- 4 (Optional) Geben Sie eine Beschreibung ein.
- 5 Geben Sie die URL und den Port für den Nova-Server ein.  
Der gültige Portbereich lautet 3000–9000.
- 6 Geben Sie einen Wert für **Geheimer Schlüssel** ein.
- 7 Wählen Sie einen NSX Edge-Cluster in der Dropdown-Liste aus.
- 8 (Optional) Wählen Sie die Mitglieder des NSX Edge-Clusters.

### Nächste Schritte

Verknüpfen Sie den Metadaten-Proxyserver mit einem logischen Switch.

## Anfügen eines Metadaten-Proxyserver an einen logischen Switch

Um Metadaten-Proxydienste für VMs zur Verfügung zu stellen, die mit einem logischen Switch verbunden sind, müssen Sie an den Switch einen Metadaten-Proxyserver anfügen.

### Voraussetzungen

Stellen Sie sicher, dass ein logischer Switch erstellt wurde. Weitere Informationen finden Sie unter [Erstellen eines logischen Switches](#).

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > DHCP > Metadaten-Proxys** aus.
- 3 Wählen Sie einen Metadaten-Proxyserver aus.
- 4 Wählen Sie die Menüoption **Aktionen > An logischen Switch anhängen** aus.
- 5 Wählen Sie in der Dropdown-Liste einen logischen Switch aus.

### Ergebnisse

Sie haben auch die Möglichkeit, einen Metadaten-Proxyserver durch Aufrufen von **Switching > Switches** und Auswählen eines Switch sowie der Menüoption **Aktionen > Metadaten-Proxyserver anfügen** an einen logischen Switch anzufügen.

## Trennen eines Metadaten-Proxy-Servers von einem logischen Switch

Wenn Sie keine Metadaten-Proxyserver mehr für VMs bereitstellen möchten, die mit einem logischen Switch verbunden sind, oder einen anderen Metadaten-Proxyserver verwenden möchten, können Sie einen Metadaten-Proxyserver von einem logischen Switch trennen.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > DHCP > Metadaten-Proxys** aus.
- 3 Wählen Sie einen Metadaten-Proxyserver aus.
- 4 Wählen Sie die Menüoption **Aktionen > Von logischem Switch trennen**.
- 5 Wählen Sie in der Dropdown-Liste einen logischen Switch aus.

## Ergebnisse


Sie können einen Metadaten-Proxyserver auch von einem logischen Switch trennen, indem Sie zu **Switching > Switches** navigieren, einen Switch auswählen und die Menüoption **Aktionen > Metadaten-Proxy trennen** wählen.

# Erweiterte IP-Adressverwaltung

# 18

Mit der IP-Adressverwaltung (IPAM) können IP-Blöcke zur Unterstützung von NSX Container Plug-in (NCP) erstellen. Weitere Informationen über NCP finden Sie im *Installations- und Administratorhandbuch zum NSX-T Container Plug-in für Kubernetes*.

---

**Hinweis** Wenn Sie die Benutzeroberfläche **Netzwerk und Sicherheit – Erweitert** verwenden, um in der Richtlinienchnittstelle erstellte Objekte zu ändern, sind einige Einstellungen möglicherweise nicht konfigurierbar. Neben diesen schreibgeschützten Einstellungen wird dieses Symbol angezeigt: . Weitere Informationen hierzu finden Sie unter [Kapitel 1 Übersicht über NSX Manager](#).

---

Dieses Kapitel enthält die folgenden Themen:

- [Verwalten von IP-Blöcken](#)
- [Verwalten von Subnetzen für IP-Blöcke](#)

## Verwalten von IP-Blöcken

Für das Einrichten von NSX Container Plug-in müssen Sie IP-Blöcke für die Container erstellen.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > IPAM** aus.
- 3 Um einen IP-Block hinzuzufügen, klicken Sie auf **Hinzufügen**.
  - a Geben Sie einen Namen und optional eine Beschreibung ein.
  - b Geben Sie einen IP-Block im CIDR-Format ein. Beispiel: 10.10.10.0/24.
- 4 Um einen IP-Block zu bearbeiten, klicken Sie auf den Namen des IP-Blocks.
  - a Klicken Sie auf der Registerkarte **Übersicht** auf **Bearbeiten**.  
Sie können den Namen, die Beschreibung oder den IP-Block-Wert ändern.



- 5 Um die Tags eines IP-Blocks zu verwalten, klicken Sie auf den Namen des IP-Blocks.
  - a Klicken Sie auf der Registerkarte **Übersicht** auf **Verwalten**.  
Sie können Tags hinzufügen oder löschen.
- 6 Um einen oder mehrere IP-Blöcke zu löschen, wählen Sie die Blöcke aus.
  - a Klicken Sie auf **Löschen**.  
IP-Blöcke, denen ein Subnetz zugewiesen wurde, können nicht gelöscht werden.

## Verwalten von Subnetzen für IP-Blöcke

Sie können Subnetze für IP-Blöcke hinzufügen oder löschen.

### Verfahren


- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > IPAM** aus.
- 3 Klicken Sie auf den Namen eines IP-Blocks.
- 4 Klicken Sie auf die Registerkarte **Subnetze**.
- 5 Um ein Subnetz hinzuzufügen, klicken Sie auf **Hinzufügen**.
  - a Geben Sie einen Namen und optional eine Beschreibung ein.
  - b Geben Sie die Größe des Subnetzes ein.
- 6 Um ein oder mehrere Subnetze zu löschen, wählen Sie die Subnetze aus.
  - a Klicken Sie auf **Löschen**.

# Erweitertes Load Balancing

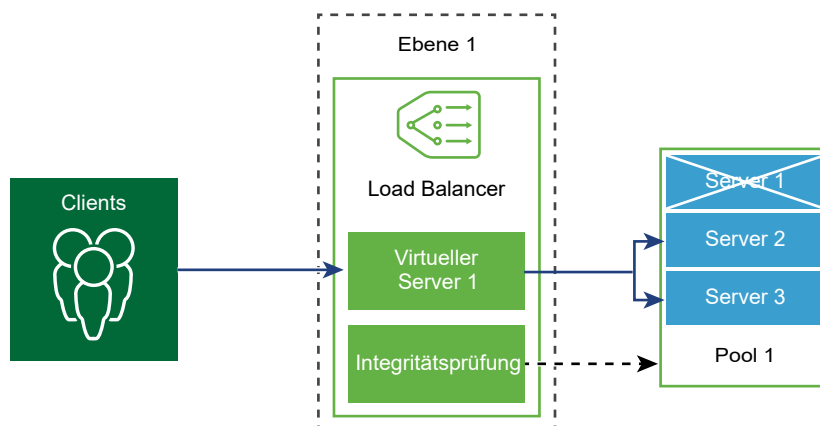
# 19

Diese Informationen beziehen sich auf die Load Balancing-Konfiguration von NSX-T Data Center, die auf der Registerkarte **Netzwerk und Sicherheit – Erweitert** zu finden ist.

Informationen zum NSX Advanced Load Balancer (AVI-Netzwerke) finden Sie unter <https://www.vmware.com/products/nsx-advanced-load-balancer.html>.

**Hinweis** Wenn Sie die Benutzeroberfläche **Netzwerk und Sicherheit – Erweitert** verwenden, um in der Richtlinienchnittstelle erstellte Objekte zu ändern, sind einige Einstellungen möglicherweise nicht konfigurierbar. Neben diesen schreibgeschützten Einstellungen wird dieses Symbol angezeigt: . Weitere Informationen hierzu finden Sie unter [Kapitel 1 Übersicht über NSX Manager](#).

Der logische NSX-T Data Center-Load Balancer bietet einen Hochverfügbarkeitsdienst für Anwendungen und verteilt die Datenverkehrslast im Netzwerk auf mehrere Server.



Der Load Balancer verteilt eingehende Dienstanforderungen über mehrere Server gleichmäßig auf eine Weise, dass die Lastverteilung für die Benutzer transparent ist. Das Load Balancing trägt dazu dabei, optimale Ressourcennutzung, maximalen Durchsatz und minimale Reaktionszeit zu erreichen sowie Überlastung zu vermeiden.

Sie können eine virtuelle IP-Adresse mehreren Poolservern für Load Balancing zuordnen. Der Load Balancer akzeptiert TCP-, UDP-, HTTP- oder HTTPS-Anforderungen über die virtuelle IP-Adresse und entscheidet, welcher Poolserver verwendet werden soll.

Abhängig von den Umgebungsanforderungen können Sie die Load Balancer-Leistung skalieren, indem Sie die Anzahl der vorhandenen virtuellen Server und Poolmitglieder zur Verarbeitung hoher Datenverkehrslasten erhöhen.

---

**Hinweis** Der logische Load Balancer wird nur vom logischen Tier-1-Router unterstützt. Ein Load Balancer kann nur an einen logischen Tier-1-Router angehängt werden.

---

Dieses Kapitel enthält die folgenden Themen:

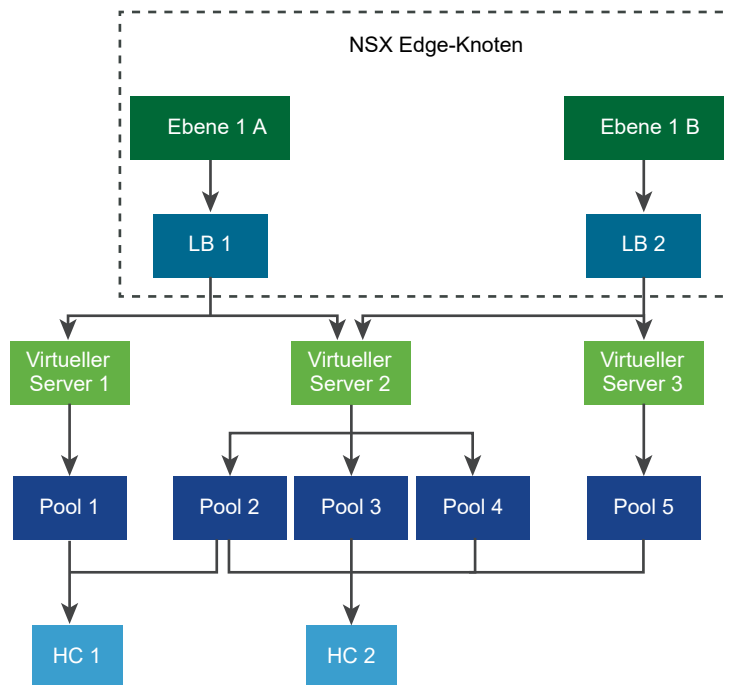
- [Wichtige Load Balancer-Konzepte](#)
- [Konfigurieren von Load Balancer-Komponenten](#)

## Wichtige Load Balancer-Konzepte

Der Load Balancer beinhaltet virtuelle Server, Serverpools und Systemdiagnoseüberwachungen.

Ein Load Balancer ist mit einem logischen Tier-1-Router verbunden. Der Load Balancer hostet einen einzelnen oder mehrere virtuelle Server. Bei einem virtuellen Server handelt es sich um einen Anwendungsdienst, der durch eine eindeutige Kombination aus IP, Port und Protokoll dargestellt wird. Der virtuelle Server ist einem einzelnen Serverpool oder mehreren Serverpools zugeordnet. Ein Serverpool besteht aus einer Gruppe von Servern. Die Serverpools enthalten einzelne Mitglieder des Serverpools.

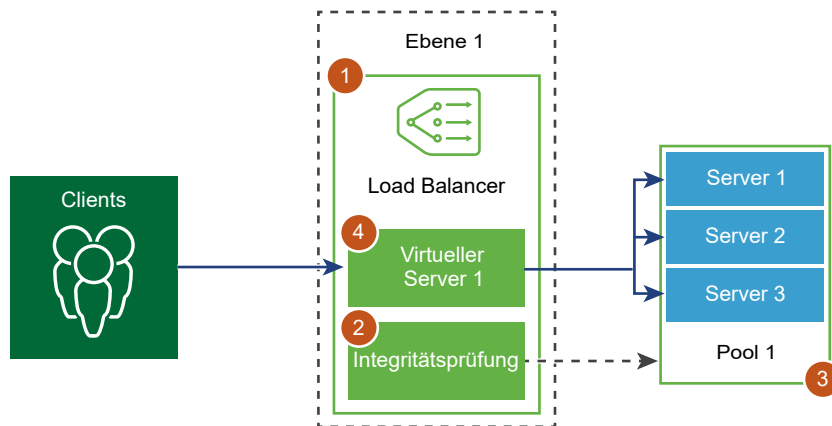
Wenn Sie die ordnungsgemäße Ausführung der Anwendung auf jedem Server prüfen möchten, können Sie Systemdiagnoseüberwachungen hinzufügen, die den Systemzustand eines Servers überprüfen.



## Konfigurieren von Load Balancer-Komponenten

Zur Verwendung logischer Load Balancer müssen Sie zuerst einen Load Balancer konfigurieren und an einen logischen Tier-1-Router anhängen.

Im nächsten Schritt können Sie die Überwachung der Integritätsprüfung für Ihre Server einrichten. In diesem Fall müssen Sie Serverpools für den Load Balancer konfigurieren. Im letzten Schritt müssen Sie einen virtuellen Server der Schicht 4 oder 7 für den Load Balancer erstellen.

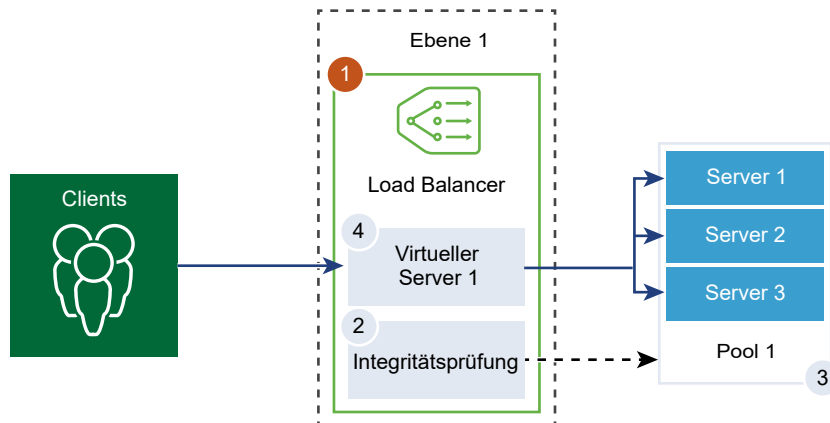


## Erstellen eines Load Balancers

Der Load Balancer wird erstellt und an einen logischen Tier-1-Router angehängt.

Sie können die Ebene der Fehlermeldungen konfigurieren, die vom Load Balancer zum Fehlerprotokoll hinzugefügt werden soll.

**Hinweis** Setzen Sie für Load Balancer mit erheblichem Datenverkehr die Protokollebene nicht auf DEBUG, da aufgrund der hohen Anzahl der in das Protokoll geschriebenen Meldungen die Leistung beeinträchtigt wird.



### Voraussetzungen

Stellen Sie sicher, dass ein logischer Tier-1-Router konfiguriert wurde. Siehe [Erstellen eines logischen Tier-1-Routers](#).

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > Load Balancer > Hinzufügen**.
- 3 Geben Sie einen Namen und eine Beschreibung für den Load Balancer ein.
- 4 Wählen Sie auf Basis der verfügbaren Ressourcen die Größe des virtuellen Servers und die Anzahl der Poolmitglieder für den Load Balancer aus.
- 5 Definieren Sie den Schweregrad des Eintrags im Fehlerprotokolls über das Dropdown-Menü.  
Der Load Balancer erfasst Informationen über aufgetretene Probleme verschiedener Schweregrade im Fehlerprotokoll.
- 6 Klicken Sie auf **OK**.
- 7 Verknüpfen Sie den neu erstellten Load Balancer mit einem virtuellen Server.
  - a Wählen Sie den Load Balancer aus und klicken Sie auf **Aktionen > An einen virtuellen Server anhängen**.
  - b Wählen Sie im Dropdown-Menü einen vorhandenen virtuellen Server aus.
  - c Klicken Sie auf **OK**.

- 8 Hängen Sie den neu erstellten Load Balancer an einen logischen Tier-1-Router an.
  - a Wählen Sie den Load Balancer aus und klicken Sie auf **Aktionen > Anhängen an einen logischen Router**.
  - b Wählen Sie im Dropdown-Menü einen vorhandenen logischen Tier-1-Router aus.  
Der Tier-1-Router muss im Modus „Aktiv/Standby“ ausgeführt werden.
  - c Klicken Sie auf **OK**.
- 9 (Optional) Löschen Sie den Load Balancer.  
Wenn Sie diesen Load Balancer nicht mehr verwenden möchten, müssen Sie den Load Balancer zuerst vom virtuellen Server und logischen Tier-1-Router trennen.

## Konfigurieren einer aktiven Systemzustandsüberwachung

Mit der aktiven Systemzustandsüberwachung können Sie testen, ob ein Server verfügbar ist. Die aktive Systemzustandsüberwachung verwendet verschiedene Arten von Tests zur Überwachung des Anwendungszustands, wie z. B. das Senden eines einfachen Pings an Server oder erweiterte HTTP-Anfragen.

Server, die innerhalb eines bestimmten Zeitraums nicht oder mit Fehlern reagieren, werden solange aus der künftigen Verbindungsverarbeitung ausgeschlossen, bis durch eine nachträgliche regelmäßig durchgeführte Systemdiagnose sichergestellt wird, dass die betreffenden Server ordnungsgemäß ausgeführt werden.

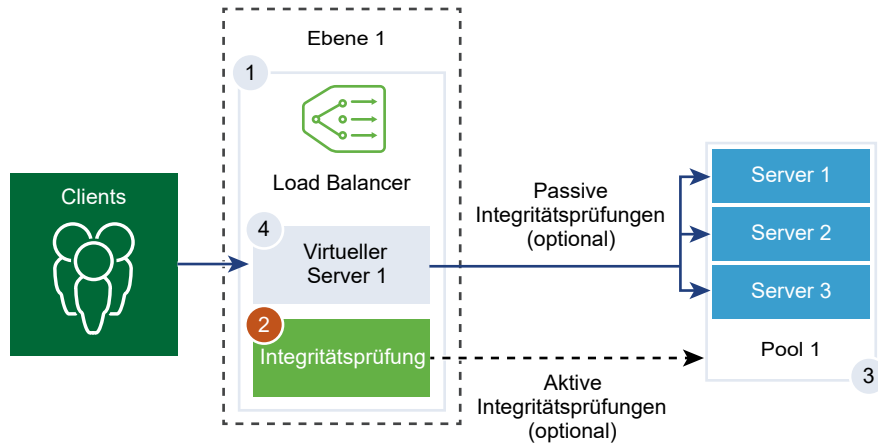
Aktive Systemdiagnosen werden auf Serverpoolmitgliedern durchgeführt, nachdem das Poolmitglied an einen virtuellen Server und dieser virtuelle Server dann an ein Tier-1-Gateway (zuvor als logischer Tier-1-Router bezeichnet) angehängt wurde.

Wenn das Tier-1-Gateway mit einem Tier-0-Gateway verbunden ist, wird ein Routerlinkport erstellt und seine IP-Adresse (normalerweise im Format 100.64.x.x) wird verwendet, um die Integritätsprüfung für den Load Balancer durchzuführen. Wenn das Tier-1-Gateway eigenständig ist (nur über einen zentralisierten Dienstport verfügt und nicht mit einem Tier-0-Gateway verbunden ist), wird die IP-Adresse des zentralisierten Dienstports verwendet, um die Integritätsprüfung für den Load Balancer durchzuführen. Informationen zu eigenständigen Tier-1-Gateways finden Sie unter [Erstellen eines eigenständigen logischen Tier-1-Routers](#).

---

**Hinweis** Pro Serverpool kann genau eine aktive Systemzustandsüberwachung konfiguriert werden.

---



## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > Load Balancer > Überwachungen > Aktive Integritätsüberwachungen > Hinzufügen**.
- 3 Geben Sie einen Namen und eine Beschreibung für die aktive Systemzustandsüberwachung ein.
- 4 Wählen Sie im Dropdown-Menü ein Systemdiagnoseprotokoll für den Server aus.  
Sie können auch vordefinierte Protokolle in NSX Manager verwenden: `http-monitor`, `https-monitor`, `Icmp-monitor`, `Tcp-monitor` und `Udp-monitor`.
- 5 Legen Sie den Wert des Überwachungsports fest.
- 6 Konfigurieren Sie die Werte zum Überwachen eines Dienstpools.  
Sie können auch die Standardwerte der aktiven Systemzustandsüberwachung übernehmen.

Option	Beschreibung
<b>Überwachungsintervall</b>	Geben Sie den Zeitraum in Sekunden an, nach dem von der Überwachung eine weitere Verbindungsanfrage an den Server gesendet wird.
<b>Fehleranzahl</b>	Legen Sie einen Wert fest. Wenn die aufeinander folgenden Fehler diesen Wert erreichen, wird der Server als vorübergehend nicht verfügbar betrachtet.
<b>Anzahl bis zum erneuten Versuch</b>	Legen Sie einen Wert fest, der angibt, nach welcher Zeit ein erneuter Verbindungsversuch mit dem Server unternommen wird, um herauszufinden, ob er verfügbar ist.
<b>Zeitüberschreitung</b>	Legen Sie fest, wie oft der Server getestet wird, bevor er als INAKTIV angesehen wird.

Wenn das Überwachungsintervall beispielsweise auf 5 Sekunden und das Zeitlimit auf 15 Sekunden festgelegt ist, sendet der Load Balancer alle 5 Sekunden Anfragen an den Server. Wenn die erwartete Antwort innerhalb von 15 Sekunden vom Server empfangen wird, lautet das Ergebnis der Systemdiagnose „OK“. Ist dies nicht der Fall, lautet das Ergebnis KRITISCH. Wenn die letzten drei Systemdiagnosen alle AKTIV ergeben haben, wird der Server als AKTIV gekennzeichnet.

- 7 Wenn Sie HTTP als Protokoll für die Systemdiagnose auswählen, geben Sie die folgenden Informationen an.

Option	Beschreibung
<b>HTTP-Methode</b>	Wählen Sie die Methode zur Erkennung des Serverstatus (GET, OPTIONS, POST, HEAD und PUT) im Dropdown-Menü aus.
<b>HTTP-Anforderungs-URL</b>	Geben Sie die Anforderungs-URI für die Methode ein.
<b>HTTP-Anforderungsversion</b>	Wählen Sie die unterstützte Anforderungsversion im Dropdown-Menü aus. Sie können auch die Standardversion HTTP_VERSION_1_1 übernehmen.
<b>HTTP-Anforderungstext</b>	Geben Sie den Anforderungstext ein. Gültig für die Methoden POST und PUT.
<b>HTTP-Antwortcode</b>	Geben Sie die Zeichenfolge, die bei der Überprüfung als Übereinstimmung erwartet wird, in der Statuszeile des HTTP-Antworttexts ein. Der Antwortcode ist eine durch Komma getrennte Liste. Beispiel: 200,301,302,401.
<b>HTTP-Antworttext</b>	Wenn der HTTP-Antworttext und der HTTP-Antworttext der Systemdiagnose übereinstimmen, wird der Server als fehlerfrei betrachtet.

- 8 Wenn Sie HTTPS als Protokoll für die Systemdiagnose auswählen, geben Sie die folgenden Informationen an.

- a Wählen Sie die SSL-Protokollliste aus.

Die TLS-Versionen TLS1.1 und TLS1.2 werden unterstützt und sind standardmäßig aktiviert. TLS1.0 wird unterstützt, ist aber standardmäßig deaktiviert.

- b Klicken Sie auf den Pfeil und verschieben Sie die Protokolle in den ausgewählten Abschnitt.



- c Weisen Sie eine SSL-Standardverschlüsselung zu oder erstellen Sie eine benutzerdefinierte SSL-Verschlüsselung.
- d Geben Sie die folgenden Details für HTTP als Protokoll für die Systemdiagnose ein.

Option	Beschreibung
<b>HTTP-Methode</b>	Wählen Sie die Methode zur Erkennung des Serverstatus im Dropdown-Menü aus: GET, OPTIONS, POST, HEAD und PUT.
<b>HTTP-Anforderungs-URL</b>	Geben Sie die Anforderungs-URI für die Methode ein.
<b>HTTP-Anforderungsversion</b>	Wählen Sie die unterstützte Anforderungsversion im Dropdown-Menü aus. Sie können auch die Standardversion HTTP_VERSION_1_1 übernehmen.
<b>HTTP-Anforderungstext</b>	Geben Sie den Anforderungstext ein. Gültig für die Methoden POST und PUT.
<b>HTTP-Antwortcode</b>	Geben Sie die Zeichenfolge, die bei der Überprüfung als Übereinstimmung erwartet wird, in der Statuszeile des HTTP-Antworttexts ein. Der Antwortcode ist eine durch Komma getrennte Liste. Beispiel: 200,301,302,401.
<b>HTTP-Antworttext</b>	Wenn der HTTP-Antworttext und der HTTP-Antworttext der Systemdiagnose übereinstimmen, wird der Server als fehlerfrei betrachtet.

- 9 Wenn Sie ICMP als Protokoll für die Systemdiagnose auswählen, weisen Sie die Datengröße des Pakets für die ICMP-Systemdiagnose in Byte zu.
- 10 Wenn Sie TCP als Protokoll für die Systemdiagnose auswählen, können Sie die Parameter leer lassen.

Wenn sowohl gesendete als auch erwartete Daten nicht aufgelistet werden, wird eine TCP-Verbindung mit Dreizeige-Handshake eingerichtet, um den Zustand des Servers zu überprüfen. Keine Daten werden gesendet. Bei den erwarteten Daten (falls aufgelistet) muss es sich um eine Zeichenfolge an einer beliebigen Stelle in der Antwort handeln. Reguläre Ausdrücke werden nicht unterstützt.

- 11 Wenn Sie UDP als Protokoll für die Systemdiagnose auswählen, geben Sie die folgenden Informationen an.

Erforderliche Option	Beschreibung
<b>Gesendete UDP-Daten</b>	Geben Sie die Zeichenfolge ein, die nach dem Verbindungsaufbau an den Server gesendet werden soll.
<b>Erwartete UDP-Daten</b>	Geben Sie die Zeichenfolge ein, die vom Server gesendet werden soll. Der Server wird nur dann als AKTIV eingestuft, wenn die empfangene Zeichenfolge mit dieser Definition übereinstimmt.

- 12 Klicken Sie auf **Fertigstellen**.

## Nächste Schritte

Verknüpfen Sie die aktive Systemzustandsüberwachung mit einem Serverpool. Siehe [Hinzufügen eines Serverpools für das Load Balancing](#).

## Konfigurieren von passiven Systemzustandsüberwachungen

Load Balancer führen passive Systemdiagnosen durch, um Fehler bei Clientverbindungen zu überwachen und Server, die durchgängig Fehler verursachen, als INAKTIV zu markieren.

Die passive Systemdiagnose überwacht den Clientdatenverkehr, der durch den Load Balancer geleitet wird, auf Fehler. Wenn ein Poolmitglied beispielsweise als Reaktion auf eine Clientverbindung ein TCP Reset (RST) sendet, erkennt der Load Balancer diesen Fehler. Treten mehrere aufeinander folgende Fehler auf, sieht der Load Balancer dieses Mitglied des Serverpools als vorübergehend nicht verfügbar an und sendet eine Weile keine Verbindungsanforderungen mehr an dieses Poolmitglied. Nach einem gewissen Zeitraum sendet der Load Balancer eine Verbindungsanforderung, um zu überprüfen, ob das Poolmitglied wiederhergestellt wurde. Wenn diese Verbindung erfolgreich hergestellt werden kann, wird das Poolmitglied als fehlerfrei angesehen. Andernfalls wartet der Load Balancer eine Zeit lang und versucht es dann erneut.

Die passive Systemdiagnose sieht die folgenden Szenarien als Fehler im Clientdatenverkehr an:

- Wenn bei Serverpools, die virtuellen Servern der Schicht 7 zugeordnet sind, die Verbindung zum Poolmitglied fehlschlägt. Sendet das Poolmitglied beispielsweise ein TCP RST, während der Load Balancer versucht, eine Verbindung herzustellen oder ein SSL-Handshake durchzuführen, schlägt das Poolmitglied fehl.
- Wenn bei Serverpools, die virtuellen TCP-Servern der Schicht 4 zugeordnet sind, das Poolmitglied ein TCP RST als Reaktion auf ein TCP SYN des Clients sendet oder überhaupt nicht reagiert.
- Wenn bei Serverpools, die virtuellen UDP-Servern der Schicht 4 zugeordnet sind, ein Port nicht erreichbar ist oder eine ICMP-Fehlermeldung bezüglich eines nicht erreichbaren Ziels als Reaktion auf ein UDP-Clientpaket empfangen wird.

Bei Serverpools, die virtuellen Servern der Schicht 7 zugeordnet sind, wird die Anzahl der fehlgeschlagenen Verbindungen erhöht, wenn TCP-Verbindungsfehler, z. B. TCP-RST-Fehler beim Senden von Daten, oder SSL-Handshake-Fehler auftreten.

Wenn in Serverpools, die virtuellen Servern der Schicht 4 zugeordnet sind, keine Antwort auf ein an das Mitglied des Serverpools gesendetes TCP SYN eingeht oder ein TCP RST als Reaktion auf ein TCP SYN empfangen wird, wird das Mitglied des Serverpools als INAKTIV angesehen. Die Fehleranzahl wird entsprechend erhöht.

Wenn bei virtuellen UDP-Servern der Schicht 4 ein ICMP-Fehler, beispielsweise eine Meldung über einen nicht erreichbaren Port oder ein nicht erreichbares Ziel, als Reaktion auf Clientdatenverkehr empfangen wird, wird der Server als INAKTIV angesehen.

---

**Hinweis** Pro Serverpool kann eine passive Systemzustandsüberwachung konfiguriert werden.

---

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > Load Balancer > Überwachungen > Passive Integritätsüberwachungen > Hinzufügen**.
- 3 Geben Sie einen Namen und eine Beschreibung für die passive Systemzustandsüberwachung ein.
- 4 Konfigurieren Sie die Werte zum Überwachen eines Dienstpools.

Sie können auch die Standardwerte der aktiven Systemzustandsüberwachung übernehmen.

Option	Beschreibung
<b>Fehleranzahl</b>	Legen Sie einen Wert fest. Wenn die aufeinander folgenden Fehler diesen Wert erreichen, wird der Server als vorübergehend nicht verfügbar betrachtet.
<b>Zeitüberschreitung</b>	Legen Sie fest, wie oft der Server getestet wird, bevor er als INAKTIV angesehen wird.

Wenn die aufeinander folgenden Fehler beispielsweise den konfigurierten Wert 5 erreicht haben, wird dieses Mitglied 5 Sekunden lang als vorübergehend nicht verfügbar angesehen. Nach Ablauf dieses Zeitraums wird wieder versucht, eine neue Verbindung mit diesem Mitglied herzustellen, um seine Verfügbarkeit zu prüfen. Bei einer erfolgreichen Verbindung wird das Mitglied als verfügbar angesehen, und die Fehleranzahl wird auf Null gesetzt. Schlägt diese Verbindung jedoch fehl, wird das Mitglied während eines weiteren 5 Sekunden langen Zeitüberschreitungsintervalls nicht verwendet.

- 5 Klicken Sie auf **OK**.

## Nächste Schritte

Verknüpfen Sie die passive Systemzustandsüberwachung mit einem Serverpool. Siehe [Hinzufügen eines Serverpools für das Load Balancing](#).

## Hinzufügen eines Serverpools für das Load Balancing

Ein Serverpool besteht aus einem oder mehreren Servern, die konfiguriert sind und die gleiche Anwendung ausführen. Ein einzelner Pool kann virtuellen Servern der Schicht 4 und 7 zugeordnet werden.

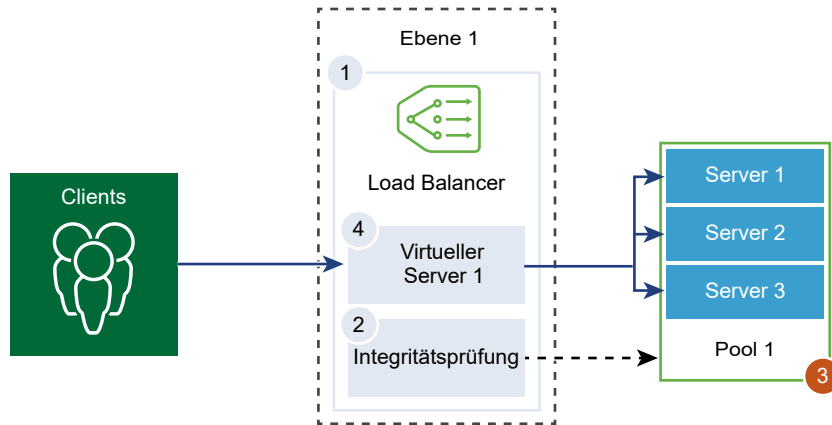
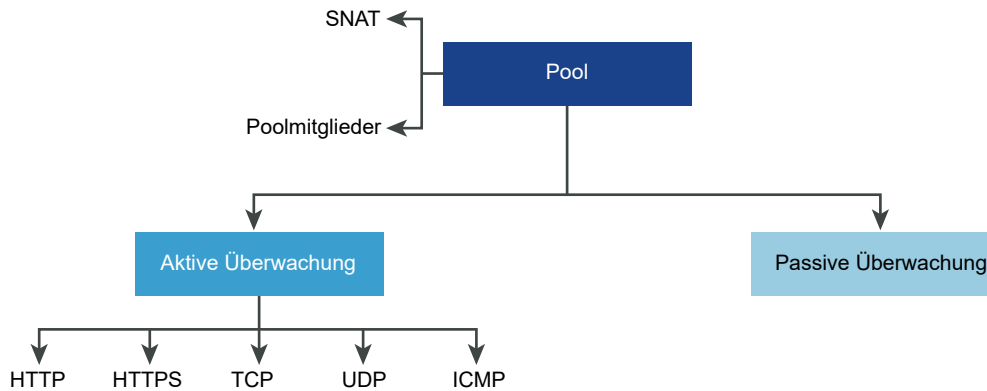


Abbildung 19-1. Konfiguration der Serverpool-Parameter



### Voraussetzungen

- Wenn Sie dynamische Poolmitglieder verwenden, muss eine NSGroup konfiguriert werden. Siehe [Erstellen einer NS-Gruppe](#).
- Stellen Sie je nach verwendeter Überwachung sicher, dass aktive oder passive Systemzustandsüberwachungen konfiguriert sind. Siehe [Konfigurieren einer aktiven Systemzustandsüberwachung](#) oder [Konfigurieren von passiven Systemzustandsüberwachungen](#).

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > Load Balancer > Serverpools > Hinzufügen**.
- 3 Geben Sie einen Namen und eine Beschreibung für den Load Balancer-Pool ein. Optional können Sie die vom Serverpool verwalteten Verbindungen beschreiben.

#### 4 Wählen Sie die Algorithmus-Ausgleichsmethode für den Serverpool aus.

Der Load Balancing-Algorithmus steuert, wie die eingehenden Verbindungen zwischen den Mitgliedern verteilt werden. Der Algorithmus kann direkt auf einem Serverpool oder einem Server verwendet werden.

Alle Load Balancing-Algorithmen überspringen Server, die eine der folgenden Bedingungen erfüllen:

- Admin-Zustand ist auf DISABLED festgelegt.
- Admin-Zustand ist auf GRACEFUL\_DISABLED und keinen übereinstimmenden Persistenzeintrag festgelegt.
- Zustand der aktiven oder passiven Systemdiagnose ist DOWN.
- Verbindungsgrenzwert für die maximale Anzahl gleichzeitiger Verbindungen des Serverpools ist erreicht.

Option	Beschreibung
<b>ROUND_ROBIN</b>	Eingehende Clientanforderungen werden durch eine Liste verfügbarer Server geleitet, die in der Lage sind, die Anforderung zu bearbeiten. Ignoriert die Gewichtungen der Serverpoolmitglieder, auch wenn sie konfiguriert sind.
<b>WEIGHTED_ROUND_ROBIN</b>	Jedem Server wird ein Gewichtungswert zugewiesen, der angibt, wie sich dieser Server im Vergleich zu anderen Servern im Pool verhält. Der Wert legt fest, wie viele Clientanforderungen im Vergleich zu anderen Servern im Pool an einen Server gesendet werden. Dieser Load Balancing-Algorithmus konzentriert sich auf eine gerechte Verteilung der Last auf die verfügbaren Serverressourcen.
<b>LEAST_CONNECTION</b>	Verteilt basierend auf der Anzahl der bereits auf den Servern aktiven Verbindungen die Client-Anforderungen an mehrere Server. Neue Verbindungen werden an den Server mit der geringsten Anzahl an Verbindungen gesendet. Ignoriert die Gewichtungen der Serverpoolmitglieder, auch wenn sie konfiguriert sind.
<b>WEIGHTED_LEAST_CONNECTION</b>	Jedem Server wird ein Gewichtungswert zugewiesen, der angibt, wie sich dieser Server im Vergleich zu anderen Servern im Pool verhält. Der Wert legt fest, wie viele Clientanforderungen im Vergleich zu anderen Servern im Pool an einen Server gesendet werden. Dieser Load Balancing-Algorithmus konzentriert sich auf die gleichmäßige Verteilung der Last auf die verfügbaren Serverressourcen anhand des Gewichtungswerts. Standardmäßig ist der Gewichtungswert 1, wenn der Wert nicht konfiguriert ist und langsamer Start aktiviert ist.
<b>IP-HASH</b>	Wählt einen Server auf der Basis eines Hash der Quell-IP-Adresse und der gesamten Gewichtung aller ausgeführten Server aus.

- 5 Schalten Sie die Schaltfläche „TCP-Multiplexing“ um, um dieses Menüelement zu aktivieren.

Mit der Funktion „TCP-Multiplexing“ können Sie dieselbe TCP-Verbindung zwischen einem Load Balancer und dem Server verwenden, um mehrere Clientanforderungen über verschiedene Client-TCP-Verbindungen zu senden.

- 6 Legen Sie die maximale Anzahl der TCP-Multiplexing-Verbindungen pro Pool fest, die zum Senden von zukünftigen Clientanforderungen beibehalten werden.
- 7 Wählen Sie den SNAT-Modus (Source NAT, Quell-NAT) aus.

Abhängig von der Topologie kann SNAT erforderlich sein, damit der Load Balancer Datenverkehr von dem Server empfängt, der für den Client bestimmt ist. SNAT kann pro Serverpool aktiviert werden.

Modus	Beschreibung
<b>Transparent-Modus</b>	Der Load Balancer verwendet die Client-IP-Adresse und Port-Spoofing, während er Verbindungen zu den Servern herstellt. SNAT ist nicht erforderlich.
<b>Modus für die automatische Zuordnung</b>	Der Load Balancer verwendet die IP-Adresse der Schnittstelle und den flüchtigen Port, um die Kommunikation mit einem Client fortzusetzen, der ursprünglich mit einem der etablierten Überwachungsports des Servers verbunden war. SNAT ist erforderlich. Aktivieren Sie die Portüberlastung, damit dieselbe SNAT-IP und derselbe Port für mehrere Verbindungen verwendet werden können, wenn das Tupel (Quell-IP, Quellport, Ziel-IP, Zielport und IP-Protokoll) nach der Ausführung des SNAT-Prozesses eindeutig ist. Sie können auch den Portüberlastungsfaktor so festlegen, dass die maximale Anzahl der gleichzeitigen Nutzung eines Ports für mehrere Verbindungen möglich ist.
<b>IP-Listenmodus</b>	Geben Sie einen einzigen IP-Adressbereich an, z. B. 1.1.1.1-1.1.1.10, der für SNAT verwendet werden soll, während Sie eine Verbindung zu einem der Server im Pool herstellen. Standardmäßig wird der Portbereich von 4000 bis 64000 für alle konfigurierten SNAT-IP-Adressen verwendet. Die Portbereiche von 1000 bis 4000 sind für bestimmte Zwecke wie z. B. Systemdiagnosen und von Linux-Anwendungen initiierte Verbindungen reserviert. Wenn mehrere IP-Adressen vorhanden sind, werden sie auf Grundlage von Round-Robin ausgewählt. Aktivieren Sie die Portüberlastung, damit dieselbe SNAT-IP und derselbe Port für mehrere Verbindungen verwendet werden können, wenn das Tupel (Quell-IP, Quellport, Ziel-IP, Zielport und IP-Protokoll) nach der Ausführung des SNAT-Prozesses eindeutig ist. Sie können auch den Portüberlastungsfaktor so festlegen, dass die maximale Anzahl der gleichzeitigen Nutzung eines Ports für mehrere Verbindungen möglich ist.

**8** Wählen Sie die Serverpoolmitglieder aus.

Der Serverpool besteht aus einem oder mehreren Poolmitgliedern. Jedes Poolmitglied verfügt über eine IP-Adresse und einen Port.

Jedes Serverpoolmitglied kann mit einer Gewichtung für die Verwendung im Load Balancing-Algorithmus konfiguriert werden. Die Gewichtung gibt an, wie viel mehr oder weniger Last ein bestimmtes Poolmitglied im Vergleich zu anderen Mitgliedern im selben Pool verarbeiten kann.

Bei der Systemzustandsüberwachung kann ein Poolmitglied als Backup-Mitglied festgelegt werden, um einen aktiven/Standby-Zustand herbeizuführen. Wenn aktive Mitglieder eine Integritätsprüfung nicht bestehen, tritt für Backup-Mitglieder ein Datenverkehrs-Failover auf.

Option	Beschreibung
<b>Statisch</b>	Klicken Sie auf <b>Hinzufügen</b> , um ein statisches Poolmitglied hinzuzufügen. Sie können auch ein vorhandenes statisches Poolmitglied klonen.
<b>Dynamisch</b>	Wählen Sie im Dropdown-Menü die NSGroup aus. Die Kriterien für die Serverpoolmitgliedschaft werden in der Gruppe definiert. Optional können Sie die maximale IP-Adressen-Gruppenliste definieren.

**9** Geben Sie die minimale Anzahl von aktiven Mitgliedern ein, die der Serverpool immer beibehalten muss.**10** Wählen Sie im Dropdown-Menü eine aktive und passive Systemzustandsüberwachung für den Serverpool aus.

Das Festlegen einer aktiven und passiven Systemzustandsüberwachung für den Serverpool ist optional. Wenn Sie eine aktive Systemzustandsüberwachung auswählen und das Tier-1-Gateway mit einem Tier-0-Gateway verbunden ist, wird ein Routerlinkport erstellt. Die IP-Adresse des Routerlinkports (normalerweise im Format 100.64.x.x) wird verwendet, um die Integritätsprüfung für den Load Balancer durchzuführen. Wenn das Tier-1-Gateway eigenständig ist (nur über einen zentralisierten Dienstport verfügt und nicht mit einem Tier-0-Gateway verbunden ist), wird die IP-Adresse des zentralisierten Dienstports verwendet, um die Integritätsprüfung für den Load Balancer durchzuführen. Informationen zu eigenständigen Tier-1-Gateways finden Sie unter [Erstellen eines eigenständigen logischen Tier-1-Routers](#).

Fügen Sie eine Firewallregel hinzu, damit die IP-Adresse die Integritätsprüfung für den Load Balancer durchführen kann.

**11** Klicken Sie auf **Fertigstellen**.

## Konfigurieren der Komponenten des virtuellen Servers

Sie können mehrere Komponenten des virtuellen Servers konfigurieren, beispielsweise Anwendungsprofile, persistente Profile und Load Balancer-Regeln.

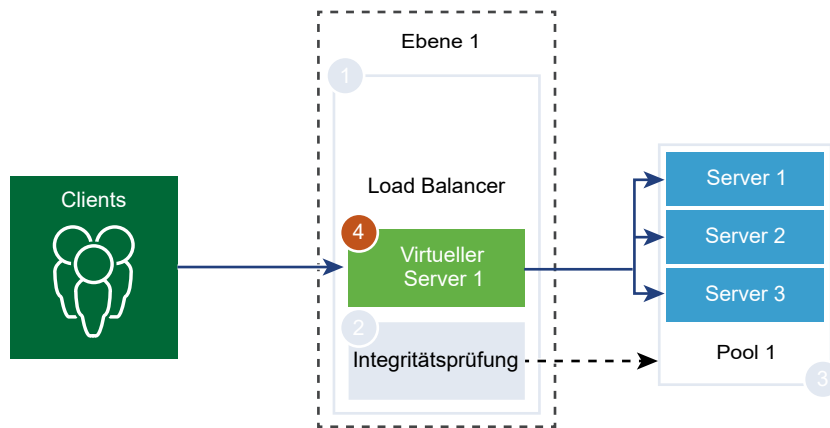
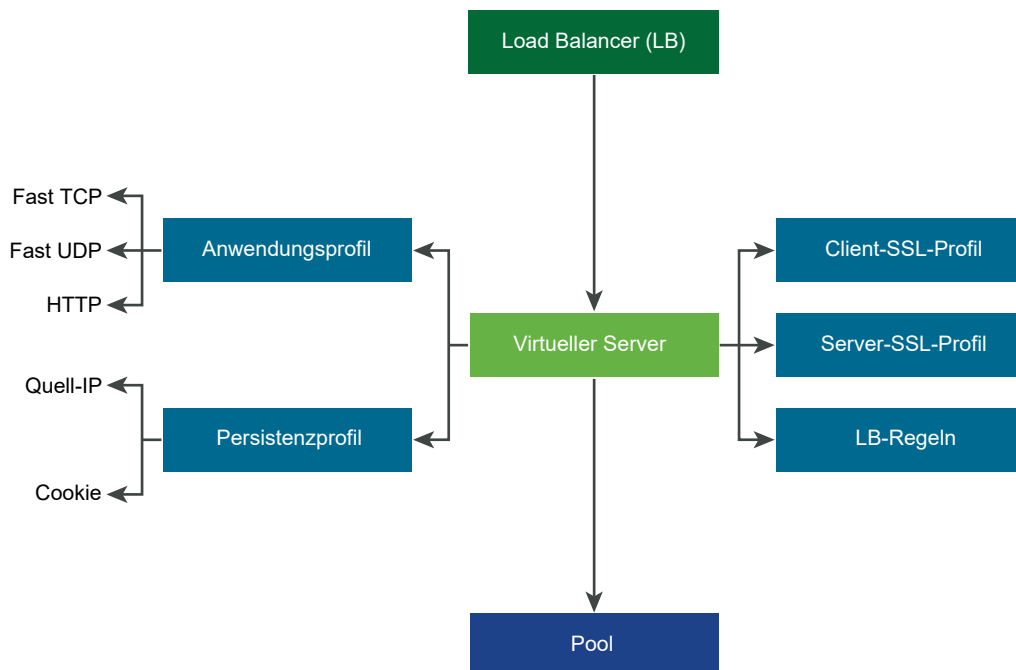


Abbildung 19-2. Komponenten des virtuellen Servers



## Konfigurieren von Anwendungsprofilen

Anwendungsprofile sind mit virtuellen Servern verknüpft, um das Load Balancing im Netzwerkverkehr zu verbessern und Aufgaben zur Verwaltung des Datenverkehrs zu vereinfachen.

Mit Anwendungsprofilen definieren Sie das Verhalten eines bestimmten Netzwerkverkehrstyps. Der verknüpfte virtuelle Server verarbeitet den Datenverkehr gemäß den im Anwendungsprofil angegebenen Werten. Fast TCP-, Fast UDP- und HTTP- Anwendungsprofile sind die unterstützten Profiltypen.



