

# Administratorhandbuch für NSX-T Data Center

Geändert am 6. Mai 2022  
VMware NSX-T Data Center 2.5

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

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

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

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

Copyright © 2022 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

# Inhalt

## Grundlegende Informationen zur Verwaltung von VMware NSX-T Data Center 13

### 1 Übersicht über NSX Manager 14

### 2 Tier-0-Gateways 17

- Hinzufügen eines Tier-0-Gateways 18
- Erstellen einer IP-Präfix-Liste 21
- Erstellen einer Community-Liste 23
- Konfigurieren einer statischen Route 24
- Erstellen einer Route Map 24
- Verwenden regulärer Ausdrücke zum Zuordnen von Community-Listen beim Hinzufügen von Route Maps 27
- Konfigurieren des BGP-Protokolls 28
- Konfigurieren von BFD 31
- Konfigurieren der IPv6-Ebene-3-Weiterleitung 32
- Erstellen von SLAAC- und DAD-Profilen für die IPv6-Adresszuweisung 33

### 3 Tier-1-Gateway 35

- Tier-1-Gateway hinzufügen 35

### 4 Segmente 38

- Segmentprofile 38
  - Grundlegendes zum QoS-Segmentprofil 39
  - Grundlegendes zum Segmentprofil für die IP Discovery 42
  - Grundlegendes zum Spoofguard-Segmentprofil 44
  - Grundlegendes zu Segmentprofilen für die Segmentsicherheit 46
  - Grundlegendes zum Segmentprofil für die MAC Discovery 48
- Hinzufügen eines Segments 50

### 5 Virtual Private Network (VPN) 52

- Grundlegendes zu IPSec-VPNs 53
  - Verwendung von richtlinienbasiertem IPSec-VPN 54
  - Verwenden von routenbasiertem IPSec-VPN 55
- Grundlegendes zu Layer 2-VPN 56
- Hinzufügen von VPN-Diensten 57
  - Hinzufügen eines IPSec-VPN-Dienstes 59
  - Hinzufügen eines L2-VPN-Diensts 61

Hinzufügen von IPSec-VPN-Sitzungen	64
Hinzufügen einer richtlinienbasierten IPSec-Sitzung	64
Hinzufügen einer routenbasierten IPSec-Sitzung	69
Informationen zu unterstützten Compliance-Suites	73
Grundlegendes zum TCP-MSS Clamping	74
Hinzufügen von L2-VPN-Sitzungen	74
Hinzufügen einer L2-VPN-Server-Sitzung	74
Hinzufügen einer L2-VPN-Clientsitzung	77
Herunterladen der L2-VPN-Konfigurationsdatei der Remoteseite	78
Hinzufügen von lokalen Endpoints	80
Hinzufügen von Profilen	81
Hinzufügen von IKE-Profilen	82
Hinzufügen von IPSec-Profilen	85
Hinzufügen von DPD-Profilen	88
Hinzufügen eines autonomen Edge als L2-VPN-Client	89
Überprüfen des realisierten Zustands einer IPSec-VPN-Sitzung	92
Überwachung und Fehlerbehebung von VPN-Sitzungen	95
<b>6 Netzwerkadressübersetzung (NAT)</b>	<b>96</b>
Konfigurieren von NAT auf einem Gateway	96
<b>7 Load Balancing</b>	<b>99</b>
Wichtige Load Balancer-Konzepte	100
Skalieren von Load Balancer-Ressourcen	100
Unterstützte Load Balancer-Funktionen	101
Load Balancer-Topologien	102
Einrichten von Load Balancer-Komponenten	104
Hinzufügen von Load Balancern	104
Hinzufügen einer aktiven Überwachung	106
Hinzufügen einer passiven Überwachung	110
Hinzufügen eines Serverpools	112
Einrichten von Komponenten des virtuellen Servers	117
Für Serverpools und virtuelle Server erstellte Gruppen	142
<b>8 Weiterleitungsrichtlinien</b>	<b>144</b>
Hinzufügen oder Bearbeiten von Weiterleitungsrichtlinien	145
<b>9 IP-Adressverwaltung (IPAM)</b>	<b>147</b>
Hinzufügen einer DNS-Zone	147
Hinzufügen eines DNS-Weiterleitungsdiensts	148
Hinzufügen eines DHCP-Servers	149



Konfigurieren eines DHCP-Relay-Servers für ein Tier-0- oder Tier-1-Gateway	150
Hinzufügen eines IP-Adressenpools	151
Hinzufügen eines IP-Adressblocks	152

## 10 Sicherheit 153

Überblick über die Sicherheitskonfiguration	153
Sicherheit – Terminologie	154
Identitätsbasierte Firewall	154
Workflow für die identitätsbasierte Firewall	155
Kontextprofil der Schicht 7	158
Workflow für Firewallregel der Schicht 7	160
Attribute	161
Verteilte Firewall	165
Firewall-Entwürfe	166
Hinzufügen einer verteilten Firewall	169
Protokolle des verteilten Firewallpakets	173
Auswählen einer Standard-Konnektivitätsstrategie	175
Verwalten einer Firewall-Ausschlussliste	176
Filtern bestimmter Domänen (FQDN/URLs)	176
Erweitern von Sicherheitsrichtlinien auf physische Arbeitslasten	178
Freigegebene Adresssätze	185
Ost-West-Netzwerksicherheit – Verkettung von Drittanbieterdiensten	185
Wichtige Konzepte des Netzwerkschutzes (Ost-West)	186
NSX-T Data Center-Anforderungen für den Ost-West-Datenverkehr	187
Allgemeine Aufgaben für die Ost-West-Netzwerksicherheit	187
Bereitstellen eines Diensts für die Selbstprüfung von Ost-West-Datenverkehr	188
Hinzufügen eines Dienstprofils	190
Hinzufügen einer Dienstkette	190
Hinzufügen von Umleitungsregeln für Ost-West-Datenverkehr	192
Konfigurieren einer Gateway-Firewall	194
Hinzufügen von Regeln und Richtlinien für eine Gateway-Firewall	194
Nord-Süd-Netzwerksicherheit – Einfügen eines Drittanbieterdiensts	198
Allgemeine Aufgaben für die Nord-Süd-Netzwerksicherheit	198
Bereitstellen eines Diensts für die Selbstprüfung von Nord-Süd-Datenverkehr	198
Konfigurieren der Umleitung des Datenverkehrs	201
Hinzufügen von Umleitungsregeln für Nord-Süd-Datenverkehr	202
Überwachung der Umleitung des Datenverkehrs	203
Endpoint-Schutz	204
Grundlegendes zum Endpoint-Schutz	204
Konfigurieren von Endpoint-Schutz	209
Verwalten des Endpoint-Schutzes	225

- Sicherheitsprofile 240
  - Erstellen eines Sitzungs-Timers 240
  - Flood Protection 242
  - Konfigurieren der DNS-Sicherheit 245
  - Gruppen-zu-Profil-Vorrang verwalten 246

## 11 Bestand 248

- Hinzufügen eines Diensts 248
- Hinzufügen einer Gruppe 249
- Hinzufügen eines Kontextprofils 251

## 12 Überwachung 253

- Hinzufügen eines Firewall-IPFIX-Profiles 253
- Hinzufügen eines Switch-IPFIX-Profiles 254
- Hinzufügen eines IPFIX-Collectors 256
- Hinzufügen eines Port-Mirroring-Profiles 256
- Simple Network Management-Protokoll (SNMP) 257
- Verwenden von vRealize Log Insight für die Systemüberwachung 258
- Verwenden von vRealize Operations Manager für die Systemüberwachung 259
- Verwenden von vRealize Network Insight Cloud für die Systemüberwachung 264
- Erweiterte Überwachungstools 279
  - Anzeigen der Portverbindungsinformationen 279
  - Traceflow 279
  - Überwachen von Port-Mirroring-Sitzungen 282
  - Konfigurieren von Filtern für eine Port-Mirroring-Sitzung 286
  - Konfigurieren von IPFIX 287
  - Überwachen einer Logischer Switch Port-Aktivität 457

## 13 Logische Switches 458

- Grundlegendes zu den BUM-Frame-Replizierungsmodi 459
- Erstellen eines logischen Switches 461
- Verbinden einer VM mit einem logischen Switch 462
  - Anfügen einer auf vCenter Server gehosteten VM an einen logischen NSX-T Data Center-Switch 463
  - Verknüpfen einer auf eigenständigem ESXi gehosteten VM mit einem logischen NSX-T Data Center-Switch 464
  - Anfügen einer auf KVM-Hosts gehosteten VM an einen logischen NSX-T Data Center-Switch 470
- Erstellen eines logischen Switch Ports 471
- Testen der Schicht-2-Konnektivität 472
- Erstellen eines logischen VLAN-Switch für den NSX Edge-Uplink 475
- Switching-Profile für logische Switches und logische Ports 477

Grundlegendes zum QoS-Switching-Profil	479
Grundlegendes zum Switching-Profil für Port-Mirroring	482
Grundlegendes zum Switching-Profil für die IP Discovery	485
Grundlegendes zu SpoofGuard	487
Grundlegendes zum Switching-Profil für die Switch-Sicherheit	489
Grundlegendes zum Switching-Profil für die MAC-Verwaltung	492
Zuordnen eines benutzerdefinierten Profils zu einem logischen Switch	493
Zuordnen eines benutzerdefinierten Profils zu einem logischen Port	495
Erweiterter Netzwerkstapel	496
Automatisches Zuweisen von logischen ENS-Kernen	496
Konfigurieren von Inter-VLAN-Routing für Gäste	497
Schicht 2-Bridging	499
Erstellen eines Edge-Bridge-Profiles	499
Konfigurieren von Edge-basiertem Bridging	500
Erstellen eines Bridge-gestützten logischen Schicht-2-Switches	503

## 14 Logische Router 506

Logischer Tier-1-Router	506
Erstellen eines logischen Tier-1-Routers	508
Hinzufügen eines Downlink-Ports auf einem logischen Tier-1-Router	510
Hinzufügen eines VLAN-Ports auf einem logischen Tier-0- oder Tier-1-Router	511
Konfigurieren von Routen-Advertisement auf einem logischen Tier-1 Router	511
Konfigurieren einer statischen Route auf einem logischen Tier-1-Router	513
Erstellen eines eigenständigen logischen Tier-1-Routers	515
Logischer Tier-0 Router	517
Erstellen eines logischen Tier-0-Routers	518
Anfügen von Tier-0 und Tier-1	520
Verbinden eines logischen Tier-0 Routers mit einem logischen VLAN-Switch für den NSX Edge-Uplink	522
Hinzufügen eines Loopback-Router-Ports	526
Hinzufügen eines VLAN-Ports auf einem logischen Tier-0- oder Tier-1-Router	526
Konfigurieren einer statischen Route	527
BGP-Konfigurationsoptionen	531
Konfigurieren von BFD auf einem logischen Tier-0 Router	538
Aktivieren von Route Redistribution auf dem logischen Tier-0 Router	538
Grundlegendes zum ECMP-Routing	541
Erstellen einer IP-Präfix-Liste	545
Erstellen einer Community-Liste	546
Erstellen einer Route Map	547
Konfigurieren des Timers für die Weiterleitung der Aktiv-Benachrichtigung	548