Das Anwendungsprofil TCP wird verwendet, wenn standardmäßig kein Anwendungsprofil mit einem virtuellen Server verknüpft ist. TCP- und UDP-Anwendungsprofile werden verwendet, wenn eine Anwendung auf einem TCP- oder UDP-Protokoll ausgeführt wird und kein Load Balancing auf Anwendungsebene benötigt, wie z. B. HTTP-URL-Load Balancing. Diese Profile werden auch verwendet, wenn Sie nur Load Balancing der Schicht 4 benötigen, der leistungsfähiger ist und Verbindungsspiegelung unterstützt.

Das HTTP-Anwendungsprofil wird für HTTP- und HTTPS-Anwendungen verwendet, wenn der Load Balancer Aktionen auf Grundlage von Schicht 7 durchführen muss, wie z. B. das Durchführen von Load Balancing für alle Bildanforderungen auf einem bestimmten Serverpoolmitglied oder das Beenden von HTTPS zum Auslagern von SSL aus Poolmitgliedern. Im Gegensatz zum TCP-Anwendungsprofil schließt das HTTP-Anwendungsprofil die TCP-Verbindung des Clients vor der Auswahl des Serverpoolmitglieds.

Abbildung 19-3. TCP- und UDP-Anwendungsprofil der Schicht 4

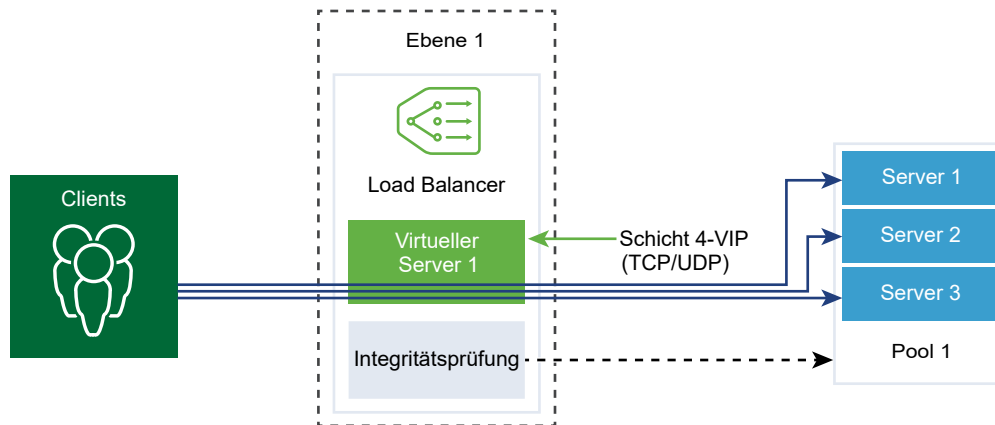
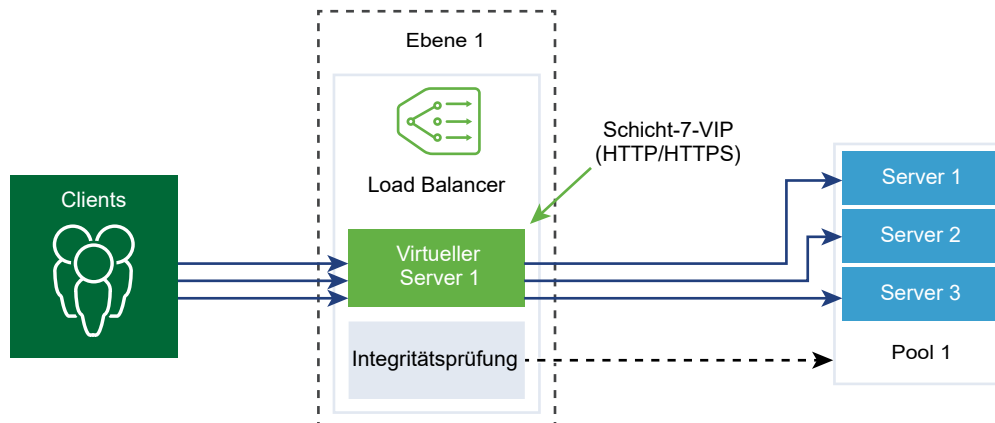


Abbildung 19-4. HTTPS-Anwendungsprofil der Schicht 7



## Verfahren

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

**2 Wählen Sie **Netzwerk und Sicherheit – Erweitert** > **Netzwerk** > **Load Balancer** > **Profile** > **Anwendungsprofile**.**

**3 Erstellen Sie ein Fast TCP-Anwendungsprofil.**

- a Wählen Sie im Dropdown-Menü die Option **Hinzufügen > Fast TCP-Profil** aus.
- b Geben Sie einen Namen und eine Beschreibung für das Fast TCP-Anwendungsprofil ein.
- c Vervollständigen Sie die Details des Anwendungsprofils.

Sie können auch die Standardprofileinstellungen für FAST TCP übernehmen.

Option	Beschreibung
<b>Leerlaufzeitlimit für Verbindung</b>	<p>Geben Sie den Zeitraum in Sekunden ein, während dem ein Server im Leerlauf ausgeführt werden kann, nachdem eine TCP-Verbindung eingerichtet wurde.</p> <p>Legen Sie die Leerlaufzeit auf die Leerlaufzeit der tatsächlichen Anwendung fest und fügen Sie ein paar Sekunden hinzu, damit der Load Balancer seine Verbindungen nicht vor der Anwendung schließt.</p>
<b>Zeitlimit vor Schließen der Verbindung</b>	<p>Geben Sie den Zeitraum in Sekunden ein, während dem eine TCP-Verbindung (FIN und RST) für eine Anwendung bestehen bleiben muss, bevor die Verbindung geschlossen wird.</p> <p>Ein kurzes Zeitlimit ist unter Umständen erforderlich, um schnelle Verbindungsraten zu unterstützen.</p>
<b>HA-Flow-Spiegelung</b>	<p>Schalten Sie die Schaltfläche um, um alle Flows zum zugehörigen virtuellen Server auf den HA-Standby-Knoten zu spiegeln.</p>

- d Klicken Sie auf **OK**.

**4 Erstellen Sie ein Fast UDP-Anwendungsprofil.**

Sie können auch die Standardprofileinstellungen für UDP übernehmen.

- a Wählen Sie im Dropdown-Menü die Option **Hinzufügen > Fast UDP-Profil** aus.
- b Geben Sie einen Namen und eine Beschreibung für das Fast UDP-Anwendungsprofil ein.

- c Vervollständigen Sie die Details des Anwendungsprofils.

Option	Beschreibung
<b>Leerlaufzeitlimit</b>	<p>Geben Sie den Zeitraum in Sekunden ein, während dem ein Server im Leerlauf ausgeführt werden kann, nachdem eine UDP-Verbindung eingerichtet wurde.</p> <p>UDP ist ein verbindungsloses Protokoll. Zu Load Balancing-Zwecken wird davon ausgegangen, dass alle UDP-Pakete mit derselben Flow-Signatur (wie z. B. IP-Quell- und IP-Zieladresse oder -ports) und IP-Protokolle, die während des Leerlaufzeitlimits empfangen wurden, zur selben Verbindung gehören und an denselben Server gesendet werden.</p> <p>Werden während des Leerlaufzeitlimits keine Pakete empfangen, wird die Verbindung, die als Verknüpfung zwischen der Flow-Signatur und dem ausgewählten Server fungiert, getrennt.</p>
<b>HA-Flow-Spiegelung</b>	Schalten Sie die Schaltfläche um, um alle Flows zum zugehörigen virtuellen Server auf den HA-Standby-Knoten zu spiegeln.

- d Klicken Sie auf **OK**.

## 5 Erstellen Sie ein HTTP-Anwendungsprofil.

Sie können auch die Standardprofileinstellungen für HTTP übernehmen.

Das HTTP-Anwendungsprofil wird für HTTP- und HTTPS-Anwendungen verwendet.

- Wählen Sie im Dropdown-Menü die Option **Hinzufügen > Fast HTTP-Profil** aus.
- Geben Sie einen Namen und eine Beschreibung für das HTTP-Anwendungsprofil ein.

## c Vervollständigen Sie die Details des Anwendungsprofils.

Option	Beschreibung
<b>Umleitung</b>	<ul style="list-style-type: none"> <li>■ <b>Keine</b> – Wenn eine Website vorübergehend nicht verfügbar ist, erhält der Benutzer eine Meldung mit dem Hinweis, dass die Seite nicht gefunden werden konnte.</li> <li>■ <b>HTTP-Umleitung</b> – Wenn eine Website vorübergehend nicht verfügbar ist oder verschoben wurde, können eingehende Anfragen für diesen virtuellen Server vorübergehend an eine hier angegebene URL umgeleitet werden. Nur eine statische Umleitung wird unterstützt.  Wenn „HTTP-Umleitung“ beispielsweise auf <code>http://sitedown.abc.com/sorry.html</code> gesetzt ist, werden ungeachtet der tatsächlichen Anfrage (z. B. <code>http://original_app.site.com/home.html</code> oder <code>http://original_app.site.com/somepage.html</code>) eingehende Anfragen an die angegebene URL umgeleitet, wenn die ursprüngliche Website nicht erreichbar ist.</li> <li>■ <b>HTTP an HTTPS umleiten</b> – Bestimmte sichere Anwendungen möchten unter Umständen Kommunikation über SSL erzwingen, aber statt Nicht-SSL-Verbindungen abzulehnen, können sie die Clientanfrage zur Verwendung von SSL umleiten. Mithilfe von „HTTP an HTTPS umleiten“ können Sie den Host und die URI-Pfade beibehalten und die Clientanfrage zur Verwendung von SSL umleiten.  Zur Verwendung von „HTTP an HTTPS umleiten“ muss der virtuelle HTTPS-Server Port 443 aufweisen und dieselbe IP-Adresse des virtuellen Servers muss auf demselben Load Balancer konfiguriert sein.  Eine Clientanfrage für <code>http://app.com/path/page.html</code> wird beispielsweise an <code>https://app.com/path/page.html</code> umgeleitet. Wenn entweder der Hostname oder die URI während der Umleitung geändert werden muss, z. B. Umleitung an <code>https://secure.app.com/path/page.html</code>, müssen Load Balancing-Regeln verwendet werden.</li> </ul>
<b>XFF (X-Forwarded-For)</b>	<ul style="list-style-type: none"> <li>■ <b>Einfügen</b> – Wenn der XFF-HTTP-Header nicht in der eingehenden Anfrage enthalten ist, fügt der Load Balancer einen neuen XFF-Header mit der IP-Adresse des Clients ein. Wenn der XFF-HTTP-Header in der eingehenden Anfrage enthalten ist, hängt der Load Balancer den XFF-Header mit der IP-Adresse des Clients an.</li> <li>■ <b>Ersetzen</b> – Wenn der XFF-HTTP-Header in der eingehenden Anfrage enthalten ist, ersetzt der Load Balancer den Header.  Webserver protokollieren jede Anfrage, die sie verarbeiten, mit der IP-Adresse des anfragenden Clients. Diese Protokolle werden zur Fehlerbehebung und Analyse verwendet. Wenn die Bereitstellungstopologie SNAT auf dem Load Balancer erfordert, verwendet der Server die IP-Adresse der Client-SNAT, was dem Zweck der Protokollierung widerspricht.  Zur Umgehung dieses Problems kann der Load Balancer so konfiguriert werden, dass der XFF-HTTP-Header mit der IP-Adresse des ursprünglichen Clients eingefügt wird. Server können so konfiguriert werden, dass anstelle der IP-Quelladresse der Verbindung die IP-Adresse im XFF-Header aufgezeichnet wird.</li> </ul>

Option	Beschreibung
<b>Leerlaufzeitlimit für Verbindung</b>	Geben Sie anstelle der TCP-Socket-Einstellung, die im TCP-Anwendungsprofil konfiguriert werden muss, den Zeitraum in Sekunden an, während dem eine HTTP-Anwendung im Leerlauf ausgeführt werden kann.
<b>Größe des Anforderungsheaders</b>	Geben Sie die maximale Puffergröße in Byte an, die zum Speichern von HTTP-Anforderungsheadern verwendet wird.
<b>NTLM-Authentifizierung</b>	<p>Schalten Sie die Schaltfläche für den Load Balancer um, um TCP-Multiplexing zu deaktivieren und HTTP-Keep-Alive zu aktivieren.</p> <p>NTLM ist ein Authentifizierungsprotokoll, das über HTTP verwendet werden kann. Für Load Balancing mit NTLM-Authentifizierung muss TCP-Multiplexing für die Serverpools deaktiviert werden, die NTLM-basierte Anwendungen hosten. Andernfalls kann eine mit den Anmeldedaten eines Clients eingerichtete serverseitige Verbindung möglicherweise dazu verwendet werden, die Anfragen eines anderen Clients zu beantworten.</p> <p>Wenn NTLM im Profil aktiviert ist und einem virtuellen Server zugeordnet wurde und TCP-Multiplexing im Serverpool aktiviert ist, hat NTLM Vorrang. TCP-Multiplexing wird für diesen virtuellen Server nicht durchgeführt. Wenn derselbe Pool jedoch einem anderen virtuellen Server ohne NTLM zugeordnet wird, steht TCP-Multiplexing für Verbindungen mit diesem virtuellen Server zur Verfügung.</p> <p>Wenn der Client HTTP/1.0 verwendet, führt der Load Balancer ein Upgrade auf das HTTP/1.1-Protokoll durch und HTTP-Keep-Alive wird eingerichtet. Alle HTTP-Anforderungen, die über dieselbe clientseitigen TCP-Verbindung empfangen wurden, werden über eine einzige TCP-Verbindung an denselben Server gesendet, um sicherzustellen, dass keine erneute Autorisierung erforderlich ist.</p>

- d Klicken Sie auf **OK**.

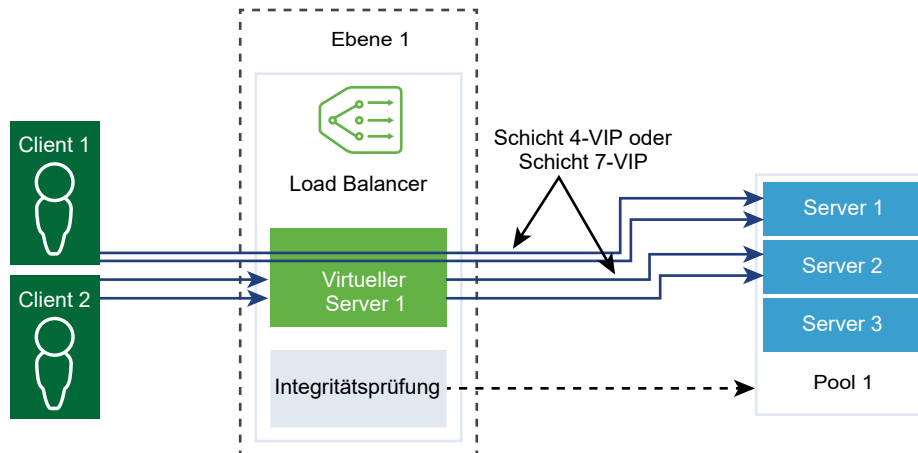
## Konfigurieren von persistenten Profilen

Zur Gewährleistung der Stabilität von statusbehafteten Anwendungen implementieren Load Balancer Persistenz, die alle zugehörigen Verbindungen an denselben Server weiterleitet. Es werden verschiedene Arten von Persistenz unterstützt, um die unterschiedlichen Anwendungsanforderungen zu erfüllen.

Einige Anwendungen verwalten den Serverstatus, z. B. Einkaufswagen. Dieser Status kann pro Client gelten und anhand der Client-IP-Adresse oder über die HTTP-Sitzung ermittelt werden. Anwendungen können während der Verarbeitung nachfolgender zugehöriger Verbindungen von demselben Client oder derselben HTTP-Sitzung auf diesen Status zugreifen oder ihn ändern.

Das Quell-IP-Persistenzprofil verfolgt Sitzungen basierend auf der Quell-IP-Adresse. Wenn ein Client eine Verbindung mit einem virtuellen Server anfordert, der die Persistenz der Quelladresse ermöglicht, überprüft der Load Balancer, ob dieser Client zuvor verbunden war. Wenn dies der Fall ist, gibt er den Client an denselben Server zurück. Andernfalls können Sie basierend auf dem Load Balancing-Algorithmus des Pools ein Mitglied des Serverpools auswählen. Das Quell-IP-Persistenzprofil wird von virtuellen Servern der Schichten 4 und 7 verwendet.

Das Cookie-Persistenzprofil fügt ein eindeutiges Cookie zur Identifizierung der Sitzung beim ersten Zugriff eines Clients auf die Site ein. Das HTTP-Cookie wird durch den Client in nachfolgenden Anforderungen weitergeleitet, und der Load Balancer verwendet diese Informationen zur Bereitstellung der Cookie-Persistenz. Das Cookie-Persistenzprofil kann nur von virtuellen Servern der Schicht 7 verwendet werden.



## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > Load Balancer > Profile > Persistenzprofile**.
- 3 Erstellen Sie ein Quell-IP-Persistenzprofil.
  - a Wählen Sie im Dropdown-Menü **Hinzufügen > Quell-IP-Persistenz** aus.
  - b Geben Sie einen Namen und eine Beschreibung für das Quell-IP-Persistenzprofil ein.

- c Geben Sie die Details des Persistenzprofils an.

Sie können auch die Standardeinstellungen des Quell-IP-Profiles übernehmen.

Option	Beschreibung
<b>Persistenz freigeben</b>	<p>Schalten Sie die Schaltfläche um, um die Persistenz freizugeben, sodass alle virtuellen Server, denen dieses Profil zugewiesen ist, die Persistenztable gemeinsam nutzen können.</p> <p>Wenn die Persistenzfreigabe in dem Quell-IP-Persistenzprofil, das einem virtuellen Server zugeordnet ist, nicht aktiviert ist, verwaltet jeder virtuelle Server, dem das Profil zugeordnet wird, eine private Persistenztable.</p>
<b>Zeitüberschreitung für Persistenzeintrag</b>	<p>Geben Sie den Zeitraum für die Persistenz bis zum Ablauf in Sekunden ein.</p> <p>Die Persistenztable des Load Balancers enthält Einträge, die die Weiterleitung von Clientanforderungen an denselben Server aufzeichnen.</p> <ul style="list-style-type: none"> <li>■ Wenn von demselben Client keine neuen Verbindungsanforderungen innerhalb des festgelegten Zeitraums empfangen werden, verfällt der Persistenzeintrag und wird gelöscht.</li> <li>■ Geht von demselben Client innerhalb des festgelegten Zeitraums eine neue Verbindungsanforderung ein, wird der Timer zurückgesetzt und die Clientanforderung an ein verfügbares Poolmitglied gesendet.</li> </ul> <p>Nach Ablauf des festgelegten Zeitraums werden neue Verbindungsanforderungen an einen über den Load Balancing-Algorithmus bestimmten Server gesendet. Für den Fall einer TCP-Quell-IP-Persistenz mit dem L7-Load Balancing legt der Persistenzeintrag den Zeitpunkt fest, ab dem einige Zeit lang keine neuen TCP-Verbindungen erstellt werden, auch wenn die vorhandenen Verbindungen weiterhin aktiv sind.</p>
<b>HA-Persistenzspiegelung</b>	<p>Schalten Sie die Schaltfläche um, um Persistenzeinträge mit dem HA-Peer zu synchronisieren.</p>
<b>Bei voller Tabelle Einträge löschen</b>	<p>Die Einträge werden gelöscht, wenn die Persistenztable voll ist.</p> <p>Ein hoher Wert für die Zeitüberschreitung führt möglicherweise dazu, dass die Persistenztable sich schnell füllt, wenn der Datenverkehr hoch ist. Wenn die Persistenztable voll ist, wird für den aktuellen Eintrag der älteste Eintrag gelöscht.</p>

- d Klicken Sie auf **OK**.

#### 4 Erstellen Sie ein Cookie-Persistenzprofil.

- Wählen Sie im Dropdown-Menü **Hinzufügen > Cookie-Persistenz** aus.
- Geben Sie einen Namen und eine Beschreibung für das Cookie-Persistenzprofil ein.

- c Schalten Sie die Schaltfläche **Persistenz freigeben** um, um die Persistenz für mehrere virtuelle Server freizugeben, die denselben Poolmitgliedern zugeordnet sind.

Das Cookie-Persistenzprofil fügt ein Cookie mit dem Format `<name>.<profile-id>.<pool-id>` ein.

Wenn die freigegebene Persistenz in dem einem virtuellen Server zugeordneten Cookie-Persistenzprofil nicht aktiviert ist, wird für jeden virtuellen Server die private Cookie-Persistenz verwendet und durch das Poolmitglied qualifiziert. Der Load Balancer fügt ein Cookie mit dem Format `<name>.<virtual_server_id>.<pool_id>` ein.

- d Klicken Sie auf **Weiter**.
- e Geben Sie die Details des Persistenzprofils an.

Option	Beschreibung
<b>Cookiemodus</b>	Wählen Sie im Dropdown-Menü einen Modus aus. <ul style="list-style-type: none"> <li>■ EINFÜGEN – Fügt ein eindeutiges Cookie zur Identifizierung der Sitzung hinzu.</li> <li>■ PRÄFIX – Wird an die vorhandenen HTTP-Cookie-Informationen angefügt.</li> <li>■ UMSCHREIBEN – Schreibt die vorhandenen HTTP-Cookie-Informationen um.</li> </ul>
<b>Cookiename</b>	Geben Sie den Cookienamen ein.
<b>Cookie Domäne</b>	Geben Sie den Domännennamen ein. Die HTTP-Cookie Domäne kann nur im Modus EINFÜGEN konfiguriert werden.
<b>Cookiepfad</b>	Geben Sie den URL-Pfad des Cookies ein. Der HTTP-Cookiepfad kann nur im Modus EINFÜGEN festgelegt werden.
<b>Cookieverschlüsselung</b>	Verschlüsseln Sie die Informationen zu IP-Adresse und Port des Cookieservers.  Schalten Sie die Schaltfläche um, um die Verschlüsselung zu deaktivieren. Wenn die Verschlüsselung deaktiviert ist, liegen die Informationen zu IP-Adresse und Port des Cookieservers unverschlüsselt vor.
<b>Cookie-Fallback</b>	Wählen Sie einen neuen Server für die Verarbeitung einer Clientanforderung aus, wenn das Cookie auf einen Server verweist, der sich im Status DEAKTIVIERT oder INAKTIV befindet.  Schalten Sie die Schaltfläche um, sodass die Clientanforderung abgelehnt wird, wenn ein Cookie auf einen Server verweist, der sich im Status DEAKTIVIERT oder INAKTIV befindet.



- f Geben Sie die Details zum Ablauf des Cookies an.

Option	Beschreibung
<b>Cookiezeittyp</b>	Wählen Sie im Dropdown-Menü einen Cookiezeittyp aus. <b>Sitzungs-Cookie</b> wird nicht gespeichert und geht verloren, wenn der Browser geschlossen wird. <b>Persistenz-Cookie</b> wird vom Browser gespeichert und geht nicht verloren, wenn der Browser geschlossen wird.
<b>Maximale Leerlaufzeit</b>	Geben Sie die Zeit in Sekunden ein, die das Cookie im Leerlauf sein kann, bevor es abläuft.
<b>Maximales Cookiealter</b>	Nur für <b>Sitzungs-Cookie</b> . Geben Sie das maximale Alter in Sekunden ein, für das ein Cookie aktiv sein kann.

- g Klicken Sie auf **Fertigstellen**.

## Konfigurieren von SSL-Profilen

SSL-Profile konfigurieren anwendungsunabhängige SSL-Eigenschaften, beispielsweise Verschlüsselungslisten, und verwenden diese Listen für mehrere Anwendungen. SSL-Eigenschaften sind unterschiedlich, wenn der Load Balancer als Client und als Server dient. Daher werden separate SSL-Profile für die Client- und die Serverseite unterstützt.

**Hinweis** SSL-Profile werden in der Version NSX-T Data Center Limited Export nicht unterstützt.

Das clientseitige SSL-Profil verweist auf den Load Balancer, der als SSL-Server agiert und die SSL-Verbindung des Clients beendet. Das serverseitige SSL-Profil verweist auf den Load Balancer, der als Client agiert und eine Verbindung mit dem Server herstellt.

Sie können sowohl in den client- als auch in den serverseitigen SSL-Profilen eine Verschlüsselungsliste angeben.

Durch das Caching von SSL-Sitzungen sind SSL-Client und -Server in der Lage, zuvor ausgehandelte Sicherheitsparameter wiederzuverwenden. Hierdurch wird das aufwändige Verfahren mit öffentlichen Schlüsseln während des SSL-Handshakes vermieden. Das Caching von SSL-Sitzungen ist standardmäßig sowohl auf Client- als auch auf Serverseite deaktiviert.

Bei SSL-Sitzungstickets handelt es sich um ein alternatives Verfahren, das dem SSL-Client und -Server die Wiederverwendung von zuvor ausgehandelten Sitzungsparametern ermöglicht. In SSL-Sitzungstickets handeln der Client und der Server aus, ob sie während des Handshake-Austauschs SSL-Sitzungstickets unterstützen. Wenn beide die Tickets unterstützen, kann der Server ein SSL-Ticket mit verschlüsselten SSL-Sitzungsparametern an den Client senden. Der Client kann dieses Ticket in nachfolgenden Verbindungen verwenden, um die Sitzung wiederzuverwenden. SSL-Sitzungstickets sind auf der Clientseite aktiviert und auf der Serverseite deaktiviert.

Abbildung 19-5. SSL-Offloading

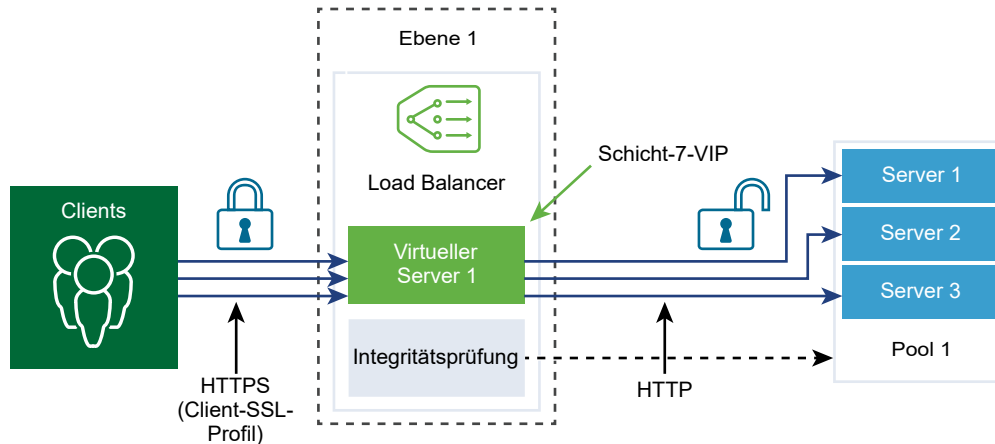
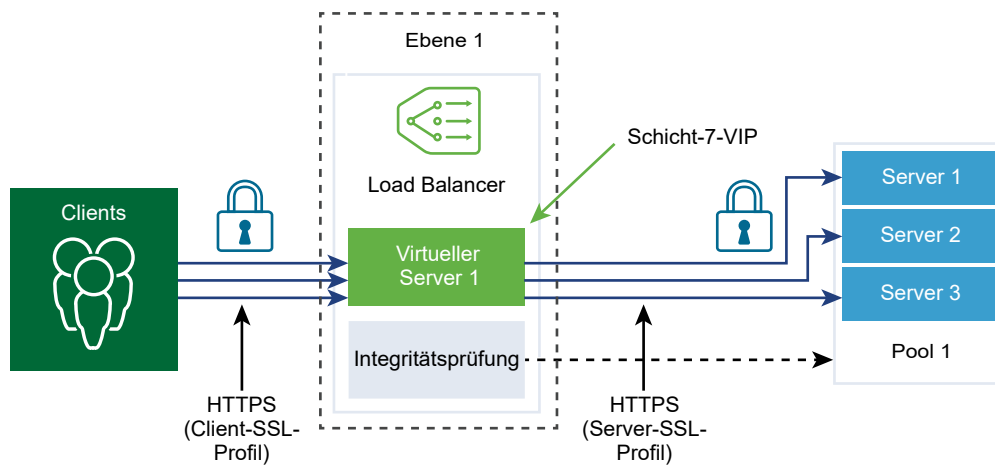


Abbildung 19-6. End-to-End-SSL



## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Netzwerk > Load Balancer > Profile > SSL-Profile**.
- 3 Erstellen Sie ein SSL-Clientprofil.
  - a Wählen Sie im Dropdown-Menü **Hinzufügen > Clientseitiges SSL** aus.
  - b Geben Sie einen Namen und eine Beschreibung für das SSL-Clientprofil ein.
  - c Weisen Sie die SSL-Verschlüsselungen zu, die in das SSL-Clientprofil aufgenommen werden sollen.  
  
Sie können auch benutzerdefinierte SSL-Verschlüsselungen erstellen.
  - d Klicken Sie auf den Pfeil, um die Verschlüsselungen in den Abschnitt „Ausgewählt“ zu verschieben.

- e Klicken Sie auf die Registerkarte **Protokolle und Sitzungen**.
- f Wählen Sie die SSL-Protokolle aus, die in das SSL-Clientprofil aufgenommen werden sollen.

Die SSL-Protokollversionen TLS1.1 und TLS1.2 sind standardmäßig aktiviert. TLS1.0 wird ebenfalls unterstützt, ist aber standardmäßig deaktiviert.

- g Klicken Sie auf den Pfeil, um das Protokoll in den Abschnitt „Ausgewählt“ zu verschieben.
- h Vervollständigen Sie die SSL-Protokolldetails.

Sie können auch die Standardeinstellungen für das SSL-Profil übernehmen.

Option	Beschreibung
<b>Sitzungs-Caching</b>	Durch das Caching von SSL-Sitzungen sind SSL-Client und -Server in der Lage, zuvor ausgehandelte Sicherheitsparameter wiederzuverwenden. Hierdurch wird das aufwändige Verfahren mit öffentlichen Schlüsseln während eines SSL-Handshakes vermieden.
<b>Zeitüberschreitung für Cache-Eintrag der Sitzung</b>	Geben Sie die Zeitüberschreitung für den Cache in Sekunden an, um festzulegen, wie lange die SSL-Sitzungsparameter beibehalten werden müssen und wiederverwendet werden können.
<b>Serververschlüsselung bevorzugen</b>	Schalten Sie die Schaltfläche um, sodass der Server die erste unterstützte Verschlüsselung aus der Liste auswählen kann, die er unterstützen kann. Während eines SSL-Handshakes sendet der Client eine sortierte Liste der unterstützten Verschlüsselungen an den Server.

- i Klicken Sie auf **OK**.

#### 4 Erstellen Sie ein SSL-Serverprofil.

- a Wählen Sie im Dropdown-Menü **Hinzufügen > Serverseitiges SSL** aus.
- b Geben Sie einen Namen und eine Beschreibung für das SSL-Serverprofil ein.
- c Wählen Sie die SSL-Verschlüsselungen aus, die in das SSL-Serverprofil aufgenommen werden sollen.

Sie können auch benutzerdefinierte SSL-Verschlüsselungen erstellen.

- d Klicken Sie auf den Pfeil, um die Verschlüsselungen in den Abschnitt „Ausgewählt“ zu verschieben.
- e Klicken Sie auf die Registerkarte **Protokolle und Sitzungen**.

- f Wählen Sie die SSL-Protokolle aus, die in das SSL-Serverprofil aufgenommen werden sollen.

Die SSL-Protokollversionen TLS1.1 und TLS1.2 sind standardmäßig aktiviert. TLS1.0 wird ebenfalls unterstützt, ist aber standardmäßig deaktiviert.

- g Klicken Sie auf den Pfeil, um das Protokoll in den Abschnitt „Ausgewählt“ zu verschieben.

- h Übernehmen Sie die Standardeinstellung für das Sitzungs-Caching.

Durch das Caching von SSL-Sitzungen sind SSL-Client und -Server in der Lage, zuvor ausgehandelte Sicherheitsparameter wiederzuverwenden. Hierdurch wird das aufwändige Verfahren mit öffentlichen Schlüsseln während eines SSL-Handshakes vermieden.

- i Klicken Sie auf **OK**.

## Konfigurieren von virtuellen Servern der Schicht 4

Virtuelle Server empfangen alle Clientverbindungen und verteilen diese an die Server. Ein virtueller Server verfügt über eine IP-Adresse, einen Port und ein Protokoll. Für virtuelle Server der Schicht 4 können anstelle einzelner TCP- oder UDP-Ports Listen mit Portbereichen angegeben werden, um komplexe Protokolle mit dynamischen Ports zu unterstützen.

Ein virtueller Server der Schicht 4 muss mit einem primären Serverpool, der auch als Standardpool bezeichnet wird, verknüpft werden.

Wenn der Status eines virtuellen Servers „Deaktiviert“ lautet, werden alle neuen Verbindungsversuche mit dem virtuellen Server abgelehnt, indem entweder ein TCP RST für die TCP-Verbindung oder eine ICMP-Fehlermeldung für UDP gesendet wird. Neue Verbindungen werden abgelehnt, selbst wenn passende Persistenzeinträge für sie vorhanden sind. Aktive Verbindungen werden weiterhin verarbeitet. Wenn ein virtueller Server gelöscht oder von einem Load Balancer getrennt wird, schlagen aktive Verbindungen mit diesem virtuellen Server fehl.

### Voraussetzungen

- Stellen Sie sicher, dass Anwendungsprofile verfügbar sind. Siehe [Konfigurieren von Anwendungsprofilen](#).
- Stellen Sie sicher, dass persistente Profile verfügbar sind. Siehe [Konfigurieren von persistenten Profilen](#).
- Stellen Sie sicher, dass SSL-Profile für Client und Server verfügbar sind. Siehe [Konfigurieren von SSL-Profilen](#).
- Stellen Sie sicher, dass Serverpools verfügbar sind. Siehe [Hinzufügen eines Serverpools für das Load Balancing](#).

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Integritätsüberwachungen > Netzwerk > Load Balancer > Virtuelle Server > Hinzufügen**.
- 3 Geben Sie einen Namen und eine Beschreibung für den virtuellen Server der Schicht 4 ein.

- 4 Wählen Sie im Dropdown-Menü ein Protokoll der Schicht 4 aus.

Virtuelle Server der Schicht 4 unterstützen entweder das Fast TCP- oder das Fast UDP-Protokoll. Damit das Fast TCP- oder das Fast UDP-Protokoll für dieselbe IP-Adresse und denselben Port unterstützt wird, wie z. B. DNS, muss für jedes Protokoll ein virtueller Server erstellt werden.

Je nach Protokolltyp wird das vorhandene Anwendungsprofil automatisch befüllt.

- 5 Klicken Sie auf die Schaltfläche „Zugriffsprotokoll“, um die Protokollierung für den virtuellen Schicht-4-Server zu aktivieren.
- 6 Klicken Sie auf **Weiter**.
- 7 Geben Sie die IP-Adresse und Portnummer des virtuellen Servers ein.
- Sie können die Portnummer oder den Portbereich des virtuellen Servers eingeben.
- 8 Geben Sie die erweiterten Eigenschaften an.

Option	Beschreibung
<b>Maximale Anzahl gleichzeitiger Verbindungen</b>	Legen Sie die maximale Anzahl gleichzeitiger Verbindungen fest, die für einen virtuellen Server zulässig sind, damit der virtuelle Server nicht die Ressourcen anderer Anwendung verbraucht, die vom selben Load Balancer gehostet werden.
<b>Maximale Anzahl neuer Verbindungen</b>	Legen Sie die maximale Anzahl neuer Verbindungen für ein Serverpoolmitglied fest, damit ein virtueller Server die Ressourcen nicht überlastet.
<b>Standardport des Poolmitglieds</b>	Geben Sie den Standardport eines Poolmitglieds ein, wenn der Port des Poolmitglieds für einen virtuellen Server nicht definiert ist.  Wenn ein virtueller Server beispielsweise mit dem Portbereich 2000-2999 definiert ist und der Standardportbereich des Poolmitglieds auf 8000-8999 festgelegt ist, wird eine eingehende Clientverbindung für Port 2500 des virtuellen Servers an ein Poolmitglied mit einem auf 8500 gesetzten Zielport gesendet.

- 9 Wählen Sie im Dropdown-Menü einen vorhandenen Serverpool aus.
- Der Serverpool besteht aus einem oder mehreren auch als Poolmitglieder bezeichneten Servern mit ähnlicher Konfiguration, auf denen dieselbe Anwendung ausgeführt wird.
- 10 Wählen Sie im Dropdown-Menü einen vorhandenen Sorry-Serverpool aus.
- Der Sorry-Serverpool stellt die Anforderung zu, wenn ein Load Balancer keinen Backend-Server auswählen kann, um die Anforderung aus dem Standardpool zuzustellen.
- 11 Klicken Sie auf **Weiter**.
- 12 Wählen Sie im Dropdown-Menü ein vorhandenes Persistenzprofil aus.
- Das Persistenzprofil kann auf einem virtuellen Server aktiviert werden, damit verwandte Clientverbindungen an denselben Server gesendet werden können.
- 13 Klicken Sie auf **Fertigstellen**.

## Konfigurieren von virtuellen Servern der Schicht 7

Virtuelle Server empfangen alle Clientverbindungen und verteilen diese an die Server. Ein virtueller Server verfügt über eine IP-Adresse, einen Port und ein TCP-Protokoll.

Load Balancer-Regeln werden nur für virtuelle Server der Schicht 7 unterstützt, die ein HTTP-Anwendungsprofil aufweisen. Verschiedene Load Balancer-Dienste können Load Balancer-Regeln verwenden.

Jede Load Balancer-Regel besteht aus einzelnen oder mehreren Übereinstimmungsbedingungen und Aktionen. Wenn keine Übereinstimmungsbedingungen angegeben sind, stimmt die Load Balancer-Regel immer überein und wird zum Definieren von Standardregeln verwendet. Wenn mehr als eine Übereinstimmungsbedingung angegeben wird, bestimmt die Übereinstimmungsstrategie, ob alle Bedingungen oder eine beliebige Bedingung erfüllt sein muss, damit die Load Balancer-Regel als Übereinstimmung angesehen wird.

Jede Load Balancer-Regel wird während einer bestimmten Phase der Load Balancing-Verarbeitung implementiert (Umschreiben der HTTP-Anfrage, Weiterleiten der HTTP-Anfrage und Umschreiben der HTTP-Antwort). Nicht alle Übereinstimmungsbedingungen und Aktionen sind auf jede Phase anwendbar.

Wenn der Status eines virtuellen Servers „Deaktiviert“ lautet, werden alle neuen Verbindungsversuche mit dem virtuellen Server abgelehnt, indem entweder ein TCP RST für die TCP-Verbindung oder eine ICMP-Fehlermeldung für UDP gesendet wird. Neue Verbindungen werden abgelehnt, selbst wenn passende Persistenzeinträge für sie vorhanden sind. Aktive Verbindungen werden weiterhin verarbeitet. Wenn ein virtueller Server gelöscht oder von einem Load Balancer getrennt wird, schlagen aktive Verbindungen mit diesem virtuellen Server fehl.

### Voraussetzungen

- Stellen Sie sicher, dass Anwendungsprofile verfügbar sind. Siehe [Konfigurieren von Anwendungsprofilen](#).
- Stellen Sie sicher, dass persistente Profile verfügbar sind. Siehe [Konfigurieren von persistenten Profilen](#).
- Stellen Sie sicher, dass SSL-Profile für Client und Server verfügbar sind. Siehe [Konfigurieren von SSL-Profilen](#).
- Stellen Sie sicher, dass Serverpools verfügbar sind. Siehe [Hinzufügen eines Serverpools für das Load Balancing](#).
- Stellen Sie sicher, dass Zertifizierungsstelle und Clientzertifikat verfügbar sind. Siehe [Erstellen einer Datei für die Zertifikatsignieranforderung](#).

- Stellen Sie sicher, dass eine Zertifikatssperrliste (CRL) verfügbar ist. Siehe [Importieren einer Zertifikatswiderrufsliste](#).
- [Konfigurieren des Pools und der Regeln eines virtuellen Servers der Schicht 7](#)  
Auf virtuellen Servern der Schicht 7 können Sie optional Load Balancer-Regeln konfigurieren und das Lastausgleichsverhalten unter Verwendung von Übereinstimmungs- oder Aktionsregeln anpassen.
- [Konfigurieren von Load Balancing-Profilen für virtuelle Server der Schicht 7](#)  
Mit virtuellen Servern der Schicht 7 können Sie optional Load Balancer-, Persistenz-, clientseitige und serverseitige SSL-Profile konfigurieren.

## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Integritätsüberwachungen > Netzwerk > Load Balancer > Virtuelle Server > Hinzufügen**.
- 3 Geben Sie einen Namen und eine Beschreibung für den virtuellen Server der Schicht 7 ein.
- 4 Wählen Sie das Menüelement „Schicht 7“ aus.  
  
Virtuelle Server der Schicht 7 unterstützen das HTTP- und HTTPS-Protokoll.  
  
Das vorhandene HTTP-Anwendungsprofil wird automatisch befüllt.
- 5 (Optional) Klicken Sie auf **Weiter** , um Serverpool- und Load Balancing-Profile zu konfigurieren.
- 6 Klicken Sie auf **Fertigstellen**.

## Konfigurieren des Pools und der Regeln eines virtuellen Servers der Schicht 7

Auf virtuellen Servern der Schicht 7 können Sie optional Load Balancer-Regeln konfigurieren und das Lastausgleichsverhalten unter Verwendung von Übereinstimmungs- oder Aktionsregeln anpassen.

Load Balancer-Regeln unterstützen die Verwendung von regulären Ausdrücken (Regex) für Übereinstimmungstypen. Regex-Muster nach PCRE-Art werden mit einigen Einschränkungen für anspruchsvollere Anwendungsfälle unterstützt. Wenn Regex in Übereinstimmungsbedingungen verwendet wird, werden benannte erfassende Gruppierungskonstrukte unterstützt.

Bezüglich der Verwendung von Regex gelten folgende Einschränkungen:

- Vereinigungen und Schnittmengen von Zeichenklassen werden nicht unterstützt. Verwenden Sie beispielsweise nicht `[a-z[0-9]]` und `[a-z&&[aeiou]]`, sondern stattdessen `[a-z0-9]` bzw. `[aeiou]`.
- Es werden nur 9 Rückverweise unterstützt, und man kann sie mit Hilfe von `\1` bis `\9` referenzieren.
- Verwenden Sie zum Abgleichen von Oktalzeichen das `\Odd`-Format, nicht das `\ddd`-Format.

- Eingebettete Flags werden auf der obersten Ebene nicht unterstützt. Sie können nur innerhalb von Gruppen verwendet werden. Verwenden Sie beispielsweise nicht „Case (?i:sensitive“, sondern stattdessen „Case ((?i:sensitive)“.
- Die Vorverarbeitungsoperationen \l, \u, \L und \U werden nicht unterstützt. Dabei steht \l für Kleinschreibung des nächsten Zeichens, \u für Großschreibung des nächsten Zeichens, \L für Kleinschreibung bis \E und \U für Großschreibung bis \E.
- „(?(condition)X)“, „(?{Code})“, „(??{Code})“ und „(?#comment)“ werden nicht unterstützt.
- Die vordefinierte Unicode-Zeichenklasse \X wird nicht unterstützt
- Die Verwendung von benannten Zeichenkonstrukten für Unicode-Zeichen wird nicht unterstützt. Verwenden Sie beispielsweise nicht „\N{name}“, sondern stattdessen „\u2018“.

Wenn Regex in Übereinstimmungsbedingungen verwendet wird, werden benannte erfassende Gruppierungskonstrukte unterstützt. Beispielsweise kann das Regex-Übereinstimmungsmuster „/news/(?<year>\d+)-(?(month>\d+)-(?(day>\d+)/(?<article>.\*))“ für den Abgleich mit einem URI wie „/news/2018-06-15/news1234.html“ verwendet werden.

Dann werden die Variablen wie folgt belegt: \$year = "2018", \$month = "06", \$day = "15" und \$article = "news1234.html". Nachdem Sie die Variablen festgelegt haben, können diese in Regeln eines Load Balancers verwendet werden. Der URI kann z. B. mithilfe der übereinstimmenden Variablen wie „/news.py?year=\$year&month=\$month&day=\$day&article=\$article“ umgeschrieben werden. Dann wird der URI in „/news.py?year=2018&month=06&day=15&article=news1234.html“ umgeschrieben.

Umschreibungsaktionen können eine Kombination von benannten Erfassungsgruppen und integrierten Variablen verwenden. Der URI kann beispielsweise als „/news.py?year=\$year&month=\$month&day=\$day&article=\$article&user\_ip=\$\_remote\_addr“ geschrieben werden. Der Beispiel-URI wird dann in „/news.py?year=2018&month=06&day=15&article=news1234.html&user\_ip=1.1.1.1“ umgeschrieben.

---

**Hinweis** Der Name einer benannten Erfassungsgruppe darf nicht mit einem Unterstrich (\_) beginnen.

---

Zusätzlich zu benannten Erfassungsgruppen können die folgenden integrierten Variablen in Umschreibungsaktionen verwendet werden. Alle Namen der integrierten Variablen beginnen mit Unterstrich (\_).

- \$\_args – Argumente der Anforderung
- \$\_cookie\_<name> – Wert des <name>-Cookies
- \$\_host – in der folgenden Rangfolge: der Hostname aus der Anforderungszeile oder der Hostname im Anforderungsheader-Feld „Host“ oder der mit einer Anforderung übereinstimmende Servername
- \$\_hostname – Hostname
- \$\_http\_<name> – beliebiges Feld des Anforderungsheaders; <name> ist der Name des Felds, konvertiert in Kleinbuchstaben, in dem Bindestriche durch Unterstriche ersetzt wurden.



- `$_https` – „on“, wenn die Verbindung im SSL-Modus arbeitet, andernfalls „“
- `$_is_args` – „?“ , wenn eine Anforderungszeile Argumente enthält, andernfalls „“
- `$_query_string` – identisch mit „`$_args`“
- `$_remote_addr` – Client-Adresse
- `$_remote_port` – Client-Port
- `$_request_uri` – vollständiger ursprünglicher Anforderungs-URI (mit Argumenten)
- `$_scheme` – Anforderungsschema, „http“ oder „https“
- `$_server_addr` – Adresse des Servers, der eine Anforderung akzeptiert hat
- `$_server_name` – Name des Servers, der eine Anforderung akzeptiert hat
- `$_server_port` – Port des-Servers, der eine Anforderung akzeptiert hat
- `$_server_protocol` – Anforderungsprotokoll, in der Regel „HTTP/1.0“ oder „HTTP/1.1“
- `$_ssl_client_cert` – gibt für eine eingerichtete SSL-Verbindung das Client-Zertifikat im PEM-Format zurück, wobei jeder Zeile außer der ersten ein Tabulatorzeichen vorangestellt ist
- `$_ssl_server_name` – gibt den über SNI angeforderten Servernamen zurück
- `$_uri` – URI-Pfad in der Anforderung
- `$_ssl_ciphers`: Gibt die Client-SSL-Verschlüsselungen zurück
- `$_ssl_client_i_dn`: Gibt die „Aussteller-DN“-Zeichenfolge des Clientzertifikats für eine eingerichtete SSL-Verbindung gemäß RFC 2253 zurück
- `$_ssl_client_s_dn`: Gibt die „Antragsteller-DN“-Zeichenfolge des Clientzertifikats für eine eingerichtete SSL-Verbindung gemäß RFC 2253 zurück
- `$_ssl_protocol`: Gibt das Protokoll einer eingerichteten SSL-Verbindung zurück
- `$_ssl_session_reused`: Gibt „r“ zurück, wenn eine SSL-Sitzung wiederverwendet wurde, oder andernfalls „“

### Voraussetzungen

Stellen Sie sicher, dass ein virtueller Server der Schicht 7 verfügbar ist. Siehe [Konfigurieren von virtuellen Servern der Schicht 7](#).

### Verfahren

- 1 Öffnen Sie den virtuellen Server der Schicht 7.
- 2 Öffnen Sie die Seite „Bezeichner für virtuelle Server“.
- 3 Geben Sie die IP-Adresse und Portnummer des virtuellen Servers ein.  
Sie können die Portnummer oder den Portbereich des virtuellen Servers eingeben.

#### 4 Geben Sie die erweiterten Eigenschaften an.

Option	Beschreibung
<b>Maximale Anzahl gleichzeitiger Verbindungen</b>	Legen Sie die maximale Anzahl gleichzeitiger Verbindungen fest, die für einen virtuellen Server zulässig sind, damit der virtuelle Server nicht die Ressourcen anderer Anwendung verbraucht, die vom selben Load Balancer gehostet werden.
<b>Maximale Anzahl neuer Verbindungen</b>	Legen Sie die maximale Anzahl neuer Verbindungen für ein Serverpoolmitglied fest, damit ein virtueller Server die Ressourcen nicht überlastet.
<b>Standardport des Poolmitglieds</b>	Geben Sie den Standardport eines Poolmitglieds ein, wenn der Port des Poolmitglieds für einen virtuellen Server nicht definiert ist.  Wenn ein virtueller Server beispielsweise mit dem Portbereich 2000-2999 definiert ist und der Standardportbereich des Poolmitglieds auf 8000-8999 festgelegt ist, wird eine eingehende Clientverbindung für Port 2500 des virtuellen Servers an ein Poolmitglied mit einem auf 8500 gesetzten Zielport gesendet.

#### 5 (Optional) Wählen Sie im Dropdown-Menü einen vorhandenen Standardserverpool aus.

Der Serverpool besteht aus einem oder mehreren als Poolmitglieder bezeichneten Servern mit ähnlicher Konfiguration, auf denen dieselbe Anwendung ausgeführt wird.

#### 6 Klicken Sie auf **Hinzufügen**, um die Load Balancer-Regel für die Phase „Umschreiben der HTTP-Anfrage“ zu konfigurieren.

Zu den unterstützten Übereinstimmungstypen gehören REGEX, STARTS\_WITH, ENDS\_WITH usw. sowie die Inverse-Option.

Unterstützte Übereinstimmungsbedingung	Beschreibung
<b>HTTP-Anforderungsmethode</b>	Zuordnen einer HTTP-Anforderungsmethode. http_request.method – zuzuordnender Wert
<b>HTTP-Anforderungs-URI</b>	Zuordnen einer HTTP-Anforderungs-URI ohne Abfrageargumente. http_request.uri – zuzuordnender Wert
<b>Argumente des HTTP-Anforderungs-URI</b>	Zuordnen des Abfragearguments eines HTTP-Anforderungs-URI. http_request.uri_arguments – zuzuordnender Wert
<b>HTTP-Anforderungsversion</b>	Zuordnen einer HTTP-Anforderungsversion. http_request.version – zuzuordnender Wert
<b>HTTP-Anforderungs-Header</b>	Zuordnen eines beliebigen HTTP-Anforderungs-Headers. http_request.header_name – zuzuordnender Header-Name http_request.header_value – zuzuordnender Wert
<b>HTTP-Anforderungsnutzlast</b>	Zuordnen des Inhalts eines HTTP-Anforderungstexts. http_request.body_value – zuzuordnender Wert

<b>Unterstützte Übereinstimmungsbedingung</b>	<b>Beschreibung</b>
<b>Felder des TCP-Headers</b>	Zuordnen einer TCP-Quelle oder des Zielports. tcp_header.source_port – zuzuordnender Quellport tcp_header.destination_port – zuzuordnender Zielport
<b>Felder des IP-Headers</b>	Zuordnen einer IP-Quelladresse oder -Zieladresse ip_header.source_address – zuzuordnende Quelladresse ip_header.destination_address – zuzuordnende Zieladresse
<b>Aktion</b>	<b>Beschreibung</b>
<b>HTTP-Anforderungs-URI umschreiben</b>	Ändern eines URI. http_request.uri – zu schreibender URI (ohne Abfrageargumente) http_request.uri_args – zu schreibende URI-Abfrageargumente
<b>HTTP-Anforderungs-Header umschreiben</b>	Ändern des Werts eines HTTP-Headers. http_request.header_name – Name des Headers http_request.header_value – zu schreibender Wert

- 7 Klicken Sie auf **Hinzufügen**, um die Load Balancer-Regeln für die HTTP-Anforderungsweiterleitung zu konfigurieren.

Alle Übereinstimmungswerte akzeptieren reguläre Ausdrücke.

<b>Unterstützte Übereinstimmungsbedingung</b>	<b>Beschreibung</b>
<b>HTTP-Anforderungsmethode</b>	Zuordnen einer HTTP-Anforderungsmethode. http_request.method – zuzuordnender Wert
<b>HTTP-Anforderungs-URI</b>	Zuordnen eines HTTP-Anforderungs-URI. http_request.uri – zuzuordnender Wert
<b>Argumente des HTTP-Anforderungs-URI</b>	Zuordnen des Abfragearguments eines HTTP-Anforderungs-URI. http_request.uri_args – zuzuordnender Wert
<b>HTTP-Anforderungsversion</b>	Zuordnen einer HTTP-Anforderungsversion. http_request.version – zuzuordnender Wert
<b>HTTP-Anforderungs-Header</b>	Zuordnen eines beliebigen HTTP-Anforderungs-Headers. http_request.header_name – zuzuordnender Header-Name http_request.header_value – zuzuordnender Wert
<b>HTTP-Anforderungsnutzlast</b>	Zuordnen des Inhalts eines HTTP-Anforderungstexts. http_request.body_value – zuzuordnender Wert

Unterstützte Übereinstimmungsbedingung	Beschreibung
<b>Felder des TCP-Headers</b>	Zuordnen einer TCP-Quelle oder des Zielports. tcp_header.source_port – zuzuordnender Quellport tcp_header.destination_port – zuzuordnender Zielport
<b>Felder des IP-Headers</b>	Zuordnen einer IP-Quelladresse ip_header.source_address – zuzuordnende Quelladresse
<b>Aktion</b>	<b>Beschreibung</b>
<b>Ablehnen</b>	Ablehnen einer Anforderung, beispielsweise durch Setzen des Status auf 5xx. http_forward.reply_status – zum Ablehnen verwendeter HTTP-Statuscode http_forward.reply_message – HTTP-Ablehnungsnachricht
<b>Umleiten</b>	Umleiten einer Anforderung. Statuscode muss auf 3xx gesetzt werden. http_forward.redirect_status – HTTP-Statuscode für Umleiten http_forward.redirect_url – HTTP-Umleitungs-URL
<b>Pool auswählen</b>	Erzwingen der Anforderung auf einem bestimmten Serverpool. Der konfigurierte Algorithmus (Prognose) der angegebenen Poolmitglieder wird verwendet, um einen Server im Serverpool auszuwählen. http_forward.select_pool – UUID des Serverpools

- 8 Klicken Sie auf **Hinzufügen**, um die Load Balancer-Regeln für das Umschreiben der HTTP-Antwort zu konfigurieren.

Alle Übereinstimmungswerte akzeptieren reguläre Ausdrücke.

Unterstützte Übereinstimmungsbedingung	Beschreibung
<b>HTTP-Antwort-Header</b>	Zuordnen eines beliebigen HTTP-Antwort-Headers. http_response.header_name – zuzuordnender Header-Name http_response.header_value – zuzuordnender Wert
<b>Aktion</b>	<b>Beschreibung</b>
<b>HTTP-Antwort-Header umschreiben</b>	Ändern des Werts eines HTTP-Antwort-Headers. http_response.header_name – Name des Headers http_response.header_value – zu schreibender Wert

- 9 (Optional) Klicken Sie auf **Weiter**, um Load Balancer-Profil zu konfigurieren.

- 10 Klicken Sie auf **Fertigstellen**.

## Konfigurieren von Load Balancing-Profilen für virtuelle Server der Schicht 7

Mit virtuellen Servern der Schicht 7 können Sie optional Load Balancer-, Persistenz-, clientseitige und serverseitige SSL-Profile konfigurieren.

---

**Hinweis** SSL-Profile werden in der Version NSX-T Data Center Limited Export nicht unterstützt.

---

Wenn eine clientseitige, nicht aber eine serverseitige SSL-Profilbindung auf einem virtuellen Server konfiguriert wurde, wird der virtuelle Server im SSL-Terminate-Modus ausgeführt, der eine verschlüsselte Verbindung zum Client und eine Klartextverbindung zum Server aufweist. Wenn sowohl die clientseitigen als auch die serverseitigen SSL-Profilbindungen konfiguriert sind, wird der virtuelle Server im SSL-Proxy-Modus ausgeführt, der eine verschlüsselte Verbindung zum Client und Server aufweist.

Das Zuordnen einer serverseitigen SSL-Profilbindung ohne Zuordnung einer clientseitigen SSL-Profilbindung wird aktuell nicht unterstützt. Wenn weder eine clientseitige noch eine serverseitige SSL-Profilbindung mit einem virtuellen Server verknüpft und die Anwendung SSL-basiert ist, wird der virtuelle Server im SSL-Unaware-Modus ausgeführt. In diesem Fall muss der virtuelle Server für Schicht 4 konfiguriert werden. Der virtuelle Server kann beispielsweise einem Fast TCP-Profil zugeordnet werden.

### Voraussetzungen

Stellen Sie sicher, dass ein virtueller Server der Schicht 7 verfügbar ist. Siehe [Konfigurieren von virtuellen Servern der Schicht 7](#).

### Verfahren

- 1 Öffnen Sie den virtuellen Server der Schicht 7.
- 2 Wechseln Sie zur Seite „Load Balancing-Profile“.
- 3 Schalten Sie die Schaltfläche „Persistenz“ zur Aktivierung des Profils um.  
Persistenzprofile ermöglichen das Senden verwandter Clientverbindungen an denselben Server.
- 4 Wählen Sie entweder das Profil „IP-Quellpersistenz“ oder „Cookie-Persistenz“ aus.
- 5 Wählen Sie im Dropdown-Menü ein vorhandenes Persistenzprofil aus.
- 6 Klicken Sie auf **Weiter**.
- 7 Schalten Sie die Schaltfläche „Clientseitiges SSL“ zum Aktivieren des Profils um.  
Clientseitige SSL-Profilbindung ermöglicht mehrere Zertifikate, damit verschiedene Hostnamen mit demselben virtuellen Server verbunden werden können.  
Das zugehörige clientseitige SSL-Profil wird automatisch befüllt.

- 8 Wählen Sie im Dropdown-Menü ein Standardzertifikat aus.

Dieses Zertifikat wird verwendet, wenn der Server nicht mehrere Hostnamen auf derselben IP-Adresse hostet oder wenn der Client keine Unterstützung für SNI-Erweiterungen (Server Name Indication) bietet.

- 9 Wählen Sie das verfügbare SNI-Zertifikat aus und klicken Sie auf den Pfeil, um das Zertifikat in den Abschnitt „Ausgewählt“ zu verschieben.

- 10 (Optional) Schalten Sie „Obligatorische Clientauthentifizierung“ zum Aktivieren dieses Menüelements um.

- 11 Wählen Sie das verfügbare CA-Zertifikat aus und klicken Sie auf den Pfeil, um das Zertifikat in den Abschnitt „Ausgewählt“ zu verschieben.

- 12 Legen Sie die Tiefe der Zertifikatskette fest, um die Tiefe in der Serverzertifikatskette zu überprüfen.

- 13 Wählen Sie die verfügbare Zertifikatssperrliste aus und klicken Sie auf den Pfeil, um das Zertifikat in den Abschnitt „Ausgewählt“ zu verschieben.

Eine Zertifikatssperrliste kann konfiguriert werden, um gefährdete Serverzertifikate nicht zuzulassen.

- 14 Klicken Sie auf **Weiter**.

- 15 Schalten Sie die Schaltfläche „Serverseitiges SSL“ zum Aktivieren des Profils um.

Das zugeordnete serverseitige SSL-Profil wird automatisch befüllt.

- 16 Wählen Sie im Dropdown-Menü ein Clientzertifikat aus.

Das Clientzertifikat wird verwendet, wenn der Server nicht mehrere Hostnamen auf derselben IP-Adresse hostet oder wenn der Client keine Unterstützung für SNI-Erweiterungen (Server Name Indication) bietet.

- 17 Wählen Sie das verfügbare SNI-Zertifikat aus und klicken Sie auf den Pfeil, um das Zertifikat in den Abschnitt „Ausgewählt“ zu verschieben.

- 18 (Optional) Schalten Sie „Serverauthentifizierung“ zum Aktivieren dieses Menüelements um.

Eine serverseitige SSL-Profilbindung gibt an, ob das dem Load Balancer während des SSL-Handshakes präsentierte Serverzertifikat validiert werden muss. Bei aktivierter Validierung muss das Serverzertifikat von einer der vertrauenswürdigen Zertifizierungsstellen signiert sein, deren selbstsignierte Zertifikate in derselben serverseitigen SSL-Profilbindung angegeben sind.

- 19 Wählen Sie das verfügbare CA-Zertifikat aus und klicken Sie auf den Pfeil, um das Zertifikat in den Abschnitt „Ausgewählt“ zu verschieben.

- 20 Legen Sie die Tiefe der Zertifikatskette fest, um die Tiefe in der Serverzertifikatskette zu überprüfen.

- 21** Wählen Sie die verfügbare Zertifikatssperrliste aus und klicken Sie auf den Pfeil, um das Zertifikat in den Abschnitt „Ausgewählt“ zu verschieben.

Eine Zertifikatssperrliste kann konfiguriert werden, um gefährdete Serverzertifikate nicht zuzulassen. OCSP und OCSP-Heftung werden serverseitig nicht unterstützt.

- 22** Klicken Sie auf **Fertigstellen**.

---

**Hinweis** Wenn Sie die Benutzeroberfläche **Netzwerk und Sicherheit – Erweitert** verwenden, um in der Richtlinienchnittstelle erstellte Objekte zu ändern, sind einige Einstellungen möglicherweise nicht konfigurierbar. Neben diesen schreibgeschützten Einstellungen wird dieses Symbol angezeigt: ☹. Weitere Informationen hierzu finden Sie unter [Kapitel 1 Übersicht über NSX Manager](#).

---

Dieses Kapitel enthält die folgenden Themen:

- [Firewallabschnitte und Firewallregeln](#)

## Firewallabschnitte und Firewallregeln

Mit Firewallabschnitten werden Firewallregeln gruppenweise zusammengefasst.

Ein Firewallabschnitt besteht aus einer oder mehreren Firewallregeln. Jede einzelne Firewallregel enthält Anweisungen, die festlegen, ob ein Paket zugelassen oder blockiert werden soll, welches Protokoll verwendet werden darf, welche Ports für die Verwendung zulässig sind etc. Abschnitte dienen der Mehrinstanzenfähigkeit, z. B. durch eigene Regeln für die Vertriebs- und die Technikabteilung in unterschiedlichen Abschnitten.

Ein Abschnitt kann für die Erzwingung zustandsbehafteter oder zustandsfreier Regeln definiert werden. Zustandsfreie Regeln werden als herkömmliche zustandsfreie ACLs behandelt. Reflexive ACLs werden für zustandsfreie Abschnitte nicht unterstützt. Die Kombination von zustandsbehafteten und zustandsfreien Regeln auf einem einzelnen logischen Switch Port wird nicht empfohlen, da dies zu einem unvorhergesehenen Verhalten führen kann.

Regeln lassen sich innerhalb eines Abschnitts nach oben und unten versetzen. Für jeden Datenverkehr, der die Firewall passieren soll, müssen die Paketinformationen den Regeln in der Reihenfolge genügen, wie Sie im Abschnitt angegeben sind. Die Überprüfung beginnt an oberster Stelle und wird bis zur Standardregel unten fortgesetzt. Für die erste Regel, die dem Paket entspricht, wird die dafür konfigurierte Aktion angewendet. Die in den konfigurierten Optionen der Regel festgelegte Verarbeitung wird durchgeführt und all nachfolgenden Regeln werden ignoriert (auch wenn eine spätere Regel besser passen würde). Deshalb ist es empfehlenswert,



spezifischere Regeln vor allgemeineren Regeln zu platzieren, um sicherzustellen, dass diese Regeln wirksam werden können. Die am Ende der Regeltabelle platzierte Standardregel ist eine „Catchall“-Regel, die grundsätzlich gilt. Für Pakete, für die keine anderen Regeln gelten, wird die Standardregel angewendet.

---

**Hinweis** Ein logischer Switch verfügt über eine Eigenschaft namens N-VDS-Modus. Diese Eigenschaft stammt aus der Transportzone, zu der der Switch gehört. Lautet der N-VDS-Modus ENS (auch bekannt als Enhanced Datapath), können Sie keine Firewallregel und keinen Firewallabschnitt erstellen, wenn der Switch oder seine Ports in den Feldern **Source**, **Destination** oder **Applied To** stehen.

---

## Hinzufügen eines Firewallregelabschnitts

Ein Firewallregelabschnitt lässt sich separat bearbeiten bzw. speichern und wird zur Anwendung eigener Firewallkonfigurationen für Mandanten verwendet.

### Verfahren

- 1 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Sicherheit > Verteilte Firewall** aus.
- 2 Klicken Sie auf die Registerkarte **Allgemein** für Schicht-3-(L3-)Regeln oder auf die Registerkarte **Ethernet** für Schicht-2-(L2-)Regeln.
- 3 Klicken Sie auf einen vorhandenen Abschnitt oder eine vorhandene Regel.
- 4 Klicken Sie in der Menüleiste auf das Symbol „Abschnitt“ und wählen Sie **Abschnitt oben hinzufügen** oder **Abschnitt unten hinzufügen** aus.

---

**Hinweis** Für jeden Datenverkehr, der die Firewall passieren soll, müssen die Paketinformationen den Regeln in der Reihenfolge genügen, wie Sie in der Regeltabelle angegeben werden. Die Überprüfung beginnt mit den Regeln an oberster Stelle und wird bis zu den Standardregeln unten fortgesetzt. In einigen Fällen kann die Rangfolge von zwei oder mehr Regeln für die Bestimmung der Disposition eines Pakets wichtig sein.

---

- 5 Geben Sie den Abschnittsnamen ein.
- 6 Um eine statusfreie Firewall zu erzwingen, wählen Sie die Option **Statusfreie Firewall aktivieren** aus. Diese Option steht nur für L3 zur Verfügung.

Zustandsfreie Firewalls überwachen den Netzwerkdatenverkehr und beschränken oder blockieren Pakete auf der Grundlage von Quell- und Zieladressen oder anderen statischen Werten. Zustandsbehaftete Firewalls ermöglichen eine End-to-End-Überwachung von Datenverkehr-Streams. Zustandsfreie Firewalls sind in der Regel schneller und bieten eine bessere Leistung bei hohem Datenverkehrsaufkommen. Mit zustandsbehafteten Firewalls lässt sich eine unberechtigte oder gefälschte Kommunikation besser ermitteln. Nach der Definition einer Firewall kann diese nicht von zustandsfrei auf zustandsbehaftet und umgekehrt geändert werden.

- 7 Wählen Sie ein oder mehrere Objekte zur Anwendung des Abschnitts aus.

Die Objekttypen sind logische Ports, logische Switches und NS-Gruppen. Wenn Sie eine NS-Gruppe auswählen, muss sie einen oder mehrere logische Switches oder logische Ports enthalten. Wenn die NS-Gruppe nur IP Sets oder MAC Sets enthält, wird sie ignoriert.

---

**Hinweis** Die Option **Angewendet auf** in einem Abschnitt hat Vorrang vor jeglichen Einstellungen für **Angewendet auf** in den Regeln dieses Abschnitts.

---

- 8 Klicken Sie auf **OK**.

#### Nächste Schritte

Fügen Sie dem Abschnitt Firewallregeln hinzu.

## Löschen eines Firewallregelabschnitts

Der Abschnitt einer Firewallregel kann gelöscht werden, wenn er nicht mehr benötigt wird.

Wenn Sie den Abschnitt einer Firewallregel löschen, werden alle Regeln dieses Abschnitts gelöscht. Sie können einen Abschnitt löschen und zu einem anderen Ort in der Firewalltabelle hinzufügen. Dazu müssen Sie den Abschnitt löschen und die Konfiguration veröffentlichen. Fügen Sie anschließend den gelöschten Abschnitt zur Firewalltabelle hinzu und veröffentlichen Sie die Konfiguration erneut.

#### Verfahren

- 1 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Sicherheit > Verteilte Firewall** aus.
- 2 Klicken Sie auf die Registerkarte **Allgemein** für L3-Regeln oder auf die Registerkarte **Ethernet** für L2-Regeln.
- 3 Klicken Sie auf das Menüsymbol in der ersten Spalte des Abschnitts und wählen Sie **Abschnitt löschen** aus.

Sie können auch den Abschnitt auswählen und auf das Symbol „Löschen“ in der Menüleiste klicken.

## Aktivieren und Deaktivieren von Abschnittsregeln

Sie können alle Regeln in einem Firewallregelabschnitt aktivieren bzw. deaktivieren.

#### Verfahren

- 1 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Sicherheit > Verteilte Firewall** aus.
- 2 Klicken Sie auf die Registerkarte **Allgemein** für L3-Regeln oder auf die Registerkarte **Ethernet** für L2-Regeln.
- 3 Klicken Sie auf das Menüsymbol in der ersten Spalte des Abschnitts und wählen Sie **Alle Regeln aktivieren** oder **Alle Regeln deaktivieren** aus.
- 4 Klicken Sie auf **Veröffentlichen**.

## Aktivieren und Deaktivieren von Abschnittsprotokollen

Durch Aktivierung von Protokollen für Abschnittsregeln werden Paketinformationen für alle Regeln eines Abschnitts dokumentiert. Je nach Anzahl der Regeln in einem Abschnitt generiert ein typischer Firewallabschnitt eine große Anzahl an Protokollinformationen, die die Leistung beeinflussen können.

Die Protokolle werden in der Datei `/var/log/dfwpktlogs.log` auf ESXi- und KVM-Hosts gespeichert.

### Verfahren

- 1 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Sicherheit > Verteilte Firewall** aus.
- 2 Klicken Sie auf die Registerkarte **Allgemein** für L3-Regeln oder auf die Registerkarte **Ethernet** für L2-Regeln.
- 3 Klicken Sie auf das Menüsymbol in der ersten Spalte des Abschnitts und wählen Sie **Protokolle aktivieren** oder **Protokolle deaktivieren** aus.
- 4 Klicken Sie auf **Veröffentlichen**.

## Informationen über Firewallregeln

NSX-T Data Center legt mit Firewallregeln die Handhabung des Datenverkehrs zu und von einem Netzwerk fest.

Eine Firewall bietet mehrere Sets konfigurierbarer Regeln: Schicht-3-Regeln (Registerkarte „Allgemein“) und Schicht-2-Regeln (Registerkarte „Ethernet“). Schicht-2-Firewallregeln werden vor Schicht-3-Regeln verarbeitet. Sie können eine Ausschlussliste mit logischen Switches, logischen Ports oder Gruppen konfigurieren, die von der Firewallerzwingung ausgeschlossen werden sollen.

Firewallregeln werden wie folgt angewendet:

- Die Regeln werden von oben nach unten verarbeitet.
- Jedes Paket wird anhand der obersten Regel in der Regeltabelle überprüft, bevor zu den nächsten Regeln in der Tabelle nach unten übergegangen wird.
- Die erste Regel in der Tabelle, die den Datenverkehrsparametern entspricht, wird erzwungen.

Es können keine nachfolgenden Regeln angewendet werden, da die Suche für dieses Paket dann beendet wird. Aufgrund dieses Verhaltens ist es empfehlenswert, immer die detailliertesten Richtlinien an den Anfang der Regeltabelle zu stellen. Damit wird sichergestellt, dass diese vor den spezifischeren Regeln angewendet werden.

Die am Ende der Regeltabelle platzierte Standardregel ist eine „Catchall“-Regel, die grundsätzlich gilt. Für Pakete, für die keinen anderen Regeln gelten, wird die Standardregel angewendet. Nach der Hostvorbereitung sind gemäß der Standardregel Aktionen möglich. Damit ist sichergestellt, dass die Kommunikation von VM zu VM während der Staging- oder Migrationsphase nicht

unterbrochen wird. Als Best Practice sollte dann diese Standardregel geändert werden, um Aktionen zu blockieren und die Zugriffskontrolle über ein positives Kontrollmodell zu erzwingen. In einem solchen Modell ist nur Datenverkehr für das Netzwerk zulässig, der in der Firewallregel definiert ist.

**Hinweis** „Strenges TCP“ kann pro Abschnitt aktiviert werden, um das Abrufen mitten in der Sitzung zu deaktivieren und die Anforderung für einen 3-Wege-Handshake zu erzwingen. Wenn Sie den Modus „Strenges TCP“ für einen bestimmten Abschnitt der verteilten Firewall aktivieren und eine standardmäßige Blockregel vom Typ ANY-ANY verwenden, werden Pakete, die die 3-Wege-Handshake-Verbindungsanforderungen nicht erfüllen und die mit einer TCP-basierten Regel in diesem Abschnitt übereinstimmen, verworfen. „Streng“ wird nur auf statusbehaftete TCP-Regeln angewendet und auf der Abschnittsebene der verteilten Firewall aktiviert. „Strenges TCP“ wird nicht für Pakete erzwungen, die mit einer standardmäßigen ANY-ANY-Zulassung übereinstimmen, wofür kein TCP-Dienst angegeben wurde.

**Tabelle 20-1. Eigenschaften einer Firewallregel**

Eigenschaft	Beschreibung
Name	Name der Firewallregel.
ID	Eindeutige, systemgenerierte ID für jede Regel.
Quelle	Bei der Quelle der Regel kann es sich entweder um eine IP- oder MAC-Adresse oder um ein anderes Objekt als eine IP-Adresse handeln. Wenn nicht definiert, bezieht sich die Regel auf alle Quellen. Für Quell- und Zielbereich werden sowohl IPv4 als auch IPv6 unterstützt.
Ziel	Die Ziel-IP- oder -MAC-Adresse/-Netmask der Verbindung, die von der Regel betroffen ist. Wenn nicht definiert, bezieht sich die Regel auf alle Ziele. Für Quell- und Zielbereich werden sowohl IPv4 als auch IPv6 unterstützt.
Dienst	Bei dem Dienst kann es sich um eine vordefinierte Portprotokollkombination für L3 handeln. Für L2 kann es „Ethernet-Typ“ sein. Sie haben sowohl für L2 wie für L3 die Möglichkeit, einen neuen Dienst oder eine neue Dienstgruppe manuell zu definieren. Wenn nicht angegeben, bezieht sich der Dienst auf alle Regeln.
Angewendet auf	Definiert den Bereich, auf den diese Regel anwendbar ist. Wenn die Option nicht definiert ist, besteht der Bereich aus allen logischen Ports. Wenn Sie in einem Abschnitt „Angewendet auf“ hinzugefügt haben, wird die Regel überschrieben.
Protokoll	Die Protokollierung lässt sich deaktivieren/aktivieren. Die Protokolle werden in der Datei /var/log/dfwpklogs.log auf ESX- und KVM-Hosts gespeichert.
Aktion	Die Regel kann die Aktionen <b>Zulassen</b> , <b>Verwerfen</b> und <b>Ablehnen</b> anwenden. Die Standardeinstellung ist <b>Zulassen</b> .
IP-Protokoll	Die Optionen sind <b>IPv4</b> , <b>IPv6</b> und <b>IPv4_IPv6</b> . Die Standardeinstellung ist <b>IPv4_IPv6</b> . Um auf diese Eigenschaft zuzugreifen, klicken Sie auf das Symbol <b>Erweiterte Einstellungen</b> .
Richtung	Die Optionen sind <b>Ein</b> , <b>Aus</b> und <b>Ein/Aus</b> . Die Standardeinstellung ist <b>Ein/Aus</b> . Dieses Feld bezieht sich auf die Richtung des Datenverkehrs aus der Sicht des Zielobjekts. <b>Eingehend</b> bedeutet, dass nur Datenverkehr an das Objekt überprüft wird, <b>Ausgehend</b> bedeutet, dass nur Datenverkehr aus dem Objekt überprüft wird, und <b>Ein/Aus</b> bedeutet, dass Datenverkehr in beide Richtungen überprüft wird. Um auf diese Eigenschaft zuzugreifen, klicken Sie auf das Symbol <b>Erweiterte Einstellungen</b> .

Tabelle 20-1. Eigenschaften einer Firewallregel (Fortsetzung)

Eigenschaft	Beschreibung
Regel-Tags	Tags, die der Regel hinzugefügt wurden. Um auf diese Eigenschaft zuzugreifen, klicken Sie auf das Symbol <b>Erweiterte Einstellungen</b> .
Flow-Statistik	Schreibgeschütztes Feld, das die Bytes, die Paketanzahl und die Sitzungen anzeigt. Um auf diese Eigenschaft zuzugreifen, klicken Sie auf das Diagrammsymbol.

**Hinweis** Wenn SpoofGuard nicht aktiviert ist, kann die Vertrauenswürdigkeit automatisch erkannter Adressbindungen nicht garantiert werden, da eine böartige virtuelle Maschine die Adresse einer anderen virtuellen Maschine beanspruchen kann. SpoofGuard (sofern aktiviert) überprüft jede erkannte Bindung, sodass nur zulässige Bindungen angezeigt werden.

## Hinzufügen einer Firewallregel

Eine Firewall ist ein Netzwerksicherheitssystem, das den eingehenden und ausgehenden Datenverkehr des Netzwerks auf der Grundlage vordefinierter Firewallregeln überwacht und kontrolliert.

Firewallregeln werden dem NSX Manager-Bereich hinzugefügt. Wenn Sie das Feld „Angewendet auf“ verwenden, können Sie den Geltungsbereich einschränken, in dem Sie die Regel anwenden möchten. Sie können mehrere Objekte auf Quell- und Zielebene für jede Regel hinzufügen, um so die Gesamtzahl der zu erstellenden Firewallregeln zu verringern.

**Hinweis** Standardmäßig gilt eine Regel für den Standard jedes Quell-, Ziel- und Dienstregelements sowie für alle Schnittstellen und Datenverkehrsrichtungen. Wenn Sie die Gültigkeit der Regel auf bestimmte Schnittstellen sowie Datenverkehrsrichtungen beschränken möchten, müssen Sie dies in der Regel entsprechend festlegen.

### Voraussetzungen

Um eine Gruppe von Adressen verwenden zu können, müssen Sie zuerst manuell die IP- und MAC-Adresse jeder VM ihrem logischen Switch zuordnen.

### Verfahren

- 1 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Sicherheit > Verteilte Firewall** aus.
- 2 Klicken Sie auf die Registerkarte **Allgemein** für L3-Regeln oder auf die Registerkarte **Ethernet** für L2-Regeln.
- 3 Klicken Sie auf einen vorhandenen Abschnitt oder eine vorhandene Regel.

- 4 Klicken Sie auf das Menüsymbol in der ersten Spalte einer Regel und wählen Sie **Regel oberhalb hinzufügen** oder **Regel unterhalb hinzufügen** aus.

Eine neue Zeile zur Definition einer Firewallregel wird angezeigt.

**Hinweis** Für jeden Datenverkehr, der die Firewall passieren soll, müssen die Paketinformationen den Regeln in der Reihenfolge genügen, wie Sie in der Regeltabelle angegeben werden. Die Überprüfung beginnt mit den Regeln an oberster Stelle und wird bis zu den Standardregeln unten fortgesetzt. In einigen Fällen kann die Rangfolge von zwei oder mehr Regeln für die Bestimmung der Disposition eines Pakets wichtig sein.

- 5 Geben Sie in der Spalte **Name** den Namen der Regel ein.
- 6 Klicken Sie in der Spalte **Quelle** auf das Symbol „Bearbeiten“ und wählen Sie die Quelle der Regel aus. Wenn nicht definiert, bezieht sich die Regel auf alle Quellen.

Option	Beschreibung
IP-Adresse n	Geben Sie mehrere IP- oder MAC-Adressen durch Kommas getrennt ein. Die Liste kann bis zu 255 Zeichen lang sein. Es wird sowohl das IPv4- als auch das IPv6-Format unterstützt.
Contain erobjekt e	Die verfügbaren Objekte sind IP Set, Logischer Port, Logischer Switch und NS-Gruppe. Wählen Sie die Objekte aus und klicken Sie auf <b>OK</b> .

- 7 Klicken Sie in der Spalte **Ziel** auf das Symbol „Bearbeiten“ und wählen Sie das Ziel aus. Wenn nicht definiert, bezieht sich die Regel auf alle Ziele.

Option	Beschreibung
IP-Adresse n	Sie können mehrere IP- oder MAC-Adressen in einer kommagetrennten Liste eingeben. Die Liste kann bis zu 255 Zeichen lang sein. Es wird sowohl das IPv4- als auch das IPv6-Format unterstützt.
Contain erobjekt e	Die verfügbaren Objekte sind IP Set, Logischer Port, Logischer Switch und NS-Gruppe. Wählen Sie die Objekte aus und klicken Sie auf <b>OK</b> .

- 8 Klicken Sie in der Spalte **Dienst** auf das Symbol „Bearbeiten“ und wählen Sie Dienste aus. Wenn nicht definiert, bezieht sich die Regel auf alle Dienste.
- 9 Um einen vordefinierten Dienst auszuwählen, wählen Sie einen oder mehrere der verfügbaren Dienste aus.

- 10 Um einen neuen Dienst zu definieren, klicken Sie auf die Registerkarte **Raw-Port-Protokoll** und anschließend auf **Hinzufügen**.

Option	Beschreibung
<b>Diensttyp</b>	<ul style="list-style-type: none"> <li>■ ALG</li> <li>■ ICMP</li> <li>■ IGMP</li> <li>■ IP</li> <li>■ L4-Port-Satz</li> </ul>
<b>Protokoll</b>	Wählen Sie eines der verfügbaren Protokolle aus.
<b>Quellports</b>	Geben Sie den Quellport ein.
<b>Zielpports</b>	Wählen Sie den Zielport aus.

- 11 Klicken Sie in der Spalte **Angewendet auf** auf das Symbol „Bearbeiten“ und wählen Sie Objekte aus.

- 12 Wählen Sie in der Spalte **Protokoll** die gewünschte Protokollierungsoption aus.

Die Protokolldaten werden in der Datei `/var/log/dfwpktlogs.log` auf ESXi- und KVM-Hosts gespeichert. Das Aktivieren der Protokollierung kann die Leistung beeinträchtigen.

- 13 Wählen Sie eine Aktion in der Spalte **Aktion** aus.

Option	Beschreibung
<b>Zulassen</b>	Ermöglicht dem gesamten L3- oder L2-Datenverkehr mit der angegebenen Quelle, dem angegebenen Ziel und Protokoll das Passieren des aktuellen Firewallkontextes. Pakete, die der Regel genügen und akzeptiert werden, durchlaufen das System wie beim Fehlen einer Firewall.
<b>Verwerfen</b>	Verwirft Pakete mit der angegebenen Quelle, dem angegebenen Ziel und Protokoll. Das Verwerfen eines Pakets erfolgt im Hintergrund ohne Benachrichtigung der Quell- oder Zielsysteme. Das Verwerfen des Pakets führt dazu, dass erneut versucht wird, die Verbindung herzustellen, bis der entsprechende Schwellenwert erreicht wird.
<b>Ablehnen</b>	Lehnt Pakete mit der angegebenen Quelle, dem angegebenen Ziel und Protokoll ab. Das Ablehnen eines Pakets ist der elegantere Weg, um das Senden eines Pakets zu verweigern. Dabei wird an den Sender eine Meldung übermittelt, dass das Ziel nicht erreichbar ist. Bei Verwendung des TCP-Protokolls wird eine TCP RST-Meldung gesendet. ICMP-Meldungen mit vom Administrator verbotenen Code werden für UDP-, ICMP- und andere IP-Verbindungen versendet. Die Methode des Ablehnens hat den Vorteil, dass die sendende Anwendung bereits nach einem Versuch benachrichtigt wird, dass die Verbindung nicht aufgebaut werden kann.

- 14 Klicken Sie auf das Symbol **Erweiterte Einstellungen**, um das IP-Protokoll, die Richtung, Regel-Tags und Kommentare anzugeben.

- 15 Klicken Sie auf **Veröffentlichen**.

## Löschen einer Firewallregel

Eine Firewall ist ein Netzwerksicherheitssystem, das den eingehenden und ausgehenden Datenverkehr des Netzwerks auf der Grundlage vordefinierter Firewallregeln überwacht und kontrolliert. Benutzerdefinierte Regeln können hinzugefügt und gelöscht werden.

### Verfahren

- 1 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Sicherheit > Verteilte Firewall** aus.
- 2 Klicken Sie auf die Registerkarte **Allgemein** für L3-Regeln oder auf die Registerkarte **Ethernet** für L2-Regeln.
- 3 Klicken Sie auf das Menüsymbol in der ersten Spalte der Regel und wählen Sie **Regel löschen** aus.
- 4 Klicken Sie auf **Veröffentlichen**.

## Bearbeiten der standardmäßigen Regel für die verteilte Firewall

Sie können die standardmäßigen Firewall Einstellungen, die für den Datenverkehr gelten, der unter keine der benutzerdefinierten Firewallregeln fällt, bearbeiten.

Die standardmäßigen Firewallregeln gelten für den Datenverkehr, der unter keine der benutzerdefinierten Firewallregeln fällt. Die standardmäßige Schicht-3-Regel finden Sie auf der Registerkarte **Allgemein**, die standardmäßige Schicht-2-Regel auf der Registerkarte **Ethernet**.

Die standardmäßigen Firewallregeln lassen die Durchleitung von L3- und L2-Datenverkehr durch alle vorbereiteten Cluster in Ihrer Infrastruktur zu. Die Standardregel befindet sich immer am Ende der Regeltabelle und kann nicht gelöscht werden. Sie können jedoch für die Regel das Element **Aktion** von **Zulassen** in **Verwerfen** oder **Ablehnen** (nicht empfohlen) ändern und angeben, ob der Datenverkehr für diese Regel protokolliert werden soll.

Die standardmäßige Schicht-3-Firewallregel gilt für den gesamten Datenverkehr, einschließlich DHCP. Wenn Sie die **Aktion** in **Verwerfen** oder **Ablehnen** ändern, wird der DHCP-Datenverkehr blockiert. Sie müssen eine Regel erstellen, um DHCP-Datenverkehr zuzulassen.

### Verfahren

- 1 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Sicherheit > Verteilte Firewall** aus.
- 2 Klicken Sie auf die Registerkarte **Allgemein** für L3-Regeln oder auf die Registerkarte **Ethernet** für L2-Regeln.
- 3 Geben Sie in der Spalte **Name** einen neuen Namen ein.
- 4 Wählen Sie in der Spalte **Aktion** eine der Optionen aus.
  - Zulassen – Ermöglicht dem gesamten L3- oder L2-Datenverkehr mit der angegebenen Quelle, dem angegebenen Ziel und Protokoll das Passieren des aktuellen Firewallkontextes. Pakete, die der Regel genügen und akzeptiert werden, durchlaufen das System wie beim Fehlen einer Firewall.



- **Verwerfen** – Verwirft Pakete mit der angegebenen Quelle, dem angegebenen Ziel und Protokoll. Das Verwerfen eines Pakets erfolgt im Hintergrund ohne Benachrichtigung der Quell- oder Zielsysteme. Das Verwerfen des Pakets führt dazu, dass erneut versucht wird, die Verbindung herzustellen, bis der entsprechende Schwellenwert erreicht wird.
- **Ablehnen** – Lehnt Pakete mit der angegebenen Quelle, dem angegebenen Ziel und Protokoll ab. Das Ablehnen eines Pakets ist der elegantere Weg, um das Senden eines Pakets zu verweigern. Dabei wird an den Sender eine Meldung übermittelt, dass das Ziel nicht erreichbar ist. Bei Verwendung des TCP-Protokolls wird eine TCP RST-Meldung gesendet. ICMP-Meldungen mit vom Administrator verbotenen Code werden für UDP-, ICMP- und andere IP-Verbindungen versendet. Die Methode des Ablehnens hat den Vorteil, dass die sendende Anwendung bereits nach einem Versuch benachrichtigt wird, dass die Verbindung nicht aufgebaut werden kann.

---

**Hinweis** Die Auswahl von **Ablehnen** als Aktion für die Standardregel wird nicht empfohlen.

---

- 5 Aktivieren oder deaktivieren Sie die Protokollierung in der Spalte **Protokoll**.

Das Aktivieren der Protokollierung kann die Leistung beeinträchtigen.

- 6 Klicken Sie auf **Veröffentlichen**.

## Ändern der Reihenfolge von Firewallregeln

Die Regeln werden von oben nach unten verarbeitet. Sie haben die Möglichkeit, die Reihenfolge der Regeln in der Liste zu ändern.

Für jeden Datenverkehr, der die Firewall passieren soll, müssen die Paketinformationen den Regeln in der Reihenfolge genügen, wie Sie in der Regeltabelle angegeben werden. Die Überprüfung beginnt mit den Regeln an oberster Stelle und wird bis zu den Standardregeln unten fortgesetzt. In einigen Fällen kann die Rangfolge von zwei oder mehr Regeln für die Bestimmung des Datenverkehrsflusses entscheidend sein.

Sie können eine benutzerdefinierte Regel in der Tabelle nach oben oder nach unten verschieben. Die Standardregel befindet sich immer am Ende der Tabelle und kann nicht verschoben werden.

### Verfahren

- 1 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Sicherheit > Verteilte Firewall** aus.
- 2 Klicken Sie auf die Registerkarte **Allgemein** für L3-Regeln oder auf die Registerkarte **Ethernet** für L2-Regeln.
- 3 Wählen Sie die zu verschiebende Regel aus und klicken Sie in der Menüleiste auf das Symbol **Nach oben** bzw. **Nach unten**.
- 4 Klicken Sie auf **Veröffentlichen**.

## Filtern der Firewallregeln

Wenn Sie zum Firewallabschnitt navigieren, werden zunächst alle Regeln angezeigt. Sie können einen Filter anwenden, um die Anzeige zu steuern und nur eine Teilmenge der Regeln anzuzeigen. Dies kann die Regelverwaltung vereinfachen.

### Verfahren

- 1 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Sicherheit > Verteilte Firewall** aus.
- 2 Klicken Sie auf die Registerkarte **Allgemein** für L3-Regeln oder auf die Registerkarte **Ethernet** für L2-Regeln.
- 3 Klicken Sie in das Suchtextfeld auf der rechten Seite der Menüleiste, wählen Sie ein Objekt aus oder geben Sie die ersten Zeichen eines Objektnamens ein, um die Liste der auszuwählenden Objekte einzugrenzen.

Nachdem Sie ein Objekt ausgewählt haben, wird der Filter angewendet, und die Liste der Regeln wird aktualisiert. Daraufhin werden nur die Regeln angezeigt, die das Objekt in einer der folgenden Spalten enthalten:

- Quellen
- Ziele
- Angewendet auf
- Dienste

- 4 Um den Filter zu entfernen, löschen Sie den Objektnamen aus dem Textfeld.

## Konfigurieren der Firewall für den Bridge-Port eines logischen Switches

Sie können Firewallabschnitte und -regeln für den Bridge-Port eines von einer Schicht--2-Bridge gestützten logischen Switches konfigurieren. Die Bridge muss unter Verwendung von NSX Edge-Knoten erstellt worden sein.

### Voraussetzungen

Vergewissern Sie sich, dass der Switch an ein Bridge-Profil angehängt ist. Siehe [Erstellen eines Bridge-gestützten logischen Schicht-2-Switches](#).

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Sicherheit > Bridge-Firewall** aus.
- 3 Wählen Sie einen logischen Switch aus.

Der Switch muss an ein Bridge-Profil angehängt sein.

- 4 Führen Sie anschließend die gleichen Schritte wie in den vorherigen Abschnitten für die Konfiguration der Schicht-2- oder Schicht-3-Firewall durch.

## Konfigurieren einer Firewall-Ausschlussliste

Sie können einen logischen Port, einen logischen Switch oder eine NSGroup von einer Firewallregel ausschließen.

Nachdem Sie einen Abschnitt mit Firewallregeln erstellt haben, können Sie einen NSX-T Data Center-Appliance-Port von den Firewallregeln ausschließen.

### Verfahren

- 1 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Sicherheit > Verteilte Firewall > Ausschlussliste > Hinzufügen** aus.
- 2 Wählen Sie einen Typ und ein Objekt aus.  
Die verfügbaren Typen lauten **Logischer Port**, **Logischer Switch** und **NSGroup**.
- 3 Klicken Sie auf **OK**.
- 4 Um ein Objekt aus der Ausschlussliste zu entfernen, wählen Sie das Objekt aus, und klicken Sie in der Menüleiste auf **Löschen**.

## Aktivieren und Deaktivieren einer verteilten Firewall

Sie können die Funktion für die verteilte Firewall aktivieren oder deaktivieren.

Wenn sie deaktiviert ist, werden keine Firewallregeln auf der Datenebene erzwungen. Bei erneuter Aktivierung werden die Regeln erneut erzwungen.

### Verfahren

- 1 Navigieren Sie zu **Netzwerk und Sicherheit – Erweitert > Sicherheit > Verteilte Firewall**.
- 2 Klicken Sie auf die Registerkarte **Einstellungen**.
- 3 Klicken Sie auf Verteilte Firewall **Bearbeiten**.
- 4 Legen Sie im Dialogfeld den Firewall-Status auf Grün (aktiviert) oder Grau (deaktiviert) fest.
- 5 Klicken Sie auf **Speichern**.

## Hinzufügen oder Löschen einer Firewallregel zu bzw. von einem logischen Router

Sie können einem logischen Tier-0- oder Tier-1-Router Firewallregeln hinzufügen, um die eingehende Router-Kommunikation zu steuern.

Edge Fire-Walling wird auf Uplink-Router-Ports implementiert. Das heißt, dass Firewallregeln nur dann anwendbar sind, wenn der auf Datenverkehr Uplink-Router-Ports auf Edge trifft. Wenn Sie Firewallregeln auf ein bestimmtes IP-Ziel anwenden möchten, müssen Sie Gruppen mit /32-Netzwerk konfigurieren. Wenn Sie ein anderes Subnetz als /32 bereitstellen, werden Firewallregeln auf das vollständige Subnetz angewendet.

### Voraussetzungen

Machen Sie sich mit den Parametern einer Firewallregel vertraut. Siehe [Hinzufügen einer Firewallregel](#).

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.
- 3 Klicken Sie auf die Registerkarte **Router**, falls sie noch nicht ausgewählt ist.
- 4 Klicken Sie auf den Namen eines logischen Routers.
- 5 Wählen Sie **Dienste > Edge-Firewall** aus.
- 6 Klicken Sie auf einen vorhandenen Abschnitt oder eine vorhandene Regel.
- 7 Klicken Sie zum Hinzufügen einer Regel in der Menüleiste auf **Regel hinzufügen**, und wählen Sie **Regel oberhalb hinzufügen** oder **Regel unterhalb hinzufügen** aus, oder klicken Sie auf das Menüsymbol in der ersten Spalte einer Regel, und wählen Sie **Regel oberhalb hinzufügen** oder **Regel unterhalb hinzufügen** aus, und geben Sie die Regelparameter an.  
  