## 15 Erweitertes NAT 550

Netzwerkadressübersetzung (NAT)	550
Tier-1-NAT	552
Tier-0-NAT	559
Reflexive NAT	560

## **16** Erweiterte Gruppierungsobjekte 564

Erstellen eines IP Sets	564
Erstellen eines IP-Pools	565
Erstellen eines MAC Set	565
Erstellen einer NS-Gruppe	566
Konfigurieren von Diensten und Dienstgruppen	568
Erstellen eines NS-Dienstes	569
Verwalten von Tags für eine virtuelle Maschine	569

## **17** Erweitertes DHCP 571

DHCP	571
Erstellen eines DHCP-Serverprofils	572
Erstellen eines DHCP-Servers	572
Anfügen eines DHCP-Servers an einen logischen Switch	573
Trennen eines DHCP-Servers von einem logischen Switch	573
Erstellen eines DHCP-Relay-Profils	574
Erstellen eines DHCP-Relay-Dienstes	574
Hinzufügen eines DHCP-Relay-Dienstes zu einem Port für einen logischen Router	574
Löschen einer DHCP-Lease	575
Metadaten-Proxyserver	575
Hinzufügen eines Metadaten-Proxyservers	576
Anfügen eines Metadaten-Proxyserver an einen logischen Switch	577
Trennen eines Metadaten-Proxy-Servers von einem logischen Switch	577

## **18** Erweiterte IP-Adressverwaltung 579

Verwalten von IP-Blöcken	579
Verwalten von Subnetzen für IP-Blöcke	580

## **19** Erweitertes Load Balancing 581

Wichtige Load Balancer-Konzepte	582
Konfigurieren von Load Balancer-Komponenten	583
Erstellen eines Load Balancers	583
Konfigurieren einer aktiven Systemzustandsüberwachung	584
Konfigurieren von passiven Systemzustandsüberwachungen	588
Hinzufügen eines Serverpools für das Load Balancing	590
Konfigurieren der Komponenten des virtuellen Servers	593

## 20 Erweiterte Firewall 617

- Hinzufügen oder Löschen einer Firewallregel zu bzw. von einem logischen Router 617
- Konfigurieren der Firewall für den Bridge-Port eines logischen Switches 618
- Firewallabschnitte und Firewallregeln 619
  - Aktivieren und Deaktivieren einer verteilten Firewall 619
  - Hinzufügen eines Firewallregelabschnitts 620
  - Löschen eines Firewallregelabschnitts 621
  - Aktivieren und Deaktivieren von Abschnittsregeln 621
  - Aktivieren und Deaktivieren von Abschnittsprotokollen 622
  - Konfigurieren einer Firewall-Ausschlussliste 622
- Informationen über Firewallregeln 623
  - Hinzufügen einer Firewallregel 624
  - Löschen einer Firewallregel 627
  - Bearbeiten der standardmäßigen Regel für die verteilte Firewall 627
  - Ändern der Reihenfolge von Firewallregeln 629
  - Filtern der Firewallregeln 629

## 21 Vorgänge und Verwaltung 631

- Anzeigen von Überwachungs-Dashboards 632
- Nutzung und Kapazität von Objektkategorien anzeigen 634
- Überprüfen des Umsetzungsstatus einer Konfigurationsänderung 636
- Suchen nach Objekten 640
- Filtern nach Objektattributen 642
- Hinzufügen eines Compute Managers 642
- Hinzufügen von Active Directory 645
- Hinzufügen eines LDAP-Servers 646
- Synchronisieren von Active Directory 647
- Verwalten von Benutzerkonten und der rollenbasierten Zugriffssteuerung 648
  - Verwalten eines Benutzerkennworts 648
  - Zurücksetzen der Kennwörter einer Appliance 649
  - Authentifizierungsrichtlinien-Einstellungen 651
  - Abrufen des Certificate Thumbprint von einem vIDM-Host 652
  - Konfigurieren der Integration von VMware Identity Manager 653
  - Validieren der VMware Identity Manager-Funktionalität 656
  - Zeitsynchronisierung zwischen NSX Manager, vIDM und zugehörigen Komponenten 658
  - Rollenbasierte Zugriffssteuerung 659
  - Hinzufügen einer Rollenzuweisung oder Prinzipalidentität 670
- Sichern und Wiederherstellen von NSX Manager 672
  - Konfigurieren von Sicherungen 673
  - Entfernen alter Sicherungen 675
  - Auflisten der verfügbaren Sicherungen 675

Wiederherstellen einer Sicherung	676
Sicherung und Wiederherstellung während Upgrades	679
Entfernen der NSX-T Data Center-Erweiterung aus vCenter Server	680
Verwalten des NSX Manager-Clusters	680
Anzeigen der Konfiguration und des Status des NSX Manager-Clusters	681
Herunterfahren und Einschalten des NSX Manager-Clusters	684
Neustarten eines NSX Manager	684
Ändern der IP-Adresse eines NSX Manager	684
Ändern der Größe eines NSX Manager-Knotens	686
Hinzufügen und Entfernen eines ESXi-Host-Transportknotens zu und von vCenter Servern	687
Ersetzen eines NSX Edge-Transportknotens in einem NSX Edge-Cluster	688
Ersetzen eines NSX Edge-Transportknotens über die NSX Manager-Benutzeroberfläche	688
Ersetzen eines NSX Edge-Transportknotens mithilfe der API	689
Wiederherstellen von NSX-T, wenn vCenter Server verlorengeht und nicht wiederhergestellt werden kann	691
Bereitstellung von NSX-T Data Center für mehrere Sites	693
Konfigurieren von Appliances	700
Hinzufügen eines Lizenzschlüssels und Generieren eines Lizenznutzungsberichts	701
Einrichten von Zertifikaten	702
Importieren eines Zertifikats	703
Erstellen einer Datei für die Zertifikatsignieranforderung	703
Importieren eines CA-Zertifikats	705
Erstellen eines selbstsignierten Zertifikats	706
Ersetzen des Zertifikats für einen NSX Manager-Knoten oder eine virtuelle NSX Manager-Cluster-IP	707
Importieren einer Zertifikatswiderrufsliste	708
Konfigurieren von NSX Manager zum Abrufen einer Zertifikatswiderrufsliste	709
Importieren eines Zertifikats für eine CSR	710
Speichern von öffentlichen Zertifikaten und privaten Schlüsseln	710
Übereinstimmungsbasierte Konfiguration	710
Anzeigen des Übereinstimmungsstatus	711
Codes für Compliance-Statusberichte	712
Konfigurieren des globalen FIPS-Übereinstimmungsmodus für den Load Balancer	715
Erfassen von Support-Paketen	718
Protokollmeldungen und Fehlercodes	719
Konfigurieren der Remoteprotokollierung	721
Protokollmeldungs-IDs	729
Fehlerbehebung für Probleme mit Syslog	730
Konfigurieren der seriellen Protokollierung auf einer Appliance-VM	731
Programm zur Verbesserung der Benutzerfreundlichkeit	731
Bearbeiten der CEIP-Konfiguration (Einstellungen bzgl. der Teilnahme am „Programm zur Verbesserung der Benutzerfreundlichkeit“)	732

- Hinzufügen von Tags zu einem Objekt 732
- Suchen nach dem SSH-Fingerabdruck eines Remote-Servers 734
- Anzeigen von Daten über Anwendungen, die auf virtuellen Maschinen ausgeführt werden 735
- Konfigurieren eines externen Load Balancer 735

## 22 Verwenden von NSX Cloud 737

- Eine kurze Einführung in Cloud Service Manager 737
  - Clouds 738
  - System 743
- Bedrohungserkennung mit der NSX Cloud-Quarantäne-Richtlinie 746
  - Quarantäne-Richtlinie im NSX-erzwungener Modus 747
  - Quarantäne-Richtlinie im Native Cloud-erzwungener Modus 753
  - Verschieben von VMs in die Whitelist 754
- NSX-erzwungener Modus 755
  - Derzeit unterstützte Betriebssysteme für Arbeitslast-VMs 755
  - Einbinden von VMs im NSX-erzwungener Modus 756
  - Verwalten von VMs im NSX-erzwungener Modus 766
- Native Cloud-erzwungener Modus 767
  - Verwalten von VMs im Native Cloud-erzwungener Modus 767
- NSX-T Data Center-Funktionen mit Support in NSX Cloud 772
  - Gruppen-VMs mit NSX-T Data Center und Public-Cloud-Tags 773
  - Verwenden von Native Cloud-Diensten 778
  - Diensteinfügung für Ihre Public Cloud 779
  - Aktivieren von NAT auf NSX-verwalteten VMs 786
  - Aktivieren von Syslog-Weiterleitung 787
  - Einrichten von VPN im erzwungenen NSX-Modus 787
- Häufig gestellte Fragen 792

## 23 Verwenden von NSX Intelligence 795

- Erste Schritte mit NSX Intelligence 795
  - Tour der NSX Intelligence-Startseite 796
  - Kennenlernen von NSX Intelligence-Grafikelementen 798
- Grundlegendes zu NSX Intelligence-Ansichten und -Flows 800
  - Arbeiten mit der Ansicht „Gruppen“ 801
  - Arbeiten mit der Ansicht „VMs“ 806
  - Arbeiten mit Datenverkehrsflows 808
- Arbeiten mit NSX Intelligence-Empfehlungen 810
  - Verstehen von NSX Intelligence-Empfehlungen 810
  - Generieren einer neuen NSX Intelligence-Empfehlung 811
  - Überprüfen und Veröffentlichen einer generierten Empfehlung 813
- Sichern und Wiederherstellen von NSX Intelligence 815

Konfigurieren von NSX Intelligence-Sicherungen	816
Sichern von NSX Intelligence	817
NSX Intelligence-Sicherungen wiederherstellen	818
Fehlerbehebung bei NSX Intelligence-Problemen	819
Überprüfen des Status der NSX Intelligence-Appliance	819
Erfassen von NSX Intelligence-Support-Paketen	824



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

## Zeitpunkt der Verwendung von Richtlinien- oder erweiterten Schnittstellen

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

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

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


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

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

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

## Verwenden der Richtlinienschnittstelle

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

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

## Wo Sie die Richtlinienschnittstellen und erweiterten Schnittstellen finden

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

Tabelle 1-2. Richtlinienchnittstellen und erweiterte Schnittstellen

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

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

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

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

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

Tabelle 1-3. Objektnamen

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

# Tier-0-Gateways

## 2

Ein Tier-0 Gateway führt die Funktionen eines logischen Tier-0 Routers aus. Es verarbeitet Datenverkehr zwischen den logischen und physischen Netzwerken.

---

**NSX Cloud-Hinweis** Wenn Sie NSX Cloud verwenden, finden Sie unter [NSX-T Data Center-Funktionen mit Support in NSX 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.

---

**Hinweis** Der Begriff „Logischer Tier-0 Router“ wird auf der Registerkarte **Netzwerk und Sicherheit – Erweitert** verwendet, um auf ein Tier-0-Gateway zu verweisen.

---

Dieses Kapitel enthält die folgenden Themen:

- [Hinzufügen eines Tier-0-Gateways](#)
- [Erstellen einer IP-Präfix-Liste](#)
- [Erstellen einer Community-Liste](#)
- [Konfigurieren einer statischen Route](#)
- [Erstellen einer Route Map](#)
- [Verwenden regulärer Ausdrücke zum Zuordnen von Community-Listen beim Hinzufügen von Route Maps](#)
- [Konfigurieren des BGP-Protokolls](#)
- [Konfigurieren von BFD](#)
- [Konfigurieren der IPv6-Ebene-3-Weiterleitung](#)
- [Erstellen von SLAAC- und DAD-Profilen für die IPv6-Adresszuweisung](#)

## Hinzufügen eines Tier-0-Gateways

Ein Tier-0-Gateway besitzt Downlink-Verbindungen zu Tier-1-Gateways und Uplink-Verbindungen zu physischen Netzwerken.

Sie können den HA-Modus (Hochverfügbarkeit) 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**.

Wenn Sie Route Redistribution für das Tier-0- oder Tier-1-Gateway konfigurieren, können Sie aus zwei Gruppen mit Quellen auswählen: Tier-0-Subnetze und angekündigte Tier-1-Subnetze. Die Quellen in der Gruppe der Tier-0-Subnetze sind:

Quellentyp	Beschreibung
Verbundene Schnittstellen und Segmente	Dazu gehören Subnetze externer Schnittstellen, Subnetze der Dienstschnittstelle und Segment-Subnetze, die mit dem Tier-0-Gateway verbunden sind.
Statische Routen	Statische Routen, die Sie auf dem Tier-0-Gateway konfiguriert haben.
NAT-IP	NAT-IP-Adressen, die dem Tier-0-Gateway angehören und von NAT-Regeln erkannt werden, die auf dem Tier-0-Gateway konfiguriert sind.
Lokale IPsec-IP	IP-Adresse des lokalen IPSEC-Endpoints zum Einrichten von VPN-Sitzungen.
DNS-Weiterleitungs-IP	Listener-IP für DNS-Abfragen von Clients, wird auch als Quell-IP verwendet, um DNS-Abfragen an den vorgeschalteten DNS-Server weiterzuleiten.

Die Quellen in der Gruppe der angekündigten Tier-1-Subnetze sind:

Quellentyp	Beschreibung
Verbundene Schnittstellen und Segmente	Dazu gehören Segment-Subnetze, die mit dem Tier-1-Gateway verbunden sind und die Subnetze der Dienstschnittstelle, die auf dem Tier-1-Gateway konfiguriert sind.
Statische Routen	Statische Routen, die Sie auf dem Ebene-1-Gateway konfiguriert haben.

Quellentyp	Beschreibung
NAT-IP	NAT-IP-Adressen, die dem Tier-1-Gateway angehören und von NAT-Regeln erkannt werden, die auf dem Tier-1-Gateway konfiguriert sind.
LB-VIP	IP-Adresse des virtuellen Servers für Load Balancing.
LB SNAT-IP	IP-Adresse oder ein Bereich mit IP-Adressen, die vom Load Balancer für Quell-NAT verwendet werden.
DNS-Weiterleitungs-IP	Listener-IP für DNS-Abfragen von Clients, wird auch als Quell-IP verwendet, um DNS-Abfragen an den vorgeschalteten DNS-Server weiterzuleiten.
Lokaler IPSec-Endpoint	IP-Adresse des lokalen IPSec-Endpoints.

## 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** aus.
- 3 Klicken Sie auf **Tier-0-Gateway hinzufügen**.
- 4 Geben Sie einen Namen für das Gateway ein.
- 5 Wählen Sie einen HA-Modus (Hochverfügbarkeit) aus.

Der Standardmodus 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 (Optional) Wählen Sie einen NSX Edge-Cluster aus.
- 8 (Optional) Fügen Sie ein oder mehrere Tags hinzu.

9 (Optional) Klicken Sie auf **Zusätzliche Einstellungen**.

- a Geben Sie im Feld **Internes Transitsubnetz** ein Subnetz ein.

Dieses Subnetz wird für die Kommunikation zwischen Komponenten innerhalb dieses Gateways verwendet. Die Standardeinstellung lautet 169.254.0.0/28.

- b Geben Sie im Feld **TO-T1-Transitsubnetz** ein oder mehrere Subnetze ein.

Diese Subnetze werden für die Kommunikation zwischen diesem Gateway und allen mit ihm verknüpften Tier-1-Gateways verwendet. Nachdem Sie dieses Gateway erstellt und ein Tier-1-Gateway mit ihm verknüpft haben, wird die tatsächliche IP-Adresse angezeigt, die dem Link auf der Tier-O-Gateway-Seite und auf der Tier-1-Gateway-Seite zugewiesen ist. Die Adresse wird unter **Zusätzliche Einstellungen > Routerverbindungen** auf der Tier-O-Gateway-Seite und auf der Tier-1-Gateway-Seite angezeigt. Die Standardeinstellung lautet 100.64.0.0/16.

- c Wählen Sie ein **ND-Profil** und ein **DAD-Profil** für die IPv6-Adresskonfiguration aus.

Diese Profile werden zur Konfiguration der statusfreien Adressenautokonfiguration (SLAAC) und der Erkennung duplizierter Adressen (DAD) für IPv6-Adressen verwendet. Das Standardprofil wird erstellt.

10 Klicken Sie auf **Speichern**.

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

Wählen Sie mindestens eine der Quellen aus:

- Tier-O-Subnetze: **Statische Routen, NAT-IP, Lokale IPSec-IP, DNS-Weiterleitungs-IP, Verbundene Schnittstellen und Segmente**.

Unter **Verbundene Schnittstellen und Segmente** können Sie eine oder mehrere der folgenden Optionen auswählen: **Subnetz der Dienstschnittstelle, Subnetz der externen Schnittstelle, Subnetz der Loopback-Schnittstelle, Verbundenes Segment**.

- Angekündigte Tier-1-Subnetze: **DNS-Weiterleitungs-IP, Statische Routen, LB-VIP, NAT-IP, LB SNAT-IP, Lokaler IPSec-Endpoint, Verbundene Schnittstellen und Segmente**

Unter **Verbundene Schnittstellen und Segmente** können Sie **Subnetz der Dienstschnittstelle** und/oder **Verbundenes Segment** auswählen.

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

- a Klicken Sie auf **Schnittstelle hinzufügen**.

- b Geben Sie einen Namen ein.

- c Wählen Sie einen Typ aus.

Wenn der HA-Modus Aktiv/Standby lautet, können Sie **Extern, Dienst** und **Loopback** auswählen. Wenn der HA-Modus Aktiv/Aktiv ist, sind die Optionen **Extern** und **Loopback** verfügbar.



- d Geben Sie eine IP-Adresse im CIDR-Format ein.
  - e Wählen Sie ein Segment aus.
  - f Wenn der Schnittstellentyp nicht **Dienst** lautet, wählen Sie einen NSX Edge-Knoten aus.
  - g (Optional) Wenn der Schnittstellentyp nicht **Loopback** lautet, geben Sie einen MTU-Wert ein.
  - h (Optional) Fügen Sie Tags hinzu und wählen Sie ein ND-Profil aus.
- 13** (Optional) Wenn der HA-Modus Aktiv/Standby ist, klicken Sie auf **Festlegen** neben **Hochverfügbarkeits-VIP-Konfiguration**, um HA-VIP zu konfigurieren.
- Wenn HA-VIP konfiguriert wurde, ist das Tier-O-Gateway auch dann betriebsbereit, wenn ein Uplink nicht verfügbar ist. Der physische Router interagiert nur mit der Hochverfügbarkeits-VIP. HA-VIP soll mit statischem Routing und nicht mit BGP arbeiten.
- a Klicken Sie auf **Hochverfügbarkeits-VIP-Konfiguration hinzufügen**.
  - b Geben Sie eine IP-Adresse und eine Subnetzmaske ein.  
  
Das HA-VIP-Subnetz muss mit dem Subnetz der Schnittstelle identisch sein, an die es gebunden ist.
  - c Wählen Sie zwei Schnittstellen aus zwei verschiedenen Edge-Knoten aus.
- 14** Klicken Sie auf **Routing**, um IP-Präfix-Listen, Community-Listen, statische Routen und Route Maps hinzuzufügen.
- 15** Klicken Sie auf **BGP**, um BGP zu konfigurieren.
- 16** Klicken Sie auf **Erweiterte Konfiguration**, um zur Seite **Netzwerk und Sicherheit – Erweitert > Router** zu wechseln und zusätzliche Konfigurationen vorzunehmen.
- a Um den Weiterleitungsmodus der Schicht 3 zu konfigurieren, klicken Sie auf die Registerkarte **Globale Konfiguration**.
  - b Klicken Sie auf **Bearbeiten**.
  - c Wählen Sie **IPv4** oder **IPv4 und IPv6** aus.  
  
Die Standardeinstellung ist nur IPv4. Nur IPv6 wird nicht unterstützt. Um IPv6 zu aktivieren, wählen Sie **IPv4 und IPv6** aus.
  - d Klicken Sie auf **Speichern**.

## 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** aus.
- 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 Route Maps anhand von Community-Listen zu ermöglichen.

Community-Listen sind benutzerdefinierte Listen mit Community-Attributwerten. Diese Listen können für das Zuordnen oder Manipulieren des Communities-Attributs in BGP-Updatemeldungen verwendet werden.

Sowohl das BGP Communities-Attribut (RFC 1997) als auch das BGP Large Communities-Attribut (RFC 8092) werden unterstützt. Das BGP Communities-Attribut ist ein 32-Bit-Wert, der in zwei 16-Bit-Werte aufgeteilt ist. Das BGP Large Communities-Attribut verfügt über 3 Komponenten, die jeweils 4 Oktette lang sind.

In Route Maps kann das BGP Communities-Attribut oder das Large Communities-Attribut zugeordnet oder festgelegt werden. Mit dieser Funktion können Netzwerkbetreiber Netzwerkrichtlinien basierend auf dem BGP Communities-Attribut implementieren.

### 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** aus.
- 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 Liste der Communities an. Verwenden Sie für eine reguläre Community das Format „aa:nn“, z. B. 300:500. Verwenden Sie für eine größere Community das Format „aa:bb:cc“, z. B. 11:22:33. Beachten Sie, dass die Liste nicht gleichzeitig reguläre Communities und große Communities enthalten kann. Sie darf nur reguläre Communities oder nur große Communities enthalten.