Das Feld „Angewendet auf“ wird nicht angezeigt werden, da diese Regel nur für den logischen Router gilt.
- 8 Wenn Sie eine Regel löschen möchten, wählen Sie die Regel aus, klicken Sie in der Menüleiste auf **Löschen** oder klicken Sie auf das Menüsymbol in der ersten Spalte und wählen Sie **Löschen** aus.

### Ergebnisse

**Hinweis** Wenn Sie eine Firewallregel zu einem logischen Tier-0-Router hinzufügen und der NSX Edge-Cluster, der den Router stützt, im Aktiv/Aktiv-Modus ausgeführt wird, kann die Firewall nur im zustandslosen Modus ausgeführt werden. Wenn Sie die Firewallregel mit zustandsbehafteten Diensten wie HTTP, SSL, TCP usw. konfigurieren, funktioniert die Firewallregel nicht wie erwartet. Um dieses Problem zu vermeiden, konfigurieren Sie den NSX Edge-Cluster für die Ausführung im Aktiv/Standby-Modus.

## CPU- und Arbeitsspeicher-Nutzungsschwellenwert mithilfe der API

Wenden Sie Schwellenwerte zur Nutzung von CPU und Arbeitsspeicher auf verteilte Firewall-Regeln mithilfe von Dienstkonfigurations-APIs an. Wenn Sie die Dienstkonfigurations-API

implementieren, können Sie eine Profilkonfiguration auf eine Entität wie beispielsweise VM-Gruppen, Transportknoten, logische Switches und logische Ports anwenden.

## Abrufen von Dienstkonfigurationsdetails

Details zu Syntax und Nutzung finden Sie im *NSX-T Data Center API-Handbuch*.

Liste aller Dienstkonfigurationen.

```
GET https://<nsx-mgr>/api/v1/service-configs
```

Tabelle 20-2. API-Attribute

Attribut	Details
Profil	<p>Profile sind Konfigurationen, die auf eine VM-Gruppe angewendet werden.</p> <p>Beispielsweise ist <code>FirewallSessionTimerProfile</code> das Profil, das auf einen Transportknoten angewendet wird, um Details zur CPU-Auslastungsrate des Transportknotens zu erfassen, wenn verteilte Firewall-Regeln ausgeführt werden.</p> <hr/> <p><b>Hinweis</b> In einer Dienstkonfiguration kann nur ein Profil enthalten sein.</p>
Applied_To	VM-Gruppe, auf die das Dienstprofil angewendet wird.
Precedence	<p>Der Vorrang wird pro Profiltyp angewendet.</p> <p>NSX-T Data Center entscheidet über die Priorität der Profile, die auf eine VM-Gruppe nach aufsteigenden Zahlen angewendet werden müssen.</p> <p>Zum Beispiel hat ein Profil mit Sequenznummer 1 höhere Priorität als die Sequenznummer 2.</p>

## Erstellen eines Dienstkonfiguration

Erstellt eine Dienstkonfiguration, die Profile und Konfiguration gruppieren kann.

```
POST https://<nsx-mgr>/api/v1/service-config
{
  "display_name": "testServiceConfig",
  "profiles": [{ "profile_type": "FirewallSessionTimerProfile",
                  "target_id": "183e372b-854c-4fcc-a24e-05721ce89a60"
                }
  ],
  "precedence": 10,
  "applied_to": [{
```

```

    "target_id": "333e372b-854c-4fcc-a24e-05721ce89b71",
    "target_type" : "NSGroup"
  }]
}

```

Example Response:

```

{
  "id": "183e372b-854c-4fcc-a24e-05721ce89a60",
  "display_name": "testServiceConfig",
  "profiles": [{ "profile_type": "FirewallSessionTimerProfile",
    "target_id": "183e372b-854c-4fcc-a24e-05721ce89a60"
  }
],
  "precedence": 10,
  "applied_to": [{
    "target_id": "333e372b-854c-4fcc-a24e-05721ce89b71",
    "target_type" : "NSGroup"
  }]
  "_create_user": "system",
  "_last_modified_user": "system",
  "_last_modified_time": 1414057732203,
  "_create_time": 1414057732203
}

```

## Löschen einer Dienstkonfiguration

Löscht die angegebene Dienstkonfiguration.

```
DELETE https://<nsx-mgr>/api/v1/service-configs/<183e372b-854c-4fcc-a24e-05721ce89a60>
```

## Abrufen von Details zu einer bestimmten Konfiguration

Gibt Informationen zur angegebenen Dienstkonfiguration zurück.

```
GET https://<nsx-mgr>/api/v1/service-configs/<183e372b-854c-4fcc-a24e-05721ce89a60>
```

Example Response:

```

{
  "_revision": 1,
  "id": "183e372b-854c-4fcc-a24e-05721ce89a60",
  "display_name": "testServiceConfig1",
  "resource_type": "ServiceConfig",
  "profiles": [{ "profile_type": "FirewallSessionTimerProfile",
    "target_id": "183e372b-854c-4fcc-a24e-05721ce89a45",
    "is_valid": true
  }
],
  "precedence": 10,
  "applied_to": [{ "target_id": "333e372b-854c-4fcc-a24e-05721ce89b71",
    "target_type": "LogicalSwitch",
    "is_valid": true
  }
]
  "_create_user": "system",

```

```

    "_last_modified_user": "system",
    "_last_modified_time": 1414057732203,
    "_create_time": 1414057732203
  }

```

## Aktualisieren einer Dienstkonfiguration

Aktualisiert die angegebene Dienstkonfiguration.

```

PUT https://<nsx-mgr>/api/v1/service-configs/183e372b-854c-4fcc-a24e-05721ce89a60
{
  "id": "183e372b-854c-4fcc-a24e-05721ce89a60",
  "display_name": "testServiceConfig1",
  "resource_type": "ServiceConfig",
  "profiles": [{ "profile_type": "FirewallSessionTimerProfile",
    "target_id": "183e372b-854c-4fcc-a24e-05721ce89a45"
  }],
  "precedence": 10,
  "applied_to": [{ "target_id": "333e372b-854c-4fcc-a24e-05721ce89b71",
    "target_type": "NSGroup"
  }]
  "_create_user": "system",
  "_last_modified_user": "system",
  "_last_modified_time": 1414057732203,
  "_create_time": 1414057732203,
  "_create_user": "admin",
  "_revision": 0
}

```

## Abrufen von effektiven Profilen

Gibt die effektiven Profile zurück, die auf die angegebene Ressource angewendet werden.

```

GET https://<nsx-mgr>/api/v1/service-configs/effective-profiles?
resource_id=<144e372b-854c-4fcc-a24e-05721ce89a60>&resource_type=NSGroup

```

Example Response:

```

{
  "cursor": "00012",
  "sort_ascending": true,
  "result_count": 2,
  "results": [
    { "profile_type": "FirewallSessionTimerProfile",
      "target_id": "183e372b-854c-4fcc-a24e-05721ce89a45",
      "target_name": "Firewall Session Timer Profile",
      "is_valid": true
    },
    { "profile_type": "FirewallCpuMemThresholdsProfile",
      "target_id": "5678372b-854c-4fcc-a24e-05721ce89a45",
      "target_name": "Firewall CPU Profile",
      "is_valid": true
    },
  ],
}

```

```
} ]
```



In manchen Fällen muss eventuell die Konfiguration der installierten Appliances geändert werden, z. B. für das Hinzufügen von Lizenzen bzw. Zertifikaten oder für das Ändern von Kennwörtern. Außerdem fallen notwendige Routinewartungsaufgaben an, inklusive der Durchführung von Sicherungen. Darüber hinaus können Sie mit speziellen Tools Informationen zu den Appliances suchen, die zur NSX-T Data Center-Infrastruktur und zu den von NSX-T Data Center erstellten logischen Netzwerken gehören, inklusive Remotesystemprotokollierung, Traceflow und Portverbindungen.

Dieses Kapitel enthält die folgenden Themen:

- [Überprüfen des Umsetzungsstatus einer Konfigurationsänderung](#)
- [Suchen nach Objekten](#)
- [Hinzufügen eines Compute Managers](#)
- [Hinzufügen von Active Directory](#)
- [Hinzufügen eines LDAP-Servers](#)
- [Synchronisieren von Active Directory](#)
- [Verwalten von Benutzerkonten und der rollenbasierten Zugriffssteuerung](#)
- [Sichern und Wiederherstellen von NSX Manager](#)
- [Entfernen der NSX-T Data Center-Erweiterung aus vCenter Server](#)
- [Verwalten des NSX Manager-Clusters](#)
- [Bereitstellung von NSX-T Data Center für mehrere Sites](#)
- [Konfigurieren von Appliances](#)
- [Hinzufügen eines Lizenzschlüssels und Generieren eines Lizenznutzungsberichts](#)
- [Einrichten von Zertifikaten](#)
- [Erfassen von Support-Paketen](#)
- [Protokollmeldungen](#)
- [Programm zur Verbesserung der Benutzerfreundlichkeit](#)

- [Hinzufügen von Tags zu einem Objekt](#)
- [Suchen nach dem SSH-Fingerabdruck eines Remote-Servers](#)
- [Anzeigen von Daten über Anwendungen, die auf virtuellen Maschinen ausgeführt werden](#)

## Überprüfen des Umsetzungsstatus einer Konfigurationsänderung

Im Fall einer Konfigurationsänderung sendet NSX Manager in der Regel eine Anfrage an eine andere Komponente, um die Änderung zu implementieren. Wenn Sie die Konfigurationsänderung mithilfe der API durchführen, können Sie für bestimmte Schicht 3-Entitäten den Status der Anfrage verfolgen, um festzustellen, ob die Änderung erfolgreich implementiert wurde.

Die von Ihnen initiierte Konfigurationsänderung wird als gewünschter Zustand bezeichnet. Das Ergebnis der Änderungsimplementierung wird als realisierter Zustand bezeichnet. Wenn NSX Manager die Änderung erfolgreich implementiert, stimmen realisierter und gewünschter Zustand überein. Wenn ein Fehler vorliegt, gibt es keine Übereinstimmung zwischen realisiertem und gewünschtem Zustand.

Wenn Sie eine API zum Durchführen einer Konfigurationsänderung aufrufen, enthält die Antwort für bestimmte Schicht 3-Entitäten den Parameter `request_id`. Sie können die Parameter `request_id` und `entity_id` verwenden, um einen API-Aufruf zum Ermitteln des Anfragestatus durchzuführen.

Diese Funktion unterstützt die folgenden Entitäten und APIs:

```
EdgeCluster
  POST /edge-clusters
  PUT /edge-clusters/<edge-cluster-id>
  DELETE /edge-clusters/<edge-cluster-id>
  POST /edge-clusters/<edge-cluster-id>?action=replace_transport_node

LogicalRouter
  POST /logical-routers
  PUT /logical-routers/<logical-router-id>
  DELETE /logical-routers/<logical-router-id>
  POST /logical-routers/<logical-router-id>?action=reprocess
  POST /logical-routers/<logical-router-id>?action=reallocate

LogicalRouterPort
  POST /logical-router-ports
  PUT /logical-router-ports/<logical-router-port-id>
  DELETE /logical-router-ports/<logical-router-port-id>

StaticRoute
  POST /logical-routers/<logical-router-id>/routing/static-routes
  PUT /logical-routers/<logical-router-id>/routing/static-routes/<static-route-id>
  DELETE /logical-routers/<logical-router-id>/routing/static-routes/<static-route-id>

BGPConfig
  PUT /logical-routers/<logical-router-id>/routing/bgp
```

**BgpNeighbor**

```
POST /logical-routers/<logical-router-id>/routing/bgp/neighbors
PUT /logical-routers/<logical-router-id>/routing/bgp/neighbors/<bgp-neighbor-id>
DELETE /logical-routers/<logical-router-id>/routing/bgp/neighbors/<bgp-neighbor-id>
POST /logical-routers/<logical-router-id>/routing/bgp/neighbors/<bgp-neighbor-id>
```

**BGPCommunityList**

```
POST /logical-routers/<logical-router-id>/routing/bgp/community-lists
PUT /logical-routers/<logical-router-id>/routing/bgp/community-lists/<community-list-id>
DELETE /logical-routers/<logical-router-id>/routing/bgp/community-lists/<community-list-id>
```

**AdvertisementConfig**

```
PUT /logical-routers/<logical-router-id>/routing/advertisement
```

**AdvertiseRouteList**

```
PUT /logical-routers/<logical-router-id>/routing/advertisement/rules
```

**NatRule**

```
POST /logical-routers/<logical-router-id>/nat/rules
PUT /logical-routers/<logical-router-id>/nat/rules/<rule-id>
DELETE /logical-routers/<logical-router-id>/nat/rules/<rule-id>
```

**DhcpRelayService**

```
POST /dhcp/relays
PUT /dhcp/relays/<relay-id>
DELETE /dhcp/relays/<relay-id>
```

**DhcpRelayProfile**

```
POST /dhcp/relay-profiles
PUT /dhcp/relay-profiles/<relay-profile-id>
DELETE /dhcp/relay-profiles/<relay-profile-id>
```

**StaticHopBfdPeer**

```
POST /logical-routers/<logical-router-id>/routing/static-routes/bfd-peers
PUT /logical-routers/<logical-router-id>/routing/static-routes/bfd-peers/<bfd-peers-id>
DELETE /logical-routers/<logical-router-id>/routing/static-routes/bfd-peers/<bfd-peers-id>
```

**IPPrefixList**

```
POST /logical-routers/<logical-router-id>/routing/ip-prefix-lists
PUT /logical-routers/<logical-router-id>/routing/ip-prefix-lists/<ip-prefix-list-id>
DELETE /logical-routers/<logical-router-id>/routing/ip-prefix-lists/<ip-prefix-list-id>
```

**RouteMap**

```
POST /logical-routers/<logical-router-id>/routing/route-maps
PUT /logical-routers/<logical-router-id>/routing/route-maps/<route-map-id>
DELETE /logical-routers/<logical-router-id>/routing/route-maps/<route-map-id>
```

**RedistributionConfig**

```
PUT /logical-routers/<logical-router-id>/routing/redistribution
```

**RedistributionRuleList**

```
PUT /logical-routers/<logical-router-id>/routing/redistribution/rules
```

**BfdConfig**

```
PUT /logical-routers/<logical-router-id>/routing/bfd-config
```

```

MplsConfig
  PUT /logical-routers/<logical-router-id>/routing/mpls

RoutingGlobalConfig
  PUT /logical-routers/<logical-router-id>/routing

IPSecVPNIKEProfile
  POST /vpn/ipsec/ike-profiles
  PUT /vpn/ipsec/ike-profiles/<ike-profile-id>
  DELETE /vpn/ipsec/ike-profiles/<ike-profile-id>

IPSecVPNDPDProfile
  POST /vpn/ipsec/dpd-profiles
  PUT /vpn/ipsec/dpd-profiles/<dpd-profile-id>
  DELETE /vpn/ipsec/dpd-profiles/<dpd-profile-id>

IPSecVPNTunnelProfile
  POST /vpn/ipsec/tunnel-profiles
  PUT /vpn/ipsec/tunnel-profiles/<tunnel-profile-id>
  DELETE /vpn/ipsec/tunnel-profiles/<tunnel-profile-id>

IPSecVPNLocalEndpoint
  POST /vpn/ipsec/local-endpoints
  PUT /vpn/ipsec/local-endpoints/<local-endpoint-id>
  DELETE /vpn/ipsec/local-endpoints/<local-endpoint-id>

IPSecVPNPeerEndpoint
  POST /vpn/ipsec/peer-endpoints
  PUT /vpn/ipsec/peer-endpoints/<peer-endpoint-id>
  DELETE /vpn/ipsec/peer-endpoints/<peer-endpoint-id>

IPSecVPNService
  POST /vpn/ipsec/services
  PUT /vpn/ipsec/services/<service-id>
  DELETE /vpn/ipsec/services/<service-id>

IPSecVPNSession
  POST /vpn/ipsec/sessions
  PUT /vpn/ipsec/sessions/<session-id>
  DELETE /vpn/ipsec/sessions/<session-id>

```

Sie können die folgenden APIs zum Abrufen der realisierten Zustände aufrufen:

```

EdgeCluster
Request – GET /edge-clusters/<edge-cluster-id>/state?request_id=<request-id>
Response – An instance of EdgeClusterStateDto which will inherit ConfigurationState. If the edge
cluster is deleted then the state will be unknown and it will return the common entity not found
error.

LogicalRouter / All L3 Entites – All L3 entities can use this API to get realization state
Request – GET /logical-routers/<logical-router-id>/state?request_id=<request-id>
Response – An instance of LogicalRouterStateDto which will inherit ConfigurationState. Delete
operation of any entity other than logical router can be covered by getting the state of logical
router but if the logical router itself is deleted then the state will be unknown and it will return

```

the common entity not found error.

**LogicalServiceRouterCluster** – All L3 entities which are the part of services can use this API to get the realization state

**Request** – GET /logical-routers/<logical-router-id>/service-cluster/state?request\_id=<request-id>

**Response** – An instance of LogicalServiceRouterClusterState which will inherit ConfigurationState.

**LogicalRouterPort / DhcpRelayService / DhcpRelayProfile**

**Request** – GET /logical-router-ports/<logical-router-port-id>/state?request\_id=<request-id>

**Response** – An instance of LogicalRouterPortStateDto which will inherit ConfigurationState.

**IPSecVPN IKEProfile / IPSecVPN DPDPProfile / IPSecVPN TunnelProfile / IPSecVPN LocalEndpoint / IPSecVPN PeerEndpoint / IPSecVPN Service / IPSecVPN Session**

**Request** – GET /vpn/ipsec/sessions/<session-id>/state?request\_id=<request-id>

**Response** – An instance of IPSecVPN SessionStateDto which will inherit ConfigurationState. If the session is deleted then the state will be unknown and it will return the common entity not found error. When IPSecVPN Service is disabled, IKE itself is down and it does not respond. It will return unknown state in such a case.

Weitere Informationen zu den APIs finden Sie in der *Referenz zur NSX-T Data Center-API*.

## Suchen nach Objekten

Sie können unter Verwendung verschiedener Kriterien in der NSX-T Data Center-Bestandsliste nach Objekten suchen.

Die Suchergebnisse werden nach Relevanz sortiert, und Sie können diese Ergebnisse basierend auf Ihre Suchabfrage filtern.

**Hinweis** Wenn Sonderzeichen in Ihrer Suchabfrage enthalten sind, die auch als Operatoren fungieren, müssen Sie einen umgekehrten Schrägstrich davor hinzufügen. Die als Operatoren fungierenden Zeichen lauten wie folgt: +, -, =, &&, ||, <, >, !, (, ), {, }, [, ], ^, ", ~, ?, :, /, \.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Geben Sie auf der Startseite ein Suchmuster für ein Objekt oder einen Objekttyp ein.

Bei der Eingabe Ihres Suchmusters unterstützt Sie die Suchfunktion, indem sie die zutreffenden Schlüsselwörter anzeigt.

Suchen	Suchabfrage
<b>Objekte mit „Logical“ als Name oder Eigenschaft</b>	Logical
<b>Exakter Name des logischen Switches</b>	display_name:LSP-301
<b>Namen mit Sonderzeichen wie !</b>	Logical\!

Alle zugehörigen Suchergebnisse werden aufgelistet und nach Ressourcentyp in verschiedenen Registerkarten gruppiert.

Sie können für bestimmte Suchergebnisse für einen Ressourcentyp auf die Registerkarten klicken.

- 3 (Optional) Klicken Sie in der Suchleiste auf das Symbol zum Speichern, um Ihre verfeinerten Suchkriterien zu speichern.

- 4 Wenn Sie in der Suchleiste auf das Symbol  klicken, wird die Spalte „Erweiterte Suche“ geöffnet, in der Sie Ihre Suche verfeinern können.

- 5 Geben Sie ein oder mehrere Kriterien an, um die Suche einzugrenzen.

- Name
- Ressourcentyp
- Beschreibung
- ID
- Erstellt von
- Geändert von
- Tags
- Erstellungsdatum
- Änderungsdatum

Sie können auch Ihre letzten Suchergebnisse und Ihre gespeicherten Suchkriterien einsehen.

- 6 (Optional) Durch Klicken auf **Alle löschen** können Sie Ihre erweiterten Suchkriterien zurücksetzen.

## Hinzufügen eines Compute Managers

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

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

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

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

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

### Voraussetzungen

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

---

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

---

### Verfahren

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

- 2 Wählen Sie **System > Fabric > Compute Managers > Hinzufügen** aus.
- 3 Vervollständigen Sie die Details zum Compute Manager.

Option	Beschreibung
<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.

## Hinzufügen von Active Directory

Active Directory wird bei der Erstellung von benutzerbasierten Identitäts-Firewallregeln verwendet.

Windows 2008 wird nicht als Active Directory-Server oder RDSH-Server-Betriebssystem unterstützt.



Sie können eine oder mehrere Windows-Domänen bei einem NSX Manager registrieren. NSX Manager ruft Gruppen- und Benutzerinformationen sowie die Beziehung zwischen diesen aus jeder Domäne ab, bei der er registriert ist. NSX Manager ruft außerdem Active Directory-Anmeldedaten (AD) ab.

Sobald NSX Manager AD-Anmeldedaten abrufen, können Sie Sicherheitsgruppen auf Basis der Benutzeridentität erstellen und identitätsbasierte Firewallregeln erstellen.

---

**Hinweis** Zur Erzwungung der identitätsbasierten Firewallregel sollte für den Windows-Zeitdienst **ein** für alle VMs festgelegt sein, die Active Directory verwenden. Dadurch wird sichergestellt, dass Datum und Uhrzeit zwischen Active Directory und VMs synchronisiert werden. Darüber hinaus werden Änderungen der AD-Gruppenmitgliedschaft, einschließlich der Aktivierung und Löschung von Benutzern, nicht sofort für angemeldete Benutzer wirksam. Damit die Änderungen wirksam werden, müssen sich die Benutzer abmelden und erneut anmelden. AD-Administratoren sollten eine Abmeldung erzwingen, wenn die Gruppenmitgliedschaft geändert wird. Dieses Verhalten ist eine Beschränkung von Active Directory.

---

#### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Navigieren Sie zu **System > Active Directory**.
- 3 Klicken Sie auf **Active Directory hinzufügen**.
- 4 Geben Sie den Namen des Active Directory ein.
- 5 Geben Sie den **NetBios-Namen** und den **Basis-DN (Distinguished Name)** ein.

Um den NetBIOS-Namen für Ihre Domäne abzurufen, geben Sie „nbtstat /n“ in einem Befehlsfenster auf einer Windows-Workstation ein, die Teil einer Domäne ist oder sich auf einem Domänencontroller befindet. In der lokalen NetBIOS-Namenstabelle ist der Eintrag mit einem Präfix <00> und dem Typ „Gruppe“ der NetBIOS-Name.

- 6 Legen Sie das **Delta-Synchronisierungsintervall** bei Bedarf fest. Eine Delta-Synchronisierung aktualisiert lokale AD-Objekte, die sich seit der letzten Synchronisierung geändert haben.

Alle Änderungen, die Sie in Active Directory vornehmen, werden in NSX Manager erst angezeigt, wenn eine Delta- oder vollständige Synchronisierung durchgeführt wurde.

- 7 Klicken Sie auf **Speichern**.

## Hinzufügen eines LDAP-Servers

Die LDAP-Server-Konfiguration und -Funktionalität dient nur zur Verwendung mit der identitätsbasierten Firewall.

LDAP (Lightweight Directory Access Protocol) bietet einen zentralen Ort für die Authentifizierung. Das heißt, wenn Sie eine Verbindung mit Ihrem LDAP-Server konfigurieren, werden die Benutzerdatensätze auf Ihrem externen LDAP-Server gespeichert.

**Verfahren**

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Navigieren Sie zu **System > Active Directory**.
- 3 Wählen Sie die Registerkarte **LDAP-Server** aus.
- 4 Klicken Sie auf **LDAP-Server hinzufügen**.
- 5 Geben Sie unter **Host** den Namen des LDAP-Servers ein.
- 6 Wählen Sie im Dropdown-Menü **Verbunden mit (Verzeichnis)** das Active Directory aus, das mit dem LDAP-Server verbunden ist.
- 7 (Optional) Wählen Sie das **Protokoll** aus: „LDAP (ungesichert)“ oder „LDAPS (gesichert)“.
- 8 Der standardmäßige LDAP-Port 389 und der LDAPS-Port 636 werden für die Active Directory-Synchronisierung verwendet und dürfen nicht über die Standardwerte bearbeitet werden. Benutzerdefinierte Ports werden nicht unterstützt.
- 9 Geben Sie den **Benutzernamen** und das **Kennwort** eines Active Directory-Kontos ein, das mindestens Lesezugriff auf die Active Directory-Domänen besitzt.
- 10 Klicken Sie auf **Speichern**.
- 11 Um sicherzustellen, dass Sie eine Verbindung zum LDAP-Server herstellen können, klicken Sie auf **Testverbindung**.

## Synchronisieren von Active Directory

Active Directory-Objekte können verwendet werden, um Sicherheitsgruppen basierend auf der Benutzeridentität und identitätsbasierten Firewallregeln zu erstellen.

---

**Hinweis** Zur Erzwingung der identitätsbasierten Firewallregel sollte für den Windows-Zeitdienst **ein** für alle VMs festgelegt sein, die Active Directory verwenden. Dadurch wird sichergestellt, dass Datum und Uhrzeit zwischen Active Directory und VMs synchronisiert werden. Änderungen der AD-Gruppenmitgliedschaft, einschließlich der Aktivierung und Löschung von Benutzern, werden nicht sofort für angemeldete Benutzer wirksam. Damit die Änderungen wirksam werden, müssen sich die Benutzer abmelden und erneut anmelden. AD-Administratoren sollten eine Abmeldung erzwingen, wenn die Gruppenmitgliedschaft geändert wird. Dieses Verhalten ist eine Beschränkung von Active Directory.

---

**Verfahren**

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

- 3 Klicken Sie neben dem zu synchronisierenden Active Directory auf das aus drei Punkten bestehende Menüsymbol und wählen Sie eine der folgenden Optionen aus:

Delta synchronisieren	Durchführen einer Delta-Synchronisierung, bei der lokale AD-Objekte aktualisiert werden, die sich seit der letzten Synchronisierung geändert haben.
Alle synchronisieren	Durchführen einer vollständigen Synchronisierung, bei der der lokale Zustand aller AD-Objekte aktualisiert wird.

- 4 Klicken Sie auf **Synchronisierungsstatus anzeigen**, um den aktuellen Status des Active Directory, den vorherigen Synchronisierungsstatus, den aktuellen Synchronisierungsstatus und den Zeitpunkt der letzten Synchronisierung anzuzeigen.

## Verwalten von Benutzerkonten und der rollenbasierten Zugriffssteuerung

NSX-T Data Center-Appliances haben zwei integrierte Benutzer: Admin und Audit. Sie können VMware Identity Manager in NSX-T Data Center (vIDM) integrieren und die rollenbasierte Zugriffssteuerung (RBAC) für Benutzer konfiguriert, die von vIDM verwaltet werden.

Für von vIDM verwaltete Benutzer gilt die vom vIDM-Administrator konfigurierte Authentifizierungsrichtlinie, und nicht die Authentifizierungsrichtlinie von NSX-T Data Center, die nur für die Benutzer Admin und Audit gilt.

### Verwalten eines Benutzerkennworts

Jede Appliance verfügt über zwei integrierte Benutzer („Admin“ und „Audit“), mit denen Sie sich bei NSX Manager oder SSH bei der Appliance anmelden und CLI-Befehle ausführen können. Sie können zwar das Kennwort für diese Benutzer verwalten, aber keine Benutzer hinzufügen oder löschen.

Standardmäßig laufen Kennwörter nach 90 Tagen ab.

Der Überwachungsbenutzer ist standardmäßig nicht aktiv. Wenn Sie ihn aktivieren möchten, melden Sie sich als Administrator an, führen Sie den Befehl `set user audit` aus und geben Sie ein neues Kennwort ein. Wenn Sie zur Eingabe des aktuellen Kennworts aufgefordert werden, drücken Sie die Eingabetaste.

#### Voraussetzungen

Machen Sie sich mit den Anforderungen an die Kennwortkomplexität für NSX Manager und NSX Edge vertraut. Weitere Informationen finden Sie unter „NSX Manager-Installation“ und „NSX Edge-Installation“ im *Installationshandbuch für NSX-T Data Center*.

#### Verfahren

- 1 Melden Sie sich bei der Appliance-CLI an.

- 2 Führen Sie zum Ändern des Kennworts den Befehl `set user` aus. Beispiel:

```
nsx> set user admin
Current password:
New password:
Confirm new password:
nsx>
```

- 3 Wenn Sie Informationen zum Kennwortablauf erhalten möchten, führen Sie den Befehl `get user <username> password-expiration` aus. Beispiel:

```
nsx> get user audit password-expiration
Password expires 90 days after last change
nsx>
```

- 4 Wenn Sie die Kennwortablaufzeit in Tagen festlegen möchten, führen Sie den Befehl `set user <username> password-expiration <number of days>` aus. Beispiel:

```
nsx> set user audit password-expiration 120
nsx>
```

- 5 Wenn Sie den Kennwortablauf deaktivieren möchten, führen Sie den Befehl `clear user <username> password-expiration` aus. Beispiel:

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

## Zurücksetzen der Kennwörter einer Appliance

Wenn Sie das Kennwort des Benutzers `root`, `admin` oder `audit` vergessen haben, können Sie es zurücksetzen, indem Sie die Appliance im Einzelbenutzermodus starten.

---

**Hinweis** Bei einem NSX Manager-Cluster wird durch Zurücksetzen des Kennworts für den `root`-, `admin`- oder `audit`-Benutzer auf einem NSX Manager automatisch auch das Kennwort für die anderen NSX Manager im Cluster zurückgesetzt.

---

**Wichtig** Wenn Sie eine Appliance neu starten, wird das GRUB-Startmenü nicht standardmäßig angezeigt. Die folgende Vorgehensweise erfordert, dass Sie die Appliance so konfiguriert haben, dass das GRUB-Startmenü angezeigt wird und Sie das Kennwort des GRUB-Root-Benutzers kennen. Weitere Informationen finden Sie unter „Konfigurieren von NSX-T Data Center zum Anzeigen des GRUB-Menüs zum Startzeitpunkt“ im *NSX-T Data Center-Installationshandbuch*.

---

## Verfahren

- 1 Wenn Sie ein Kennwort auf einem NSX Manager zurücksetzen, führen Sie die folgenden Schritte aus:
  - a Fahren Sie die NSX Manager herunter.
  - b Laden Sie die .iso-Datei von Ubuntu 16.04 unter <http://releases.ubuntu.com/16.04/ubuntu-16.04.6-server-amd64.iso> herunter.
  - c Starten Sie die grafische Benutzeroberfläche (GUI) von vSphere oder ESXi.
  - d Importieren Sie die .iso-Datei von Ubuntu in den entsprechenden Datenspeicher für die NSX Manager-VM.
  - e Bearbeiten Sie die Einstellungen der NSX Manager-VM und fügen Sie ein CD-ROM-Laufwerk hinzu, falls keines vorhanden ist.
  - f Aktivieren Sie in der Konfiguration **CD-ROM-Laufwerk** das Kontrollkästchen **Beim Einschalten verbinden**.
  - g Drücken Sie unter **CD/DVD-Medium** auf **Durchsuchen** und wählen Sie `ubuntu-16.04.6-server-amd64.iso` aus dem entsprechenden Datenspeicher aus.
  - h Klicken Sie auf **Speichern**, um die Seite **Einstellungen bearbeiten** zu verlassen.
  - i Schalten Sie den NSX Manager ein.
- 2 Stellen Sie eine Verbindung mit der Appliance-Konsole her.
- 3 Starten Sie das System neu.
- 4 Wenn das GRUB-Startmenü eingeblendet wird, drücken Sie schnell die linke **UMSCHALTSTASTE** oder die **ESC**-Taste. Wenn Sie zu lange gewartet haben und sich die Startsequenz nicht unterbrechen lässt, müssen Sie das System erneut starten.
- 5 Drücken Sie **e**, um das Menü zu bearbeiten.
 

Geben Sie den Benutzernamen (**root**) und das Kennwort ein. Beachten Sie, dass es sich hierbei um einen GRUB-Root-Benutzer handelt, der nicht mit dem Root-Benutzer der Appliance identisch ist.
- 6 Halten Sie den Cursor auf der Ubuntu-Auswahl.
- 7 Drücken Sie **e**, um die ausgewählte Option zu bearbeiten.
- 8 Suchen Sie nach der Zeile, die mit `linux` beginnt.
- 9 Entfernen Sie alle Optionen nach `root=UUID=`.
- 10 Fügen Sie die folgende Option hinzu.
 

```
rw single init=/bin/bash
```
- 11 Drücken Sie zum Starten auf **Strg+X**.

- 12 Drücken Sie die Eingabetaste, wenn die Protokollmeldungen stoppen.

Sie sehen die Aufforderung `root@(none) :/#`.

- 13 Wenn Sie das Kennwort für `root` zurücksetzen, führen Sie den Befehl `passwd` aus.

Wenn Sie das Kennwort für `admin` oder `audit` zurücksetzen, führen Sie den Befehl `passwd <admin or audit user ID>` aus.

Sie können den Befehl `passwd` mehrmals ausführen.

- 14 Geben Sie ein neues Kennwort ein.

- 15 Geben Sie das Kennwort erneut ein.

- 16 Führen Sie den Befehl `sync` aus.

- 17 Führen Sie den Befehl `reboot -f` aus.

Wichtig: Wenn Sie ein Kennwort auf einem NSX Manager zurücksetzen, nachdem Sie diesen Befehl ausgeführt haben, drücken Sie die Taste **Esc** rechtzeitig, damit Sie den nächsten Schritt durchführen können. Wenn Sie zu lange gewartet haben und sich die Startsequenz nicht unterbrechen lässt, starten Sie das System erneut.

- 18 Wenn Sie ein Kennwort auf einem NSX Manager zurücksetzen und die Startsequenz im vorherigen Schritt erfolgreich angehalten haben, führen Sie die folgenden Schritte aus:

- a Scrollen Sie mit der nach unten weisenden Pfeiltaste nach unten zu **<Setup aufrufen>** (**<Enter Setup>**) und drücken Sie **Eingabe (Enter)**.

- b Navigieren Sie mit der rechten Pfeiltaste zur Menüoption „Start“.

- c Machen Sie CD-ROM zum ersten Gerät mithilfe der Taste **+** oder **-**.

- d Drücken Sie **F10** zum Speichern und Beenden.

- e Drücken Sie **Eingabe (Enter)** bei der Option **Ja (Yes)** zum Speichern der Konfigurationsänderungen und Beenden.

Dadurch kommt es zu einem Neustart und die Seite BIOS-Trennseite wird angezeigt. Drücken Sie keine Tasten.

- f Nach einigen Sekunden wird Ubuntu über die `.iso`-Datei des CD-ROM-Laufwerks gestartet.

- g Wählen Sie eine Sprache aus und drücken Sie **Eingabe (Enter)**.

Es wird ein Ubuntu-Menü angezeigt.

- h Wählen Sie **Beschädigtes System reparieren (Rescue a broken system)** mit der nach unten weisenden Pfeiltaste und drücken Sie **Eingabe(Enter)**.

- i Wählen Sie auf aufeinanderfolgenden Bildschirmen eine Sprache, ein Land und ein Tastaturlayout aus und drücken Sie **Eingabe (Enter)**.

- j Geben Sie einen temporären Hostnamen ein oder übernehmen Sie die Standardeinstellungen.

- k Legen Sie bei Bedarf die richtige Uhrzeit und Zeitzone fest.
- l Sie werden aufgefordert, ein Gerät einzugeben, das als Root-Dateisystem verwendet werden soll. Wählen Sie die Option **Kein Root-Dateisystem verwenden (Do not use a root file system)** mit der nach unten weisenden Pfeiltaste und drücken Sie **Eingabe (Enter)**.
- m Sie werden nun aufgefordert, in den Rettungsmodus zu wechseln. Wählen Sie **Shell in der Installationsumgebung ausführen (Execute a shell in the installer environment)** und drücken Sie **Eingabe(Enter)**.
- n Bestätigen Sie dies mithilfe der Option **Fortfahren (Continue)** und drücken Sie **Eingabe (Enter)**.
- o Sie müssen nun eine Linux-Shell eingeben. Geben Sie die folgenden Linux-Befehle ein:

```
mount /dev/sda2 /mnt
mount --bind /dev /mnt/dev
chroot /mnt
mount /config
touch /config/vmware/nsx-node-api/reset_cluster_credentials
umount /config
exit
umount /mnt/dev
umount /mnt
sync
exit
```

- p Sie sehen nun erneut den Bildschirm **In Rettungsmodus wechseln (Enter rescue mode)**. Wählen Sie die Option **System neu starten (Reboot the system)** mit der nach unten weisenden Pfeiltaste und drücken Sie **Eingabe (Enter)**.

Wenn die Seite BIOS-Trennseite angezeigt wird, drücken Sie schnell die Taste **Esc**.

- q Scrollen Sie mit der nach unten weisenden Pfeiltaste nach unten zu **<Setup aufrufen> (<Enter Setup>)** und drücken Sie **Eingabe (Enter)**.
- r Navigieren Sie mit der rechten Pfeiltaste zur Menüoption „Start“.
- s Navigieren Sie mit der nach unten weisenden Pfeiltaste zur Option **Festplatte (Hard Drive)** und drücken Sie dann **+**, bis dies das erste Gerät ist.
- t Drücken Sie **F10** zum Speichern und Beenden.
- u Drücken Sie **Eingabe (Enter)** bei der Option **Ja (Yes)** zum Speichern der Konfigurationsänderungen und Beenden. Das System wird neu gestartet.
- v Wenn das GRUB-Menü angezeigt wird, wählen Sie die Ubuntu-Option aus und drücken Sie **Eingabe (Enter)**.

Der NSX Manager wird gestartet und verfügt über das neue Kennwort.

- w Entfernen Sie das CD-ROM-Gerät bei Gelegenheit mithilfe der Option **Einstellungen bearbeiten (Edit Settings)** in der vSphere- oder ESXi-GUI für die NSX Manager-VM.

## Authentifizierungsrichtlinien-Einstellungen

Sie können die Authentifizierungsrichtlinien-Einstellungen über die Befehlszeilenschnittstelle (CLI) anzeigen oder ändern.

Sie können die Mindestlänge des Kennworts mit den folgenden Befehlen anzeigen oder festlegen:

```
get auth-policy minimum-password-length
set auth-policy minimum-password-length <password-length>
```

Die folgenden Befehle gelten für die Anmeldung bei der NSX Manager-Benutzeroberfläche oder für einen API-Aufruf:

```
get auth-policy api lockout-period
get auth-policy api lockout-reset-period
get auth-policy api max-auth-failures
set auth-policy api lockout-period <lockout-period>
set auth-policy api lockout-reset-period <lockout-reset-period>
set auth-policy api max-auth-failures <auth-failures>
```

Die folgenden Befehle gelten für die Anmeldung bei der Befehlszeilenschnittstelle (CLI) auf einem NSX Manager- oder einem NSX Edge-Knoten:

```
get auth-policy cli lockout-period
get auth-policy cli max-auth-failures
set auth-policy cli lockout-period <lockout-period>
set auth-policy cli max-auth-failures <auth-failures>
```

Weitere Informationen zu den CLI-Befehlen finden Sie in der *Referenz zur NSX-T-Befehlszeilenschnittstelle*.

Standardmäßig wird nach fünf aufeinander folgenden Fehlversuchen zur Anmeldung bei der NSX Manager-Benutzeroberfläche das Administratorkonto 15 Minuten lang gesperrt. Sie können die Kontosperrung mit dem folgenden Befehl deaktivieren:

```
set auth-policy api lockout-period 0
```

Gleichermaßen können Sie die Kontosperrung für die Befehlszeilenschnittstelle (CLI) mit dem folgenden Befehl deaktivieren:

```
set auth-policy cli lockout-period 0
```

## Abrufen des Certificate Thumbprint von einem vIDM-Host

Bevor Sie die Integration von vIDM mit NSX-T konfigurieren, müssen Sie den Certificate Thumbprint vom vIDM-Host abrufen.

Sie müssen für den Fingerabdruck OpenSSL-Version 1.x oder höher verwenden. Im vIDM-Host führt der Befehl `openssl` eine ältere OpenSSL-Version aus. Daher müssen Sie den Befehl `openssl1` im vIDM-Host verwenden. Dieser Befehl ist nur über den vIDM-Host verfügbar.



Auf einem Server, der nicht der vIDM-Host ist, können Sie den `openssl`-Befehl verwenden, mit dem OpenSSL-Version 1.x oder höher ausgeführt wird.

### Verfahren

- 1 Melden Sie sich bei der Konsole des vIDM-Hosts oder unter Verwendung von SSH an oder melden Sie sich bei einem Server an, der den vIDM-Host anpingen kann.
- 2 Verwenden Sie OpenSSL-Version 1.x oder höher, um den Fingerabdruck des vIDM-Hosts abzurufen.
  - *openssl*: Wenn Sie beim vIDM-Host in einer Konsole oder unter Verwendung von SSH angemeldet sind, führen Sie den folgenden Befehl aus, um den Fingerabdruck abzurufen:

```
openssl s_client -connect <FQDN of vIDM host>:443 < /dev/null 2> /dev/null | openssl x509 -sha256 -fingerprint -noout -in /dev/stdin
```

- *openssl*: Wenn Sie bei einem Server angemeldet sind, der den vIDM-Host anpingen kann, aber nicht der vIDM-Host ist, führen Sie den folgenden Befehl aus, um den Fingerabdruck abzurufen:

```
openssl s_client -connect <FQDN of vIDM host>:443 < /dev/null 2> /dev/null | openssl x509 -sha256 -fingerprint -noout -in /dev/stdin
```

## Konfigurieren der Integration von VMware Identity Manager

Sie können NSX-T Data Center in VMware Identity Manager (vIDM) integrieren, der Identitätsverwaltungsdienste bereitstellt.

Der vIDM-Server sollte über ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat verfügen. Andernfalls funktioniert die Anmeldung bei vIDM über den NSX Manager möglicherweise nicht mit bestimmten Browsern wie Microsoft Edge oder Internet Explorer 11. Informationen zum Installieren eines von einer Zertifizierungsstelle signierten Zertifikats auf vIDM finden Sie in der VMware Identity Manager-Dokumentation unter <https://docs.vmware.com/de/VMware-Identity-Manager/index.html>.

Wenn Sie NSX Manager bei vIDM registrieren, geben Sie einen Umleitungs-URI an, der auf NSX Manager verweist. Sie können entweder den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse angeben. Merken Sie sich unbedingt, ob Sie den FQDN oder die IP-Adresse verwenden. Bei dem Versuch, sich über vIDM bei NSX Manager anzumelden, müssen Sie den

Hostnamen in der URL in derselben Weise angeben. Das heißt, wenn Sie den FQDN beim Registrieren von NSX Manager bei vIDM verwenden, müssen Sie den FQDN in der URL verwenden. Verwenden Sie hingegen die IP-Adresse bei der Registrierung von NSX Manager bei vIDM, müssen Sie die IP-Adresse auch in der URL verwenden. Die Anmeldung schlägt sonst fehl.

---

**Hinweis** NSX Manager und vIDM müssen sich in derselben Zeitzone befinden. Die empfohlene Vorgehensweise ist die Verwendung von UTC.

Wenn vIDM aktiviert ist, können Sie sich weiterhin bei NSX Manager mit einem lokalen Benutzerkonto anmelden, falls Sie die URL `https://<nsx-manager-ip-address>/login.jsp?local=true` verwenden.

Wenn Sie sich mit dem UserPrincipalName (UPN) bei vIDM anmelden, schlägt die Authentifizierung bei NSX-T möglicherweise fehl. Um dieses Problem zu vermeiden, verwenden Sie einen anderen Anmeldeinformationstyp, z. B. SAMAccountName.

Wenn Sie NSX Cloud verwenden, können Sie sich mit der URL `https://<csn-ip-address>/login.jsp?local=true` separat bei CSM anmelden.

---

#### Voraussetzungen

- Stellen Sie sicher, dass Sie über den Fingerabdruck des Zertifikats vom vIDM-Host verfügen. Siehe [Abrufen des Certificate Thumbprint von einem vIDM-Host](#).
- Stellen Sie sicher, dass NSX Manager als OAuth-Client für den vIDM-Host registriert ist. Notieren Sie sich während der Registrierung die Client-ID und den geheimen Client-Schlüssel. Weitere Informationen finden Sie in der VMware Identity Manager-Dokumentation unter <https://docs.vmware.com/de/VMware-Identity-Manager/index.html>.

---

**Hinweis zu NSX Cloud** Wenn Sie NSX Cloud verwenden, überprüfen Sie auch, ob CSM als OAuth-Client auf dem vIDM-Host registriert ist.

---

#### 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 > Benutzer**.
- 3 Klicken Sie auf die Registerkarte **Konfiguration**.
- 4 Klicken Sie auf **Bearbeiten**.

- 5 Klicken Sie zum Aktivieren der Integration externer Load Balancer auf die Umschaltfläche **Integration des externen Load Balancers**.

**Hinweis** Wenn Sie eine virtuelle IP (VIP) eingerichtet haben (überprüfen Sie **System > Anwendungen > Virtuelle IP**), können Sie die **Integration des externen Load Balancers** auch dann nicht verwenden, wenn Sie sie aktivieren. Dies liegt daran, dass entweder die VIP oder der externe Load Balancer aktiv sein kann, während Sie vIDM konfigurieren, aber nicht beides. Deaktivieren Sie VIP, wenn Sie den externen Load Balancer verwenden möchten. Weitere Informationen finden Sie unter [Konfigurieren einer virtuellen IP-Adresse \(VIP\) für einen Cluster](#) im *Installationshandbuch für NSX-T Data Center*.

- 6 Klicken Sie zum Aktivieren der Integration von VMware Identity Manager auf die Umschaltfläche **VMware Identity Manager-Integration**.
- 7 Geben Sie die folgenden Informationen an.

Parameter	Beschreibung
<b>VMware Identity Manager-Appliance</b>	Der vollqualifizierte Domänenname (FQDN) des vIDM-Hosts.
<b>OAuth-Client-ID</b>	Die ID, die beim Registrieren von NSX Manager für den vIDM-Host erstellt wird.
<b>OAuth-Client-Secret</b>	Der geheime Schlüssel, der beim Registrieren von NSX Manager für den vIDM-Host erstellt wird.
<b>SSL-Fingerabdruck</b>	Der Fingerabdruck des Zertifikats für den vIDM-Host.
<b>NSX-Appliance</b>	Die IP-Adresse oder der vollqualifizierte Domänenname (FQDN) von NSX Manager. Wenn Sie einen NSX Manager-Cluster nutzen, verwenden Sie den FQDN des Load Balancer, den VIP-FQDN oder die IP-Adresse des Clusters. Wenn Sie einen FQDN angeben, müssen Sie über einen Browser mit dem FQDN des Managers in der URL auf NSX Manager zugreifen, und wenn Sie eine IP-Adresse angeben, müssen Sie die IP-Adresse in der URL verwenden. Alternativ dazu kann der vIDM-Administrator den NSX Manager-Client so konfigurieren, dass die Verbindung entweder über den FQDN oder über die IP-Adresse hergestellt werden kann.

- 8 Klicken Sie auf **Speichern**.
- 9 Wenn Sie NSX Cloud verwenden, wiederholen Sie die Schritte 1 bis 8 von der CSM-Appliance, indem Sie sich bei CSM statt bei NSX Manager anmelden.