Darüber hinaus können Sie eine oder mehrere der folgenden regulären Communities auswählen: Beachten Sie, dass sie nicht hinzugefügt werden können, wenn die Liste große Communities enthält.

- 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-O-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-O-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-O-Gateways** aus.
- 3 Um ein Tier-O-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 bei der Routenzuordnung 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](#).
- Einzelheiten zur Verwendung regulärer Ausdrücke zum Definieren von Übereinstimmungskriterien zur Route Map für Community-Listen finden Sie unter [Verwenden regulärer Ausdrücke zum Zuordnen von Community-Listen beim Hinzufügen von Route Maps](#).

### 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** aus.
- 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 Map hinzufügen**.
- 7 Geben Sie einen Namen ein und klicken Sie auf **Festlegen**, um Übereinstimmungskriterien hinzuzufügen.
- 8 Klicken Sie auf **Übereinstimmungskriterien hinzufügen**, um ein oder mehrere Übereinstimmungskriterien hinzuzufügen.

**9 Wählen Sie für jedes Kriterium **IP-Präfix** oder **Community-Liste** aus und klicken Sie auf **Festlegen**, um einen oder mehrere Übereinstimmungsausdrücke 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:
- **MATCH ANY** – führen Sie die festgelegte Aktion in der Route Map aus, wenn eine der Communities in der Community-Liste übereinstimmt.
  - **MATCH ALL** – führen Sie die festgelegte Aktion in der Route Map aus, wenn alle Communitys in der Community-Liste unabhängig von der Reihenfolge übereinstimmen.
  - **MATCH EXACT** – führen Sie die festgelegte Aktion in der Route Map aus, wenn alle Communitys in der Community-Liste in genau derselben Reihenfolge abgeglichen werden.
  - **MATCH COMMUNITY REGEXP** – führen Sie die festgelegte Aktion in der Route Map aus, wenn alle regulären Communities, die mit dem NRLI verknüpft sind, mit dem regulären Ausdruck übereinstimmen.
  - **MATCH LARGE COMMUNITY REGEXP** – führen Sie die festgelegte Aktion in der Route Map aus, wenn alle mit dem NRLI verknüpften großen Communities mit dem regulären Ausdruck übereinstimmen.

Sie sollten das Übereinstimmungskriterium `MATCH_COMMUNITY_REGEX` verwenden, um Routen mit Standard-Communities abzugleichen. Verwenden Sie das Übereinstimmungskriterium `MATCH_LARGE_COMMUNITY_REGEX`, um Routen mit großen Communities abzugleichen. Wenn Sie Routen zulassen möchten, die entweder den Wert einer Standard-Community oder einer großen Community enthalten, müssen Sie zwei Übereinstimmungskriterien erstellen. Wenn die Übereinstimmungsausdrücke im gleichen Übereinstimmungskriterium angegeben werden, sind nur die Routen zulässig, die sowohl die Standard-Community als auch große Communities enthalten.

Für jedes Übereinstimmungskriterium werden die Übereinstimmungsausdrücke in einem AND-Vorgang angewendet, d. h., alle Übereinstimmungsausdrücke müssen erfüllt sein, damit eine Übereinstimmung vorliegt. Wenn mehrere Übereinstimmungskriterien vorhanden sind, werden Sie in einem OR-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	Geben Sie eine Liste der Communities an. Verwenden Sie für eine reguläre Community das Format „aa:nn“, z. B. 300:500. Verwenden Sie für eine große Community das Format „aa:bb:cc“, z. B. 11:22:33. 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>
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 zulassen oder verweigern, die durch die IP-Präfixlisten oder Community-Listen für die Ankündigung übereinstimmen.

12 Klicken Sie auf **Speichern**.

## Verwenden regulärer Ausdrücke zum Zuordnen von Community-Listen beim Hinzufügen von Route Maps

Sie können reguläre Ausdrücke verwenden, um die Übereinstimmungskriterien für die Route Map für Community-Listen zu definieren. Reguläre BGP-Ausdrücke basieren auf regulären POSIX 1003.2-Ausdrücken.

Die folgenden Ausdrücke sind eine Teilmenge der regulären POSIX-Ausdrücke.

Ausdruck	Beschreibung
.	Entspricht einem einzelnen Zeichen.
*	Entspricht 0 oder mehr Vorkommen von Mustern.
+	Entspricht 1 oder mehr Vorkommen von Mustern.
?	Entspricht 0 oder 1 Vorkommen von Mustern.
^	Entspricht dem Zeilenanfang.
\$	Entspricht dem Zeilenende.
—	Dieses Zeichen hat eine besondere Bedeutung in regulären BGP-Ausdrücken. Es entspricht einem Leerzeichen, Komma, AS-Satztrennzeichen {and} und AS-Verbundtrennzeichen (and). Entspricht auch dem Anfang der Zeile und dem Ende der Zeile. Daher kann dieses Zeichen für eine Übereinstimmung mit den AS-Grenzwerten verwendet werden. Technisch wird dieses Zeichen zu (^ [,{}() \$) ausgewertet.

Es folgen einige Beispiele für die Verwendung regulärer Ausdrücke in Route Maps:

Ausdruck	Beschreibung
↑ 101	Entspricht Routen mit einem Community-Attribut, das mit 101 beginnt.
^[0-9]+	Entspricht Routen mit einem Community-Attribut, das mit einer Zahl zwischen 0-9 und einer oder mehreren Instanzen einer solchen Zahl beginnt.

Ausdruck	Beschreibung
.*	Entspricht Routen, die ein beliebiges oder kein Community-Attribut aufweisen.
.+	Entspricht Routen mit einem Community-Wert.
^\$	Entspricht Routen, die keinen Community-Wert oder den Community-Wert Null aufweisen.

## Konfigurieren des BGP-Protokolls

Um den Zugriff zwischen Ihren VMs und der Außenwelt zu ermöglichen, können Sie eine externe oder interne BGP-Verbindung (eBGP oder iBGP) 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. Sie müssen auch die Remote-AS-Nummer konfigurieren. EBGP-Nachbarn müssen direkt verbunden sein und sich im selben Subnetz wie der Tier-0-Uplink befinden. Wenn Sie sich nicht im selben Subnetz befinden, sollte BGP-Multi-Hop verwendet werden.

BGPv6 wird für Single-Hop und für Multihop unterstützt. Ein BGPv6-Nachbar unterstützt nur IPv6-Adressen. Redistribution, Präfix-Liste und Route Maps 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.

Die Implementierung von ECMP auf NSX Edge basiert auf dem 5-Tupel der Protokollnummer, der Quell- und Zieladresse sowie dem Quell- und Zielpport.

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.

### 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** aus.
- 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.

Im Aktiv/Aktiv-Modus ist der Standard-ASN-Wert 65000 bereits eingetragen. Im Aktiv/Standby-Modus gibt es keinen ASN-Standardwert.

- b Klicken Sie auf die **BGP**-Umschaltfläche, um BGP zu aktivieren oder zu deaktivieren.

Im Aktiv/Aktiv-Modus ist **BGP** standardmäßig aktiviert. Im Aktiv/Standby-Modus ist **BGP** standardmäßig deaktiviert.

- 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. Standardmäßig ist die Option aktiviert.

Wenn sich das Gateway im Aktiv/Standby-Modus befindet, ist diese Funktion nicht verfügbar.

- 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 Wählen Sie im Feld **Graceful Restart Deaktivieren, Nur Helfer** oder **Graceful Restart und Helfer** aus.

Optional können Sie den **Graceful Restart-Timer** und den **Stale-Timer für Graceful Restart** ändern.

Standardmäßig ist der Modus „Graceful Restart“ auf **Nur Helfer** festgelegt. Der Hilfsmodus beseitigt und/oder reduziert Unterbrechungen des Datenverkehrs mit Routen eines Nachbarn, der einen „Graceful Restart“ durchführen kann. Der Nachbar muss während eines Neustarts seine Weiterleitungstabelle beibehalten können.

Die Funktion „Graceful Restart“ sollte nicht auf den Tier-0-Gateways aktiviert werden, da die BGP-Peerings von allen Gateways immer aktiv sind. Bei einem Failover erhöht die Funktion „Graceful Restart“ die Dauer, während der ein Remote-Nachbar ein alternatives Tier-0-Gateway auswählt. Dadurch wird die BFD-basierte Konvergenz verzögert.

Hinweis: Sofern die Tier-0-Konfiguration nicht von einer spezifischen Nachbarkonfiguration überschrieben wurde, gilt sie für alle BGP-Nachbarn.

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

Sie müssen die globale BGP-Konfiguration speichern, bevor Sie BGP-Nachbarn konfigurieren können.

## 7 Konfigurieren Sie **BGP-Nachbarn**.

- a Geben Sie die IP-Adresse des Nachbarn ein.
- b Aktivieren oder deaktivieren Sie **BFD**.
- c Geben Sie einen Wert für die **Remote-AS-Nummer** ein.

Geben Sie für iBGP die gleiche AS-Nummer wie in Schritt 4a ein. Geben Sie für eBGP die AS-Nummer des physischen Routers ein.

- d Konfigurieren Sie den **Filter für ausgehende Daten**.
- e Konfigurieren Sie den **Filter für eingehende Daten**.
- 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 Dienstanbieter miteinander verbunden sind. Diese Funktion gilt für alle Adressfamilien und kann nicht auf bestimmte Adressfamilien angewendet werden.

- g Im Feld **Quelladressen** können Sie eine Quelladresse auswählen, um eine Peering-Sitzung mit einem Nachbarn unter Verwendung dieser bestimmten Quelladresse einzurichten. Wenn Sie keine auswählen, wird vom Gateway automatisch eine ausgewählt.
- h Wählen Sie im Feld **IP-Adressfamilie** die Option **IPv4**, **IPv6** oder **Deaktiviert** aus.
- i Geben Sie einen Wert für den **Max. Hop-Grenzwert** ein.

- j Optional können Sie im Feld **Graceful Restart Deaktivieren**, **Nur Helfer** oder **Graceful Restart und Helfer** auswählen.

Option	Beschreibung
Keine ausgewählt	Der „Graceful Restart“ für diesen Nachbarn folgt der BGP-Konfiguration des Tier-O-Gateways.
<b>Deaktivieren</b>	<ul style="list-style-type: none"> <li>■ Wenn das Tier-O-Gateway-BGP mit <b>Deaktivieren</b> konfiguriert ist, wird der „Graceful Restart“ für diesen Nachbarn deaktiviert.</li> <li>■ Wenn das Tier-O-Gateway-BGP mit <b>Nur Helfer</b> konfiguriert ist, wird der „Graceful Restart“ für diesen Nachbarn deaktiviert.</li> <li>■ Wenn das Tier-O-Gateway-BGP mit <b>Graceful Restart und Helfer</b> konfiguriert ist, wird der „Graceful Restart“ für diesen Nachbarn deaktiviert.</li> </ul>
<b>Nur Helfer</b>	<ul style="list-style-type: none"> <li>■ Wenn das Tier-O-Gateway-BGP mit <b>Deaktivieren</b> konfiguriert ist, wird der „Graceful Restart“ für diesen Nachbarn als „Nur Helfer“ konfiguriert.</li> <li>■ Wenn das Tier-O-Gateway-BGP mit <b>Nur Helfer</b> konfiguriert ist, wird der „Graceful Restart“ für diesen Nachbarn als „Nur Helfer“ konfiguriert.</li> <li>■ Wenn das Tier-O-Gateway-BGP mit <b>Graceful Restart und Helfer</b> konfiguriert ist, wird der „Graceful Restart“ für diesen Nachbarn als „Nur Helfer“ konfiguriert.</li> </ul>
<b>Graceful Restart und Helfer</b>	<ul style="list-style-type: none"> <li>■ Wenn das Tier-O-Gateway-BGP mit <b>Deaktivieren</b> konfiguriert ist, wird der „Graceful Restart“ für diesen Nachbarn als „Graceful Restart und Helfer“ konfiguriert.</li> <li>■ Wenn das Tier-O-Gateway-BGP mit <b>Nur Helfer</b> konfiguriert ist, wird der „Graceful Restart“ für diesen Nachbarn als „Graceful Restart und Helfer“ konfiguriert.</li> <li>■ Wenn das Tier-O-Gateway-BGP mit <b>Graceful Restart und Helfer</b> konfiguriert ist, wird der „Graceful Restart“ für diesen Nachbarn als „Graceful Restart und Helfer“ konfiguriert.</li> </ul>

- k Klicken Sie auf **Timer und Kennwort**.

- l Geben Sie einen Wert für **BFD-Intervall** ein.

Die Einheit ist Millisekunden. Für einen Edge-Knoten, der auf einer VM ausgeführt wird, lautet der Minimalwert 1000. Bei einem Bare-Metal-Edge-Knoten lautet der Minimalwert 300.

- m Geben Sie einen Wert für **BFD-Multiplikator** ein.

- n Geben Sie einen Wert für **Hold Down-Zeit** ein.

- o Geben Sie einen Wert für **Keep Alive-Zeit** ein.

- p Geben Sie ein Kennwort ein.

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

- 8 Klicken Sie auf **Speichern**.

## Konfigurieren von BFD

BFD (Bidirectional Forwarding Detection, Bidirektionale Weiterleitungserkennung) ist ein Protokoll zur Erkennung von Fehlern bei Weiterleitungspfaden.

## 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** aus.
- 3 Um ein Tier-0-Gateway zu bearbeiten, klicken Sie auf das Menüsymbol (drei Punkte) und wählen Sie **Bearbeiten**.
- 4 Klicken Sie auf **Erweiterte Konfiguration**.

Sie gelangen daraufhin auf die Seite **Netzwerk und Sicherheit – Erweitert > Router**. Das Gateway wird als einer der logischen Router angezeigt. Befolgen Sie die Anweisungen unter [Konfigurieren von BFD auf einem logischen Tier-0 Router](#).

## Konfigurieren der IPv6-Ebene-3-Weiterleitung

Die IPv4-Ebene-3-Weiterleitung ist standardmäßig aktiviert. Sie können auch die IPv6-Layer-3-Weiterleitung 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 > Tier-0-Gateways** aus.
- 3 Bearbeiten Sie ein Tier-0-Gateway, indem Sie auf das Menüsymbol (drei Punkte) klicken und **Bearbeiten** auswählen.
- 4 Klicken Sie auf **Erweiterte Konfiguration**.

Sie gelangen daraufhin auf die Seite **Netzwerk und Sicherheit – Erweitert > Router**. Das Gateway wird als einer der logischen Router angezeigt.

- 5 Klicken Sie auf die Registerkarte **Globale Konfiguration**.
- 6 Wählen Sie im Feld **L3-Weiterleitungsmodus** die Option **IPv4 und IPv6** aus.  
Nur IPv6 wird nicht unterstützt.
- 7 Bearbeiten Sie das Gateway erneut, indem Sie zur Registerkarte **Netzwerk** navigieren.
- 8 Navigieren Sie zu **Zusätzliche Einstellungen**.
  - a Es gibt keine konfigurierbaren IPv6-Adressen für **Internes Transitsubnetz**. Das System verwendet automatisch die lokalen IPv6-Adressen des Links.
  - b Geben Sie ein IPv6-Subnetz für **T0-T1-Transitsubnetze** ein.
- 9 Navigieren Sie zu **Schnittstellen** und fügen Sie eine Schnittstelle für IPv6 hinzu.

## Erstellen von SLAAC- und DAD-Profilen für die IPv6-Adresszuweisung

Wenn Sie IPv6 auf einer logischen Router-Schnittstelle verwenden, können Sie für die Zuweisung von IP-Adressen eine statusfreie Adress-Autokonfiguration (SLAAC) einrichten. SLAAC aktiviert die Adressierung eines Hosts basierend auf einem Netzwerkpräfix, das von einem lokalen Netzwerkrouter über Routerankündigungen angekündigt wird. Die Erkennung doppelter Adressen (DAD) stellt die Eindeutigkeit von IP-Adressen sicher.

### Voraussetzungen

Navigieren Sie zu **Netzwerk und Sicherheit – Erweitert > Router > Globale Konfiguration** und wählen Sie **IPv4 und IPv6** als **L3-Weiterleitungsmodus** aus.

### 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** aus.
- 3 Um ein Tier-0-Gateway zu bearbeiten, klicken Sie auf das Menüsymbol (drei Punkte) und wählen Sie **Bearbeiten**.
- 4 Klicken Sie auf **Zusätzliche Einstellungen**.
- 5 Klicken Sie zum Erstellen eines **ND-Profiles** (SLAAC-Profil) auf das Menüsymbol (drei Punkte) und wählen Sie **Neue erstellen** aus.
  - a Geben Sie einen Namen für das Profil ein.
  - b Wählen Sie einen Modus aus:
    - **Deaktiviert** – Routerankündigungsmeldungen sind deaktiviert.
    - **SLAAC mit DNS über RA** – die Adress- und DNS-Informationen werden mit der Routerankündigungsmeldung generiert.
    - **SLAAC mit DNS über DHCP** – die Adresse wird mit der Routerankündigungsmeldung generiert und die DNS-Informationen werden vom DHCP-Server generiert.
    - **DHCP mit Adresse und DNS über DHCP** – die Adress- und DNS-Informationen werden vom DHCP-Server generiert.
    - **SLAAC mit Adresse und DNS über DHCP** – die Adress- und DNS-Informationen werden vom DHCP-Server generiert. Diese Option wird nur von NSX Edge und nicht von KVM-Hosts oder ESXi-Hosts unterstützt.
  - c Geben Sie die erreichbare Zeit und das Intervall für die erneute Übertragung der Routerankündigungsmeldung ein.

- d Geben Sie den Domänennamen ein und geben Sie eine Lebensdauer für den Domänennamen an. Geben Sie diese Werte nur für den Modus **SLAAC mit DNS über RA** ein.
  - e Geben Sie einen DNS-Server ein und geben Sie eine Lebensdauer für den DNS-Server an. Geben Sie diese Werte nur für den Modus **SLAAC mit DNS über RA** ein.
  - f Geben Sie die Werte für die Routerankündigung ein:
    - **RA-Intervall** – das Zeitintervall zwischen der Übertragung aufeinander folgender Routerankündigungsmeldungen.
    - **Hop-Grenzwert** – die Lebensdauer der angekündigten Routen.
    - **Routerlebensdauer** – die Lebensdauer des Routers.
    - **Präfix Lebensdauer** – die Lebensdauer des Präfixes in Sekunden.
    - **Bevorzugte Zeit für Präfix** – die Zeit, zu der eine gültige Adresse bevorzugt wird.
- 6 Wenn Sie ein **DAD-Profil** erstellen möchten, klicken Sie auf das Menüsymbol (drei Punkte) und wählen Sie **Neue erstellen** aus.
- a Geben Sie einen Namen für das Profil ein.
  - b Wählen Sie einen Modus aus:
    - **Locker** – eine Benachrichtigung über doppelte Adressen wird empfangen, aber es erfolgt keine Aktion, wenn eine doppelte Adresse erkannt wird.
    - **Streng** – eine Benachrichtigung über doppelte Adressen wird empfangen und die doppelte Adresse wird nicht mehr verwendet.
  - c Geben Sie die **Wartezeit (Sekunden)** ein, die das Zeitintervall zwischen den NS-Paketen angibt.
  - d Geben Sie die **Anzahl der NS-Wiederholungen** ein, die die Anzahl NS-Pakete zur Erkennung doppelter Adressen in Intervallen angibt, die unter **Wartezeit (Sekunden)** definiert werden.

# 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** aus.
- 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.
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. Dies ist die Standardoption.

- 7 (Optional) Wählen Sie einen NSX Edge-Cluster aus, wenn dieses Tier-1-Gateway statusbehaftete Dienste (NAT, Load Balancer oder Firewall) 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 (Optional) Klicken Sie auf den Umschalter **Standby-Verlagerung aktivieren**, 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.
- 10 Klicken Sie auf **Speichern**.
- 11 (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**
- **Alle lokalen IPSec-Endpoints**



Klicken Sie im Feld **Routen-Advertisement-Regeln festlegen** auf **Festlegen**, um Routen-Advertisement-Regeln hinzuzufügen.

- 12 (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 Geben Sie im Feld **MTU** einen Wert zwischen 64 und 9000 ein.
- e Wählen Sie im Feld **ND-Profil** ein Profil aus.
- f Klicken Sie auf **Speichern**.

- 13 (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
Name	Name des Profils.
Modus	<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>
Priorität	<p>Legen Sie den CoS-Prioritätswert fest.</p> <p>Die Prioritätswerte liegen zwischen 0 und 63, wobei 0 der höchsten Priorität entspricht.</p>
Dienstklasse	<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>
Ingress	<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 0,10/8 = 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.

**Hinweis** Die Methoden für die Konfiguration von IP-Adressen für IPv6 sind im standardmäßigen IP Discovery-Segmentprofil deaktiviert. Um die IP Discovery für IPv6 für Segmente zu aktivieren, müssen Sie ein IP Discovery-Profil mit aktivierten IPv6-Optionen erstellen und das Profil an die Segmente anhängen. Stellen Sie außerdem sicher, dass die verteilte Firewall IPv6 Neighbor Discovery-Pakete zwischen allen Arbeitslasten zulässt (standardmäßig zulässig).