## Zeitsynchronisierung zwischen NSX Manager, vIDM und zugehörigen Komponenten

Zur Gewährleistung einer ordnungsgemäßen Authentifizierung müssen NSX Manager, vIDM und andere Dienstanbieter wie z. B. Active Directory zeitlich miteinander synchronisiert sein. In diesem Abschnitt wird beschrieben, wie eine Zeitsynchronisierung für diese Komponenten vorgenommen wird.

## VMware Infrastructure

Befolgen Sie die Anweisungen in den folgenden KB-Artikeln, um ESXi-Hosts zu synchronisieren.

- <https://kb.vmware.com/kb/1003736>
- <https://kb.vmware.com/kb/2012069>

## Drittanbieter-Infrastruktur

Konsultieren Sie die Dokumentation des Anbieters hinsichtlich der Synchronisierung von VMs und Hosts.

## Konfigurieren von NTP auf dem vIDM-Server (nicht empfohlen)

Wenn das Synchronisieren der Zeit auf allen Hosts nicht möglich ist, können Sie die Synchronisierung mit dem Host deaktivieren und NTP auf dem vIDM-Server konfigurieren. Diese Methode wird jedoch nicht empfohlen, da hierfür UDP-Port 123 auf dem vIDM-Server geöffnet werden muss.

- Überprüfen Sie die Uhr auf dem vIDM-Server, um sich zu vergewissern, dass sie korrekt eingestellt ist.

```
# hwclock
Tue May 9 12:08:43 2017 -0.739213 seconds
```

- Bearbeiten Sie `/etc/ntp.conf` und fügen Sie die folgenden Einträge hinzu, sofern sie noch nicht vorhanden sind.

```
server server time.nist.gov
server server pool.ntp.org
server server time.is dynamic
```

- Öffnen Sie UDP-Port 123.

```
# iptables -A INPUT -p udp --dport 123 -j ACCEPT
```

Führen Sie den folgenden Befehl aus, um zu überprüfen, ob der Port geöffnet ist.

```
# iptables -L -n
```

- Starten Sie den NTP-Dienst.

```
/etc/init.d/ntp start
```

- Legen Sie fest, dass NTP nach einem Neustart automatisch ausgeführt wird.

```
# chkconfig --add ntp
# chkconfig ntp on
```

- Überprüfen Sie, ob der NTP-Server erreicht werden kann.

```
# ntpq -p
```

Die Spalte `reach` sollte nicht 0 anzeigen. Die Spalte `st` sollte eine Ziffer, nicht jedoch 16 anzeigen.

## Rollenbasierte Zugriffssteuerung

Mit der rollenbasierten Zugriffssteuerung (RBAC) können Sie den Systemzugriff auf autorisierte Benutzer einschränken. Benutzern werden Rollen zugewiesen, und jede Rolle verfügt über bestimmte Berechtigungen.

Es gibt vier Arten von Berechtigungen:

- Vollzugriff
- Ausführen
- Lesen
- Keine

Vollzugriff gewährt dem Benutzer sämtliche Berechtigungen. Die Ausführungsberechtigung schließt die Leseberechtigung ein.

NSX-T Data Center hat die folgenden integrierten Rollen. Sie können keine neuen Rollen hinzufügen.

- Enterprise-Administrator
- Auditor
- Netzwerktechniker
- Netzwerkvorgänge
- Sicherheitstechniker
- Sicherheitsvorgänge
- Cloud-Dienstadministrator
- Cloud-Dienstauditor
- Load Balancer-Administrator
- Load Balancer-Auditor
- VPN-Administrator
- Guest Introspection-Administrator
- Network Introspection-Administrator

Nachdem einem Active Directory-Benutzer eine Rolle zugewiesen wurde, müssen Sie die Rolle unter Verwendung des neuen Benutzernamens erneut zuweisen, wenn der Benutzername auf dem Active Directory-Server geändert wird.

## Rollen und Berechtigungen

**Tabelle 21-1. Rollen und Berechtigungen** zeigt die Berechtigungen an, die die einzelnen Rollen für verschiedene Vorgänge haben. Die folgenden Abkürzungen werden verwendet:

- EA – Enterprise-Administrator
- A – Auditor
- NE – Netzwerktechniker
- NO – Netzwerkvorgänge
- SE – Sicherheitstechniker
- SO – Sicherheitsvorgänge
- CS Adm – Cloud-Dienstadministrator
- CS Aud – Cloud-Dienstauditor
- LB Adm – Load Balancer-Administrator
- LB Aud – Load Balancer-Auditor
- VPN Adm – VPN-Administrator
- GI Adm – Guest Introspection-Administrator
- NI Adm – Network Introspection-Administrator
- FA – Vollzugriff
- E – Ausführen
- R – Lesen

**Tabelle 21-1. Rollen und Berechtigungen**

Vorgang	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud	VPN Adm	GI Adm	NI Adm
Tools > Portverbindung	E	R	E	E	E	E	E	R	E	E	Keine	Keine	Keine
Tools > Traceflow	E	R	E	E	E	E	E	R	E	E	Keine	Keine	Keine
Tools > Portspiegelung	FA	R	FA	FA	FA	FA	FA	R	Keine	Keine	Keine	Keine	Keine
Tools > IPFIX	FA	R	FA	R	FA	R	FA	R	Keine	Keine	R	R	R
Firewall > Allgemein	FA	R	R	R	FA	R	FA	R	Keine	Keine	Keine	Keine	R

Tabelle 21-1. Rollen und Berechtigungen (Fortsetzung)

<b>Vorgang</b>	<b>EA</b>	<b>A</b>	<b>NE</b>	<b>NO</b>	<b>SE</b>	<b>SO</b>	<b>CS Adm</b>	<b>CS Aud</b>	<b>LB Adm</b>	<b>LB Aud</b>	<b>VPN Adm</b>	<b>GI Adm</b>	<b>NI Adm</b>
Firewall > Konfiguration	FA	R	R	R	FA	R	FA	R	Keine	Keine	Keine	Keine	Keine
Routing > Router	FA	R	FA	R	R	R	FA	R	R	R	Keine	Keine	Keine
Routing > NAT	FA	R	FA	R	FA	R	FA	R	R	R	Keine	Keine	Keine
DHCP > Serverprofile	FA	R	FA	R	FA	Keine	FA	R	Keine	Keine	Keine	Keine	Keine
DHCP > Server	FA	R	FA	R	FA	Keine	FA	R	Keine	Keine	Keine	Keine	Keine
DHCP > Relay- Profile	FA	R	FA	R	FA	Keine	FA	R	Keine	Keine	Keine	Keine	Keine
DHCP > Relay- Dienste	FA	R	FA	R	FA	Keine	FA	R	Keine	Keine	Keine	Keine	Keine
DHCP > Metadaten- Proxys	FA	R	FA	R	FA	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine
IPAM	FA	R	FA	R	FA	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine
Switching > Switches	FA	R	FA	FA	R	R	FA	R	R	R	Keine	Keine	Keine
Switching > Ports	FA	R	FA	FA	R	R	FA	R	R	R	Keine	Keine	Keine
Switching > Switching- Profile	FA	R	FA	FA	FA	FA	FA	R	R	R	Keine	Keine	Keine

Tabelle 21-1. Rollen und Berechtigungen (Fortsetzung)

<b>Vorgang</b>	<b>EA</b>	<b>A</b>	<b>NE</b>	<b>NO</b>	<b>SE</b>	<b>SO</b>	<b>CS Adm</b>	<b>CS Aud</b>	<b>LB Adm</b>	<b>LB Aud</b>	<b>VPN Adm</b>	<b>GI Adm</b>	<b>NI Adm</b>
Richtlinie > Netzwerk > Load Balance rs	FA	R	Keine	Keine	Keine	Keine	FA	R	FA	R	Keine	Keine	Keine
Lastausgleich > Virtuelle Server	FA	R	Keine	Keine	Keine	Keine	FA	R	FA	R	Keine	Keine	Keine
Lastausgleich > Profile > Anwendungsprofile	FA	R	Keine	Keine	Keine	Keine	FA	R	FA	R	Keine	Keine	Keine
Lastausgleich > Profile > Persistenzprofile	FA	R	Keine	Keine	Keine	Keine	FA	R	FA	R	Keine	Keine	Keine
Lastausgleich > Profile > SSL- Profile	FA	R	Keine	Keine	FA	R	FA	R	FA	R	Keine	Keine	Keine
Lastausgleich > Serverpools	FA	R	Keine	Keine	Keine	Keine	FA	R	FA	R	Keine	Keine	Keine
Lastausgleich > Überwachung	FA	R	Keine	Keine	Keine	Keine	FA	R	FA	R	Keine	Keine	Keine
Bestand > Gruppen	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
Bestand > IP Sets	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R



Tabelle 21-1. Rollen und Berechtigungen (Fortsetzung)

<b>Vorgang</b>	<b>EA</b>	<b>A</b>	<b>NE</b>	<b>NO</b>	<b>SE</b>	<b>SO</b>	<b>CS Adm</b>	<b>CS Aud</b>	<b>LB Adm</b>	<b>LB Aud</b>	<b>VPN Adm</b>	<b>GI Adm</b>	<b>NI Adm</b>
Bestand > IP-Pools	FA	R	FA	R	Keine	R	Keine	Keine	R	R	R	R	R
Bestand > MAC Sets	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
Bestand > Dienste	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
Bestand > Virtuelle Maschinen	R	R	R	R	R	R	R	R	R	R	R	R	R
Bestand > VM > Tags erstellen und zuweisen	FA	R	FA	FA	FA	FA	FA	R	R	R	R	FA	FA
Bestand > VM > Tags konfigurieren	FA	Keine	Keine	Keine	FA	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine
Fabric > Knoten > Hosts	FA	R	R	R	R	R	R	R	Keine	Keine	Keine	Keine	Keine
Fabric > Knoten > Knoten	FA	R	FA	R	FA	R	R	R	Keine	Keine	Keine	Keine	Keine
Fabric > Knoten > Edges	FA	R	FA	R	R	R	R	R	Keine	Keine	Keine	Keine	Keine
Fabric > Knoten > Edge-Cluster	FA	R	FA	R	R	R	R	R	Keine	Keine	Keine	Keine	Keine
Fabric > Knoten > Bridges	FA	R	FA	R	R	R	Keine	Keine	R	R	Keine	Keine	Keine

Tabelle 21-1. Rollen und Berechtigungen (Fortsetzung)

Vorgang	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud	VPN Adm	GI Adm	NI Adm
Fabric > Knoten > Transpo rtknote n	FA	R	R	R	R	R	R	R	R	R	Keine	Keine	Keine
Fabric > Knoten > Tunnel	R	R	R	R	R	R	R	R	R	R	Keine	Keine	Keine
Fabric > Profile > Uplink- Profile	FA	R	R	R	R	R	R	R	R	R	Keine	Keine	Keine
Fabric > Profile > Edge- Cluster- Profile	FA	R	FA	R	R	R	R	R	R	R	Keine	Keine	Keine
Fabric > Profile > Konfigu- ration	FA	R	Keine	Keine	Keine	Keine	R	R	Kein e	Kei ne	Keine	Keine	Keine
Fabric > Transpo rtzonen > Transpo rtzonen	FA	R	R	R	R	R	R	R	R	R	Keine	Keine	Keine
Fabric > Transpo rtzonen > Transpo rtzonen profile	FA	R	R	R	R	R	R	R	R	R	Keine	Keine	Keine
Fabric > Berechn ungsma nager	FA	R	R	R	R	R	R	R	Kein e	Kei ne	Keine	R	R
System > Vertrau en	FA	R	Keine	Keine	FA	R	Keine	Kein e	FA	R	FA	Keine	Keine

Tabelle 21-1. Rollen und Berechtigungen (Fortsetzung)

<b>Vorgang</b>	<b>EA</b>	<b>A</b>	<b>NE</b>	<b>NO</b>	<b>SE</b>	<b>SO</b>	<b>CS Adm</b>	<b>CS Aud</b>	<b>LB Adm</b>	<b>LB Aud</b>	<b>VPN Adm</b>	<b>GI Adm</b>	<b>NI Adm</b>
System > Konfiguration	FA	R	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine
System > Dienstprogramm me > Support-Paket	FA	R	R	R	R	R	R	R	Keine	Keine	Keine	Keine	Keine
System > Dienstprogramm me > Sicherung	FA	R	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine
System > Dienstprogramm me > Wiederherstellen	FA	R	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine
System > Dienstprogramm me > Upgrade	FA	R	R	R	R	R	Keine	Keine	Keine	Keine	Keine	Keine	Keine
System > Benutzer > Rollenzuweisung	FA	R	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine
System > Benutzer > Konfiguration	FA	R	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine

## Hinzufügen einer Rollenzuweisung oder Prinzipalidentität

Sie können Benutzern oder Benutzergruppen Rollen zuweisen, wenn VMware Identity Manager in NSX-T Data Center integriert ist. Rollen können auch Prinzipalidentitäten zugewiesen werden.

Ein Prinzipal ist eine NSX-T Data Center-Komponente oder eine Drittanbieteranwendung, wie z. B. ein OpenStack-Produkt. Ein Prinzipal mit einer Prinzipalidentität kann den Identitätsnamen dazu verwenden, ein Objekt zu erstellen und sicherzustellen, dass nur eine Entität mit demselben Identitätsnamen das Objekt ändern oder löschen kann. Eine Prinzipalidentität hat folgende Attribute:

- Name
- Knoten-ID: Dies kann ein alphanumerischer Wert sein, der einer Prinzipalidentität zugewiesen wurde
- Zertifikat
- RBAC-Rolle, welche die Zugriffsrechte des Prinzipals definiert

Benutzer (lokale, Remote- oder Prinzipalidentität) mit der Enterprise-Administrator-Rolle können Objekte ändern oder löschen, die im Besitz von Prinzipalidentitäten sind. Benutzer (lokale, Remote- oder Prinzipalidentität) ohne die Enterprise-Administrator-Rolle können geschützte Objekte im Besitz von Prinzipalidentitäten weder ändern noch löschen. Ungeschützte Objekte können jedoch geändert oder gelöscht werden.

Wenn das Zertifikat eines Prinzipalidentitätsbenutzers abläuft, müssen Sie ein neues Zertifikat importieren und einen API-Aufruf durchführen, um das Zertifikat des Prinzipalidentitätsbenutzers zu aktualisieren. (Weitere Informationen finden Sie im nachfolgenden Verfahren.) Weitere Informationen zur NSX-T Data Center-API und einen Link zur API-Ressource finden Sie unter <https://docs.vmware.com/de/VMware-NSX-T-Data-Center>.

Das Zertifikat eines Prinzipal-Identitätsbenutzers muss die folgenden Anforderungen erfüllen:

- SHA256-basiert.
- RSA/DSA-Meldungsalgorithmus mit einer Schlüsselgröße von 2048 Bits oder mehr.
- Kann kein Stammzertifikat sein.

Sie können eine Prinzipalidentität mithilfe der API löschen. Wenn Sie jedoch eine Prinzipalidentität löschen, wird das entsprechende Zertifikat nicht automatisch gelöscht. Sie müssen das Zertifikat manuell gelöscht haben.

Schritte zum Löschen einer Prinzipalidentität und ihres Zertifikats:

- 1 Erhalten Sie die Details der Prinzipalidentität, um den Wert der `certificate_id` in der Antwort zu löschen.

```
GET /api/v1/trust-management/principal-identities/<principal-identity-id>
```

- 2 Löschen Sie die Prinzipalidentität.

```
DELETE /api/v1/trust-management/principal-identities/<principal-identity-id>
```

- 3 Löschen Sie das Zertifikat mithilfe des in Schritt 1 erzielten `certificate_id`-Werts.

`DELETE /api/v1/trust-management/certificates/<certificate_id>`

#### Voraussetzungen

- Wenn Sie Benutzern Rollen zuweisen möchten, stellen Sie sicher, dass ein vIDM-Host mit NSX-T verknüpft ist. Weitere Informationen finden Sie unter [Konfigurieren der Integration von VMware Identity 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 > Benutzer**.
- 3 Wählen Sie zum Zuweisen von Rollen zu Benutzern **Hinzufügen > Rollenzuweisung** aus.
  - a Wählen Sie einen Benutzer oder eine Benutzergruppe aus.
  - b Wählen Sie eine Rolle aus.
  - c Klicken Sie auf **Speichern**.
- 4 Wählen Sie zum Hinzufügen einer Prinzipalidentität **Hinzufügen > Prinzipalidentität mit Rolle** aus.
  - a Geben Sie einen Namen für die Prinzipalidentität ein.
  - b Wählen Sie eine Rolle aus.
  - c Geben Sie eine Knoten-ID ein.
  - d Geben Sie ein Zertifikat im PEM-Format ein.
  - e Klicken Sie auf **Speichern**.
- 5 (Optional) Wenn Sie NSX Cloud verwenden, melden Sie sich bei der CSM-Appliance statt beim NSX Manager an und wiederholen Sie die Schritte 1 bis 4.

**6** Wenn das Zertifikat für die Prinzipalidentität abläuft, führen Sie die folgenden Schritte aus:

- a Importieren Sie ein neues Zertifikat und notieren Sie sich die ID des Zertifikats. Siehe [Importieren eines Zertifikats](#).
- b Rufen Sie die folgende API auf, um die ID der Prinzipalidentität zu erhalten.

GET `https://<nsx-mgr>/api/v1/trust-management/principal-identities`

- c Rufen Sie die folgende API auf, um das Zertifikat der Prinzipalidentität zu aktualisieren. Sie müssen die ID des importierten Zertifikats und die ID des Prinzipalidentitätsbenutzers angeben.

Beispiel:

```
POST https://<nsx-mgr>/api/v1/trust-management/principal-identities?action=update_certificate
{
  "principal_identity_id": "ebd3032d-728e-44d4-9914-d4f81c9972cb",
  "certificate_id" : "abd3032d-728e-44d4-9914-d4f81c9972cc"
}
```

## Sichern und Wiederherstellen von NSX Manager

Wenn der NSX Manager-Cluster nicht mehr funktionsfähig ist oder wenn Sie Ihre Umgebung auf einen früheren Zustand zurücksetzen möchten, können Sie eine Wiederherstellung anhand einer Sicherung durchführen. Während NSX Manager nicht mehr funktionsfähig ist, ist die Datenebene nicht betroffen, aber Sie können keine Änderungen an der Konfiguration vornehmen.

Es gibt zwei Arten von Sicherungen:

### Clustersicherung

Diese Sicherung umfasst den gewünschten Zustand des virtuellen Netzwerks.

### Knotensicherung

Hierbei handelt es sich um eine Sicherung der NSX Manager-Knoten.

Es gibt zwei Sicherungsmethoden:

#### Manuell

Sie können die Sicherung jederzeit manuell ausführen.

#### Automatisiert

Automatische Sicherungen werden nach einem von Ihnen festgelegten Zeitplan durchgeführt. Automatische Sicherungen werden dringend empfohlen, um sicherzustellen, dass die Sicherungen aktuell sind.

Sie können NSX-T Data Center-Konfigurationen wieder in den Zustand zurückversetzen, der bei einer beliebigen Sicherung gespeichert wurde. Sicherungen müssen auf neuen NSX Manager-Appliances wiederhergestellt werden, die in derselben NSX Manager-Version wie die gesicherten Appliances ausgeführt werden.

## Konfigurieren von Sicherungen

Bevor Sicherungen durchgeführt werden können, müssen Sie einen Sicherungsdateiserver konfigurieren. Nach der Konfiguration eines Sicherungsdateiservers können Sie jederzeit eine Sicherung starten oder einen Zeitplan für automatische Sicherungen erstellen.

### Voraussetzungen

Stellen Sie sicher, dass Sie über den SSH-Fingerabdruck des Sicherungsdateiservers verfügen. Ausschließlich ein SHA256-gehashter ECDSA-Schlüssel (256 Bit) wird als Fingerabdruck akzeptiert. Siehe [Suchen nach dem SSH-Fingerabdruck eines Remote-Servers](#).

### 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 > Sichern und Wiederherstellen**.
- 3 Klicken Sie oben rechts auf der Seite auf **Bearbeiten**, um Sicherungen zu konfigurieren.
- 4 Geben Sie die IP-Adresse oder den Hostnamen des Sicherungsdateiservers ein.
- 5 Ändern Sie gegebenenfalls den Standardport.
- 6 Das Protokollfeld ist bereits ausgefüllt. Ändern Sie den Wert nicht.

SFTP ist das einzige unterstützte Protokoll.

- 7 Geben Sie den Benutzernamen und das Kennwort ein, die für die Anmeldung beim Sicherungsdateiserver erforderlich sind.

Beim erstmaligen Konfigurieren eines Dateiservers müssen Sie ein Kennwort angeben. Wenn Sie den Dateiserver danach neu konfigurieren und die Server-IP (oder der Hostname), der Port und der Benutzername gleich bleiben, müssen Sie das Kennwort nicht erneut eingeben.

- 8 Geben Sie im Feld **Zielverzeichnis** den absoluten Verzeichnispfad ein, unter dem die Sicherungen gespeichert werden sollen.

Das Verzeichnis muss bereits vorhanden sein und darf nicht / lauten. Wenn Sie über mehrere NSX-T Data Center-Bereitstellungen verfügen, müssen Sie für jede Bereitstellung ein eigenes

Verzeichnis verwenden. Wenn es sich bei dem Sicherungsdateiserver um eine Windows-Maschine handelt, verwenden Sie beim Angeben des Zielverzeichnisses weiterhin den Schrägstrich. Wenn das Sicherungsverzeichnis auf der Windows-Maschine beispielsweise `c:\SFTP_Root\backup` lautet, geben Sie `/SFTP_Root/backup` als Zielverzeichnis an.

---

**Hinweis** Beim Sicherungsvorgang wird ein Name für die Sicherungsdatei generiert, der recht lang sein kann. Auf einem Windows-Server kann die Länge des vollständigen Pfadnamens der Sicherungsdatei den von Windows festgelegten Grenzwert überschreiten und dazu führen, dass Sicherungen fehlschlagen. Um dieses Problem zu vermeiden, lesen Sie den KB-Artikel <https://kb.vmware.com/s/article/76528>.

---

- 9 Klicken Sie zum Verschlüsseln der Sicherungen auf die Umschaltfläche **Verschlüsselungs-Passphrase ändern** und geben Sie die Passphrase für die Verschlüsselung ein.  
  
Diese Passphrase wird benötigt, um eine Sicherung wiederherzustellen. Wenn Sie die Passphrase vergessen, können Sie keine Sicherungen wiederherstellen.
- 10 Geben Sie den SSH-Fingerabdruck des Servers ein, auf dem die Sicherungen gespeichert sind.  
  
Sie können dieses Feld leer lassen und den vom Server bereitgestellten Fingerabdruck akzeptieren oder ablehnen.
- 11 Klicken Sie auf die Registerkarte **Zeitplan**.
- 12 Klicken Sie zum Aktivieren automatischer Sicherungen auf die Umschaltfläche **Automatische Sicherung**.
- 13 Klicken Sie auf **Wöchentlich** und legen Sie die Tage und Uhrzeiten für die Sicherungen fest oder klicken Sie auf **Intervall**, um den Zeitraum zwischen den Sicherungen anzugeben.
- 14 Zum Auslösen einer Sicherung bei einer Änderung der Netzwerkkonfiguration legen Sie die Umschaltfläche **NSX-Konfigurationsänderung erkennen** auf **Aktiviert** fest.  
  
Sie können das Intervall zwischen den Sicherungen festlegen, die durch die Konfigurationsänderungen ausgelöst werden. Die Standardeinstellung ist 5 Minuten.
- 15 Klicken Sie auf **Speichern**.

### Ergebnisse

Nachdem Sie einen Sicherungsdateiserver konfiguriert haben, können Sie zum Starten einer Sicherung jederzeit auf **Jetzt sichern** klicken.

## Entfernen alter Sicherungen

Sicherungen können sich auf dem Sicherungsdateiserver ansammeln und große Mengen an Speicherplatz verbrauchen. Sie können ein im Lieferumfang von NSX-T Data Center enthaltenes Skript zum automatischen Löschen alter Sicherungen ausführen.



Das Python-Skript `nsx_backup_cleaner.py` steht im Verzeichnis `/var/vmware/nsx/file-store` von NSX Manager zur Verfügung. Sie müssen sich als Root-Benutzer anmelden, um auf diese Datei zugreifen zu können. In der Regel planen Sie einen Auftrag auf dem Sicherungsdateiserver, um dieses Skript in regelmäßigen Abständen zum Löschen alter Sicherungen auszuführen. In den folgenden Nutzungsinformationen wird die Ausführung des Skripts beschrieben:

```
nsx_backup_cleaner.py -d backup_dir [-k 1] [-l 5] [-h]
Or
nsx_backup_cleaner.py --dir backup_dir [--retention-period 1] [--min-count 5] [--help]
```

**Required parameters:**

- d/--dir: Backup root directory
- k/--retention-period: Number of days need to retain a backup file

**Optional parameters:**

- l/--min-count: Minimum number of backup files to be kept, default value is 100
- h/--help: Display help message

Das Alter einer Sicherung wird als Differenz zwischen dem Zeitstempel der Sicherung und der Uhrzeit der Skriptausführung berechnet. Ist dieser Wert größer als der Aufbewahrungszeitraum, wird die Sicherung gelöscht, wenn sich auf der Festplatte mehr Sicherungen als die Mindestanzahl an Sicherungen befinden.

Weitere Informationen zum Einrichten eines Skripts, das in regelmäßigen Abständen auf einem Linux- oder Windows-Server ausgeführt werden soll, finden Sie in den Kommentaren am Anfang des Skripts.

## Auflisten der verfügbaren Sicherungen

Der Sicherungsdateiserver speichert Sicherungen von allen NSX Managern. Damit Sie die wiederherzustellende Liste finden können, müssen Sie die Liste der Sicherungen abrufen. Führen Sie dazu das Skript `get_backup_timestamps.sh` aus.

Das Skript befindet sich in einem NSX Manager. Der vollständige Pfadname lautet `/var/vmware/nsx/file-store/get_backup_timestamps.sh`. Sie können dieses Skript auf jeder Linux-Maschine oder NSX-T Data Center-Appliance ausführen. Es empfiehlt sich, dieses Skript nach der Installation von NSX-T Data Center auf einen Computer kopieren, der kein NSX Manager ist, damit Sie dieses Skript selbst dann ausführen können, wenn nicht auf alle NSX Manager zugegriffen werden kann. Wenn Sie eine Sicherung wiederherstellen müssen, aber keinen Zugriff auf dieses Skript haben, können Sie einen neuen NSX Manager installieren und das Skript dort ausführen.

Sie können das Skript auf eine andere Maschine oder auf den Sicherungsdateiserver kopieren, indem Sie sich bei NSX Manager als Administrator anmelden und einen CLI-Befehl ausführen. Beispiel:

```
nsxmgr-1> copy file get_backup_timestamps.sh url scp://admin@10.127.1.20/tmp/
admin@10.127.1.20's password:
nsxmgr-1>
```

Das Skript ist interaktiv und fordert Sie auf, die Informationen einzugeben, die Sie bei der Konfiguration des Sicherungsdateiservers angegeben haben. Sie können die Anzahl der anzuzeigenden Sicherungen angeben. Jede Sicherung wird mit den folgenden Angaben aufgeführt: einem Zeitstempel, der IP-Adresse des NSX Manager-Knotens oder dem FQDN, wenn der NSX Manager-Knoten für die Veröffentlichung des FQDN eingerichtet ist, und der Knoten-ID. Beispiel:

```
admin@host1:/home/admin# ./get_backup_timestamps.sh
Enter file server ip:
10.108.115.108
Enter port:
22
Enter directory path:
/home/nsx/backups
Enter number of latest backup or press Enter to list all backups:

root@10.108.115.108's password:
Latest backups:
[Backup timestamp; IP address/FQDN; Node id]
2019-01-22;09:00:33 10.196.196.77 35163642-6623-8f6d-7af0-52e03f16faed
2019-01-22;09:01:52 10.196.196.77 35163642-6623-8f6d-7af0-52e03f16faed
2019-01-22;09:13:30 wdc75.platformqe.com 41893642-597b-915f-5117-7da576df4ff2
2019-01-22;09:14:42 wdc75.platformqe.com 41893642-597b-915f-5117-7da576df4ff2
2019-01-22;09:16:43 wdc75.platformqe.com 41893642-597b-915f-5117-7da576df4ff2
```

## Wiederherstellen einer Sicherung

Durch das Wiederherstellen einer Sicherung wird der Status des Netzwerks zum Zeitpunkt der Sicherung wiederhergestellt. Darüber hinaus werden die von NSX Manager verwalteten Konfigurationen ebenfalls wiederhergestellt, und alle Änderungen, wie z. B. das Hinzufügen oder Löschen von Knoten, die an der Fabric vorgenommen wurden, seit die Sicherung erstellt wurde, werden abgeglichen.

Sie müssen eine Sicherung auf einer neuen Installation von NSX Manager wiederherstellen. Dies wird unten im ersten Schritt beschrieben.

### Voraussetzungen

- Stellen Sie sicher, dass Sie über die Anmeldedaten für den Sicherungsdateiserver verfügen.
- Stellen Sie sicher, dass Sie über den SSH-Fingerabdruck des Sicherungsdateiservers verfügen. Ausschließlich ein SHA256-gehashter ECDSA-Schlüssel (256 Bit) wird als Fingerabdruck akzeptiert. Siehe [Suchen nach dem SSH-Fingerabdruck eines Remote-Servers](#).
- Stellen Sie sicher, dass die Passphrase der Sicherungsdatei zur Verfügung steht.

## Verfahren

- 1 Installieren Sie einen neuen NSX Manager-Knoten, auf dem die Sicherung wiederhergestellt werden soll.

Wenn der ursprüngliche NSX Manager mit der Standardeinstellung zur Nichtveröffentlichung des FQDN konfiguriert wurde, also mit "publish\_fqdns": false, muss die neue Installation von NSX Manager mit derselben IP-Adresse installiert werden, die vom ursprünglichen NSX Manager verwendet wurde. Wenn der ursprüngliche NSX Manager zum Veröffentlichen des FQDN eingerichtet wurde, also mit "publish\_fqdns": true, kann der neue NSX Manager mit einer anderen IP-Adresse installiert werden. Allerdings muss der neue NSX Manager auch so konfiguriert werden, dass der FQDN veröffentlicht wird. Wurde zum Zeitpunkt der Sicherung ein NSX Manager-Cluster verwendet, muss die Wiederherstellung ebenfalls in einem NSX Manager-Cluster durchgeführt werden. Der Wiederherstellungsprozess stellt zunächst einen NSX Manager-Knoten wieder her. Anschließend werden Sie aufgefordert, die anderen NSX Manager-Knoten hinzuzufügen.

- a Schalten Sie alle NSX Manager-Knoten aus.
- b Stellen Sie einen neuen NSX Manager-Knoten mit dem Namen und der IP-Adresse des ursprünglichen NSX Manager-Knotens bereit.

Um den ursprünglichen NSX Manager-Knoten zu identifizieren, öffnen Sie das NSX Manager Dashboard und navigieren Sie zu **System > Appliances**, um den Verwaltungscluster anzuzeigen. Dadurch werden die NSX Manager-Knoten angezeigt. Der ursprüngliche Knoten ist der Knoten, für dessen Bereitstellungstyp „Manuell“ angezeigt wird.

Sobald der neue NSX Manager-Knoten ausgeführt wird und online ist, können Sie mit dem restlichen Verfahren fortfahren.

- 2 Melden Sie sich über den Browser mit Administratorrechten bei einem neuen NSX Manager an.

Die IP-Adresse oder der FQDN dieses NSX Manager-Knotens muss mit der IP-Adresse oder dem FQDN des NSX Manager identisch sein, für den die Sicherung erstellt wurde.

- 3 Wählen Sie **System > Sichern und Wiederherstellen**.
- 4 Klicken Sie auf die Registerkarte **Wiederherstellen**.
- 5 Um den Sicherungsdateiserver zu konfigurieren, klicken Sie auf **Bearbeiten**.
- 6 Geben Sie die IP-Adresse oder den Hostnamen ein.
- 7 Ändern Sie die Portnummer, falls erforderlich.  
Die Standardeinstellung ist 22.
- 8 Um sich beim Server anzumelden, geben Sie den Benutzernamen und das Kennwort ein.
- 9 Geben Sie im Textfeld **Zielverzeichnis** den absoluten Verzeichnispfad ein, unter dem die Sicherungen gespeichert werden.

- 10 Geben Sie die zur Verschlüsselung der Sicherungsdaten verwendete Passphrase ein.
- 11 Geben Sie den SSH-Fingerabdruck des Servers ein, auf dem die Sicherungen gespeichert sind.
- 12 Klicken Sie auf **Speichern**.
- 13 Wählen Sie eine Sicherung aus.
- 14 Klicken Sie auf **Wiederherstellen**.

Der Status des Wiederherstellungsvorgangs wird angezeigt. Wenn Sie Fabric-Knoten oder Transportknoten seit der Sicherung hinzugefügt oder gelöscht haben, werden Sie zu bestimmten Aktionen aufgefordert, z. B. zum Anmelden bei einem Knoten und Ausführen eines Skripts.

Enthält die Sicherung Informationen über einen NSX Manager-Cluster, werden Sie aufgefordert, NSX Manager-Knoten hinzuzufügen. Wenn Sie keine NSX Manager-Knoten hinzufügen, können Sie dennoch mit der Wiederherstellung fortfahren.

Nachdem der Wiederherstellungsvorgang abgeschlossen ist, wird der Bildschirm „Wiederherstellung abgeschlossen“ angezeigt. Er zeigt das Ergebnis der Wiederherstellung, den Zeitstempel der Sicherungsdatei und die Start- und Endzeit des Wiederherstellungsvorgangs. Wenn die Wiederherstellung fehlgeschlagen ist, wird auf dem Bildschirm der Schritt angezeigt, in dem der Fehler aufgetreten ist, z. B. Current Step: Restoring Cluster (DB) oder Current Step: Restoring Node. Wenn entweder nur die Cluster- oder Knotenwiederherstellung fehlgeschlagen ist, liegt der Fehler möglicherweise nur vorübergehend vor. In diesem Fall müssen Sie nicht auf **Wiederholen** klicken. Sie können den Manager neu starten. Daraufhin wird die Wiederherstellung fortgesetzt. Sie können auch bestimmen, ob bei der Cluster- oder Knotenwiederherstellung ein Fehler aufgetreten ist, indem Sie den folgenden CLI-Befehl ausführen, um die Systemprotokolldatei anzuzeigen und nach den Zeichenfolgen Cluster-Wiederherstellung fehlgeschlagen und Knotenwiederherstellung fehlgeschlagen zu suchen.

```
get log-file syslog
```

Führen Sie zum Neustarten des Managers den folgenden CLI-Befehl aus:

```
restart service manager
```

Führen Sie zum Neustarten des Managers den folgenden CLI-Befehl aus:

```
reboot
```

- 15 Nachdem der erste NSX Manager-Knoten bereit und funktionsfähig ist, stellen Sie zwei weitere Knoten bereit, um den NSX Manager-Cluster zu vervollständigen.

Weitere Informationen finden Sie unter *Bereitstellen von NSX Manager-Knoten zur Bildung eines Clusters über die Benutzeroberfläche* im *Installationshandbuch für NSX-T Data Center*.

- 16** Nachdem der neue NSX Manager-Cluster bereitgestellt wurde, löschen Sie die ursprünglichen NSX Manager-Cluster-VMs, die Sie in Schritt 1a dieses Verfahrens heruntergefahren haben.

## Ergebnisse

**Hinweis** Wenn Sie nach der Sicherung einen Compute Manager hinzugefügt haben und nach der Wiederherstellung versuchen, den Compute Manager erneut hinzuzufügen, erhalten Sie eine Fehlermeldung über die fehlgeschlagene Registrierung. Sie können auf die Schaltfläche **Auflösen** klicken, um den Fehler zu beheben und den Compute Manager erfolgreich hinzuzufügen. Weitere Informationen finden Sie in Schritt 4 unter [Hinzufügen eines Compute Managers](#). Wenn Sie die in einem vCenter Server gespeicherten Informationen zu NSX-T Data Center entfernen möchten, führen Sie die Schritte unter [Entfernen der NSX-T Data Center-Erweiterung aus vCenter Server](#) aus.

## Entfernen der NSX-T Data Center-Erweiterung aus vCenter Server

Wenn Sie einen Compute Manager hinzufügen, fügt NSX Manager seine Identität als Erweiterung in vCenter Server hinzu. Wenn Sie den Compute Manager entfernen, wird die Erweiterung in vCenter Server automatisch entfernt. Wenn die Erweiterung aus irgendeinem Grund nicht entfernt wird, können Sie sie mit dem folgenden Verfahren manuell entfernen.

### Voraussetzungen

Aktivieren Sie den Zugriff auf den Browser für verwaltete Objekte (Managed Object Browser, MOB) von vCenter Server, indem Sie das Verfahren in <https://kb.vmware.com/s/article/2042554> durchführen.

### Verfahren

- 1** Melden Sie sich beim MOB unter `https://<Hostname oder IP-Adresse für vCenter Server>/mob` an.
- 2** Klicken Sie auf den Link **content**, der den Wert für die Eigenschaft **content** in der Tabelle „Eigenschaften“ darstellt.
- 3** Klicken Sie auf den Link **ExtensionManager**, der den Wert der Eigenschaft **extensionManager** aus der Tabelle „Eigenschaften“ darstellt.
- 4** Klicken Sie auf den Link **UnregisterExtension** in der Tabelle „Methoden“.
- 5** Geben Sie `com.vmware.nsx.management.nsx` im Textfeld **Wert** ein.
- 6** Klicken Sie rechts auf der Seite unter der Tabelle „Parameter“ auf den Link **Methode aufrufen**.  
Das Ergebnis der Methode ist `void`, aber die Erweiterung wird entfernt.

- 7 Um sicherzustellen, dass die Erweiterung entfernt wurde, klicken Sie auf der vorherigen Seite auf die Methode **FindExtension** und rufen Sie sie durch Eingabe desselben Werts für die Erweiterung auf.

Das Ergebnis sollte void sein.

## Verwalten des NSX Manager-Clusters

Sie können einen NSX Manager neu starten, wenn er nicht mehr funktionsfähig ist. Sie können auch die IP-Adresse eines NSX Manager ändern.

In einer Produktionsumgebung wird dringend empfohlen, dass der NSX Manager-Cluster zur Bereitstellung von Hochverfügbarkeit aus drei Mitgliedern besteht. Wenn Sie einen NSX Manager löschen und einen neuen bereitstellen, kann der neue NSX Manager dieselbe oder eine andere IP-Adresse aufweisen.

---

**Hinweis** Der primäre NSX Manager-Knoten ist der Knoten, den Sie zuerst erstellen, bevor Sie einen Manager-Cluster erstellen. Dieser Knoten kann nicht gelöscht werden. Nachdem Sie zwei weitere Manager-Knoten aus der Benutzeroberfläche des primären Manager-Knotens bereitgestellt haben, um einen Cluster zu bilden, verfügen nur der zweite und der dritte Manager-Knoten über die Option (über das Zahnradsymbol) zum Löschen. Informationen zum Entfernen und Hinzufügen eines Manager-Knotens finden Sie unter [Ändern der IP-Adresse eines NSX Manager](#).

---

## Anzeigen der Konfiguration und des Status des NSX Manager-Clusters

Sie können die Konfiguration und den Status des NSX Manager-Clusters über die Benutzeroberfläche von NSX Manager anzeigen. Weitere Informationen können Sie über die CLI abrufen.

### Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie **System > Übersicht**.  
Der Status des NSX Manager-Clusters wird angezeigt.
- 3 Führen Sie den folgenden CLI-Befehl aus, um zusätzliche Informationen zur Konfiguration anzuzeigen:

```
manager1> get cluster config
Cluster Id: 18807edd-56d1-4107-b7b7-508d766a08e3
Cluster Configuration Version: 3
Number of nodes in the cluster: 3

Node UUID: 43cd0642-275c-af1d-fe46-1f5200f9e5f9
Node Status: JOINED
```

ENTITY			UUID	IP
ADDRESS	PORT	FQDN		
HTTPS			5c8d01f1-f3ee-4f94-b517-a093d8fbfad3	
10.160.71.225	443	ychin-nsxmanager-ob-12065118-1-F5		
CONTROLLER			06fd0574-69c0-432e-a8af-53d140dbef8f	
10.160.71.225	-	ychin-nsxmanager-ob-12065118-1-F5		
CLUSTER_BOOT_MANAGER			da8d535e-7a0c-4dd8-8919-d88bdde006b8	
10.160.71.225	-	ychin-nsxmanager-ob-12065118-1-F5		
DATASTORE			3c9c4ec1-afef-47bd-aadb-1ed6a5536bc4	
10.160.71.225	9000	ychin-nsxmanager-ob-12065118-1-F5		
MANAGER			eb5e8922-23bd-4c3a-ae22-d13d9195a6bc	
10.160.71.225	-	ychin-nsxmanager-ob-12065118-1-F5		
POLICY			f9da1039-08ad-4a20-bacc-5b91c5d67730	
10.160.71.225	-	ychin-nsxmanager-ob-12065118-1-F5		
Node UUID: 8ebb0642-201e-6a5f-dd47-a1e38542e672				
Node Status: JOINED				
ENTITY			UUID	IP
ADDRESS	PORT	FQDN		
HTTPS			3757f155-8a5d-4b53-828f-d67041d5a210	
10.160.93.240	443	ychin-nsxmanager-ob-12065118-2-F5		
CONTROLLER			7b1c9952-8738-4900-b68b-ca862aa4f6a9	
10.160.93.240	-	ychin-nsxmanager-ob-12065118-2-F5		
CLUSTER_BOOT_MANAGER			b5e12db1-5e0d-4e33-a571-6ba258dceb2e	
10.160.93.240	-	ychin-nsxmanager-ob-12065118-2-F5		
DATASTORE			bee1f629-4e23-4ab8-8083-9e0f0bb83178	
10.160.93.240	9000	ychin-nsxmanager-ob-12065118-2-F5		
MANAGER			45ccd6e3-1497-4334-944c-e6bbcd5c723e	
10.160.93.240	-	ychin-nsxmanager-ob-12065118-2-F5		
POLICY			d5ba5803-b059-4fbc-897c-3aace8cf1219	
10.160.93.240	-	ychin-nsxmanager-ob-12065118-2-F5		
Node UUID: 2e7e0642-df4a-b2ec-b9e8-633d1469f1ea				
Node Status: JOINED				
ENTITY			UUID	IP
ADDRESS	PORT	FQDN		
HTTPS			bce3cc4c-7d60-45e2-aa7b-cdc75e445a14	
10.160.76.33	443	ychin-nsxmanager-ob-12065118-3-F5		
CONTROLLER			ced46f5c-9e52-4b31-a1cb-b3dead991c71	
10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5		
CLUSTER_BOOT_MANAGER			88b70d31-3428-4ccc-ab57-55859f45030c	
10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5		
DATASTORE			fb4aec3c-cae3-4386-b5b9-c0b99b7d9048	
10.160.76.33	9000	ychin-nsxmanager-ob-12065118-3-F5		
MANAGER			82b07440-3ff6-4f67-a1c9-e9327d1686ad	
10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5		
POLICY			61f21a78-a56c-4af1-867b-3f24132d53c7	
10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5		

- 4 Führen Sie den folgenden CLI-Befehl aus, um zusätzliche Informationen zum Status anzuzeigen:

```
manager1> get cluster status
Cluster Id: 18807edd-56d1-4107-b7b7-508d766a08e3
Group Type: DATASTORE
```

Group Status: STABLE

Members:

UUID	FQDN
IP STATUS	
43cd0642-275c-af1d-fe46-1f5200f9e5f9	ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225 UP	
8ebb0642-201e-6a5f-dd47-a1e38542e672	ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240 UP	
2e7e0642-df4a-b2ec-b9e8-633d1469f1ea	ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33 UP	

Group Type: CLUSTER\_BOOT\_MANAGER

Group Status: STABLE

Members:

UUID	FQDN
IP STATUS	
43cd0642-275c-af1d-fe46-1f5200f9e5f9	ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225 UP	
8ebb0642-201e-6a5f-dd47-a1e38542e672	ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240 UP	
2e7e0642-df4a-b2ec-b9e8-633d1469f1ea	ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33 UP	

Group Type: CONTROLLER

Group Status: STABLE

Members:

UUID	FQDN
IP STATUS	
7b1c9952-8738-4900-b68b-ca862aa4f6a9	ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240 UP	
ced46f5c-9e52-4b31-a1cb-b3dead991c71	ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33 UP	
06fd0574-69c0-432e-a8af-53d140dbef8f	ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225 UP	

Group Type: MANAGER

Group Status: STABLE

Members:

UUID	FQDN
IP STATUS	
43cd0642-275c-af1d-fe46-1f5200f9e5f9	ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225 UP	
8ebb0642-201e-6a5f-dd47-a1e38542e672	ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240 UP	
2e7e0642-df4a-b2ec-b9e8-633d1469f1ea	ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33 UP	

Group Type: POLICY

Group Status: STABLE

Members:



UUID		FQDN
IP	STATUS	
43cd0642-275c-af1d-fe46-1f5200f9e5f9		ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225	UP	
8ebb0642-201e-6a5f-dd47-a1e38542e672		ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240	UP	
2e7e0642-df4a-b2ec-b9e8-633d1469f1ea		ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33	UP	
Group Type: HTTPS		
Group Status: STABLE		
Members:		
UUID		FQDN
IP	STATUS	
43cd0642-275c-af1d-fe46-1f5200f9e5f9		ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225	UP	
8ebb0642-201e-6a5f-dd47-a1e38542e672		ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240	UP	
2e7e0642-df4a-b2ec-b9e8-633d1469f1ea		ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33	UP	

## Neustarten eines NSX Manager

Sie können einen NSX Manager mit einem CLI-Befehl neu starten, um ihn nach kritischen Fehlern wiederherzustellen.

Wenn Sie mehrere NSX Manager neu starten möchten, müssen Sie diese nacheinander starten. Warten Sie, bis der neugestartete NSX Manager online ist, bevor Sie einen anderen NSX Manager neu starten.

### Verfahren

- 1 Melden Sie sich bei der CLI von NSX Manager an.
- 2 Führen Sie folgenden Befehl aus.

```
nsx-manager> reboot
Are you sure you want to reboot (yes/no): y
```

## Ändern der IP-Adresse eines NSX Manager

Sie können die IP-Adresse eines NSX Manager in einem NSX Manager-Cluster ändern. In diesem Abschnitt werden verschiedene Ansätze beschrieben.

Wenn Sie beispielsweise über einen Cluster mit Manager A, Manager B und Manager C verfügen, können Sie die IP-Adresse eines oder mehrerer Manager wie folgt ändern:

- Szenario A:
  - Manager A hat IP-Adresse 172.16.1.11.
  - Manager B hat IP-Adresse 172.16.1.12.