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 der erkannten Liste, aber nicht der realisierten Bindungsliste hinzugefügt. Allen doppelten IPs ist ein Ermittlungszeitstempel zugeordnet. Wenn die IP, die sich in der realisierten Bindungsliste befindet, entweder durch Hinzufügen zur Ignorieren-Bindungsliste 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 erkannt und der Liste der realisierten Bindungen hinzugefügt wird, bleibt diese Bindung für immer in der realisierten Liste. TOFU wird auf die ersten 'n' eindeutigen <IP-, MAC-, VLAN >- Bindungen angewendet, 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 erkannt wird, wird sie der Liste der realisierten Bindungen hinzugefügt und wenn sie gelöscht oder abgelaufen ist, wird sie aus der Liste der realisierten Bindungen entfernt. DHCP-Snooping und VM-Tools werden immer im TOEU-Modus betrieben.

---

**Hinweis** TOFU ist nicht identisch mit SpoofGuard und blockiert den Datenverkehr nicht auf dieselbe Weise wie SpoofGuard. Weitere Informationen finden Sie unter [Grundlegendes zum Spoofguard-Segmentprofil](#).

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>.

---

NSX Manager verwaltet für jeden Port eine Ignorieren-Bindungsliste, die IP-Adressen enthält, die nicht an den Port gebunden werden können. Durch Navigieren zu **Netzwerk und Sicherheit – Erweitert > Switching > Ports** und Auswählen eines Ports können Sie erkannte Bindungen der Liste der ignorierten Bindungen hinzufügen. Sie können auch eine vorhandene erkannte oder realisierte Bindung löschen, indem Sie sie nach **Ignorierte Bindungen** kopieren.

## Erstellen eines Segmentprofils für die IP Discovery

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

### Voraussetzungen

Machen Sie sich mit dem Konzept des Switching-Profils für die IP Discovery 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 > Segmentprofil**.
- 3 Klicken Sie auf **Segmentprofil hinzufügen** und wählen Sie **IP Discovery** aus.
- 4 Geben Sie die Details des Switching-Profiles für die IP Discovery 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. Der zulässige Mindestwert ist 1 (Standard), der maximale Wert 256.
<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 konfiguriertem 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.

Beachten Sie, dass für das standardmäßige Segmentsicherheitsprofil die DHCP-Einstellungen `Server Block` und `Server Block - IPv6` aktiv sind. Das bedeutet, dass ein Segment, das das standardmäßige Segmentsicherheitsprofil verwendet, Datenverkehr von einem DHCP-Server zu einem DHCP-Client blockieren wird. Wenn ein Segment Datenverkehr von einem DHCP-Server zulassen soll, müssen Sie ein benutzerdefiniertes Segmentsicherheitsprofil für dieses Segment erstellen.

## 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>Serverblock - IPv6</b> und <b>Clientblock - IPv6</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
Name	Name des Profils.
MAC-Änderung	Aktivieren oder deaktivieren Sie die Funktion zum Ändern der MAC-Adresse. Standardmäßig ist sie deaktiviert.
MAC Learning	Aktivieren oder deaktivieren Sie MAC Learning. Standardmäßig ist sie deaktiviert.
MAC-Grenzwertrichtlinie	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.
Unbekanntes Unicast Flooding	Aktivieren oder deaktivieren Sie die unbekannte Unicast Flooding-Funktion. Standardmäßig ist sie aktiviert. Diese Option ist verfügbar, wenn Sie Mac Learning aktivieren.
MAC-Grenzwert	Legen Sie die maximale Anzahl an MAC-Adressen fest. Die Standardeinstellung ist 4096. Diese Option ist verfügbar, wenn Sie Mac Learning aktivieren.
MAC Learning-Alterungszeit	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 über das 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 **Segment hinzufügen**.
- 4 Geben Sie einen Namen für das Segment ein.
- 5 Wählen Sie ein verbundenes Gateway aus.

Sie können ein vorhandenes Tier-0- oder Tier-1-Gateway oder die Option **Keine** auswählen. Der Standardwert ist **Keine**, was bedeutet, dass das Segment einfach ein logischer Switch ist. Mit einem konfigurierten Subnetz kann das Segment mit einem Tier-0- oder einem Tier-1-Gateway verbunden werden.

- 6 Handelt es sich bei dem verbundenen Gateway um ein Tier-1-Gateway, wählen Sie entweder 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 Um ein Subnetz anzugeben, klicken Sie auf **Subnetze festlegen**.
- 8 Wählen Sie eine Transportzone aus, bei der es sich um ein Overlay oder ein VLAN handeln kann.
- 9 Geben Sie bei einer Transportzone vom Typ „VLAN“ eine Liste der VLAN-IDs an.
- 10 Wenn Sie Schicht-2-VPN verwenden möchten, um das Segment zu erweitern, klicken Sie auf das Textfeld **L2-VPN** und wählen Sie einen L2 VPN-Server oder eine Client-Sitzung aus.  
Sie können mehr als einen Server bzw. eine Client-Sitzung auswählen.
- 11 Geben Sie als **ID des VPN-Tunnels** einen eindeutigen Wert ein, der zur Identifizierung des Segments verwendet wird.
- 12 Klicken Sie auf **Speichern**.

**13** Um Segment-Ports hinzuzufügen, klicken Sie bei der entsprechenden Aufforderung auf **Ja**, wenn Sie die Konfiguration des Segments fortsetzen möchten.

- a Klicken Sie auf **Ports** und **Einstellen**.
- b Klicken Sie auf **Segment-Port hinzufügen**.
- c Geben Sie einen Portnamen ein.
- d Geben Sie für **ID** die VIF-UUID der VM oder des Servers ein, der sich mit diesem Port verbindet.
- e Wählen Sie einen Typ aus: **Übergeordnetes Element**, **Untergeordnetes Element** oder **Unabhängig**.

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

- f Geben Sie eine Kontext-ID ein.

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

- g Geben Sie ein Datenverkehrs-Tag ein.

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

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

- i Geben Sie Tags an.

- j Wenden Sie die Adressbindung an, indem Sie die IP (IPv4-Adresse, IPv6-Adresse oder IPv6-Subnetz) und die MAC-Adresse des logischen Ports angeben, auf den Sie die Adressbindung anwenden möchten. Für IPv6 ist z. B. 2001::/64 ein IPv6-Subnetz, 2001::1 eine Host-IP-Adresse, wohingegen 2001::1/64 eine ungültige Eingabe ist. Sie können auch eine VLAN-ID angeben.

Wenn manuelle Adressbindungen angegeben werden, überschreiben diese die automatisch erkannten Adressbindungen.

- k Wählen Sie Segmentprofile für diesen Port aus.

**14** Um Segmentprofile auszuwählen, klicken Sie auf **Segmentprofile**.

**15** 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 Limited Export-Version nicht unterstützt.

---

Sie müssen über einen funktionierenden NSX Edge-Knoten mit mindestens einem konfigurierten Tier-0- oder Tier-1-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- oder Tier-1-Router, die vor NSX-T Data Center Version 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](#)
- [Hinzufügen eines autonomen Edge als L2-VPN-Client](#)
- [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 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.

NSX Edge unterstützt ein Richtlinien- oder ein Routen-basiertes IPSec-VPN.

IPSec-VPN-Dienste werden nur auf Tier-0-Gateways unterstützt, die im Hochverfügbarkeitsmodus `Active-Standby` ausgeführt werden müssen. Weitere Informationen finden Sie unter [Hinzufügen eines Tier-0-Gateways](#). Ab NSX-T Data Center 2.5 wird IPSec-VPN auch auf Tier-1-Gateways unterstützt. 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 einen Hochverfügbarkeitsdienst 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

## 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.

**Hinweis** DNAT wird auf einem Gateway der Ebene 1 nicht unterstützt, bei dem richtlinienbasiertes IPSec-VPN konfiguriert ist.

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 von statischen Routen oder von Routen, die dynamisch über eine spezielle Schnittstelle (Virtual Tunnel Interface, VTI) erlernt werden, indem z. B. BGP als Protokoll verwendet wird. IPSec schützt den gesamten Datenverkehr, der über die VTI geleitet wird.

---

### Hinweis

- Das dynamische OSPF-Routing wird nicht für das Routing über IPSec-VPN-Tunnel unterstützt.
- Dynamisches Routing für VTI wird auf VPN, das auf Tier-1-Gateways basiert, nicht unterstützt.

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 die VPN-Tunnel-Redundanz mit einer routenbasierten IPSec-VPN-Sitzung konfigurieren, die auf einem Tier-0-Gateway konfiguriert ist. Bei der Tunnel-Redundanz können mehrere Tunnel zwischen zwei Sites eingerichtet werden, wobei ein Tunnel als primärer Tunnel mit Failover zu den anderen Tunneln verwendet wird, wenn der primäre Tunnel nicht mehr verfügbar ist. Diese Funktion ist besonders nützlich, wenn eine Site über mehrere Konnektivitätsoptionen verfügt, z. B. mit verschiedenen ISPs zur Verbindungsredundanz.

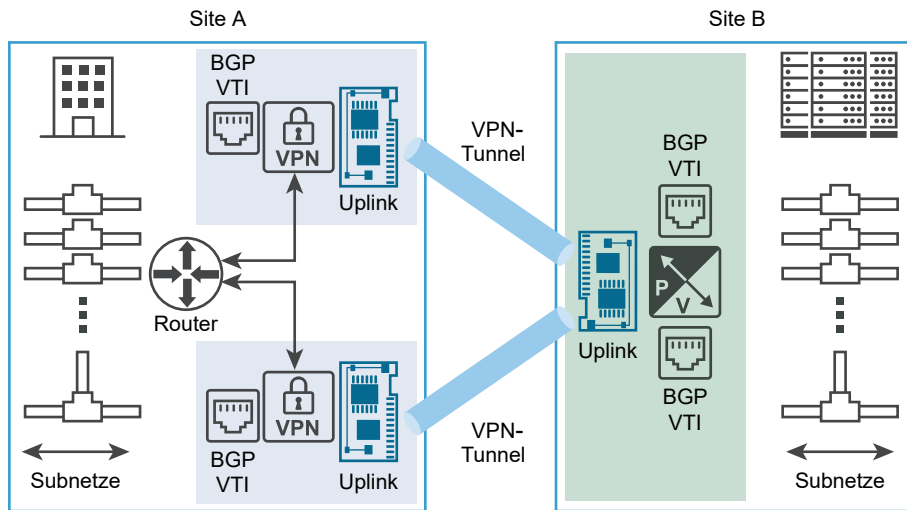
---

### Wichtig

- In NSX-T Data Center wird IPSec-VPN-Tunnel-Redundanz nur mithilfe von BGP 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](#).

## Grundlegendes zu Layer 2-VPN

Mit Layer 2-VPN (L2 VPN) können Sie Layer 2-Netzwerke (VNIs oder VLANs) auf mehrere Sites in derselben Broadcast-Domäne erweitern. Diese Verbindung ist mit einem routenbasierten IPSec-Tunnel zwischen dem L2-VPN-Server und dem L2-VPN-Client gesichert.