- Manager C hat IP-Adresse 172.16.1.13.
- Fügen Sie Manager D mit einer neuen IP-Adresse hinzu, z. B. 192.168.55.11.
- Entfernen Sie Manager A.
- Fügen Sie Manager E mit einer neuen IP-Adresse hinzu, z. B. 192.168.55.12.
- Entfernen Sie Manager B.
- Fügen Sie Manager F mit einer neuen IP-Adresse hinzu, z. B. 192.168.55.13.
- Entfernen Sie Manager C.
- Szenario B:
  - Manager A hat IP-Adresse 172.16.1.11.
  - Manager B hat IP-Adresse 172.16.1.12.
  - Manager C hat IP-Adresse 172.16.1.13.
  - Fügen Sie Manager D mit einer neuen IP-Adresse hinzu, z. B. 192.168.55.11.
  - Fügen Sie Manager E mit einer neuen IP-Adresse hinzu, z. B. 192.168.55.12.
  - Fügen Sie Manager F mit einer neuen IP-Adresse hinzu, z. B. 192.168.55.13.
  - Entfernen Sie Manager A, Manager B und Manager C.
- Szenario C:
  - Manager A hat IP-Adresse 172.16.1.11.
  - Manager B hat IP-Adresse 172.16.1.12.
  - Manager C hat IP-Adresse 172.16.1.13.
  - Entfernen Sie Manager A.
  - Fügen Sie Manager D mit einer neuen IP-Adresse hinzu, z. B. 192.168.55.11.
  - Entfernen Sie Manager B.
  - Fügen Sie Manager E mit einer neuen IP-Adresse hinzu, z. B. 192.168.55.12.
  - Entfernen Sie Manager C.
  - Fügen Sie Manager F mit einer neuen IP-Adresse hinzu, z. B. 192.168.55.13.

Die ersten beiden Szenarien erfordern zusätzliche virtuelle RAM-, CPU- und Festplattenkapazitäten für die zusätzlichen NSX Manager während dieser Änderung der IP-Adresse.

Szenario C wird nicht empfohlen, da die Anzahl der NSX Manager vorübergehend reduziert wird und ein Verlust eines der beiden aktiven Manager während der Änderung der IP-Adresse Auswirkungen auf den NSX-T-Betrieb hat. Dieses Szenario ist für Situationen gedacht, in denen zusätzliche virtuelle RAM-, CPU- und Festplattenkapazität nicht verfügbar ist und eine Änderung der IP-Adresse erforderlich ist.

---

**Hinweis** Wenn Sie die Cluster-VIP-Funktion verwenden, müssen Sie entweder dasselbe Subnetz für die neuen IP-Adressen verwenden oder die Cluster-VIP während der IP-Adressänderungen deaktivieren, da für die Cluster-VIP alle NSX Manager sich in demselben Subnetz befinden müssen.

---

### Voraussetzungen

Machen Sie sich mit dem Verfahren zur Bereitstellung eines NSX Manager in einem Cluster vertraut. Weitere Informationen finden Sie im *Installationshandbuch zu NSX-T Data Center*.

### Verfahren

- 1 Wenn der NSX Manager, den Sie entfernen möchten, manuell bereitgestellt wurde, führen Sie die folgenden Schritte aus.
  - a Führen Sie den folgenden CLI-Befehl zum Trennen des NSX Manager vom Cluster aus.
 

```
detach node <node-id>
```
  - b Löschen Sie die NSX Manager-VM.
- 2 Wenn der NSX Manager, den Sie löschen möchten, automatisch über die Benutzeroberfläche von NSX Manager bereitgestellt wurde, führen Sie die folgenden Schritte aus.
  - a Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
 

Dieser NSX Manager darf nicht mit demjenigen übereinstimmen, den Sie löschen möchten.
  - b Klicken Sie auf die Registerkarte **Systeme**.
 

Der Status des NSX Manager-Clusters wird angezeigt.
  - c Klicken Sie für den NSX Manager, den Sie löschen möchten, auf das Zahnrad-Symbol und wählen Sie **Löschen** aus.
- 3 Stellen Sie einen neuen NSX Manager bereit.

## Ändern der Größe eines NSX Manager-Knotens

Sie können die Anzahl CPU-Kerne oder den Arbeitsspeicher NSX Manager-Knotens jederzeit ändern.

Beachten Sie, dass alle drei Manager-Knoten unter normalen Betriebsbedingungen über dieselbe Anzahl CPU-Kerne und denselben Arbeitsspeicher verfügen müssen. Eine Nichtübereinstimmung von CPU oder Arbeitsspeicher zwischen NSX Managern in einem NSX Management-Cluster sollte nur beim Übergang von einer Größe von NSX Manager in eine andere Größe von NSX Manager durchgeführt werden.

Wenn Sie die Reservierung der Ressourcenzuteilung für die NSX Manager-VMs in vCenter Server konfiguriert haben, müssen Sie möglicherweise die Reservierung anpassen. Weitere Informationen finden Sie in der vSphere-Dokumentation.

### Voraussetzungen

- Stellen Sie sicher, dass die neue Größe die Systemanforderungen für einen Manager-Knoten erfüllt. Weitere Informationen finden Sie unter „Systemanforderungen für NSX Manager-VMs“ im *Installationshandbuch zu NSX-T Data Center*.
- Machen Sie sich mit dem Verfahren zur Bereitstellung eines NSX Manager in einem Cluster vertraut. Weitere Informationen finden Sie im *Installationshandbuch zu NSX-T Data Center*.
- Informationen zum Entfernen eines Manager-Knotens aus einem Cluster finden Sie unter [Ändern der IP-Adresse eines NSX Manager](#).

### Verfahren

- 1 Stellen Sie einen neuen Manager-Knoten mit der neuen Größe bereit.
- 2 Fügen Sie den neuen Manager-Knoten dem Cluster hinzu.
- 3 Entfernen Sie einen alten Manager-Knoten.
- 4 Wiederholen Sie die Schritte 1 bis 3, um die anderen beiden alten Manager-Knoten zu ersetzen.

## Bereitstellung von NSX-T Data Center für mehrere Sites

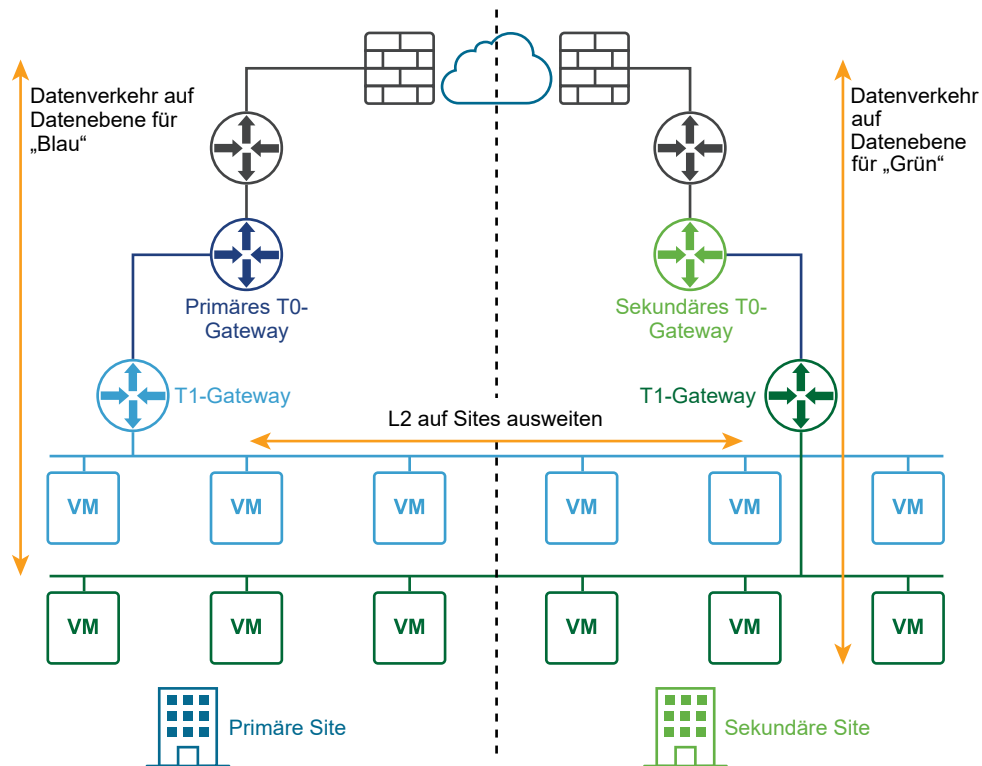
NSX-T Data Center unterstützt Bereitstellungen für mehrere Sites. Dabei können Sie alle Sites von einem zentralen NSX Manager-Cluster aus verwalten.

Zwei Arten von Bereitstellungen für mehrere Sites werden unterstützt:

- Aktiv-Aktiv
- Notfallwiederherstellung

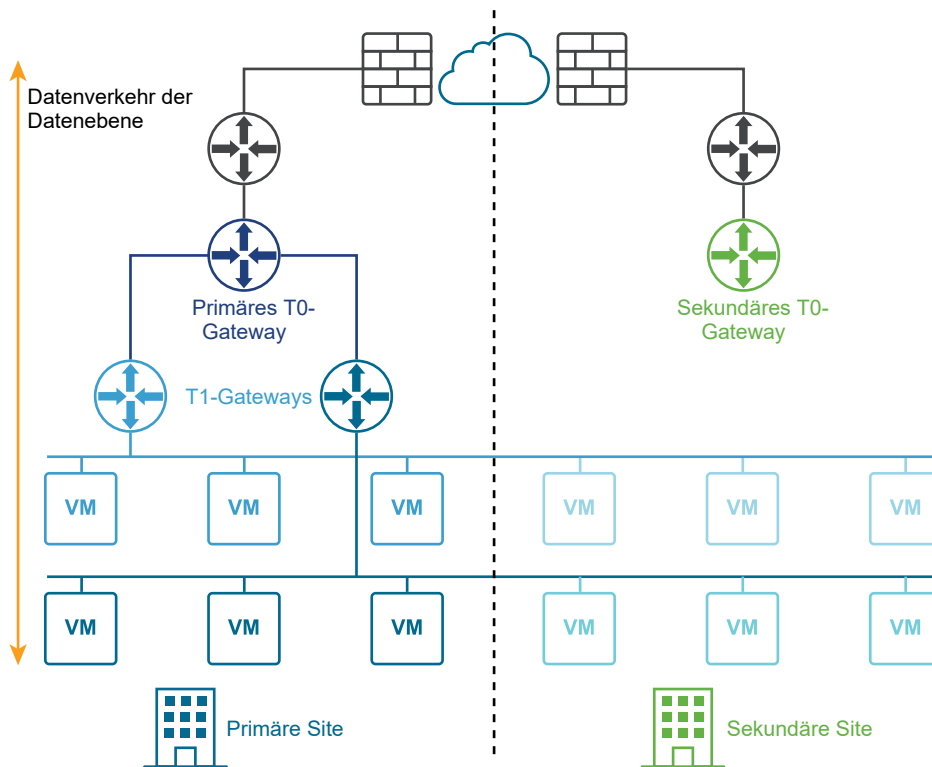
In einer Aktiv-Aktiv-Bereitstellung sind alle Sites aktiv, und Datenverkehr der Schicht 2 überschreitet die Site-Grenzen. In einer Bereitstellung für die Notfallwiederherstellung verarbeitet NSX-T Data Center an der primären Site Netzwerke für das Unternehmen. Die sekundäre Site steht bereit, um zu übernehmen, wenn ein schwerwiegender Fehler an der primären Site auftritt.

Das folgende Diagramm veranschaulicht eine Aktiv-Aktiv-Bereitstellung.

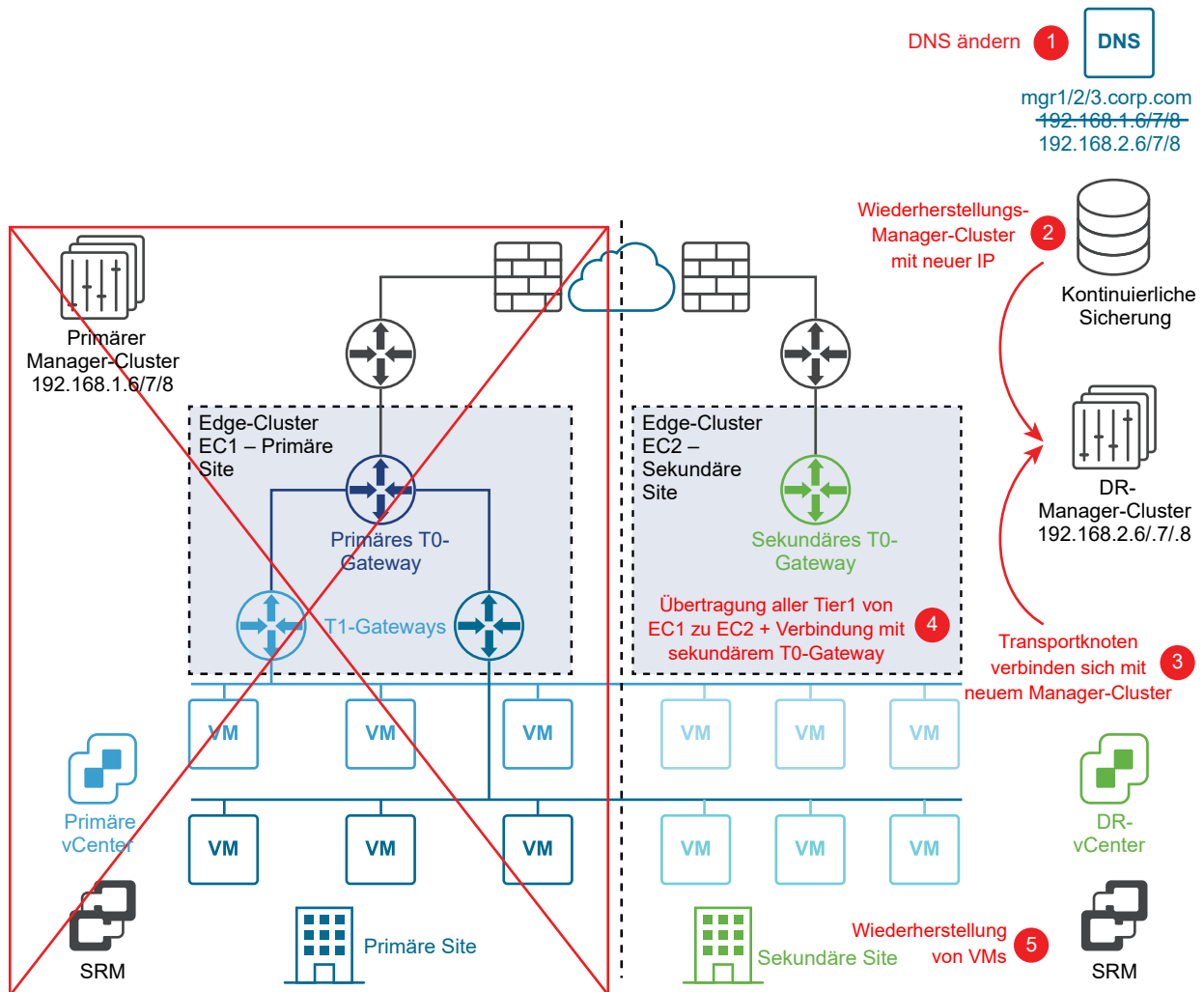


Wenn das primäre Gateway in einer aktiv-aktiv-Bereitstellung ausfällt, wird ein Failover zum sekundären Gateway durchgeführt. Wenn die primäre Site ausfällt, müssen alle für die Notfallwiederherstellung beschriebenen Schritte abgeschlossen werden.

Das folgende Diagramm veranschaulicht eine Bereitstellung für die Notfallwiederherstellung.



Das folgende Diagramm veranschaulicht den Ablauf einer Notfallwiederherstellung.



Die Wiederherstellung erfolgt mit den folgenden Schritten:

- 1 Ändern des DNS-Eintrags, sodass der NSX Manager-Cluster unterschiedliche IP-Adressen hat.
- 2 Wiederherstellen des NSX Manager-Clusters aus einer Sicherung.
- 3 Verbinden der Transportknoten mit dem neuen NSX Manager-Cluster.
- 4 Übertragen von Tier-1-Gateways aus NSX Edge-Clustern an der primären Site auf NSX Edge-Cluster an der sekundären Site.
- 5 Wiederherstellung der VMs.

## Voraussetzungen für Bereitstellungen für mehrere Sites

### Site-übergreifende Kommunikation

- Die Bandbreite muss mindestens 1 GBit/s betragen und die Latenz (RTT) muss kleiner als 150 ms sein.
- Die MTU muss mindestens 1600 betragen. 9000 wird empfohlen.

## NSX Manager-Konfiguration

- Automatische Sicherung, wenn Änderungen der NSX-T Data Center-Konfiguration aktiviert werden müssen.
- NSX Manager muss eingerichtet werden, um FQDN verwenden zu können.

## Wiederherstellung der Datenebene

- Derselbe Internetanbieter muss verwendet werden, wenn öffentliche IP-Adressen über Dienste wie NAT oder den Load Balancer verfügbar gemacht werden.

## Cloud-Management-System

- Das Cloud-Management-System (CMS) muss ein NSX-T Data Center-Plug-In unterstützen. In dieser Version erfüllen VMware Integrated OpenStack (VIO) und vRealize Automation (vRA) diese Anforderung.

## Einschränkungen

- Keine lokalen Ausgangsfunktionen. Der gesamte Nord-Süd-Datenverkehr muss innerhalb derselben Site stattfinden.
- Die Orchestrierung der Notfallwiederherstellungsberechnung muss NSX-T Data Center unterstützen.

## Konfigurieren von Appliances

Einige Aufgaben der Systemkonfiguration müssen mithilfe der Befehlszeile oder der API durchgeführt werden.

Vollständige Informationen zur Befehlszeilenschnittstelle finden Sie in der *Befehlszeilenschnittstellen-Referenz zu NSX-T Data Center*. Vollständige Erläuterungen zur API-Schnittstelle erhalten Sie im *API-Handbuch zu NSX-T Data Center*.

**Tabelle 21-2. Befehle und API-Anforderungen für die Systemkonfiguration.**

Aufgabe	Befehlszeile (NSX Manager und NSX Edge)	API-Anforderung (nur NSX Manager)
Systemzeitzone festlegen	set timezone <timezone>	PUT https://<nsx-mgr>/api/v1/node
NTP-Server festlegen	set ntp-server <ntp-server>	PUT https://<nsx-mgr>/api/v1/node/services/ntp
DNS-Server festlegen	set name-servers <dns-server>	PUT https://<nsx-mgr>/api/v1/node/network/name-servers
DNS-Suchdomäne festlegen	set search-domains <domain>	PUT https://<nsx-mgr>/api/v1/node/network/search-domains



## Hinzufügen eines Lizenzschlüssels und Generieren eines Lizenznutzungsberichts

Sie können Lizenzschlüssel hinzufügen und einen Lizenznutzungsbericht generieren. Der Nutzungsbericht ist eine Datei im CSV-Format.

Die folgenden Typen von Nicht-Evaluierungslizenzen für NSX-T Data Center sind verfügbar:

- Standard
- Professional
- Erweitert
- Enterprise Plus

Bei der Installation von NSX Manager wird eine vorinstallierte Evaluierungslizenz aktiviert, die 60 Tage gültig ist. Die Evaluierungslizenz ermöglicht die Verwendung sämtlicher Funktionen einer Enterprise-Lizenz. Sie können eine Evaluierungslizenz nicht installieren oder deren Zuweisung aufheben.

Sie haben die Möglichkeit, eine oder mehrere Nicht-Evaluierungslizenzen zu installieren. Für jeden Typ lässt sich aber immer nur ein Schlüssel installieren. Wenn Sie eine Standard-, Erweiterte oder Enterprise-Lizenz installieren, ist die Evaluierungslizenz nicht mehr verfügbar. Sie können auch die Zuweisung von Nicht-Evaluierungslizenzen aufheben. Wenn Sie die Zuweisung aller Nicht-Evaluierungslizenzen aufheben, wird die Evaluierungslizenz wiederhergestellt.

Wenn Sie über mehrere Schlüssel des gleichen Lizenztyps verfügen und diese kombinieren möchten, müssen Sie zu <https://my.vmware.com> wechseln und dafür die Funktion Schlüssel kombinieren anwenden. In der Benutzeroberfläche von NSX Manager ist diese Funktion nicht verfügbar.

### 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 > Lizenzen > Hinzufügen** aus.
- 3 Geben Sie einen Lizenzschlüssel ein.
- 4 Um einen Lizenznutzungsbericht zu generieren, wählen Sie **Exportieren > Lizenznutzungsbericht**.

Der CSV-Bericht listet die Nutzungsnummern für VM, CPU, eindeutige gleichzeitige Benutzer und vCPU für folgenden Funktionen auf:

- Switching und Routing
- NSX Edge-Lastausgleich
- VPN
- DFW

- Kontextsensitive Mikrosegmentierung – Anwendungsidentifizierung
- Kontextsensitive Mikrosegmentierung – Identitäts-Firewall für Remotedesktop-Sitzungshost
- Service Insertion
- Identitätsbasierte Firewall
- Erweiterte Guest Introspection

## Einrichten von Zertifikaten

Sie können Zertifikate importieren, eine Zertifikatssignieranforderung (Certificate Signing Request, CSR) erstellen, selbstsignierte Zertifikate generieren und eine Zertifikatswiderrufsliste (certificate Revocation List, CRL) importieren.

Nach der Installation von NSX-T Data Center verfügen die Manager-Knoten und der Cluster über selbstsignierte Zertifikate. Um die Sicherheit zu verbessern, wird dringend empfohlen, die selbstsignierten Zertifikate durch von einer Zertifizierungsstelle signierte Zertifikate zu ersetzen.

## Importieren eines Zertifikats

Sie können ein Zertifikat mit einem privaten Schlüssel importieren, um das selbstsignierte Standardzertifikat nach der Aktivierung zu ersetzen.

Beachten Sie, dass nur RSA-basierte Zertifikate unterstützt werden.

### Voraussetzungen

Stellen Sie sicher, dass ein Zertifikat verfügbar ist.

### 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 > Zertifikate**.
- 3 Wählen Sie **Importieren > Zertifikat importieren** aus, und geben Sie die Zertifikatdetails ein.

Option	Beschreibung
<b>Name</b>	Weisen Sie dem Zertifikat einen Namen zu.
<b>Zertifikatsinhalte</b>	Wechseln Sie in das Verzeichnis der Zertifikatdatei auf Ihrem Computer und fügen Sie die Datei hinzu. Das Zertifikat darf nicht verschlüsselt sein. Wenn es sich um ein von einer Zertifizierungsstelle signiertes Zertifikat handelt, stellen Sie sicher, dass die gesamte Kette in dieser Reihenfolge enthalten ist: Zertifikat – Zwischenzertifikat – Stamm.
<b>Privater Schlüssel</b>	Wechseln Sie in das Verzeichnis der Datei für den privaten Schlüssel auf Ihrem Computer und fügen Sie die Datei hinzu.

Option	Beschreibung
<b>Passphrase</b>	Fügen Sie eine Passphrase für dieses Zertifikat hinzu, wenn es verschlüsselt ist. In dieser Version wird dieses Feld nicht verwendet, da das verschlüsselte Zertifikat nicht unterstützt wird.
<b>Beschreibung</b>	Geben Sie eine Beschreibung des Inhalts dieses Zertifikats ein.
<b>Dienstzertifikat</b>	Wählen Sie <b>Ja</b> , um dieses Zertifikat für Dienste (z. B. den Load Balancer) und VPN zu verwenden. Legen Sie <b>Nein</b> fest, wenn dieses Zertifikat für die NSX Manager-Knoten gilt.

- 4 Klicken Sie auf **Import**.

## Erstellen einer Datei für die Zertifikatsignieranforderung

Bei der Zertifikatsignieranforderung (CSR, Certificate Signing Request) handelt es sich um einen verschlüsselten Text mit spezifischen Informationen wie Organisationsname, allgemeiner Name, Ort und Land/Region. Sie senden die CSR-Datei an eine Zertifizierungsstelle (CA, Certificate Authority) für ein Zertifikat der digitalen Identität.

### Voraussetzungen

- Stellen Sie die Informationen zusammen, die in die CSR-Datei eingetragen werden müssen. Sie benötigen den vollqualifizierten Domännennamen (FQDN) des Servers, die organisatorische Einheit (OU), die Stadt, das Bundesland und das Land/die Region.
- Stellen Sie sicher, dass die Paare für den öffentlichen und privaten Schlüssel verfügbar sind.

### 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 > Zertifikate**.
- 3 Klicken Sie auf die Registerkarte **CSRs**.
- 4 Klicken Sie auf **CSR generieren**.
- 5 Vervollständigen Sie die Details für die CSR-Datei.

Option	Beschreibung
<b>Name</b>	Weisen Sie Ihrem Zertifikat einen Namen zu.
<b>Allgemeiner Name</b>	Geben Sie den vollqualifizierten Domännennamen (FQDN) Ihres Servers ein. Beispiel: test.vmware.de.
<b>Name der Organisation</b>	Geben Sie Ihren Organisationsnamen mit den erforderlichen Suffixen ein. Beispiel: VMware Global Inc.
<b>Organisationseinheit</b>	Geben Sie die Abteilung innerhalb Ihrer Organisation ein, die dieses Zertifikat verwaltet. Beispiel: IT-Abteilung.

Option	Beschreibung
<b>Ort</b>	Geben Sie die Stadt ein, in der Ihre Organisation ihren Standort hat. Beispiel: Unterschleißheim.
<b>Bundesland</b>	Geben Sie das Bundesland ein, in dem Ihre Organisation ihren Standort hat. Beispiel: Bayern.
<b>Land/Region</b>	Geben Sie das Land/die Region ein, in dem/der Ihre Organisation ihren Standort hat. Beispiel: Deutschland.
<b>Meldungsalgorithmus</b>	Legen Sie den Verschlüsselungsalgorithmus für Ihr Zertifikat fest. RSA-Verschlüsselung – wird für digitale Signaturen und für die Verschlüsselung der Meldung verwendet. Deshalb ist diese Methode beim Erstellen eines verschlüsselten Token langsamer, aber bei der Analyse und Validierung dieses Token schneller als die DSA-Methode. Diese Verschlüsselung ist langsamer bei der Entschlüsselung und schneller bei der Verschlüsselung. DSA-Verschlüsselung – wird für digitale Signaturen verwendet. Deshalb ist diese Methode beim Erstellen eines verschlüsselten Token schneller, aber bei der Analyse und Validierung dieses Token langsamer als die RSA-Methode. Diese Verschlüsselung ist schneller bei der Entschlüsselung und langsamer bei der Verschlüsselung.
<b>Schlüsselgröße</b>	Legen Sie die Schlüsselgröße des Verschlüsselungsalgorithmus in Bits fest. Der Standardwert (2048) ist ausreichend, solange Sie keine spezielle andere Schlüsselgröße benötigen. Viele Zertifizierungsstellen verlangen einen Mindestwert von 2048. Je größer der Schlüssel, desto höher ist die Sicherheit, desto mehr wird aber auch die Leistung reduziert.
<b>Beschreibung</b>	Geben Sie Informationen ein, mit denen sich dieses Zertifikat zu einem späteren Zeitpunkt einfach identifizieren lässt.

## 6 Klicken Sie auf **Generieren**.

Eine benutzerdefinierte Zertifikatsignieranforderung (CSR) wird als Link angezeigt.

## 7 Wählen Sie die CSR aus und klicken Sie auf **Aktionen**.

## 8 Wählen Sie **CSR-PEM herunterladen** im Dropdown-Menü aus.

Sie können die CSR-PEM-Datei für Ihr Archiv und für die Einreichung bei der Zertifizierungsstelle (CA, Certificate Authority) speichern.

## 9 Mit dem Inhalt der CSR-Datei lässt sich eine Zertifikatanforderung an die Zertifizierungsstelle in Übereinstimmung mit dem CA-Registrierungsvorgang weiterleiten.

## Ergebnisse

Die CA erstellt ein Serverzertifikat auf der Basis der Informationen in der CSR-Datei, signiert dieses mit ihrem privaten Schlüssel und sendet es Ihnen zu. Die CA sendet Ihnen auch ein Stammzertifizierungsstellenzertifikat zu.

## Importieren eines CA-Zertifikats

Sie können ein signiertes CA-Zertifikat importieren. Nach dem Import und der Aktivierung werden andere von dieser CA signierte Zertifikate von NSX-T Data Center als vertrauenswürdig eingestuft.

Beachten Sie, dass nur RSA-basierte Zertifikate unterstützt werden.

### Voraussetzungen

Stellen Sie sicher, dass ein CA-Zertifikat verfügbar ist.

### 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 > Zertifikate**.
- 3 Wählen Sie **Importieren > CA-Zertifikat importieren** aus, und geben Sie die Zertifikatdetails ein.

Option	Beschreibung
<b>Name</b>	Weisen Sie dem CA-Zertifikat einen Namen zu.
<b>Zertifikatsinhalte</b>	Wechseln Sie in das Verzeichnis der CA-Zertifikat-Datei auf Ihrem Computer und fügen Sie die Datei hinzu.
<b>Beschreibung</b>	Geben Sie eine zusammenfassende Beschreibung ein, was in diesem CA-Zertifikat enthalten ist.
<b>Dienstzertifikat</b>	Wählen Sie <b>Ja</b> , um dieses Zertifikat für Dienste (z. B. den Load Balancer) und VPN zu verwenden. Legen Sie <b>Nein</b> fest, wenn dieses Zertifikat für die NSX Manager-Knoten gilt.

- 4 Klicken Sie auf **Import**.

## Erstellen eines selbstsignierten Zertifikats

Sie können ein selbstsigniertes Zertifikat erstellen. Die Verwendung eines selbstsignierten Zertifikats ist jedoch weniger sicher als die Verwendung eines vertrauenswürdigen Zertifikats.

Wenn Sie ein selbstsigniertes Zertifikat verwenden, erhält der Clientbenutzer eine Warnmeldung wie z. B. Ungültiges Sicherheitszertifikat. Der Clientbenutzer muss dann das selbstsignierte Zertifikat akzeptieren, bevor er eine Verbindung mit dem Server herstellen kann. Wenn Benutzer damit selbst entscheiden können, ob sie dieses Zertifikat verwenden, ist die Sicherheit gegenüber anderen Authentifizierungsmethoden eingeschränkt.

### Voraussetzungen

Stellen Sie sicher, dass eine CSR verfügbar ist. Siehe [Erstellen einer Datei für die Zertifikatsignieranforderung](#).

## 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 > Zertifikate**.
- 3 Klicken Sie auf die Registerkarte **CSRs**.
- 4 Wählen Sie eine CSR aus.
- 5 Wählen Sie **Aktionen > Selbstsigniertes Zertifikat für CSR** aus.
- 6 Geben Sie die Anzahl der Tage ein, die das selbstsignierte Zertifikat gültig ist.  
Die Standardeinstellung ist 10 Jahre.
- 7 Klicken Sie auf **Hinzufügen**.

## Ergebnisse

Das selbstsignierte Zertifikat wird auf der Registerkarte **Zertifikate** angezeigt.

## Ersetzen des Zertifikats für einen NSX Manager-Knoten oder eine virtuelle NSX Manager-Cluster-IP

Sie können das Zertifikat für einen Manager-Knoten oder die virtuelle IP-Adresse (VIP) des Manager-Clusters durch einen API-Aufruf ersetzen.

Nach der Installation von NSX-T Data Center verfügen die Manager-Knoten und der Cluster über selbstsignierte Zertifikate. Um die Sicherheit zu verbessern, wird dringend empfohlen, die selbstsignierten Zertifikate durch von einer Zertifizierungsstelle signierte Zertifikate zu ersetzen und für jeden Knoten ein eigenes Zertifikat zu verwenden.

In Version 2.4 kann das Ersetzen eines vorhandenen Zertifikats durch ein von einer Zertifizierungsstelle signiertes Zertifikat fehlschlagen. Dieses Problem wurde in Version 2.4.1 behoben.

## Voraussetzungen

Stellen Sie sicher, dass ein Zertifikat in NSX Manager verfügbar ist. Siehe [Importieren eines Zertifikats](#).

## 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 > Zertifikate**.
- 3 Klicken Sie in der Spalte „ID“ auf die ID des gewünschten Zertifikats und kopieren Sie die Zertifikat-ID aus dem Popup-Fenster.

Stellen Sie sicher, dass beim Importieren dieses Zertifikats die Option **Dienstzertifikat** auf **Nein** festgelegt wurde.

- 4 Um das Zertifikat eines Manager-Knotens zu ersetzen, verwenden Sie den POST `/api/v1/node/services/http?action=apply_certificate`-API-Aufruf. Beispiel:

```
POST https://<nsx-mgr>/api/v1/node/services/http?
action=apply_certificate&certificate_id=e61c7537-3090-4149-b2b6-19915c20504f
```

Weitere Informationen finden Sie in der *Referenz zur NSX-T Data Center-API*.

- 5 Um das Zertifikat der Manager-Cluster-VIP zu ersetzen, verwenden Sie den POST `/api/v1/cluster/api-certificate?action=set_cluster_certificate`-API-Aufruf. Beispiel:

```
POST https://<nsx-mgr>/api/v1/cluster/api-certificate?
action=set_cluster_certificate&certificate_id=d60c6a07-6e59-4873-8edb-339bf75711ac
```

Weitere Informationen finden Sie in der *Referenz zur NSX-T Data Center-API*. Dieser Schritt ist nicht erforderlich, wenn Sie keine VIP konfiguriert haben.

## Importieren einer Zertifikatswiderrufsliste

Eine Zertifikatswiderrufsliste (Certificate Revocation List, CRL) besteht aus einer Liste von Abonnenten und deren Zertifikatsstatus. Wenn ein potenzieller Benutzer versucht, auf einen Server zuzugreifen, wird anhand des CRL-Eintrags für den jeweiligen Benutzer der Zugriff verweigert.

Die Liste enthält die folgenden Elemente:

- widerrufen Zertifikate und den Grund für den Widerruf
- Datumsangaben für die Ausstellung der Zertifikate
- Aussteller der Zertifikate
- vorgeschlagenes Datum für die nächste Freigabe

### Voraussetzungen

Stellen Sie sicher, dass eine CRL verfügbar ist.

### 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 > Zertifikate**.
- 3 Klicken Sie auf die Registerkarte **CRLs**.

#### 4 Klicken Sie auf **Importieren** und fügen Sie die CRL-Details hinzu.

Option	Beschreibung
<b>Name</b>	Weisen Sie der CRL einen Namen zu.
<b>Zertifikatsinhalte</b>	<p>Kopieren Sie alle Elemente in der CRL und fügen Sie sie in diesem Abschnitt ein.</p> <p>Beispiel-CRL</p> <pre>-----BEGIN X509 CRL----- MIIBODCB4zANBgkqhkiG9w0BAQQFADBGMQswCQYDVQQGEwJBVTEMMAoGA1UECBM D UUxEMRkwFwYDVQQKEwBNaw5jb20gUHR5LiBMdGQuMQswCQYDVQQLEwJDUzEbMBk G A1UEAxMSU1NMZW5IGRlbW8gc2VydMVFw0wMTAxMTUxNjI2NTdaFw0wMTAyMTQ x NjI2NTdaMFIwEgIBARcNOTUxMDA5MjMzMjA1WjASAgEDFw05NTEyMDEwMTAwMD a MBMCAhI0Fw0wMTAxMTUxNjE5NDdaMBMCAhI1Fw0wMTAxMTUxNjIzNDZaMA0GCSq G SIb3DQEBAUAA0EAHPjQ3M93Q0j8Ufi+jZM7Y78TfAzG4jJn/ E6MYBPFVQFY0/Gp UZexfjSVo5CIyyS0tYscz8o07avwBxTiMpDEQg== -----END X509 CRL--</pre>
<b>Beschreibung</b>	Geben Sie eine Übersicht über den Inhalt dieser CRL ein.

#### 5 Klicken Sie auf **Import**.

##### Ergebnisse

Die importierte CRL wird als Link angezeigt.

## Konfigurieren von NSX Manager zum Abrufen einer Zertifikatswiderrufsliste

Mithilfe der API können Sie NSX Manager so konfigurieren, dass eine Zertifikatswiderrufsliste (Certificate Revocation List, CRL) abgerufen wird. Sie können dann die CRL überprüfen, indem Sie einen API-Aufruf an NSX Manager statt an die Zertifizierungsstelle vornehmen.

Diese Funktion bietet die folgenden Vorteile:

- Es ist effizienter, die CRL auf dem Server, also in NSX Manager, zwischenzuspeichern.
- Der Client muss keine ausgehende Verbindung zur Zertifizierungsstelle erstellen.

Die folgenden APIs sind im Zusammenhang mit Zertifikatsperrlisten verfügbar:

```
GET /api/v1/trust-management
GET /api/v1/trust-management/crl-distribution-points
POST /api/v1/trust-management/crl-distribution-points
DELETE /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>
GET /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>
PUT /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>
GET /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>/status
POST /api/v1/trust-management/crl-distribution-points/pem-file
```



Sie können CRL-Verteilungspunkte verwalten und die in NSX Manager gespeicherten CRLs abrufen. Weitere Informationen finden Sie in der *Referenz zur NSX-T Data Center-API*.

## Importieren eines Zertifikats für eine CSR

Sie können ein signiertes Zertifikat für eine CSR importieren.

Wenn Sie ein selbstsigniertes Zertifikat verwenden, erhält der Clientbenutzer eine Warnmeldung wie z. B. **Ungültiges Sicherheitszertifikat**. Der Clientbenutzer muss dann das selbstsignierte Zertifikat akzeptieren, bevor er eine Verbindung mit dem Server herstellen kann. Wenn Benutzer damit selbst entscheiden können, ob sie dieses Zertifikat verwenden, ist die Sicherheit gegenüber anderen Authentifizierungsmethoden eingeschränkt.

### Voraussetzungen

Stellen Sie sicher, dass eine CSR verfügbar ist. Siehe [Erstellen einer Datei für die Zertifikatsignieranforderung](#).

### 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 > Zertifikate**.
- 3 Klicken Sie auf die Registerkarte **CSRs**.
- 4 Wählen Sie eine CSR aus.
- 5 Wählen Sie **Aktionen > Zertifikat für CSR importieren** aus.
- 6 Wechseln Sie in das Verzeichnis der signierten Zertifikatdatei auf Ihrem Computer, und fügen Sie die Datei hinzu.
- 7 Klicken Sie auf **Hinzufügen**.

### Ergebnisse

Das selbstsignierte Zertifikat wird auf der Registerkarte **Zertifikate** angezeigt.

## Speichern von öffentlichen Zertifikaten und privaten Schlüsseln

Öffentliche Zertifikate und private Schlüssel werden auf den NSX Managern gespeichert. Wenn ein Load Balancer oder ein VPN-Dienst erstellt wird, der einen privaten Schlüssel erfordert, sendet NSX Manager eine Kopie des privaten Schlüssels an den Edge-Knoten, auf dem der Load Balancer oder der VPN-Dienst ausgeführt wird.

## Erfassen von Support-Paketen

Sie können Support-Pakete auf registrierten Clustern und Fabric-Knoten erfassen und die Pakete auf Ihren Computer herunterladen bzw. auf einen Dateiserver hochladen.

Wenn Sie die Pakete auf Ihren Computer herunterladen, erhalten Sie eine einzelne Archivdatei, die aus einer Manifestdatei und Support-Paketen für jeden Knoten besteht. Wenn Sie die Pakete auf einen Dateiserver hochladen, werden die Manifestdatei und die einzelnen Pakete gesondert hochgeladen.

---

**Hinweis zu NSX Cloud** Wenn Sie das Support-Paket für CSM erfassen möchten, melden Sie sich bei CSM an, navigieren Sie zu **System > Dienstprogramme > Support-Paket** und klicken Sie auf **Download**. Das Support-Paket für PCG ist bei NSX Manager unter Verwendung der folgenden Anleitung erhältlich. Die Support-Paket für PCG enthält außerdem Protokolle für alle Arbeitslast-VMs.

---

#### 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 > Support-Paket** aus.
- 3 Wählen Sie die Zielknoten aus.  
  
Bei den verfügbaren Knotentypen handelt es sich um **Verwaltungsknoten, Edges, Hosts** und **Public Cloud Gateways** (PCGs).
- 4 (Optional) Geben Sie den Protokollierungszeitraum in Tagen an, um Protokolle auszuschließen, die vor der festgelegten Anzahl an Tagen erstellt wurden.
- 5 (Optional) Schalten Sie den Switch um, der angibt, ob Core-Dateien und Überwachungsprotokolle einbezogen werden sollen.

---

**Hinweis** Core-Dateien und Überwachungsprotokolle können vertrauliche Informationen wie etwa Kennwörter oder Verschlüsselungsschlüssel enthalten.

---

- 6 (Optional) Aktivieren Sie das entsprechende Kontrollkästchen, um die Pakete auf einen Dateiserver hochzuladen.
- 7 Klicken Sie auf **Paketerfassung starten**, um mit der Erfassung der Support-Pakete zu beginnen.  
  
Je nach der Anzahl der Protokolldateien kann die Erfassung für jeden Knoten mehrere Minuten dauern.
- 8 Überwachen Sie den Status des Erfassungsvorgangs.  
  
Auf der Registerkarte „Status“ wird der Fortschritt beim Sammeln von Support-Paketen angezeigt.
- 9 Wenn die Option für das Senden des Pakets an einen Dateiserver nicht aktiviert ist, klicken Sie auf **Herunterladen**, um das Paket herunterzuladen.

## Protokollmeldungen

Protokollmeldungen aller NSX-T Data Center-Komponenten einschließlich den auf ESXi-Hosts ausgeführten entsprechen dem Syslog-Format gemäß RFC 5424. Protokollmeldungen von KVM-Hosts sind im RFC-3164-Format. Die Protokolldateien befinden sich im Verzeichnis `/var/log`.

Auf NSX-T Data Center-Appliances können Sie den folgenden NSX-T Data Center-CLI-Befehl zum Anzeigen der Protokolle ausführen:

```
get log-file <auth.log | http.log | kern.log | manager.log | node-mgmt.log | syslog> [follow]
```

Auf Hypervisoren können Sie Linux-Befehle wie z. B. `tail`, `grep` oder `more` verwenden, um die Protokolle anzuzeigen. Diese Befehle können Sie auch auf NSX-T Data Center--Appliances verwenden.

Weitere Informationen zu RFC 5424 finden Sie unter <https://tools.ietf.org/html/rfc5424>. Weitere Informationen zu RFC 3164 finden Sie unter <https://tools.ietf.org/html/rfc3164>.

RFC 5424 legt für Protokollmeldungen das folgende Format fest:

```
<facility * 8 + severity> version UTC-TZ hostname APP-NAME procid MSGID [structured-data] msg
```

Beispiel für eine Protokollmeldung:

```
<187>1 2016-03-15T22:53:00.114Z nsx-manager NSX - SYSTEM [nsx@6876 comp="nsx-manager"
errorCode="MP4039" subcomp="manager"] Connection verification failed for broker '10.160.108.196'.
Marking broker unhealthy.
```

Jede Nachricht enthält Komponentendetails (`comp`) und Unterkomponentendetails (`subcomp`), die es erleichtern, die Quelle der Nachricht zu identifizieren.

NSX-T Data Center erzeugt Protokolle mit Facility `local6` mit einem numerischen Wert von 22. Jeder API-Aufruf erzeugt ein Überwachungsprotokoll, das `audit="true"` im Feld „Strukturierte Daten“ enthält.

Ein Eintrag im Überwachungsprotokoll, der einem API-Aufruf zugeordnet ist, enthält die folgende Informationen:

- Den Parameter `entId` mit einer Element-ID zur Identifizierung des Objekts der-API.
- Den Parameter `req-id` mit einer Anforderungs-ID zur Identifizierung eines bestimmten API-Aufrufs.
- Den Parameter `ereqId` mit einer ID, die auf eine externe Anforderung verweist, wenn der API-Aufruf den Header `X-NSX-EREQID:<string>` enthält.
- Den Parameter `euser` der auf einen externen Benutzer verweist, wenn der API-Aufruf den Header `X-NSX-EUSER:<string>` enthält.

RFC 5424 definiert die folgenden Ebenen für den Schweregrad:

Schweregrad	Beschreibung
0	Notfall: Das System steht nicht zur Verfügung
1	Ernste Warnung: Es muss sofort reagiert werden
2	Kritisch: Kritische Bedingungen
3	Fehler: Fehlerbedingungen
4	Warnung: Warnbedingungen
5	Hinweis: Normale, aber signifikante Bedingung
6	Information: Informationsmeldungen
7	Debug: Meldungen auf Debug-Ebene

Alle Protokolle mit dem Schweregrad „Notfall“, „Ernste Warnung“, „Kritisch“ und „Fehler“ enthalten einen eindeutigen Fehlercode im Abschnitt der strukturierten Daten der Protokollmeldung. Der Fehlercode besteht aus einer Zeichenfolge und einer Dezimalzahl. Die Zeichenfolge steht für ein bestimmtes Modul.

Das MSGID-Feld identifiziert den Meldungstyp. Eine Liste der Meldungs-IDs finden Sie unter [Protokollmeldungs-IDs](#).

## Konfigurieren der Remoteprotokollierung

Sie können NSX-T Data Center-Appliances und -Hypervisoren für das Senden von Meldungen zu einem Server für Remoteprotokollierung konfigurieren.

Remoteprotokollierung wird auf , NSX Manager, NSX Edge und Hypervisoren unterstützt. Sie müssen die Remoteprotokollierung auf jedem Knoten einzeln konfigurieren.

Auf einem KVM-Host konfiguriert das NSX-T Data Center-Installationspaket den rsyslog-Daemon automatisch, indem es entsprechende Konfigurationsdateien im Verzeichnis `/etc/rsyslog.d` platziert.

### Voraussetzungen

- Konfigurieren Sie einen Protokollierungsserver für den Empfang der Protokolle.

## Verfahren

### 1 So konfigurieren Sie die Remoteprotokollierung auf einer NSX-T Data Center-Appliance:

- a Führen Sie den folgenden Befehl aus, um einen Protokollserver zu konfigurieren und festzulegen, welche Arten von Meldungen an den Protokollserver gesendet werden sollen. Mehrere facility- oder messageid-Parameter können, durch Kommas ohne Leerzeichen getrennt, als Liste angegeben werden.

```
set logging-server <hostname-or-ip-address[:port]> proto <proto> level <level> [facility <facility>] [messageid <messageid>] [certificate <filename>] [structured-data <structured-data>]
```

Weitere Informationen zu diesem Befehl finden Sie in der *Referenz zur NSX-T-CLI*. Sie haben die Möglichkeit, den Befehl mehrmals zum Hinzufügen mehrerer Konfigurationen für Protokollierungsserver auszuführen. Beispiel:

```
nsx> set logging-server 192.168.110.60 proto udp level info facility syslog messageid SYSTEM,FABRIC
nsx> set logging-server 192.168.110.60 proto udp level info facility auth,user
```

- b Sie können die Protokollierungskonfiguration mit dem Befehl `get logging-server` anzeigen. Beispiel:

```
nsx> get logging-servers
192.168.110.60 proto udp level info facility syslog messageid SYSTEM,FABRIC
192.168.110.60 proto udp level info facility auth,user
```

### 2 So konfigurieren Sie die Remoteprotokollierung auf einem ESXi-Host:

- a Führen Sie die folgenden Befehle aus, um Syslog zu konfigurieren und eine Testnachricht zu senden:

```
esxcli network firewall ruleset set -r syslog -e true
esxcli system syslog config set --loghost=udp://<log server IP>:<port>
esxcli system syslog reload
esxcli system syslog mark -s "This is a test message"
```

- b Sie können die Konfiguration durch Ausführen des folgenden Befehls anzeigen:

```
esxcli system syslog config get
```

**3** So konfigurieren Sie die Remoteprotokollierung auf einem KVM-Host:

- a Bearbeiten Sie die Datei `/etc/rsyslog.d/10-vmware-remote-logging.conf`, um sie an Ihre Umgebung anzupassen.
- b Fügen Sie der Datei die folgende Zeile hinzu:

```
*.* @<ip>:514;RFC5424fmt
```

- c Führen Sie den folgenden Befehl aus:

```
service rsyslog restart
```

## Protokollmeldungs-IDs

In einer Protokollmeldung identifiziert das Meldungs-ID-Feld den Meldungstyp. Sie können den Parameter `messageid` im Befehl `set logging-server` verwenden, um zu filtern, welche Protokollmeldungen an den Protokollierungsserver gesendet werden.