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

Das erweiterte Netzwerk ist ein einzelnes Subnetz mit einer einzelnen Broadcast-Domäne. Somit verbleiben VMs im selben Subnetz, wenn sie zwischen Sites verschoben werden und ihre IP-Adressen bleiben gleich. Daher können Unternehmen VMs nahtlos zwischen Netzwerk-Sites migrieren. Die VMs können in VNI-basierten Netzwerken 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.

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-Segmente erweitert werden.

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

Ab der Version 2.5 von NSX-T Data Center können VLAN-basierte Segmente mithilfe des L2 VPN-Diensts auf einem NSX Edge erweitert werden, das in einer NSX-T Data Center-Umgebung verwaltet wird. Diese Unterstützung ermöglicht die Erweiterung von L2-Netzwerken von VLAN zu VNI, VLAN zu VLAN und VNI zu VNI.

Unterstützt wird auch das VLAN-Trunking mithilfe eines ESX NSX-verwalteten Virtual Distributed Switch (N-VDS). Wenn die Computing- und E/A-Ressourcen dies zulassen, ermöglicht VLAN-Trunking einem NSX Edge-Cluster, mehrere VLAN-Netzwerke über eine einzelne Schnittstelle zu erweitern.

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 einem in einer NSX Data Center for vSphere-Umgebung verwalteten NSX Edge gehostet wird. Ein verwalteter L2-VPN-Client unterstützt VLANs und VNIs.
- 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 nur VLANs.
- Zwischen einem L2-VPN-Server in NSX-T Data Center und einem L2-VPN-Client, der auf einem eigenständigen NSX Edge gehostet wird. Ein eigenständiger L2-VPN-Client unterstützt nur 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.

## 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 Informationen zu den Workflows, die zum Einrichten des benötigten VPN-Diensts 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- oder Tier-1-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 Verwenden Sie [Hinzufügen von lokalen Endpoints](#), um einen VPN-Server zu erstellen, der auf dem NSX Edge gehostet wird.
- 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](#). Geben Sie die lokalen Subnetze und Peer-Subnetze an, die für den Tunnel verwendet werden sollen. Der Datenverkehr von einem lokalen Subnetz an ein Peer-Subnetz wird mithilfe des Tunnels geschützt, der in der Sitzung definiert wird.

## 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 und aktivieren Sie einen IPSec-VPN-Dienst mithilfe eines vorhandenen Tier-0- oder Tier-1-Gateways. Siehe [Hinzufügen eines IPSec-VPN-Dienstes](#).
- 2 Definieren Sie ein IKE-Profil, sofern Sie das standardmäßige IKE-Profil nicht verwenden möchten. Siehe [Hinzufügen von IKE-Profilen](#).
- 3 Wenn Sie das standardmäßige IPSec-Profil des Systems nicht verwenden möchten, erstellen Sie eines mit [Hinzufügen von IPSec-Profilen](#).
- 4 Erstellen Sie ein DPD-Profil, wenn Sie das Standard-DPD-Profil nicht verwenden möchten. Siehe [Hinzufügen von DPD-Profilen](#).
- 5 Gehen Sie wie unter [Hinzufügen von lokalen Endpoints](#) beschrieben vor, um einen lokalen Endpoint hinzuzufügen.
- 6 Konfigurieren Sie eine routenbasierte IPSec-VPN-Sitzung, wenden Sie die Profile an und hängen Sie den lokalen Endpoint an die Sitzung an. Stellen Sie eine VTI-IP in der Konfiguration bereit und verwenden Sie dieselbe IP-Adresse, um das Routing zu konfigurieren. Die Routen können statisch oder dynamisch sein (unter Verwendung von BGP). 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. Sie müssen auch die Sitzungen für den L2-VPN-Server und den L2 VPN-Client mithilfe des Peer-Codes konfigurieren, der vom L2-VPN-Server generiert wird. 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 durch [Herunterladen der L2-VPN-Konfigurationsdatei der Remotesite](#) den Peer-Code für die Sitzung des L2-VPN-Serverdienstes, der auf die Remote-Site angewendet und zur automatischen Konfiguration der L2-VPN-Client-Sitzung verwendet werden muss.
- 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- oder Tier-1-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 Limited Export-Version 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-0- oder Tier-1-Gateway muss konfiguriert und zur Verwendung verfügbar sein. Weitere Informationen hierzu finden Sie unter [Hinzufügen eines Tier-0-Gateways](#) oder [Tier-1-Gateway hinzufügen](#).

## 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 **Gateway** das Tier-0- oder Tier-1-Gateway aus, das diesem IPSec-VPN-Dienst zugeordnet werden soll.
- 6 Aktivieren oder deaktivieren Sie **Administrativer Status**.  
Standardmäßig ist der Wert auf `Enabled` festgelegt. Dies bedeutet, dass der IPSec-VPN-Dienst auf dem Tier-0- oder Tier-1-Gateway aktiviert wird, nachdem der neue IPSec-VPN-Dienst konfiguriert wurde.
- 7 Legen Sie den Wert für **IKE-Protokollebene** fest.  
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 in den Textfeldern **Lokale Netzwerke** und **Remotenetzwerke** 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-Diensts 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 **Sitzungen** 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 konfigurieren einen L2-VPN-Dienst auf einem Tier-0-Gateway. Um den L2-VPN-Dienst zu aktivieren, müssen Sie zuerst einen IPSec-VPN-Dienst auf dem Tier-0-Gateway erstellen, sofern er noch nicht vorhanden ist. Anschließend konfigurieren Sie einen L2-VPN-Tunnel zwischen einem L2-VPN-Server (Ziel-Gateway) und einem L2-VPN-Client (Quell-Gateway).

Zum Konfigurieren eines L2-VPN-Diensts 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](#)

Nach der Konfiguration des L2-VPN-Serverdienstes konfigurieren Sie den L2-VPN-Dienst im Clientmodus auf einer anderen NSX Edge-Instanz.

## 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.

### Verfahren

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

- 2 (Optional) Wenn noch kein IPSec-VPN-Dienst auf dem Tier-O-Gateway vorhanden ist, das Sie als L2-VPN-Server konfigurieren möchten, erstellen Sie den Dienst mithilfe der folgenden Schritte.
  - 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 & 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

Nach der Konfiguration des L2-VPN-Serverdiensts konfigurieren Sie den L2-VPN-Dienst im Clientmodus auf einer anderen NSX Edge-Instanz.

### Verfahren

- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 (Optional) Wenn noch keine vorhanden ist, erstellen Sie mithilfe der folgenden Schritte einen IPSec-VPN-Dienst für den L2-VPN-Client Dienst.
  - 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 Legen Sie optional die Werte für **Beschreibung** und **Tags** fest.
- 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 **Administrativer Status**.  
Als Standardwert ist `Enabled` festgelegt. Das bedeutet, dass die IPSec-VPN-Sitzung bis hinunter zum NSX Edge-Knoten konfiguriert werden muss.
- 10 (Optional) Wählen Sie im Dropdown-Menü **Übereinstimmungs-Suite** eine Sicherheits-Übereinstimmungs-Suite aus.

---

**Hinweis** Übereinstimmungs-Suites werden ab NSX-T Data Center 2.5 unterstützt. Weitere Informationen finden Sie unter [Informationen zu unterstützten Compliance-Suites](#).

---

Der ausgewählte Standardwert ist `None`. Wenn Sie eine Compliance-Suite auswählen, wird der **Authentifizierungsmodus** auf `Certificate` festgelegt und im Abschnitt **Erweiterte Eigenschaften** werden die Werte für das **IKE-Profil** und das **IPSec-Profil** auf die vom System definierten Profile für die ausgewählte Sicherheits-Compliance-Suite festgelegt. Sie können diese vom System definierten Profile nicht bearbeiten.

- 11 Wenn die **Übereinstimmungs-Suite** auf `None` festgelegt ist, wählen Sie einen Modus aus dem Dropdown-Menü **Authentifizierungsmodus** 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.

- 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 Wenn der **Authentifizierungsmodus** auf `PSK` festgelegt ist, 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.

---

#### 14 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. Im Folgenden finden Sie ein Beispiel.

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

#### 15 Um die Profile, den Initiierungsmodus, den Modus der TCP-MSS-Klemmung und die Tags, die von der richtlinienbasierten IPsec-VPN-Sitzung verwendet werden, zu ändern, klicken Sie auf **Erweiterte Eigenschaften**.

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 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 Wenn das Dropdown-Menü **IKE-Profil** aktiviert ist, wählen Sie das IKE-Profil aus.
- b Wählen Sie das IPsec-Tunnelprofil aus, wenn das Dropdown-Menü **IPSec-Profil** nicht deaktiviert ist.
- c Wählen Sie das bevorzugte DPD-Profil aus, wenn das Dropdown-Menü **DPD-Profil** aktiviert ist.

- 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 5-2. 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.

- e Wenn Sie die maximale Segmentgröße (MSS) für die Nutzlast der TCP-Sitzung während der IPSec-Verbindung reduzieren möchten, aktivieren Sie **TCP-MSS-Klemmung**, wählen Sie den Wert **TCP-MSS-Richtung** aus und legen Sie optional den **TCP-MSS-Wert** fest.

Weitere Informationen hierzu finden Sie unter [Grundlegendes zum TCP-MSS Clamping](#).

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

**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-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. 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** aus.
- 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 (Optional) Wählen Sie im Dropdown-Menü **Übereinstimmungs-Suite** eine Sicherheits-Übereinstimmungs-Suite aus.

---

**Hinweis** Übereinstimmungs-Suites werden ab NSX-T Data Center 2.5 unterstützt. Weitere Informationen finden Sie unter [Informationen zu unterstützten Compliance-Suites](#).

---

Als Standardwert ist `None` festgelegt. Wenn Sie eine Compliance-Suite auswählen, wird der **Authentifizierungsmodus** auf `Certificate` festgelegt und im Abschnitt **Erweiterte Eigenschaften** werden die Werte für das **IKE-Profil** und das **IPSec-Profil** auf die vom System definierten Profile für die ausgewählte Compliance-Suite festgelegt. Sie können diese vom System definierten Profile nicht bearbeiten.

- 11 Geben Sie eine IP-Subnetz-Adresse in **Tunnelschnittstelle** in der CIDR-Notation ein.  
Diese Adresse ist erforderlich.
- 12 Wenn die **Übereinstimmungs-Suite** auf `None` festgelegt ist, wählen Sie einen Modus aus dem Dropdown-Menü **Authentifizierungsmodus** 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.

- 13 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.