**Tabelle 21-3. Protokollmeldungs-IDs**

Meldungs-ID	Beispiele
FABRIC	Hostknoten Hostvorbereitung Edge-Knoten Transportzone Transportknoten Uplink-Profil Clusterprofil Edge-Cluster Bridge-Cluster und -Endpoints
SWITCHING	Logischer Switch Logischer Switch Port Switching-Profil Funktionen der Switch-Sicherheit
ROUTING	Logischer Router Logische Routerports Statisches Routing Dynamisches Routing NAT
FIREWALL	Firewallregeln Firewallregelabschnitte
FIREWALL-PKTLOG	Protokolle der Firewallverbindung Protokolle des Firewallpakets

Tabelle 21-3. Protokollmeldungs-IDs (Fortsetzung)

Meldungs-ID	Beispiele
GROUPING	IP Sets MAC Sets NS-Gruppen NS-Dienste NS-Dienstgruppen VNI-Pool IP-Pool
DHCP	DHCP-Relay
SYSTEM	Appliance-Verwaltung (remote syslog, ntp, etc.) Clusterverwaltung Vertrauensverwaltung Lizenzierung Benutzer und Rollen Aufgabenverwaltung Installieren Upgrade (NSX Manager, NSX Edge und Upgrades von Hostpaketen) Umsetzung Tags
MONITORING	SNMP Portverbindung Traceflow
-	Alle anderen Protokollmeldungen

## Programm zur Verbesserung der Benutzerfreundlichkeit

NSX-T Data Center nimmt am VMware-Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) teil.

Einzelheiten zu den im Rahmen des CEIP erfassten Daten sowie zum Zweck der Verwendung durch VMware können im Trust & Assurance Center unter <https://www.vmware.com/solutions/trustvmware/ceip.html> eingesehen werden.

Informationen zur Teilnahme am CEIP für NSX-T Data Center bzw. zum Abmelden davon und zum Bearbeiten von Programmeinstellungen finden Sie unter [Bearbeiten der CEIP-Konfiguration \(Einstellungen bzgl. der Teilnahme am „Programm zur Verbesserung der Benutzerfreundlichkeit“\)](#).

## Bearbeiten der CEIP-Konfiguration (Einstellungen bzgl. der Teilnahme am „Programm zur Verbesserung der Benutzerfreundlichkeit“)

Beim Installieren oder Aktualisieren von NSX Manager haben Sie die Möglichkeit, sich dem CEIP anzuschließen und die zugehörigen Datenerfassungseinstellungen zu konfigurieren.

Sie können auch die vorhandene CEIP-Konfiguration bearbeiten, um dem Programm beizutreten oder es zu verlassen, die Erfassungshäufigkeit und die Tage festlegen, an denen die Informationen gesammelt werden, sowie den Proxyserver konfigurieren.

### Voraussetzungen

- Stellen Sie sicher, dass der NSX Manager verbunden ist und mit Ihrem Hypervisor synchronisiert werden kann.
- Stellen Sie sicher, dass NSX-T Data Center mit einem öffentlichen Netzwerk für das Hochladen von Daten verbunden ist.

### 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 > Programm** aus.
- 3 Klicken Sie im Abschnitt „Programm zur Verbesserung der Benutzerfreundlichkeit“ auf **Bearbeiten**.
- 4 Aktivieren Sie im Dialogfeld „Programm zur Verbesserung der Benutzerfreundlichkeit bearbeiten“ das Kontrollkästchen **Am Programm zur Verbesserung der Benutzerfreundlichkeit von VMware teilnehmen**.
- 5 Verwenden Sie die Umschaltfläche **Zeitplan**, um die Datenerfassung zu aktivieren oder zu deaktivieren.  
Der Zeitplan ist standardmäßig aktiviert.
- 6 (Optional) Konfigurieren Sie die Einstellungen zur Datenerfassung und zur Wiederholung der Uploads.
- 7 Klicken Sie auf **Speichern**.

## Hinzufügen von Tags zu einem Objekt

Sie können Objekten Tags hinzufügen, um die Suche zu erleichtern. Beim Angeben eines Tags können Sie auch einen Geltungsbereich festlegen.

---

**NSX Cloud-Hinweis** Wenn Sie NSX Cloud verwenden, finden Sie unter [Verwendung von NSX-T Data Center-Funktionen mit der Public Cloud](#) eine Liste der automatisch generierten logischen Einheiten, unterstützten Funktionen und Konfigurationen, die für NSX Cloud erforderlich sind.

---



## Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Bearbeiten Sie ein Objekt.  
Rufen Sie beispielsweise die Registerkarte **Segmente** auf und bearbeiten Sie ein Segment.
- 3 Wechseln Sie zum Feld **Tags** und fügen Sie Tags hinzu.  
Jedes Tag hat einen Tag-Wert, der erforderlich ist und einen Wert für den Geltungsbereich, der optional ist. Ein Objekt kann maximal 30 Tags aufweisen. Tags dürfen höchstens 256 Zeichen enthalten. Bereiche dürfen höchstens 128 Zeichen enthalten.
- 4 Klicken Sie auf **Speichern**.

## Suchen nach dem SSH-Fingerabdruck eines Remote-Servers

Für einige API-Anforderungen, bei denen Dateien zu oder von einem Remote-Server kopiert werden, müssen Sie den SSH-Fingerabdruck für den Remote-Server im Anforderungstext bereitstellen. Der SSH-Fingerabdruck wird aus einem Hostschlüssel auf dem Remote-Server abgeleitet.

Um eine Verbindung über SSH herzustellen, müssen NSX Manager und der Remote-Server über den gleichen Hostschlüsseltyp verfügen. Wenn sie mehrere Hostschlüsseltypen gemeinsam haben, wird derjenige verwendet, der entsprechend der Konfiguration von HostKeyAlgorithm in NSX Manager bevorzugt wird.

Mithilfe des Fingerabdrucks für einen Remote-Server lässt sich sicherstellen, dass Sie mit dem korrekten Server verbunden und vor „Man-in-the-Middle“-Angriffen geschützt sind. Den SSH-Fingerabdruck des Servers erhalten Sie beim Administrator des Remote-Servers. Alternativ können Sie auch eine Verbindung mit dem Remote-Server herstellen, um den Fingerabdruck zu suchen. Dabei ist die Herstellung einer Serververbindung über eine Konsole sicherer als über das Netzwerk.

In der folgende Tabelle wird die Unterstützung von NSX Manager angefangen von der bevorzugteren bis hin zur weniger bevorzugten Variante aufgelistet.

**Tabelle 21-4. NSX Manager-Hostschlüssel in der Reihenfolge der bevorzugten Verwendung**

Von NSX Manager unterstützte Host-Schlüsseltypen	Standardspeicherort des Schlüssels
ECDSA (256 Bit)	/etc/ssh/ssh_host_ecdsa_key.pub
ED25519	/etc/ssh/ssh_host_ed25519_key.pub

## Verfahren

- 1 Melden Sie sich beim Remote-Server als Root-Benutzer an.  
Die Anmeldung mithilfe einer Konsole ist sicherer als über das Netzwerk.

- 2 Zeigen Sie die Dateien für den öffentlichen Schlüssel im Verzeichnis `/etc/ssh` an.

```
$ ls -al /etc/ssh/*pub
-rw-r--r-- 1 root root 601 Apr  8 18:10 ssh_host_dsa_key.pub
-rw-r--r-- 1 root root 93 Apr  8 18:10 ssh_host_ed25519_key.pub
-rw-r--r-- 1 root root 393 Apr  8 18:10 ssh_host_rsa_key.pub
```

- 3 Vergleichen Sie die verfügbaren Schlüssel mit der NSX Manager-Unterstützung.

In diesem Beispiel ist ED25519 der einzig zulässige Schlüssel.

- 4 Rufen Sie den Fingerabdruck des Schlüssels ab.

```
# awk '{print $2}' /etc/ssh/ssh_host_ed25519_key.pub | base64 -d | sha256sum -b | sed 's/ .*$//'
| xxd -r -p | base64 | sed 's/.//44g' | awk '{print "SHA256:"$1}'
SHA256:KemgftCfsd/hn7EEflhJ4m1698rRhMmNN2IW8y9iq2A
```

## Anzeigen von Daten über Anwendungen, die auf virtuellen Maschinen ausgeführt werden

Sie können Informationen über Anwendungen anzeigen, die auf virtuellen Maschinen ausgeführt werden, die Mitglieder einer NSGroup sind. Dies ist eine tech preview-Funktion.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie im Navigationsbereich die Option **Bestand > Gruppen** aus.
- 3 Klicken Sie auf den Namen einer NSGroup.
- 4 Klicken Sie auf die Registerkarte **Anwendungen**.
- 5 Klicken Sie auf **ANWENDUNGSDATEN ERFASSEN**.

Dieser Vorgang kann einige Minuten in Anspruch nehmen. Wenn der Vorgang abgeschlossen ist, werden die folgenden Informationen angezeigt:

- Die Gesamtzahl Prozesse.
  - Verschiedene Ebenen repräsentierende Kreise, z. B. Web-, Datenbank- und Anwendungsebene. Zudem wird die Anzahl Prozesse in den einzelnen Ebenen angezeigt.
- 6 Klicken Sie auf einen Kreis, um weitere Informationen über die Prozesse in der jeweiligen Ebene anzuzeigen.

# Verwenden von NSX Cloud

# 22

NSX Cloud ermöglicht es Ihnen, Ihre Public Cloud-Bestandsliste unter Verwendung von NSX-T Data Center zu verwalten und zu sichern.

Weitere Informationen finden Sie unter [Installieren von NSX Cloud-Komponenten](#) im *Installationshandbuch für NSX-T Data Center* für den Workflow für die NSX Cloud-Bereitstellung.

Siehe auch: [Public Cloud](#).

Dieses Kapitel enthält die folgenden Themen:

- [Der Cloud Service Manager](#)
- [Verwalten der Quarantäne-Richtlinie](#)
- [Überblick über Onboarding und Verwaltung von Workload-VMs](#)
- [Onboarden von Workload-VMs](#)
- [Verwalten von Workload-VMs](#)
- [Verwenden von erweiterten NSX Cloud-Funktionen](#)
- [FAQ](#)

## Der Cloud Service Manager

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

Die CSM-Schnittstelle ist in folgende Kategorien unterteilt:

- **Suche:** Sie können das Textfeld „Suchen“ verwenden, um Public-Cloud-Konten oder zugehörige Konstrukte zu finden.
- **Clouds:** Ihr Public-Cloud-Bestand wird über die Abschnitte unter dieser Kategorie verwaltet.
- **System:** Über diese Kategorie können Sie auf **Einstellungen**, **Dienstprogramme** und **Benutzer** für Cloud Service Manager zugreifen.

Um Public Cloud-Vorgänge durchzuführen, wechseln Sie zum Unterabschnitt **Clouds** von CSM.

Navigieren Sie zum Unterabschnitt **System**, um systembasierte Operationen wie z. B. Sicherung, Wiederherstellung, Upgrade und Benutzerverwaltung durchzuführen.

## Clouds

Dies sind die Abschnitte unter **Clouds**:

### Clouds > (Übersicht)

Sie können auf Ihr Public Cloud-Konto zugreifen, indem Sie auf **Clouds** klicken.

**Übersicht:** Jede Kachel auf dieser Seite repräsentiert Ihr Public Cloud-Konto mit der Anzahl der Konten, Regionen, VPCs bzw. VNets und Instanzen (Arbeitslast-VMs), die es einschließt.

Sie können die folgenden Aufgaben durchführen:

Public Cloud-Konto oder -Abonnement hinzufügen	Sie können ein oder mehrere Public Cloud-Konten oder -Abonnements hinzufügen. Dies ermöglicht es Ihnen, Ihren Public Cloud-Bestand in CSM einzusehen, und gibt die Anzahl der VMs, die von NSX-T Data Center verwaltet werden, und ihren Zustand wieder.  Detaillierte Anweisungen finden Sie unter <b>Ihr Public Cloud-Konto hinzufügen</b> im <i>Installationshandbuch für NSX-T Data Center</i> .
NSX Public Cloud Gateway bereitstellen oder dessen Bereitstellung aufheben	Sie können ein oder (bei Hochverfügbarkeit) zwei PCG(s) bereitstellen. Sie können die Bereitstellung eines PCG auf CSM auch aufheben.  Detaillierte Anweisungen finden Sie unter <b>PCG bereitstellen</b> oder <b>Bereitstellung von PCG aufheben</b> im <i>Installationshandbuch für NSX-T Data Center</i> .
Quarantäne-Richtlinie aktivieren oder deaktivieren	Sie können die Quarantäne-Richtlinie aktivieren oder deaktivieren. Weitere Informationen finden Sie unter <a href="#">Verwalten der Quarantäne-Richtlinie</a> .
Zwischen Tabellen- und Kartenansicht umschalten	Die Karten zeigen eine Übersicht über Ihren Bestand an. Die Tabelle zeigt weitere Details. Klicken Sie auf die Symbole, um zwischen den Anzeigearten zu wechseln.

CSM bietet eine ganzheitliche Ansicht aller Ihrer Public Cloud-Konten, die Sie mit NSX Cloud verbunden haben, indem Ihr Public Cloud-Bestand auf unterschiedliche Weise dargestellt wird:

- Sie können die Anzahl der Regionen anzeigen, in denen Sie tätig sind.
- Sie können die Anzahl der privaten Netzwerke pro Region anzeigen.
- Sie können die Anzahl der Workload-VMs pro privatem Netzwerk anzeigen.

Unter **Clouds** gibt es vier Registerkarten.

### Clouds > {Ihre Public Cloud} > Konten

Der Abschnitt „Konten“ von CSM enthält Informationen zu den Public Cloud-Konten, die Sie bereits hinzugefügt haben.

Jede Karte stellt ein Public Cloud-Konto des Cloud-Anbieters dar, den Sie unter „Clouds“ ausgewählt haben.

Von diesem Abschnitt aus können Sie die folgenden Aktionen ausführen:

- Konto hinzufügen

- Konto bearbeiten
- Konto löschen
- Konto neu synchronisieren

## Clouds > {Ihre Public Cloud} > Regionen

Der Abschnitt „Regionen“ zeigt die Bestandsliste für eine ausgewählte Region an.

Sie können die Regionen nach Ihrem Public Cloud-Konto filtern. Jede Region hat VPCs bzw. VNets sowie Instanzen. Wenn Sie PCGs bereitgestellt haben, werden diese hier als Gateways mit einem Indikator für die PCG-Integrität angezeigt.

## Clouds > {Ihre Public Cloud} > VPCs oder VNets

Der Abschnitt „VPCs“ bzw. „VNets“ zeigt Ihre Private-Cloud-Bestandsliste an.

Sie können die Bestandsliste nach Konto und Region filtern.

- Jede Karte steht für eine VPC oder ein VNet.
- In Transit-VPCs/-VNets können ein oder (bei HA) zwei PCGs bereitgestellt werden.
- Sie können Computing-VPCs/-VNets mit Transit-VPCs/-VNets verknüpfen.
- Sie können zu jeder VPC oder jedem VNet weitere Details anzeigen, indem Sie zur Rasteransicht wechseln.

---

**Hinweis** In der Rasteransicht werden drei Registerkarten angezeigt: **Übersicht**, **Instanzen** und **Segmente**.

- **Übersicht** listet die Optionen unter „Aktionen“ auf, wie im nächsten Schritt beschrieben.
  - **Instanzen** zeigt eine Liste der Instanzen in VPC/VNet an.
  - **Segmente** zeigt Overlay-Segmente in NSX-T an. Diese Funktion wird in der aktuellen Version von NSX Cloud nicht unterstützt. Kennzeichnen Sie Ihre Arbeitslast-VMs in AWS oder Microsoft Azure nicht mit Tags, die auf diesem Bildschirm angezeigt werden.
- 
- Durch Klicken auf **Aktionen** erhalten Sie Zugriff auf die folgenden Aktionen:
    - **Konfiguration bearbeiten** (nur verfügbar für Transit-VPCs/-VNets):
      - Quarantäne-Richtlinie aktivieren oder deaktivieren.
      - Proxy-Server-Auswahl ändern.
    - **Mit Transit-VPC/-VNet verknüpfen**: Diese Option ist nur für VPCs/VNets verfügbar, auf denen kein PCG bereitgestellt ist. Klicken Sie auf diese Option, um eine Transit-VPC oder ein Transit-VNet auszuwählen, zu dem eine Verknüpfung hergestellt werden soll.

- **NSX Cloud-Gateway bereitstellen:** Diese Option ist nur für VPCs/VNets verfügbar, auf denen kein PCG bereitgestellt ist. Klicken Sie auf diese Option, um mit der Bereitstellung des PCG auf dieser VPC oder diesem VNet zu beginnen und eine Transit- oder selbstverwaltete VPC bzw. ein Transit- oder selbstverwaltetes VNet zu erstellen. Ausführliche Anweisungen finden Sie unter **Bereitstellen oder Verknüpfen von NSX Public Cloud-Gateways** im *Installationshandbuch für NSX-T Data Center*.

## Clouds > {Ihre Public Cloud} > Instanzen

Der Abschnitt „Instanzen“ zeigt Details zu den Instanzen in Ihrem VPC oder VNet an.

Sie können die Bestandsliste der Instanzen nach Konto, Region und VPC bzw. VNet filtern.

Jede Karte repräsentiert eine Instanz (Arbeitslast-VM) und zeigt eine Übersicht zu dieser an.

Ausführlichere Informationen zu einer Instanz erhalten Sie, indem Sie auf die Karte klicken oder zur Rasteransicht wechseln.

---

**Hinweis** CSM zeigt den Wert für die Betriebssystemversion für NSX-verwaltete VMs an, jedoch ist der angezeigte Betriebssystemtyp für VMs, die nicht von NSX verwaltet werden, im Detail minimal, da er von den Cloud-Anbieter-APIs übernommen wird.

---

## System

Dies sind die Abschnitte unter **System**:

### System > Einstellungen

Diese Einstellungen werden zuerst konfiguriert, wenn Sie CSM installieren. Anschließend können Sie sie bearbeiten.

### 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](#).

#### (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.
<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.

## System > Dienstprogramme

Die folgenden Dienstprogramme stehen zur Verfügung.

### Sichern und Wiederherstellen

Folgen Sie für das Sichern und Wiederherstellen von CSM den gleichen Anweisungen wie für NSX Manager. Weitere Informationen finden Sie unter [Sichern und Wiederherstellen von NSX Manager](#).

### Support-Paket

Klicken Sie auf **Download**, um das Support-Paket für CSM abzurufen. Dies wird für die r-Fehlerbehebung verwendet. Weitere Informationen hierzu finden Sie im *Handbuch zur Fehlerbehebung von NSX-T Data Center*.



## System > Benutzer

Benutzer werden mithilfe der rollenbasierten Zugriffssteuerung (RBAC) verwaltet.

Weitere Informationen finden Sie unter [Verwalten von Benutzerkonten und der rollenbasierten Zugriffssteuerung](#).

## Verwalten der Quarantäne-Richtlinie

Informationen zum Aktivieren oder Deaktivieren von Quarantäne-Richtlinien und deren Auswirkungen auf Ihre Arbeitslast-VMs

NSX Cloud verwendet Public-Cloud-Sicherheitsgruppen zur Erkennung von Bedrohungen. Wenn beispielsweise bei aktivierter Quarantäne-Richtlinie der NSX-Agent auf einer verwalteten VM mit böswilliger Absicht gewaltsam gestoppt wird, wird die gefährdete VM mit der Sicherheitsgruppe *quarantine* (in Microsoft Azure) oder *default* (in AWS) unter Quarantäne gestellt.

### Allgemeine Empfehlung:

Beginnen Sie für **Brownfield**-Bereitstellungen mit *deaktiviert* (disabled): Quarantäne-Richtlinie ist standardmäßig deaktiviert. Wenn Sie in Ihrer Public Cloud-Umgebung bereits VMs eingerichtet haben, verwenden Sie den Modus „deaktiviert“ (disabled) für die Quarantäne-Richtlinie, bis Sie Ihre Workload-VMs integrieren. Dadurch wird sichergestellt, dass Ihre vorhandenen VMs nicht automatisch in Quarantäne verschoben werden.

Beginnen Sie mit *aktiviert* (enabled) für **Greenfield**-Bereitstellungen: Für Greenfield-Bereitstellungen wird empfohlen, dass Sie die Quarantäne-Richtlinie aktivieren, damit die Bedrohungserkennung für Ihre VMs von NSX Cloud verwaltet werden kann.

---

**Hinweis** Wenn die Quarantäne-Richtlinie aktiviert ist, wenden Sie die `vm_override_sg` auf Arbeitslast-VMs an, um diese einbinden zu können, und entfernen Sie dann diese Sicherheitsgruppe, nachdem sie von NSX Cloud verwaltet werden. Entsprechende Sicherheitsgruppen werden innerhalb von zwei Minuten auf die VMs angewendet.

---

## Quarantäne-Richtlinie aktivieren oder deaktivieren

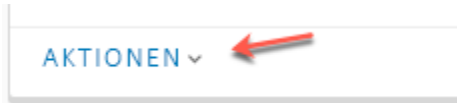
Beim Bereitstellen von PCG auf einer Transit-VPC bzw. einem Transit-VNet oder Verknüpfen einer Computing-VPC bzw. eines Computing-VNet mit einem Transit besteht die Möglichkeit, die Quarantäne-Richtlinie ein- oder auszuschalten. Führen Sie diese Schritte aus, um die Quarantäne-Richtlinie anschließend zu aktivieren oder zu deaktivieren.

### Voraussetzungen

Ein oder mehrere PCGs müssen bereitgestellt und in der Transit-VPC bzw. dem Transit-VNet ausgeführt werden.

## Verfahren

- 1 Melden Sie sich bei CSM an und gehen Sie zu Ihrer Public Cloud:
  - a Klicken Sie bei Verwendung von AWS auf **Clouds > AWS > VPCs**. Klicken Sie auf die Transit- oder Computing-VPC.
  - b Klicken Sie bei Verwendung von Microsoft Azure auf **Clouds > Azure > VNets**. Klicken Sie auf das Transit- oder Computing-VNet.
- 2 Aktivieren Sie die Option mit einer der folgenden Vorgehensweisen:
  - Klicken Sie in der Kachelansicht auf **AKTIONEN > Konfiguration bearbeiten**.



- Wenn Sie sich in der Rasteransicht befinden, aktivieren Sie das Kontrollkästchen neben der VPC oder dem VNet und klicken Sie dann auf **AKTIONEN > Konfiguration bearbeiten**.



- ◆ Wenn Sie sich auf der VPC- oder VNet-Seite befinden, klicken Sie auf das Symbol

„AKTIONEN“ und wählen Sie dann **Konfigurationen bearbeiten**.

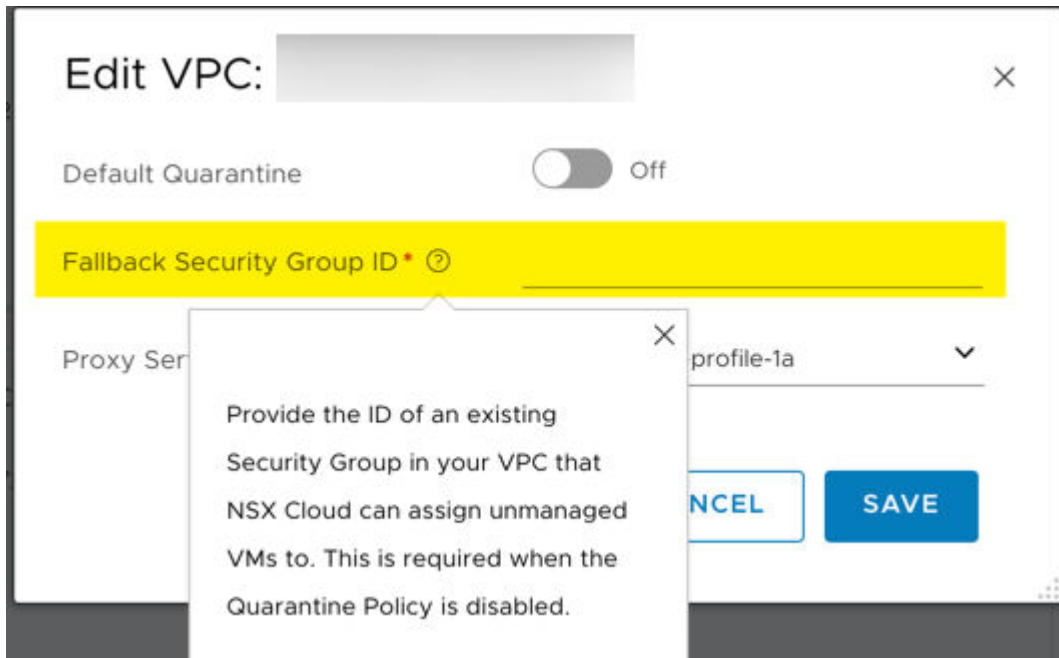


- 3 Schalten Sie **Standard-Quarantäne** ein oder aus, um sie zu aktivieren oder zu deaktivieren.
- 4 Wenn Sie die Quarantäne-Richtlinie deaktivieren, müssen Sie eine Fallback-Sicherheitsgruppe einrichten.

---

**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 [NSX Cloud-Sicherheitsgruppen für die Public Cloud](#).

---



- Allen nicht verwalteten oder unter Quarantäne stehenden VMs in dieser VPC oder diesem VNet wird beim Deaktivieren der Quarantäne-Richtlinie die ihnen zugeordnete Fallback-Sicherheitsgruppe zugewiesen.
- Alle verwalteten VMs behalten die von NSX Cloud zugewiesene Sicherheitsgruppe. Wenn solche VMs nach dem Deaktivieren der Quarantäne-Richtlinie zum ersten Mal nicht mehr gekennzeichnet sind und nicht mehr verwaltet werden, erhalten auch sie die ihnen zugewiesene Fallback-Sicherheitsgruppe.

5 Klicken Sie auf **SPEICHERN**.

## Quarantäne-Richtlinie-Auswirkungen bei Deaktivierung

### Quarantäne-Richtlinie: deaktiviert

Wenn die Quarantäne-Richtlinie deaktiviert ist:

- NSX Cloud weist den in dieser VPC bzw. diesem VNet gestarteten virtuellen Maschinen keine Sicherheitsgruppen zu. Sie müssen den virtuellen Maschinen die richtigen NSX Cloud-Sicherheitsgruppen zuweisen, um die Bedrohungserkennung zu aktivieren.

Vom Microsoft Azure-Portal oder der AWS-Konsole aus:

- Weisen Sie `vm-underlay-sg` VMs zu, für die Sie das von Microsoft Azure bzw. AWS bereitgestellte Underlay-Netzwerk verwenden möchten.
- Stellen Sie sicher, dass die folgenden Ports geöffnet sind:
  - Eingehender UDP 6081: für Overlay-Datenpakete. Dieser Port sollte für die VTEP-IP-Adresse (eth1-Schnittstelle) des PCG (Aktiv/Standby) zulässig sein.

- Ausgehender TCP 5555: für Steuerpakete. Dieser Port sollte für die Verwaltungs-IP-Adresse (eth0-Schnittstelle) des PCG (aktiv/Standby) zulässig sein.
- TCP 8080: für Installation/Upgrade der Verwaltungs-IP-Adresse des PCG.
- TCP 80: zum Herunterladen der Abhängigkeiten von Drittanbietern bei der Installation des NSX-Agenten.
- UDP 67, 68: für DHCP-Pakete.
- UDP 53: für die DNS-Auflösung.

## Quarantänerichtlinie: erst aktiviert, dann deaktiviert

In der folgenden Tabelle sind die Auswirkungen auf die Zuweisungen von Sicherheitsgruppen dargestellt, wenn die Quarantäne-Richtlinie aktiviert war und Sie sie dann deaktivieren.

Tabelle 22-1. Auswirkungen der Deaktivierung der Quarantäne-Richtlinie auf Sicherheitsgruppen

VM-ID	Verwaltet?	Sicherheitsgruppe	Sicherheitsgruppe für virtuelle Maschine, nachdem die Quarantäne-Richtlinie deaktiviert wurde
VM 1	Ja	vm_underlay_sg	vm_underlay_sg . Wenn Sie das Tag <code>nsx.network</code> von dieser VM entfernen, um sie aus der NSX-Verwaltung zu nehmen, wird dieser VM auch die ihr zugeordnete Fallback-Sicherheitsgruppe zugewiesen.
VM 2	Ja	default (AWS) oder quarantine (Microsoft Azure)	Die Fallback-Sicherheitsgruppe, die Sie beim Deaktivieren der Quarantäne-Richtlinie angeben. Weitere Informationen finden Sie unter <a href="#">Quarantäne-Richtlinie aktivieren oder deaktivieren</a> .

Tabelle 22-1. Auswirkungen der Deaktivierung der Quarantäne-Richtlinie auf Sicherheitsgruppen (Fortsetzung)

VM-ID	Verwaltet?	Sicherheitsgruppe	Sicherheitsgruppe für virtuelle Maschine, nachdem die Quarantäne-Richtlinie deaktiviert wurde
VM 3	Nein	vm_override_sg	Die Fallback-Sicherheitsgruppe, die Sie beim Deaktivieren der Quarantäne-Richtlinie angeben.
VM 4	Nein	default (AWS) oder quarantine (Microsoft Azure)	Die Fallback-Sicherheitsgruppe, die Sie beim Deaktivieren der Quarantäne-Richtlinie angeben.

**Hinweis** Die Quarantäne-Richtlinie muss deaktiviert werden, bevor die Bereitstellung von PCG aufgehoben werden kann. Einzelheiten hierzu erhalten Sie unter **Aufhebung der Bereitstellung von PCGs** in der *Installationshandbuch für NSX-T Data Center*.

## Quarantäne-Richtlinie-Auswirkungen bei Aktivierung

### Quarantäne-Richtlinie: aktiviert

Wenn die Quarantäne-Richtlinie aktiviert ist:

- Die Zuweisung der Sicherheitsgruppe (SG bzw. der Netzwerk-Sicherheitsgruppe (NSG) für alle Schnittstellen für beliebige Workload-VMs, die zu dieser VPC bzw. diesem VNet gehören, wird von NSX Cloud wie folgt verwaltet:
  - Nicht verwaltete VMs werden in Microsoft Azure der NSG quarantine und in AWS der Sicherheitsgruppe default zugewiesen und in Quarantäne gestellt. Dies begrenzt den ausgehenden Datenverkehr und beendet allen eingehenden Datenverkehr zu solchen VMs.
  - Nicht verwaltete VMs können NSX-verwaltete VMs werden, wenn Sie NSX Agent auf der virtuellen Maschine installieren und Sie sie in der Public Cloud mit nsx.network taggen. Im Standardszenario weist NSX Cloud vm-underlay-sg zu, um entsprechenden eingehenden/ ausgehenden Datenverkehr zuzulassen.
  - Einer NSX-verwalteten VM kann nach wie vor die Sicherheitsgruppe quarantine oder default zugewiesen werden, und sie kann in Quarantäne gestellt werden, wenn eine Bedrohung auf der VM erkannt wird, z. B. wenn NSX Agent auf der VM angehalten wird.
  - Alle manuellen Änderungen an den Sicherheitsgruppen werden innerhalb von zwei Minuten zu der/den durch NSX festgelegten Sicherheitsgruppe(n) zurückgesetzt.

- Wenn Sie eine beliebige VM aus der Quarantäne verschieben möchten, weisen Sie `vm-override-sg` als einzige Sicherheitsgruppe für diese VM zu. NSX Cloud unterstützt keine automatische Änderung der Sicherheitsgruppe `vm-override-sg` und lässt den Zugriff auf die VM durch SSH und RDP zu. Das Entfernen von `vm-override-sg` bewirkt erneut, dass die VM-Sicherheitsgruppe(n) auf die durch NSX festgelegte Sicherheitsgruppe zurückgesetzt wird/werden.

**Hinweis** Wenn die Quarantäne-Richtlinie aktiviert ist, weisen Sie Ihren VMs `vm-override-sg` zu, bevor Sie NSX Agent darauf installieren. Nachdem Sie den Installationsprozess von NSX Agent abgeschlossen und die VM als „Underlay“ markiert haben, entfernen Sie die NSG `vm-override-sg` aus der VM. NSX Cloud weist den von NSX verwalteten VMs anschließend automatisch die richtige Sicherheitsgruppe zu. Dieser Schritt ist notwendig, weil er sicherstellt, dass der VM nicht die Sicherheitsgruppe `quarantine` oder `default` zugewiesen wird, während Sie sie für NSX Cloud vorbereiten.

## Quarantäne-Richtlinie: erst deaktiviert, dann aktiviert

In der folgenden Tabelle sind die Auswirkungen auf die Zuweisungen von Sicherheitsgruppen dargestellt, wenn die Quarantäne-Richtlinie deaktiviert war und Sie sie dann aktivieren.

**Tabelle 22-2. Auswirkungen der Aktivierung der Quarantäne-Richtlinie auf Sicherheitsgruppen**

VM-ID	Verwaltet?	Bedrohung erkannt?	Sicherheitsgruppe nach der Aktivierung der Quarantäne-Richtlinie
VM 1	Ja	Nein	<code>vm_underlay_sg</code>
VM 2	Ja	Ja	<code>default</code> (AWS) oder <code>quarantine</code> (Microsoft Azure)
<b>Hinweis</b> Sie können <code>vm_override_sg</code> manuell verwalteten VMs zuweisen. Dadurch wird der Quarantäne-Modus für sie beendet und Sie können das Problem beheben, indem Sie über SSH oder RDP auf diese VMs zugreifen. Siehe <a href="#">Quarantäne-Richtlinie: aktiviert</a> .			
VM 3	Nein	Nicht verfügbar	<code>default</code> (AWS) oder <code>quarantine</code> (Microsoft Azure)

## NSX Cloud-Sicherheitsgruppen für die Public Cloud

Die folgenden Sicherheitsgruppen werden von NSX Cloud bei der Bereitstellung von PCG erstellt.

Die Sicherheitsgruppen **gw** werden auf die entsprechenden PCG-Schnittstellen angewendet.

Tabelle 22-3. Von NSX Cloud für PCG-Schnittstellen erstellte Public-Cloud-Sicherheitsgruppen

Name der Sicherheitsgruppe	Verfügbar in Microsoft Azure?	Verfügbar in AWS?	Vollständiger Name
gw-mgmt-sg	Ja	Ja	Gateway-Management-Sicherheitsgruppe
gw-uplink-sg	Ja	Ja	Gateway-Uplink-Sicherheitsgruppe
gw-vtep-sg	Ja	Ja	Gateway-Downlink-Sicherheitsgruppe

Tabelle 22-4. Von NSX Cloud für Workload-VMs erstellte Public Cloud-Sicherheitsgruppen

Name der Sicherheitsgruppe	Verfügbar in Microsoft Azure?	Verfügbar in AWS?	Beschreibung
quarantine	Ja	Nein	Quarantäne-Sicherheitsgruppe für Microsoft Azure
default	Nein	Ja	Quarantäne-Sicherheitsgruppe für AWS
vm-underlay-sg	Ja	Ja	Nicht-Overlay-VM-Sicherheitsgruppe
vm-override-sg	Ja	Ja	Überschreiben-VM-Sicherheitsgruppe
vm-overlay-sg	Ja	Ja	Overlay-VM-Sicherheitsgruppe (diese wird in der aktuellen Version nicht verwendet)
vm-outbound-bypass-sg	Ja	Ja	Ausgehende VM-Bypass-Sicherheitsgruppe (diese wird in der aktuellen Version nicht verwendet)
vm-inbound-bypass-sg	Ja	Ja	Eingehende VM-Bypass-Sicherheitsgruppe (diese wird in der aktuellen Version nicht verwendet)

## Überblick über Onboarding und Verwaltung von Workload-VMs

In dieser Prüfliste finden Sie eine Übersicht über die Schritte zum Onboarding und Verwalten von Arbeitslast-VMs.

Weitere Informationen für den Tag-O-Workflow finden Sie unter [Übersicht über die Installation und Konfiguration von NSX Cloud-Komponenten für Ihre Public Cloud](#) im *Installationshandbuch für NSX-T Data Center*.

## Onboarding und Verwaltung von Arbeitslast-VMs

In diesem Flussdiagramm finden Sie eine Übersicht über die Schritte zum Onboarding und zur Verwaltung von Arbeitslast-VMs von Ihrer Public Cloud.

Tabelle 22-5. Tag-N-Workflow zum Onboarding Ihrer Arbeitslast-VMs in NSX Cloud

Aufgabe	Persona	Anweisungen
<input type="checkbox"/> Wenn die Quarantänerichtlinie aktiviert ist, platzieren Sie die VMs in der Sicherheitsgruppe <b>vm_underlay_sg</b> . Wenn die Quarantänerichtlinie deaktiviert ist, platzieren Sie die VMs in der Sicherheitsgruppe <b>vm_override_sg</b> .	Public-Cloud-Administrator	Befolgen Sie die Anleitung in Ihrer Public-Cloud-Dokumentation für das Platzieren von Arbeitslast-VMs in bestimmten Sicherheitsgruppen.
<input type="checkbox"/> Taggen Sie Arbeitslast-VMs mit dem Schlüsselwert <b>nsx.network=default</b> .	Public-Cloud-Administrator	Befolgen Sie die Anleitung in Ihrer Public-Cloud-Dokumentation für das Taggen von Arbeitslast-VMs.
<input type="checkbox"/> Installieren Sie den NSX Agent auf Ihren Windows- oder Linux-Arbeitslast-VMs. <b>Hinweis</b> Wenn die <b>automatische Agent-Installation</b> in CSM für Microsoft Azure-Konten aktiviert ist, wird der NSX Agent automatisch installiert.	Public-Cloud-Administrator	Siehe <a href="#">Installieren von NSX Agent</a> .
<input type="checkbox"/> Wenn die Quarantänerichtlinie aktiviert ist, platzieren Sie die VMs in der Sicherheitsgruppe <b>default</b> .	Public-Cloud-Administrator	Befolgen Sie die Anleitung in Ihrer Public-Cloud-Dokumentation für das Platzieren von Arbeitslast-VMs in bestimmten Sicherheitsgruppen.
<input type="checkbox"/> Um eingehenden Zugriff auf Arbeitslast-VMs zu ermöglichen, erstellen Sie nach Bedarf DFW-Regeln (verteilte Firewall).	NSX-T Data Center Enterprise-Administrator	Siehe <a href="#">DFW-Regeln für NSX-verwaltete Arbeitslast-VMs</a> .
<input type="checkbox"/> Gruppieren Sie Ihre Arbeitslast-VMs mithilfe von Public-Cloud-Tags oder NSX-T Data Center-Tags und richten Sie die Mikrosegmentierung ein.	NSX-T Data Center Enterprise-Administrator	Siehe <a href="#">Gruppen-VMs mit NSX-T Data Center und Public-Cloud-Tags</a> .



## Onboarden von Workload-VMs

Integrieren Sie Ihre Arbeitslast-VMs, um sie mithilfe von NSX-T Data Center zu verwalten.

### Unterstützte Betriebssysteme

Dies ist die Liste der derzeit von NSX Cloud unterstützten Betriebssysteme für Ihre Workload-VM.

Derzeit werden die folgenden Betriebssysteme unterstützt:

---

**Hinweis** Im *Versionshinweise für NSX-T Data Center* erhalten Sie im Abschnitt „Bekannte Probleme bei NSX Cloud“ Informationen zu Ausnahmen.

---

- Red Hat Enterprise Linux (RHEL) 7.2, 7.3, 7.4, 7.5
- CentOS 7.2, 7.3, 7.4, 7.5
- Ubuntu 14.04, 16.04
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows 10

### Taggen von virtuellen Maschinen in der Public Cloud

Wenden Sie das Tag **nsx.network** auf die VMs an, die Sie mithilfe von NSX-T Data Center verwalten möchten.

#### Voraussetzungen

Die VPC oder das VNet, in denen die Arbeitslast-VMs gehostet werden, muss mit NSX Cloud integriert sein. Weitere Informationen finden Sie unter **Hinzufügen Ihrer Public-Cloud-Bestandsliste** in *Installationshandbuch für NSX-T Data Center*.

#### Verfahren

- 1 Melden Sie sich bei Ihrem Public-Cloud-Konto an und navigieren Sie zu Ihrer VPC oder Ihrem VNet, die/das mit NSX Cloud integriert wurde.
- 2 Wählen Sie die VMs, die Sie mithilfe von NSX-T Data Center verwalten möchten.
- 3 Fügen Sie die folgenden Tag-Details für die VMs hinzu und speichern Sie Ihre Änderungen.

```
Name: nsx.network
Value: default
```

---

**Hinweis** Sie können dieses Tag entweder auf VM-Ebene oder auf der Ebene der Schnittstelle anwenden – beides hat denselben Effekt.

---

#### Beispiel

## Nächste Schritte

Installieren Sie den NSX Agent auf diesen VMs. Siehe [Installieren von NSX Agent](#).

Wenn Sie Microsoft Azure verwenden, können Sie den NSX Agent automatisch auf gekennzeichneten VMs installieren. Weitere Informationen finden Sie unter [Automatische Installation von NSX Agent](#).

## Installieren von NSX Agent

Installieren von NSX Agent auf Ihren Workload-VMs

Eine Anleitung zum Erstellen von AMIs oder verwalteten Images mit installiertem NSX Agent finden Sie unter [Erzeugen replizierbarer Images](#).

### Installieren von NSX Agent auf virtuellen Windows-Maschinen

Folgen Sie diesen Anweisungen, um NSX Agent auf Ihrer Windows-Workload-VM zu installieren.

Unter [Unterstützte Betriebssysteme](#) finden Sie eine Liste der Microsoft Windows-Versionen, die gegenwärtig unterstützt werden.

---

**Hinweis** Navigieren Sie zum Überprüfen der Prüfsumme für dieses Skript zu **VMware-Downloads > Treiber & Tools > NSX Cloud-Skripts**.

---

#### Verfahren

- 1 Melden Sie sich bei CSM an und gehen Sie zu Ihrer Public Cloud:
  - a Klicken Sie bei Verwendung von AWS auf **Clouds > AWS > VPCs**. Klicken Sie auf eine Transit- oder Computing-VPC.
  - b 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.

**Hinweis:** In einer/einem Transit-VPC/-VNet werden ein oder zwei PCGs bereitgestellt und ausgeführt. Die/Das Computing-VPC/-VNet ist mit einer/einem Transit-VPC/-VNet verknüpft und kann die hier bereitgestellten PCGs verwenden.

- 2 Notieren Sie sich im Bildschirmabschnitt **Agent-Download und -Installation** den **Downloadspeicherort** und den **Installationsbefehl** unter **Windows**.

---

**Hinweis** Für VNets wird das DNS-Suffix im Installationsbefehl in Übereinstimmung mit den DNS-Einstellungen dynamisch erzeugt, die Sie beim Bereitstellen von PCG auswählen. Für Transit-VNets ist der Parameter `-dnsServer <dns-server-ip>` optional. Für Computing-VNets müssen Sie die DNS-Weiterleitungs-IP-Adresse bereitstellen, um diesen Befehl abzuschließen.

---

- 3 Stellen Sie als Administrator eine Verbindung mit Ihrer Windows-Workload-VM her.

- 4 Laden Sie das Installationsskript von dem **Downloadspeicherort**, den Sie sich aus CSM notiert haben, auf Ihre virtuelle Windows-Maschine herunter. Sie können einen beliebigen Browser, beispielsweise Internet Explorer, verwenden, um das Skript herunterzuladen. Es wird in das Download-Standardverzeichnis Ihres Browsers, z. B. *C:\Downloads* heruntergeladen.

---

**Hinweis** Navigieren Sie zum Überprüfen der Prüfsumme für dieses Skript zu **VMware-Downloads > Treiber & Tools > NSX Cloud-Skripts**.

---

**Hinweis:**

- 5 Öffnen Sie eine PowerShell-Eingabeaufforderung und wechseln Sie zu dem Verzeichnis, das das heruntergeladene Skript enthält.
- 6 Verwenden Sie zum Ausführen des heruntergeladenen Skripts den **Installationsbefehl**, den Sie aus CSM notiert haben.

Beispiel:

```
c:\> powershell -file 'nsx_install.ps1' -operation install -dnsSuffix <>
```

---

**Hinweis** Das Dateiarargument benötigt den vollständigen Pfad, sofern Sie sich nicht in demselben Verzeichnis befinden oder wenn sich das PowerShell-Skript bereits unter diesem Pfad befindet. Wenn Sie das Skript beispielsweise in *C:\Downloads* herunterladen und Sie sich momentan noch nicht in diesem Verzeichnis befinden, dann muss das Skript folgenden Speicherort enthalten: *powershell -file 'C:\Downloads\nsx\_install.ps1'...*

---

- 7 Das Skript wird ausgeführt, und wenn dies abgeschlossen ist, wird eine Meldung angezeigt, die angibt, ob NSX Agent erfolgreich installiert wurde.

---

**Hinweis** Für das Skript ist die primäre Netzwerkschnittstelle die Standardeinstellung.

---

## Nächste Schritte

### [Verwalten von Workload-VMs](#)

## Installieren von NSX Agent auf virtuellen Linux-Maschinen

Befolgen Sie diese Anweisungen, um NSX Agent auf Ihren Linux-Workload-VMs zu installieren.

Unter [Unterstützte Betriebssysteme](#) finden Sie eine Liste der aktuell unterstützten Linux-Distributionen.

---

**Hinweis** Navigieren Sie zum Überprüfen der Prüfsumme für dieses Skript zu **VMware-Downloads > Treiber & Tools > NSX Cloud-Skripts**.

---

## Voraussetzungen

Sie benötigen die folgenden Befehle, um das Installationsskript für NSX Agent auszuführen:

- **wget**

- **nslookup**
- **dmidecode**

## Verfahren

- 1 Melden Sie sich bei CSM an und gehen Sie zu Ihrer Public Cloud:
  - a Klicken Sie bei Verwendung von AWS auf **Clouds > AWS > VPCs**. Klicken Sie auf eine Transit- oder Computing-VPC.
  - b 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.

**Hinweis:** In einer/einem Transit-VPC/-VNet werden ein oder zwei PCGs bereitgestellt und ausgeführt. Die/Das Computing-VPC/-VNet ist mit einer/einem Transit-VPC/-VNet verknüpft und kann die hier bereitgestellten PCGs verwenden.

- 2 Notieren Sie sich im Bildschirmabschnitt **Agent Download & Installation** den **Downloadspeicherort** und den **Befehl zur Installation** unter **Linux**.

---

**Hinweis** Für VNets wird das DNS-Suffix im Installationsbefehl in Übereinstimmung mit den DNS-Einstellungen dynamisch erzeugt, die Sie beim Bereitstellen von PCG auswählen. Für Transit-VNets ist der Parameter `-dnsServer <dns-server-ip>` optional. Für Computing-VNets müssen Sie die DNS-Weiterleitungs-IP-Adresse bereitstellen, um diesen Befehl abzuschließen.

---

- 3 Melden Sie sich bei der Linux-Workload-VM mit Superuser-Rechten an.
- 4 Verwenden Sie `wget` oder einen vergleichbaren Befehl zum Herunterladen des Installationsskripts auf Ihre virtuelle Linux-Maschine von dem **Downloadspeicherort**, den Sie sich aus CSM notiert haben. Das Installationsskript wird in das Verzeichnis heruntergeladen, in dem Sie den Befehl `wget` ausführen.

---

**Hinweis** Navigieren Sie zum Überprüfen der Prüfsumme für dieses Skript zu **VMware-Downloads > Treiber & Tools > NSX Cloud-Skripts**.

---

- 5 Ändern Sie gegebenenfalls Berechtigungen für das Installationsskript, um es ausführbar zu machen, und führen Sie es aus:

```
$ chmod +x install_nsx_vm_agent.sh && sudo ./install_nsx_vm_agent.sh
```

**Hinweis:** SELinux wird unter Red Hat Enterprise Linux und dessen Derivaten nicht unterstützt. Deaktivieren Sie SELinux, um den NSX-Agent zu installieren.

- 6 Nach dem Start der Installation von NSX Agent geht die Verbindung mit Ihrer Linux-VM verloren. Meldungen wie die folgende werden auf dem Bildschirm angezeigt: `Installation completed!!! Starting NSX Agent service. SSH connection will now be lost..` Stellen Sie wieder eine Verbindung mit Ihrer VM her, um den Onboarding-Vorgang abzuschließen.

## Ergebnisse

Der NSX Agent wird auf Ihren Workload-VMs installiert.

---

### Hinweis

- Nachdem der NSX Agent erfolgreich installiert wurde, wird der Port 8888 auf der VM als offen angezeigt, ist aber für VMs im Underlay-Modus blockiert und sollte nur verwendet werden, wenn er für die erweiterte Fehlerbehebung benötigt wird.
  - Das Skript verwendet eth0 als die Standardschnittstelle.
- 

## Nächste Schritte

### Verwalten von Workload-VMs

## Deinstallieren von NSX Agent

Verwenden Sie diese betriebssystemspezifische-Befehle, um NSX Agent zu deinstallieren.

### Deinstallieren von NSX Agent von einer Windows-VM

---

**Hinweis** Um weitere Optionen für das Installationsskript anzuzeigen, verwenden Sie `-help`.

---

- 1 Melden Sie sich mithilfe von RDP remote bei der VM an.
- 2 Führen Sie das Installationsskript mit der Deinstallationsoption aus:

```
\nsx_install.ps1 -operation uninstall
```

### Deinstallieren von NSX Agent von einer Linux-VM

---

**Hinweis** Um weitere Optionen für das Installationsskript anzuzeigen, verwenden Sie `--help`.

---

- 1 Melden Sie sich mithilfe von SSH remote bei der VM an.
- 2 Führen Sie das Installationsskript mit der Deinstallationsoption aus:

```
sudo ./install_nsx_vm_agent.sh --uninstall
```

## Automatische Installation von NSX Agent

Wird derzeit nur für Microsoft Azure unterstützt.

Wenn die folgenden Kriterien erfüllt sind, wird der NSX-Agent in Microsoft Azure automatisch installiert:

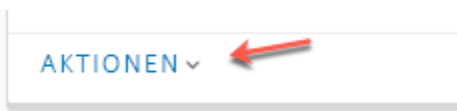
- Azure-VM-Erweiterungen, die auf den virtuellen Maschinen im VNet installiert sind, werden NSX Cloud hinzugefügt. Weitere Informationen erhalten Sie in der [Microsoft Azure-Dokumentation zu VM-Erweiterungen](#).

- Die Sicherheitsgruppe, die auf VMs in Microsoft Azure angewendet wird, muss die Installation des NSX-Agenten zulassen. Wenn die Quarantänerichtlinie aktiviert ist, wenden Sie den Parameter `vm-override-sg` auf die Arbeitslast-VMs an. Wenn die Quarantänerichtlinie deaktiviert ist, wenden Sie `vm_underlay_sg` auf sie an.
- Mit `nsx.network` und dem Wert `default` getaggte VMs.

So aktivieren Sie diese Funktion:

- 1 Klicken Sie auf **Clouds > Azure > VNets**.
- 2 Wählen Sie das VNet aus, auf dessen VMs der NSX-Agent automatisch installiert werden soll.
- 3 Aktivieren Sie die Option mit einer der folgenden Vorgehensweisen:

- Klicken Sie in der Kachelansicht auf **AKTIONEN > Konfiguration bearbeiten**.



- In der Rasteransicht aktivieren Sie das Kontrollkästchen neben dem VNet. Klicken Sie dann auf **AKTIONEN > Konfiguration bearbeiten**.
- Klicken Sie auf der Seite des VNet auf das Symbol „AKTIONEN“ und wählen Sie dann

**Konfigurationen bearbeiten.**

- 4 Aktivieren Sie die Option **Automatische Agent-Installation** mit dem Schieberegler.

---

**Hinweis** Wenn die Installation des NSX-Agenten fehlschlägt, gehen Sie wie folgt vor:

---

- 1 Melden Sie sich beim Microsoft Azure-Portal an und navigieren Sie zu der VM, auf der die Installation des NSX-Agenten fehlgeschlagen ist.
- 2 Wechseln Sie zu den Erweiterungen der VM, und deinstallieren Sie die Erweiterung namens `VMwareNsxAgentInstallCustomScriptExtension`.
- 3 Entfernen Sie das Tag `nsx.network` von dieser VM.
- 4 Fügen Sie das Tag `nsx.network` auf dieser VM erneut hinzu.

Innerhalb von etwa drei Minuten wird der NSX-Agent auf dieser VM installiert.

## Verwalten von Workload-VMs

Nachdem Sie erfolgreich Workload-VMs integriert haben, können Sie NSX-T Data Center dazu verwenden, diese zu verwalten.

## DFW-Regeln für NSX-verwaltete Arbeitslast-VMs

Beim Bereitstellen des PCG in der Transit-VPC oder auf dem Transit-VNet oder beim Verknüpfen einer Computing-VPC oder eines Computing-VNet mit einem Transit erstellt NSX Cloud DFW-Standardregeln für NSX-verwaltete Arbeitslast-VMs, die alle Verbindungen zu ihnen blockieren.

Die beiden statusfreien Regeln gelten für den DHCP-Zugriff und wirken sich nicht auf den Zugriff auf Ihre Arbeitslast-VMs aus.

Die beiden statusbehafteten Regeln lauten wie folgt:

Von NSX Cloud unter folgender Richtlinie erstellte DFW-Regeln: <code>ccloud-stateful-cloud-&lt;VPC/VNet ID&gt;</code>	Eigenschaften
<code>ccloud-&lt;VPC/VNet ID&gt;-managed</code>	Ermöglicht den Zugriff auf die VMs innerhalb derselben VPC oder desselben VNet.
<code>ccloud-&lt;VPC/VNet ID&gt;-inbound</code>	Sperrt den Zugriff auf NSX-verwaltete VMs von überall außerhalb der VPC oder des VNet.

**Hinweis** Bearbeiten Sie keine der Standardregeln.

Sie können eine Kopie der vorhandenen eingehenden Regel erstellen, die Quellen und Ziele anpassen und die Einstellung **Zulassen** auswählen. Platzieren Sie die Regel **Zulassen** über der Standardregel **Ablehnen**. Sie können auch neue Richtlinien und Regeln hinzufügen. Weitere Anweisungen finden Sie unter [Hinzufügen einer verteilten Firewall](#).

## Gruppen-VMs mit NSX-T Data Center und Public-Cloud-Tags

Mit NSX Cloud können Sie die Public-Cloud-Tags verwenden, die Ihren Workload-VMs zugewiesen sind.

NSX Manager verwendet Tags, um VMs zu gruppieren – genauso, wie Public Clouds dies handhaben. Daher übernimmt NSX Cloud zur vereinfachten Gruppierung von VMs die auf Ihre Arbeitslast-VMs angewendeten Public Cloud-Tags in NSX Manager. Voraussetzung hierfür ist jedoch, dass die Tags die vordefinierten Kriterien für Größe und reservierte Wörter erfüllen.

**Hinweis** Die DFW-Regeln hängen von den Tags ab, die VMs zugewiesen sind. Da diese Tags von jeder Person mit den entsprechenden Public-Cloud-Berechtigungen geändert werden können, geht NSX-T Data Center davon aus, dass diese Benutzer vertrauenswürdig sind und dass die Verantwortung für die Sicherstellung und Überwachung, dass VMs zu jeder Zeit korrekt gekennzeichnet sind, beim Public-Cloud-Netzwerkadministrator liegt.

## Tags-Terminologie

Ein **Tag** in NSX Manager bezieht sich auf das, was im Kontext einer Public Cloud als **Wert** bezeichnet wird. Der **Schlüssel** eines Public-Cloud-Tags wird in NSX Manager als **Geltungsbereich** bezeichnet.

Tag-Komponenten	
in NSX Manager	Äquivalente Komponenten von Tags in der Public Cloud
Geltungsbereich	Schlüssel
Tag	Wert

## Tag-Typen und Einschränkungen

NSX Cloud lässt drei Typen Tags für NSX-verwaltete Public-Cloud-VMs zu.

- **System-Tags:** Diese Tags sind vom System definiert, und Sie können sie nicht hinzufügen, bearbeiten oder löschen. NSX Cloud verwendet die folgenden System-Tags:
  - azure:subscription\_id
  - azure:region
  - azure:vm\_rg
  - azure:vnet\_name
  - azure:vnet\_rg
  - azure:transit\_vnet\_name
  - azure:transit\_vnet\_rg
  - aws:account
  - aws:availabilityzone
  - aws:region
  - aws:vpc
  - aws:subnet
  - aws:transit\_vpc
- **Ermittelte Tags:** Tags, die Sie Ihren VMs in der Public Cloud hinzugefügt haben, werden automatisch von NSX Cloud ermittelt und für Ihre Workload-VMs im NSX Manager-Bestand angezeigt. Diese Tags können innerhalb von NSX Manager nicht bearbeitet werden. Es gibt keine Begrenzung der Anzahl ermittelter Tags. Diese Tags werden mit dem `dis:azure:` oder `dis:aws` versehen, um anzugeben, dass sie in Microsoft Azure bzw. AWS ermittelt wurden.
 

Wenn Sie beliebige Änderungen an den Tags in der Public Cloud vornehmen, werden die Änderungen innerhalb von drei Minuten in NSX Manager wiedergegeben.

Diese Funktion ist standardmäßig aktiviert. Sie können die Erkennung von Microsoft Azure- oder AWS-Tags beim Hinzufügen des Microsoft Azure-Abonnements oder AWS-Kontos aktivieren oder deaktivieren.
- **Benutzer-Tags:** Sie können bis zu 25 Benutzer-Tags erstellen. Sie verfügen über die Berechtigungen „Hinzufügen“, „Bearbeiten“ und „Löschen“ für Benutzer-Tags. Informationen zum Verwalten von Benutzer-Tags finden Sie unter [Verwalten von Tags für eine virtuelle Maschine](#).



Tabelle 22-6. Zusammenfassung der Tag-Typen und Einschränkungen

Tag-Typ	Tag-Geltungsbereich oder vorab festgelegtes Präfix	Einschränkungen	Enterprise-Administrator Berechtigungen	Auditor Berechtigungen
Systemdefiniert	Vollständige System-Tags: <ul style="list-style-type: none"> <li>■ azure:subscription_id</li> <li>■ azure:region</li> <li>■ azure:vm_rg</li> <li>■ azure:vnet_name</li> <li>■ azure:vnet_rg</li> <li>■ aws:vpc</li> <li>■ aws:availability zone</li> </ul>	Geltungsbereich (Schlüssel): 20 Zeichen Tag (Wert): 65 Zeichen Möglicher Maximalwert: 5	Nur Lesen	Nur Lesen
Ermittelt	Präfix für Microsoft Azure-Tags, die aus Ihrem VNet importiert werden: <b>dis:azure:</b> Präfix für AWS-Tags, die von Ihrem VPC importiert werden: <b>dis:aws:</b>	Geltungsbereich (Schlüssel): 20 Zeichen Tag (Wert): 65 Zeichen Zulässiger Maximalwert: unbegrenzt <b>Hinweis</b> Die Grenzwerte für Zeichen schließen das Präfix <b>dis:&lt;public cloud name&gt;</b> aus. Tags, die diese Grenzwerte überschreiten, werden in NSX Manager nicht wiedergegeben. Tags mit dem Präfix <b>nsx</b> werden ignoriert.	Nur Lesen	Nur Lesen
Benutzer	Benutzer-Tags können einen beliebigen Geltungsbereich (Schlüssel) und Wert innerhalb der	Geltungsbereich (Schlüssel): 30 Zeichen Tag (Wert): 65 Zeichen Zulässiger Maximalwert: 25	Hinzufügen/Bearbeiten/Löschen	Nur Lesen

Tabelle 22-6. Zusammenfassung der Tag-Typen und Einschränkungen (Fortsetzung)

Tag-Typ	Tag-Geltungsbereich oder vorab festgelegtes Präfix	Einschränkungen	Enterprise-Administrator Berechtigungen	Auditor Berechtigungen
	zulässigen Anzahl Zeichen haben; mit Ausnahme von: <ul style="list-style-type: none"> <li>■ das Scope- (Schlüssel-)Präfix <b>dis:azure:</b> oder <b>dis:aws:</b></li> <li>■ derselbe Geltungsbereich (Schlüssel) wie System-Tags</li> </ul>			

## Beispiele ermittelter Tags

**Hinweis** Tags liegen im Format **key=value** für die Public Cloud und **scope=tag** in NSX Manager vor.

Tabelle 22-7.

Public Cloud-Tag für die Arbeitslast-VM	Durch NSX Cloud erkannt?	Äquivalentes NSX Manager-Tag für die Workload-VM
Name=Developer	Ja	dis:azure:Name=Developer
ValidDisTagKeyLength=ValidDisTagValue	Ja	dis:azure:ValidDisTagKeyLength=ValidDisTagValue
Abcdefghijklmnopqrstuvwxyz=value2	Nein (Schlüssel überschreitet 20 Zeichen)	keine
tag3=AbcdefghijklmnopqrstuvwxyzAb2369Ohgjjuytreswqacvbcdefghijklmnopqrstuvwxyz	Nein (Wert überschreitet 65 Zeichen)	keine
nsx.name=Tester	Nein (Schlüssel hat das Präfix <b>nsx</b> )	keine

## Wie Sie Tags in NSX Manager verwenden

- Siehe [Verwalten von Tags für eine virtuelle Maschine](#).
- Siehe [Suchen nach Objekten](#).
- Siehe [Einrichten von Mikro-Segmentierung für Workload-VMs](#).

## Einrichten von Mikro-Segmentierung für Workload-VMs

Sie können die Mikro-Segmentierung für verwaltete Workload-VMs einrichten.

Führen Sie folgende Schritte aus, um Regeln für verteilte Firewalls auf von NSX verwalteten Arbeitslast-VMs anzuwenden:

- 1 Erstellen Sie mithilfe des VM-Namens oder der Tags oder sonstiger Kriterien für die Mitgliedschaft Gruppen, z. B. die Ebenen **web**, **app**, **DB**. Eine Anleitung dafür finden Sie unter [Hinzufügen einer Gruppe](#).

---

**Hinweis** Sie können die folgenden Tags für die Kriterien für Mitgliedschaft verwenden. Einzelheiten dazu finden Sie unter [Gruppen-VMs mit NSX-T Data Center und Public-Cloud-Tags](#).

- vom System definierte Tags
  - Tags aus Ihrer VPC oder Ihrem VNet, die von NSX Cloud ermittelt werden
  - oder Ihre eigenen benutzerdefinierten Tags
- 

**Hinweis** Die DFW-Regeln hängen von den Tags ab, die VMs zugewiesen sind. Da diese Tags von jeder Person mit den entsprechenden Public-Cloud-Berechtigungen geändert werden können, geht NSX-T Data Center davon aus, dass diese Benutzer vertrauenswürdig sind und dass die Verantwortung für die Sicherstellung und Überwachung, dass VMs zu jeder Zeit korrekt gekennzeichnet sind, beim Public-Cloud-Netzwerkadministrator liegt.

---

- 2 Erstellen Sie eine Richtlinie und eine Regel für eine verteilte Firewall für Ost-West-Datenverkehr und wenden Sie diese auf die von Ihnen erstellte Gruppe an. Siehe [Hinzufügen einer verteilten Firewall](#).

Diese Mikro-Segmentierung wird wirksam, wenn die Bestandsliste entweder manuell erneut über CSM synchronisiert wird, oder innerhalb von etwa drei Minuten, wenn die Änderungen von Ihrer Public Cloud in CSM übertragen werden.

## Verwendung von NSX-T Data Center-Funktionen mit der Public Cloud

NSX Cloud erstellt eine Netzwerktopologie für Ihre Public Cloud und Sie dürfen die automatisch generierten logischen NSX-T Data Center-Entitäten nicht bearbeiten oder löschen.

Verwenden Sie diese Liste als Kurzreferenz für automatisch generierte Funktionen und die Verwendung von NSX-T Data Center-Funktionen, wie sie für die Public Cloud gelten.

## NSX Manager-Konfigurationen

Weitere Informationen zu den logischen Entitäten, die nach der erfolgreichen Bereitstellung einer PCG erstellt werden, finden Sie unter „Automatisch erstellte logische NSX-T-Entitäten“ im *Installationshandbuch für NSX-T Data Center*.

**Wichtig** Bearbeiten oder löschen Sie keine dieser automatisch erstellten Entitäten.

**Hinweis** Wenn Sie auf einige Funktionen auf Windows-Arbeitslast-VMs nicht zugreifen können, sollten Sie überprüfen, ob die Windows-Firewalleinstellungen korrekt konfiguriert sind.

## Häufig gestellte Fragen zu logischen Segmenten

Tabelle 22-8.

Frage	Antwort
Wo finde ich detaillierte Informationen über logische Segmente?	Siehe <a href="#">Kapitel 4 Segmente</a>
Wo finde ich detaillierte Informationen über logische Switches?	Siehe <a href="#">Kapitel 13 Logische Switches</a> .

## Häufig gestellte Fragen zu logischen Routern

Tabelle 22-9.

Frage	Antwort
Erstellt NSX Cloud automatisch einen logischen Router, wenn ein PCG bereitgestellt wird?	Ja. Wenn PCG auf einer Transit-VPC oder einem VNet bereitgestellt wird, wird von NSX Cloud automatisch ein logischer Tier-0-Router erstellt. Pro Computing-VPC/-VNet wird ein Tier-1-Router erstellt, wenn sie bzw. es mit einem Transit-VPC/-VNet verknüpft ist.
Wo finde ich weitere Informationen über logische Router?	Siehe <a href="#">Kapitel 2 Tier-0-Gateways</a> und <a href="#">Kapitel 3 Tier-1-Gateway</a> .

## Häufig gestellte Fragen zu IPFIX

Tabelle 22-10.

Frage	Antwort
Sind für die Arbeit in der Public Cloud bestimmte Konfigurationen für IPFIX erforderlich?	Ja, <ul style="list-style-type: none"> <li>■ IPFIX wird in NSX Cloud nur auf UDP-Port 4739 unterstützt.</li> <li>■ <b>Switch und DFW IPFIX:</b> Befindet sich der Collector in demselben Subnetz wie die virtuelle Windows-Maschine, auf die das IPFIX-Profil angewendet wurde, ist ein statischer ARP-Eintrag für den Collector auf der virtuellen Windows-Maschine erforderlich, da Windows UDP-Pakete unbeaufsichtigt verwirft, wenn kein ARP-Eintrag gefunden wird.</li> </ul>
Wo finde ich weitere Informationen über IPFIX?	Siehe <a href="#">Konfigurieren von IPFIX</a> .

## Häufig gestellte Fragen zur Portspiegelung

Tabelle 22-11.

Frage	Antwort
Sind für die Portspiegelung in der Public Cloud bestimmte Konfigurationen erforderlich?	Die Portspiegelung wird in der aktuellen Version nur in AWS unterstützt. <ul style="list-style-type: none"> <li>■ Für NSX Cloud konfigurieren Sie die Portspiegelung unter <b>Tools &gt; Portspiegelungssitzungen</b>.</li> <li>■ Nur die L3SPAN-Portspiegelung wird unterstützt.</li> <li>■ Der Collector muss sich in derselben VPC bzw. demselben VNet befinden wie die Quell-Arbeitslast-VM.</li> </ul>
Wo finde ich weitere Informationen über die Portspiegelung?	Siehe <a href="#">Überwachen von Port-Mirroring-Sitzungen</a> .

## Sonstige FAQ

Tabelle 22-12.

Frage	Antwort
Sind die Tags, die ich auf meine Arbeitslast-VMs in der Public Cloud anwende, in NSX-T Data Center verfügbar?	Ja. Weitere Informationen finden Sie unter <a href="#">Gruppen-VMs mit NSX-T Data Center und Public-Cloud-Tags</a> .
Wie richte ich eine Mikrosegmentierung für meine Arbeitslast-VMs ein, die von NSX-T Data Center verwaltet werden?	Siehe <a href="#">Einrichten von Mikro-Segmentierung für Workload-VMs</a> .

## Verwenden von erweiterten NSX Cloud-Funktionen

## Überprüfen von NSX Cloud-Komponenten

Es wird empfohlen sicherzustellen, dass alle Komponenten eingerichtet sind und ausgeführt werden, bevor diese in einer Produktionsumgebung bereitgestellt werden.

### Überprüfen Sie, ob der NSX Agent mit PCG verbunden ist

Um sicherzustellen, dass der NSX Agent auf Ihrer Workload-VM mit PCG verbunden ist, führen Sie folgende Schritte aus:

- 1 Geben Sie den Befehl `nsxcli` ein, um die NSX-T Data Center-Befehlszeilenschnittstelle zu öffnen.
- 2 Geben Sie den folgenden Befehl zum Abrufen des Gateway-Verbindungsstatus ein, zum Beispiel:

```
get gateway connection status
Public Cloud Gateway : nsx-gw.vmware.com:5555 Connection Status : ESTABLISHED
```

### Verifizieren Sie das VM-Schnittstellen-Tag in AWS oder Microsoft Azure

Die Arbeitslast-VMs müssen über die korrekten Tags verfügen, um eine Verbindung zum PCG herstellen zu können.

- 1 Melden Sie sich bei der AWS-Konsole oder dem Microsoft Azure-Portal an.
- 2 Überprüfen Sie die Tags „eth0“ und „interface“ der VM.

Der Schlüssel `nsx.network` muss den Wert `default` aufweisen.

### Aktivieren von NAT auf NSX-verwalteten VMs

NSX Cloud unterstützt die Aktivierung von NAT- auf NSX-verwalteten VMs.

Sie können Nord-Süd-Datenverkehr auf VMs in NSX-verwalteten VMs mithilfe von Public Cloud-Tags aktivieren.

Wenden Sie auf der NSX-verwalteten VM, für die NAT aktiviert werden soll, das folgende Tag an:

**Tabelle 22-13.**

Schlüssel	Wert
<code>nsx.publicip</code>	öffentliche IP-Adresse aus Ihrer Public Cloud, z. B. 50.1.2.3

**Hinweis** Die hier angegebene öffentliche IP-Adresse muss frei verfügbar sein und darf keiner anderen VM zugewiesen sein, auch nicht der Arbeitslast-VM, für die NAT aktiviert werden soll. Wenn Sie eine öffentliche IP-Adresse zuweisen, die zuvor mit einer anderen Instanz oder einer privaten IP-Adresse verknüpft war, funktioniert NAT nicht. Heben Sie in diesem Fall die Zuweisung der öffentlichen IP-Adresse auf.

Nach der Anwendung dieses Tags kann die Arbeitslast-VM auf Internetdatenverkehr zugreifen.

## Erzeugen replizierbarer Images

Sie können eine AMI (in AWS) oder ein verwaltetes Image (in Microsoft Azure) einer VM erzeugen, auf der der NSX-Agent installiert ist.

Mit dieser Funktion können Sie mehrere VMs starten, auf denen der Agent konfiguriert ist und ausgeführt wird.

Es gibt zwei Möglichkeiten zum Erzeugen einer AMI oder eines verwalteten Images (im Rest dieses Themas nur als „Image“ bezeichnet) einer VM, auf der der NSX-Agent installiert ist:

- **Erzeugen eines Images mit einem nicht konfigurierten NSX-Agent:** Sie können ein Image einer VM erzeugen, auf der der NSX-Agent installiert ist, die aber nicht mithilfe der Option `-noStart` konfiguriert wurde. Bei Verwendung dieser Option kann das NSX-Agent-Paket abgerufen und installiert werden, die NSX-Service werden jedoch nicht gestartet. Darüber hinaus werden keine NSX-Konfigurationen erstellt, wie z. B. Zertifikatserzeugung.
- **Erzeugen eines Images nach dem Entfernen vorhandener NSX-Agent-Konfigurationen:** Sie können Konfigurationen aus einer vorhandenen NSX-verwalteten VM entfernen und zum Erzeugen eines Images verwenden.

### Erzeugen einer AMI mit einem nicht konfigurierten NSX-Agent

Sie können eine AMI einer VM erzeugen, auf der der NSX-Agent installiert, aber nicht konfiguriert ist.

Zum Erzeugen eines Images einer VM, auf der der NSX-Agent mithilfe der Option `-noStart` installiert wurde, gehen Sie folgendermaßen vor:

#### Verfahren

- 1 Kopieren Sie den Installationsbefehl des NSX-Agent aus CSM und fügen Sie ihn ein. Anweisungen finden Sie unter [Installieren von NSX Agent](#)

- a Bearbeiten Sie den Befehl für Windows wie folgt:

```
c:\> powershell -file 'nsx_install.ps1' -operation install -dnsSuffix <> -noStart true
```

- b Bearbeiten Sie den Befehl für Linux wie folgt:

```
$ chmod +x install_nsx_vm_agent.sh && sudo ./install_nsx_vm_agent.sh --no-start
```

- 2 Wechseln Sie zu dieser VM in Ihrer Public Cloud und erstellen Sie ein Image.

### Erzeugen eines Images nach dem Entfernen vorhandener NSX-Agent-Konfigurationen

Sie können ein Image einer VM erzeugen, die über einen konfigurierten NSX-Agent verfügt.

Zum Entfernen von Konfigurationen aus einer vorhandenen NSX-verwalteten VM und Verwenden der VM zum Erzeugen von Images gehen Sie folgendermaßen vor:

## Verfahren

- 1 Entfernen von NSX-Agent-Konfigurationen aus einer Windows- oder Linux-VM:
  - a Melden Sie sich mithilfe eines Jump Hosts (vorzugsweise) bei der Arbeitslast-VM an.
  - b Öffnen der NSX-T-Befehlszeilenschnittstelle:

```
sudo nsxcli
```

- c Geben Sie die folgenden Befehle ein:

```
hostname> set debug
hostname> clear nsx-vm-agent state
```

- 2 Suchen Sie nach dieser VM in Ihrer Public Cloud und erstellen Sie ein Image.

## Diensteinfügung für Ihre Public Cloud

NSX Cloud unterstützt die Verwendung von Drittanbieterdiensten in Ihrer Public Cloud für NSX-verwaltete Arbeitslast-VMs.

Zur Nutzung der Diensteinfügung für die Arbeitslast-VMs in Ihrer Public Cloud müssen Sie die Dienst-Appliance in der Public Cloud und nicht im NSX-T Data Center hosten. Es wird empfohlen, die Dienst-Appliance in einer Transit-VPC oder einem Transit-VNet zu hosten.

Vor der Aktivierung der Diensteinfügung müssen Sie das PCG in einer Transit-VPC oder einem Transit-VNet bereitstellen.

Im Folgenden erhalten Sie einen Überblick über die einmaligen Konfigurationen, die Diensteinfügung für NSX-verwaltete Arbeitslast-VMs ermöglichen.

**Tabelle 22-14. Überblick über die Konfigurationen, die für die Diensteinfügung bei NSX-verwalteten Arbeitslast-VMs in der Public Cloud benötigt werden.**

Häufigkeit	Aufgabe	Anweisungen
Einmal für die erste Einrichtung	Einrichten der Dienst-Appliance in Ihrer Public Cloud vorzugsweise in einer Transit-VPC oder einem Transit-VNet, in dem das PCG bereitgestellt wird.	Weitere Informationen finden Sie in den Anweisungen zu Dienst-Appliances von Drittanbietern und zur Public Cloud.
	Registrieren des Drittanbieterdiensts bei NSX-T Data Center.	Siehe <a href="#">Erstellen der Dienstdefinition und eines entsprechenden virtuellen Endpoints</a> .
	Erstellen eines virtuellen Instanz-Endpoints des Diensts mithilfe einer /32 VSIP (Virtual Service IP), die nur zur Diensteinfügung von der Dienst-Appliance verwendet werden darf. Die VSIP sollte nicht mit dem CIDR-Bereich der VPCs oder VNets kollidieren. Diese VSIP wird über BGP beim PCG angekündigt.	Siehe <a href="#">Erstellen der Dienstdefinition und eines entsprechenden virtuellen Endpoints</a> .



**Tabelle 22-14. Überblick über die Konfigurationen, die für die Dienstefügung bei NSX-verwalteten Arbeitslast-VMs in der Public Cloud benötigt werden. (Fortsetzung)**

Häufigkeit	Aufgabe	Anweisungen
	Erstellen eines IPSec-VPN-Tunnels zwischen der Dienst-Appliance und dem PCG.	Siehe <a href="#">Einrichten einer IPSec-VPN-Sitzung</a> .
	Konfigurieren von BGP zwischen dem PCG und der Dienst-Appliance.	Siehe <a href="#">Konfigurieren von BGP und Route Redistribution</a> .
	<b>Hinweis</b> Konfigurieren Sie die Dienst-Appliance, um die VSIP anzukündigen, und das PCG, um die Standardroute (0.0.0.0/0) anzukündigen.	
Bei Bedarf	Einrichten von Umleitungsregeln nach Abschluss der einmaligen Konfigurationen, um selektiven Datenverkehr von NSX-verwalteten Arbeitslast-VMs an die VSIP umzuleiten. Diese Regeln werden auf den Uplink-Port des PCG angewendet.	Siehe <a href="#">Einrichten von Umleitungsregeln</a> .

## Verfahren

### 1 Erstellen der Dienstdefinition und eines entsprechenden virtuellen Endpoints

Sie müssen NSX Manager-APIs verwenden, um eine Dienstdefinition und einen virtuellem Endpoint für die Dienst-Appliance in Ihrer Public Cloud zu erstellen.

### 2 Einrichten einer IPSec-VPN-Sitzung

Richten Sie eine IPSec-VPN-Sitzung zwischen dem PCG und Ihrer Dienst-Appliance ein.

### 3 Konfigurieren von BGP und Route Redistribution

Konfigurieren Sie BGP zwischen dem PCG und der Dienst-Appliance über den IPSec-VPN-Tunnel.

### 4 Einrichten von Umleitungsregeln

Umleitungsregeln können gemäß Ihren Anforderungen angepasst werden.

## Erstellen der Dienstdefinition und eines entsprechenden virtuellen Endpoints

Sie müssen NSX Manager-APIs verwenden, um eine Dienstdefinition und einen virtuellem Endpoint für die Dienst-Appliance in Ihrer Public Cloud zu erstellen.

### Voraussetzungen

Wählen Sie eine reservierte /32-IP-Adresse aus, die als virtueller Endpoint für die Dienst-Appliance in Ihrer Public Cloud dienen soll, z. B. 100.100.100.100/32. Diese wird als virtuelle Dienst-IP (VSIP, Virtual Service IP) bezeichnet.

**Hinweis** Wenn Sie Ihre Dienst-Appliance in einem Hochverfügbarkeitspaar bereitgestellt haben, erstellen Sie keine weitere Dienstdefinition, aber verwenden Sie während der BGP-Konfiguration dieselbe VSIP zur Ankündigung beim PCG.

## Verfahren

- 1 Zum Erstellen einer Dienstdefinition für die Dienst-Appliance führen Sie den folgenden API-Aufruf mithilfe der NSX Manager-Anmeldedaten für die Autorisierung durch:

```
POST https://{NSX Manager-IP}/policy/api/v1/enforcement-points/default/service-definitions
```

Beispielanforderung:

```
{
  "resource_type": "ServiceDefinition",
  "description": "NS-Service",
  "display_name": "Service_Appliance1",
  "attachment_point": [
    "TIER0_LR"
  ],
  "transports": [
    "L3_ROUTED"
  ],
  "functionalities": [
    "NG_FW", "BYOD"
  ],
  "on_failure_policy": "ALLOW",
  "implementations": [
    "NORTH_SOUTH"
  ],
  "vendor_id" : "Vendor1"
}
```

Beispielantwort:

```
{
  "resource_type": "ServiceDefinition",
  "description": "NS-Service",
  "id": "33890153-6eea-4c9d-8e34-7b6532b9d65c",
  "display_name": "Service_Appliance1",
  "attachment_point": [
    "TIER0_LR"
  ],
  "transports": [
    "L3_ROUTED"
  ],
  "functionalities": [
    "NG_FW", "BYOD"
  ],
  "vendor_id": "Vendor1",
  "on_failure_policy": "ALLOW",
  "implementations": [
    "NORTH_SOUTH"
  ],
  "_create_time": 1540424262137,
  "_last_modified_user": "nsx_policy",
  "_system_owned": false,
  "_protection": "REQUIRE_OVERRIDE",
}
```

```

    "_last_modified_time": 1540424262137,
    "_create_user": "nsx_policy",
    "_revision": 0
  }

```

- 2 Zum Erstellen eines virtuellen Endpoints für die Dienst-Appliance führen Sie den folgenden API-Aufruf mithilfe der NSX Manager-Anmeldedaten für die Autorisierung durch:

```

PATCH https://{NSX Manager-IP}policy/api/v1/infra/tier-0s/<tier-0 router ID>/locale-services/
cloud/endpoints/virtual-endpoints/Service_Appliance1_Endpoint

```

Beispielanforderung:

```

{
  "resource_type": "VirtualEndpoint",
  "display_name": "Service_Appliance1_Endpoint",
  "target_ips": [
    {
      "ip_addresses": [ "100.100.100.100"
    ],
      "prefix_length": 32
    }
  ],
  "service_names": [ "Service_Appliance1"
  ]
}

```

Beispielantwort:

```

200 OK

```

---

**Hinweis** Der display\_name in Schritt 1 muss den service\_names in Schritt 2 entsprechen.

---

## Nächste Schritte

### [Einrichten einer IPSec-VPN-Sitzung](#)

## Einrichten einer IPSec-VPN-Sitzung

Richten Sie eine IPSec-VPN-Sitzung zwischen dem PCG und Ihrer Dienst-Appliance ein.

### Voraussetzungen

- Ein PCG oder ein Hochverfügbarkeitspaar aus PCGs muss in einer Transit-VPC bzw. einem Transit-VNet bereitgestellt werden.
- Die Dienst-Appliance muss in Ihrer Public Cloud eingerichtet werden, vorzugsweise in der Transit-VPC bzw. dem Transit-VNet.

### Verfahren

- 1 Navigieren Sie zu **Netzwerk > VPN**

- 2 Fügen Sie einen **VPN-Dienst** vom Typ „IPSec“ hinzu und beachten Sie die folgenden für NSX Cloud spezifischen Konfigurationsoptionen. Weitere Informationen finden Sie unter [Hinzufügen eines IPSec-VPN-Dienstes](#).

Option	Beschreibung
<b>Name</b>	Der Name dieses VPN-Dienstes wird zum Einrichten des lokalen Endpoints und der IPSec-VPN-Sitzungen verwendet. Notieren Sie sich den Namen.
<b>Diensttyp</b>	Bestätigen Sie, dass dieser Wert auf IPSec festgelegt ist.
<b>Tier-O-Gateway</b>	Wählen Sie das Tier-O-Gateway aus, das automatisch für die Transit-VPC bzw. das Transit-VNet erstellt wurde. Sein Name enthält die VPC-/VNet-ID, wie z. B. cloud-t0-vpc-6bcd2c13.

- 3 Fügen Sie unter **Lokaler Endpoint** einen lokalen Endpoint für das PCG hinzu. Die IP-Adresse des lokalen Endpoints ist der Wert des Tags nsx:local\_endpoint\_ip für das PCG, das in der Transit-VPC bzw. dem Transit-VNet bereitgestellt wird. Melden Sie sich an der Transit-VPC bzw. dem Transit-VNet an, um diesen Wert abzurufen. Beachten Sie die folgenden für NSX Cloud spezifischen Konfigurationen. Weitere Informationen finden Sie unter [Hinzufügen von lokalen Endpoints](#).

Option	Beschreibung
<b>Name</b>	Der Name des lokalen Endpoints wird verwendet, um die IPSec-VPN-Sitzungen einzurichten. Notieren Sie sich den Namen.
<b>VPN-Dienst</b>	Wählen Sie den in Schritt 2 hinzugefügten VPN-Dienst aus.
<b>IP-Adresse</b>	Suchen Sie nach diesem Wert, indem Sie sich bei der AWS-Konsole oder dem Microsoft Azure-Portal anmelden. Es handelt sich um den Wert des Tags nsx:local_endpoint_ip, das auf die Uplink-Schnittstelle des PCG angewendet wird.

- 4 Erstellen Sie eine **Routenbasierte IPSec-Sitzung** zwischen dem PCG und der Dienst-Appliance in Ihrer Public Cloud (wird vorzugsweise in der Transit-VPC bzw. dem Transit-VNet gehostet).

Option	Beschreibung
<b>Typ</b>	Bestätigen Sie, dass dieser Wert auf <b>Routenbasiert</b> festgelegt ist.
<b>VPN-Dienst</b>	Wählen Sie den in Schritt 2 hinzugefügten VPN-Dienst aus.
<b>Lokaler Endpoint</b>	Wählen Sie den in Schritt 3 erstellten lokalen Endpoint aus.
<b>Remote-IP</b>	Geben Sie die private IP-Adresse der Dienst-Appliance ein.  <b>Hinweis</b> Wenn der Zugriff auf die Dienst-Appliance mithilfe einer öffentlichen IP-Adresse möglich ist, weisen Sie der logischen Endpoint-IP (auch als sekundäre IP bezeichnet) der Uplink-Schnittstelle des PCG eine öffentliche IP-Adresse zu.

Option	Beschreibung
<b>Tunnelschnittstelle</b>	Dieses Subnetz muss mit dem Subnetz der Dienst-Appliance für den VPN-Tunnel übereinstimmen. Geben Sie den Subnetzwert ein, den Sie in der Dienst-Appliance für den VPN-Tunnel festgelegt haben, oder notieren Sie sich den hier eingegebenen Wert, um sicherzustellen, dass dasselbe Subnetz beim Einrichten des VPN-Tunnels in der Dienst-Appliance verwendet wird.  <b>Hinweis</b> Sie konfigurieren BGP in dieser Tunnelschnittstelle. Siehe <a href="#">Konfigurieren von BGP und Route Redistribution</a> .
<b>Remote-ID</b>	Geben Sie die private IP-Adresse Ihrer Dienst-Appliance in der Public Cloud ein.
<b>IKE-Profil</b>	Die IPSec-VPN-Sitzung muss einem IKE-Profil zugeordnet werden. Wenn Sie ein Profil erstellt haben, wählen Sie es im Dropdown-Menü aus. Sie können auch das Standardprofil verwenden.

## Nächste Schritte

### [Konfigurieren von BGP und Route Redistribution](#)

## Konfigurieren von BGP und Route Redistribution

Konfigurieren Sie BGP zwischen dem PCG und der Dienst-Appliance über den IPSec-VPN-Tunnel.

Sie legen BGP-Nachbarn auf der Schnittstelle des IPSec-VPN-Tunnels fest, die Sie zwischen PCG und der Dienst-Appliance eingerichtet haben. Weitere Informationen finden Sie unter [Konfigurieren des BGP-Protokolls](#).

BGP muss ähnlich wie auf Ihrer Dienst-Appliance eingerichtet werden. In der Dokumentation finden Sie ausführliche Informationen zum entsprechenden Dienst in der Public Cloud.

Richten Sie Route Redistribution im nächsten Schritt folgendermaßen ein:

- Das PCG kündigt seine Standardroute (0.0.0.0/0) bei der Dienst-Appliance an.
- Die Dienst-Appliance kündigt die VSIP beim PCG an. Hierbei handelt es sich um dieselbe IP-Adresse, die auch beim Registrieren des Diensts verwendet wird. Siehe [Erstellen der Dienstdefinition und eines entsprechenden virtuellen Endpoints](#).

**Hinweis** Wenn Ihre Dienst-Appliance in einem Hochverfügbarkeitspaar bereitgestellt wird, kündigen Sie dieselbe VSIP aus beiden Dienst-Appliances an.

## Voraussetzungen

## Verfahren

- 1 Navigieren Sie zu **Netzwerk > Tier-O-Gateways**
- 2 Wählen Sie das automatisch erstellte Tier-O-Gateway für die Transit-VPC bzw. das Transit-VNet mit dem Beispielnamen `cloud-t0-vpc-6bcd2c13` aus und klicken Sie auf **Bearbeiten**.

3 Klicken Sie auf die Zahl oder das Symbol neben **BGP-Nachbarn** unter dem Abschnitt **BGP**.

4 Beachten Sie die folgenden Konfigurationen:

Option	Beschreibung
<b>IP-Adresse</b>	Verwenden Sie die IP-Adresse, die in der Tunnelschnittstelle der Dienst-Appliance für das VPN zwischen dem PCG und der Dienst-Appliance konfiguriert wurde.
<b>Remote-AS-Nummer</b>	Diese Zahl muss mit der AS-Nummer der Dienst-Appliance in Ihrer Public Cloud übereinstimmen.

5 (Erforderlich) Richten Sie im Abschnitt **Statische Route** eine statische Route zur Standardroute (0.0.0.0/0) des PCG ein.

6 Wählen Sie im Abschnitt **Route Redistribution** die mit der Standardroute verknüpfte statische Route aus.

#### Nächste Schritte

#### [Einrichten von Umleitungsregeln](#)

### Einrichten von Umleitungsregeln

Umleitungsregeln können gemäß Ihren Anforderungen angepasst werden.

Nach Abschluss des erstmaligen Setups können Sie Umleitungsregeln erstellen und bearbeiten, die zum Umleiten verschiedener Datenverkehrstypen für die NSX-verwalteten Arbeitslast-VMs über die Dienst-Appliance benötigt werden.

#### Voraussetzungen

Das gesamte Service Insertion-Setup muss abgeschlossen sein, bevor Umleitungsregeln erstellt werden können.

#### Verfahren

1 Navigieren Sie zu **Sicherheit > Nord-Süd-Firewall > Netzwerk-Introspektion (N-S)**

2 Klicken Sie auf **Richtlinie hinzufügen**.

Option	Beschreibung
<b>Domäne</b>	NSX-T Data Center 2.4: Wählen Sie die Domäne aus, die automatisch für das Tier-O-Gateway dieser Transit-VPC bzw. dieses Transit-VNet erstellt wurde, z. B. cloud-vpc-6bcd2c13. NSX-T Data Center 2.4.1: Das Domänenobjekt ist nicht auf der Benutzeroberfläche sichtbar. Keine Aktion erforderlich.
<b>Umleiten an:</b>	Wählen Sie den Namen des virtuellen Endpoints aus, den Sie beim Registrieren des Diensts für diese Dienst-Appliance erstellt haben. Siehe <a href="#">Erstellen der Dienstdefinition und eines entsprechenden virtuellen Endpoints</a> .

- 3 Wählen Sie die neue Richtlinie aus und klicken Sie auf **Regel hinzufügen**. Beachten Sie die folgenden Werte, die für Service Insertion spezifisch sind:

Option	Beschreibung
<b>Quellen</b>	Wählen Sie eine Gruppe von Subnetzen aus, deren Datenverkehr umgeleitet werden muss, wie z. B. eine Gruppe NSX-verwalteter Arbeitslast-VMs.
<b>Ziele</b>	Wählen Sie eine Liste der IP-Zieladressen oder Dienste aus. Beispielsweise <b>Google</b> zum Durchleiten durch die Dienst-Appliance.
<b>Angewendet auf</b>	Wählen Sie den Uplink-Port des aktiven und Standby-PCG aus.
<b>Aktion</b>	Wählen Sie <b>Umleiten</b> aus.

## Aktivieren von Syslog-Weiterleitung

NSX Cloud unterstützt Syslog-Weiterleitung.

Sie können Syslog-Weiterleitung für Verteilte-Firewall-Pakete (DFW-Pakete) auf verwalteten VMs aktivieren. Weitere Informationen finden Sie unter **Konfigurieren der Remoteprotokollierung** im *Handbuch zur Fehlerbehebung von NSX-T Data Center*.

Gehen Sie wie folgt vor:

### Verfahren

- 1 Melden Sie sich unter Verwendung des Jump-Hosts bei PCG an.
- 2 Geben Sie **nsxcli** ein, um die Befehlszeilenschnittstelle (CLI) von NSX-T Data Center zu öffnen.
- 3 Geben Sie die folgenden Befehle zum Aktivieren der DFW-Protokollweiterleitung ein:

```
nsx-public-cloud-gateway> set gw-controller vm-log-forwarding enabled
nsx-public-cloud-gateway> set logging-server <server-IP-address> proto udp level info messageid
FIREWALL-PKTLOG
```

Nachdem dies eingerichtet ist, sind NSX Agent-DFW-Paketprotokolle unter `/var/log/syslog` auf PCG verfügbar.

- 4 Um Protokollweiterleitung je VM zu aktivieren, geben Sie den folgenden Befehl ein:

```
nsx-public-cloud-gateway> set gw-controller vm-log-forwarding enabled <vm-id>
```

## FAQ

Hier finden Sie eine Auflistung einiger häufig gestellter Fragen.

**Ich habe meine VM korrekt gekennzeichnet und den Agenten installiert, aber meine VM steht unter Quarantäne. Was soll ich tun?**

Versuchen Sie Folgendes, wenn dieses Problem auftritt:

- Überprüfen Sie, ob das NSX Cloud-Tag: `nsx.managed` und dessen Wert: `default` korrekt eingegeben wurden. Beachten Sie dabei Groß- und Kleinschreibung.
- Synchronisieren Sie das AWS- oder Microsoft Azure-Konto erneut über CSM.
  - Melden Sie sich bei CSM an.
  - Navigieren Sie zu **Clouds > AWS/Azure > Konten**.
  - Klicken Sie in der Public-Cloud-Konto-Kachel auf **Aktionen** und klicken Sie auf **Account erneut synchronisieren**.

## Was soll ich tun, wenn ich nicht auf meine Arbeitslast-VM zugreifen kann?

Unter bestimmten, selten auftretenden Bedingungen können Sie die Verbindung zu Ihren verwalteten Linux- oder Windows-basierten Arbeitslast-VMs verlieren. Führen Sie die folgenden Schritte aus:

### Aus Ihrer Public Cloud (AWS oder Microsoft Azure)

- Stellen Sie sicher, dass alle Ports auf der VM, einschließlich der von NSX Cloud verwalteten Ports, der Betriebssystem-Firewall (Microsoft Windows oder IPTables) und NSX-T Data Center ordnungsgemäß konfiguriert sind, um Datenverkehr zuzulassen,

Um beispielsweise ping für eine VM zuzulassen, muss Folgendes richtig konfiguriert sein:

- Sicherheitsgruppe in AWS oder Microsoft Azure. Weitere Informationen hierzu finden Sie unter [Verwalten der Quarantäne-Richtlinie](#).
- NSX-T Data Center-DFW-Regeln Weitere Informationen finden Sie unter [DFW-Regeln für NSX-verwaltete Arbeitslast-VMs](#).
- Windows-Firewall oder IPTables unter Linux.
- Versuchen Sie, das Problem zu beheben, indem Sie sich über SSH oder andere Methoden, wie z. B. die serielle Konsole in Microsoft Azure, bei der VM anmelden.
- Sie können die gesperrte VM neu starten.
- Wenn Sie immer noch nicht auf die VM zugreifen können, hängen Sie eine sekundäre NIC an die Arbeitslast-VM an, von der aus Sie auf diese Arbeitslast-VM zugreifen können.