- 14 Geben Sie einen Wert in **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"
```

- 15 Wenn Sie diese IPsec-Sitzung als Teil eines bestimmten Gruppentags einschließen möchten, geben Sie den Namen des Tags in **Tags** ein.
- 16 Um die Profile, den Initiierungsmodus, den Modus der TCP-MSS-Klemmung und die Tags, die von der routenbasierten IPsec-VPN-Sitzung verwendet werden, zu ändern, klicken Sie auf **Erweiterte Eigenschaften**.

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](#).

- Wenn das Dropdown-Menü **IKE-Profil** aktiviert ist, wählen Sie das IKE-Profil aus.
- Wählen Sie das IPsec-Tunnelprofil aus, wenn das Dropdown-Menü **IPsec-Profil** nicht deaktiviert ist.

- c Wählen Sie das bevorzugte DPD-Profil aus, wenn das Dropdown-Menü **DPD-Profil** aktiviert ist.
- 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.

- 17 Wenn Sie die maximale Segmentgröße (MSS) für die Nutzlast der TCP-Sitzung während der IPSec-Verbindung reduzieren möchten, aktivieren Sie **TCP-MSS-Klemmung**, wählen Sie den Wert für die **TCP-MSS-Richtung** aus und legen Sie optional den **TCP-MSS-Wert** fest. []

Weitere Informationen finden Sie unter [Grundlegendes zum TCP-MSS Clamping](#).

- 18 Wenn Sie diese IPSec-Sitzung als Teil eines bestimmten Gruppentags einschließen möchten, geben Sie den Namen des Tags in **Tags** ein.
- 19 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.

## Informationen zu unterstützten Compliance-Suites

Ab NSX-T Data Center 2.5 können Sie eine Sicherheits-Compliance-Suite angeben, die zum Konfigurieren der Sicherheitsprofile für eine IPSec-VPN-Sitzung verwendet werden soll.

Eine Sicherheits-Compliance-Suite verfügt über vordefinierte Werte für verschiedene Sicherheitsparameter, die nicht geändert werden können. Wenn Sie eine Sicherheits-Compliance-Suite auswählen, werden die vordefinierten Werte automatisch für das Sicherheitsprofil der von Ihnen konfigurierten IPSec-VPN-Sitzung verwendet.

Die folgende Tabelle enthält die Sicherheits-Compliance-Suites, die für IKE-Profile in NSX-T Data Center unterstützt werden, sowie die jeweiligen vordefinierten Werte.

Name der Compliance-Suite	IKE-Version	Verschlüsselungsalgorithmus	Digest-Algorithmus	Diffie-Hellman Group
CNSA	IKEv2	AES 256	SHA2 384	Gruppe 15, Gruppe 20
FIPS	IKE-Flex	AES 128	SHA2 256	Gruppe 20
Grundlage	IKEv1	AES 128	SHA2 256	Gruppe 14
PRIME	IKEv2	AES-GCM 128	Nicht festgelegt	Gruppe 19
Suite-B-GCM-128	IKEv2	AES 128	SHA2 256	Gruppe 19
Suite-B-GCM-256	IKEv2	AES 256	SHA2 384	Gruppe 20

Die folgende Tabelle enthält die Übereinstimmungs-Suites, die für IPSec-Profile in NSX-T Data Center unterstützt werden, sowie die jeweiligen vordefinierten Werte.

Name der Compliance-Suite	Verschlüsselungsalgorithmus	Digest-Algorithmus	PFS-Gruppe	Diffie-Hellman Group
CNSA	AES 256	SHA2 384	Aktiviert	Gruppe 15, Gruppe 20
FIPS	AES-GCM 128	Nicht festgelegt	Aktiviert	Gruppe 20
Grundlage	AES 128	SHA2 256	Aktiviert	Gruppe 14
PRIME	AES-GCM 128	Nicht festgelegt	Aktiviert	Gruppe 19
Suite-B-GCM-128	AES-GCM 128	Nicht festgelegt	Aktiviert	Gruppe 19
Suite-B-GCM-256	AES-GCM 256	Nicht festgelegt	Aktiviert	Gruppe 20

## Grundlegendes zum TCP-MSS Clamping

Die TCP-MSS-Klemmung ermöglicht es Ihnen, den Wert für die maximale Segmentgröße (MSS), der von einer TCP-Sitzung während des Verbindungsaufbaus über einen IPSec-Tunnel verwendet wird, zu reduzieren. Diese Funktion wird ab NSX-T Data Center 2.5 unterstützt.

TCP MSS entspricht der maximalen Datenmenge in Byte, die ein Host in einem einzigen TCP-Segment zu akzeptieren bereit ist. Jedes Ende einer TCP-Verbindung sendet seinen gewünschten MSS-Wert während eines 3-Wege-Handshake an das entsprechende Peer-Ende, wobei MSS eine der TCP-Kopfzeilenoptionen ist, die in einem TCP-SYN-Paket verwendet werden. TCP MSS wird basierend auf der maximalen Übertragungseinheit (MTU) der Egress-Schnittstelle des Sender-Hosts berechnet.

Wenn TCP-Datenverkehr durch ein IPSec-VPN oder eine beliebige Art von VPN-Tunnel geleitet wird, werden dem Originalpaket aus Sicherheitsgründen zusätzliche Kopfzeilen hinzugefügt. Für den IPSec-Tunnelmodus werden zusätzlich IP-, ESP- und optional UDP-Kopfzeilen verwendet (wenn eine Portübersetzung im Netzwerk vorhanden ist). Durch diese zusätzlichen Kopfzeilen geht die Größe des gekapselten Pakets über die MTU der VPN-Schnittstelle hinaus. Das Paket kann basierend auf der DF-Richtlinie fragmentiert oder verworfen werden.

Um die Fragmentierung oder das Verwerfen eines Pakets zu vermeiden, können Sie den MSS-Wert für die IPSec-Sitzung anpassen, indem Sie die Funktion „TCP-MSS-Klemmung“ aktivieren. Navigieren Sie zu **Netzwerk > VPN > IPSec-Sitzungen**. Wenn Sie eine IPSec-Sitzung hinzufügen oder eine bestehende Sitzung bearbeiten, erweitern Sie den Abschnitt **Erweiterte Eigenschaften** und aktivieren Sie **TCP-MSS-Klemmung**.

Sie können den vorberechneten MSS-Wert für die IPSec-Sitzung konfigurieren, indem Sie sowohl die **TCP-MSS-Richtung** als auch den **TCP-MSS-Wert** einstellen. Der konfigurierte MSS-Wert wird für das MSS Clamping verwendet. Sie können die dynamische MSS-Berechnung verwenden, indem Sie die **TCP-MSS-Richtung** festlegen und den **TCP-MSS-Wert** leer lassen. Der MSS-Wert wird basierend auf der VPN-Schnittstellen-MTU, dem VPN-Overhead und der Pfad-MTU (PMTU), wenn bereits festgelegt, automatisch berechnet. Der effektive MSS-Wert wird bei jedem TCP-Handshake neu berechnet, um die MTU- oder PMTU-Änderungen dynamisch zu verarbeiten.

## 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 dieser als vertrauliche Information gilt.

---

- 10 Geben Sie eine IP-Subnetz-Adresse in die **Tunnelschnittstelle** 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 „L2-VPN-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 im Dropdown-Menü **Segment** das VNI- oder VLAN-basierte Segment aus, das Sie an die Sitzung anhängen möchten.
- d Geben Sie einen eindeutigen Wert im Feld **ID des VPN-Tunnels** ein, der verwendet wird, um das von Ihnen ausgewählte Segment 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 den Peer-Code ab, der während der Konfiguration des L2-VPN-Servers generiert wurde. Siehe [Herunterladen der L2-VPN-Konfigurationsdatei der Remoteseite](#).
- 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 die L2-VPN-Clientsitzung verwendet werden soll.
- 8 Geben Sie im Textfeld **Peer-Konfiguration** den Peer-Code ein, der bei der Konfiguration des L2-VPN-Serverdienstes generiert wurde.
- 9 Aktivieren oder deaktivieren Sie **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.
- 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 VNI- oder VLAN-basierte Segment aus, das Sie an die L2-VPN-Clientsitzung anhängen möchten.
  - d Geben Sie einen eindeutigen Wert im Feld **ID des VPN-Tunnels** ein, der verwendet wird, um das von Ihnen ausgewählte Segment zu identifizieren.
  - e Klicken Sie auf **Schließen**.
- 12 Klicken Sie auf **Bearbeitung 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-Konfigurationsdatei der Remoteseite

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** Seien Sie beim Speichern und Freigeben des Peer-Codes vorsichtig, da er einen PSK-Wert enthält, der als vertrauliche Information gilt.

`L2VPNSession_L2VPNServer_config.txt` enthält beispielsweise die folgende Konfiguration.

```
[
  {
    "transport_tunnel_path": "/infra/tier-0s/ServerT0_AS/locale-services/1-
policyconnectivity-693/ipsec-vpn-services/IpsecService1/sessions/Routebase1",
    "peer_code":
    "MCw3ZjBjYzdjLHsic2l0ZU5hbWUiOiJSb3V0ZWJhc2UxIiwic3JjVGFwSXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYXB
BJcCI6IjE2OS4yNTQuNjQuMSIsImlrZU9wdG1
vbiI6ImlrZXxyIiwic2l0ZU5hbWUiOiJSb3V0ZWJhc2UxIiwic3JjVGFwSXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYXB
VzdCI6ImFlcylnY20vc2hhLTI1NiIsInBzayI
6IlZNd2FyZTEyMyIsInRlbn5lbHMt7ImxvY2FsSWQiOiI2MC42MC42MC4xIiwicGVlc2lkIjoINTAuNTAuNTAuMS
IsImxvY2FsVnR5cSXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYXB"
  }
]
```

- 5 Kopieren Sie den Peer-Code, den Sie zum Konfigurieren des L2-VPN-Clientdiensts und der -Sitzung verwenden.

Im Beispiel der oben aufgeführten Konfigurationsdatei würden Sie den folgenden Peer-Code für die L2-VPN-Client-Konfiguration kopieren.

```
MCw3ZjBjYzdjLHsic2l0ZU5hbWUiOiJSb3V0ZWJhc2UxIiwic3JjVGFwSXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYXB
JcCI6IjE2OS4yNTQuNjQuMSIsImlrZU9wdG1
vbiI6ImlrZXxyIiwic2l0ZU5hbWUiOiJSb3V0ZWJhc2UxIiwic3JjVGFwSXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYXB
VzdCI6ImFlcylnY20vc2hhLTI1NiIsInBzayI
6IlZNd2FyZTEyMyIsInRlbn5lbHMt7ImxvY2FsSWQiOiI2MC42MC42MC4xIiwicGVlc2lkIjoINTAuNTAuNTAuMS
IsImxvY2FsVnR5cSXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYXB
```

## 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** auswählen. 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 im Dropdown-Menü **VPN-Dienst** den IPSec-VPN-Dienst aus, dem dieser lokale Endpoint zugeordnet werden soll.
- 5 Geben Sie eine IP-Adresse oder einen lokalen Endpoint ein.

Bei einem IPSec-VPN-Dienst, der auf einem Tier-0-Gateway ausgeführt wird, muss sich die lokale Endpoint-IP-Adresse von der IP-Adresse der Uplink-Schnittstelle des Tier-0-Gateways unterscheiden. Die von Ihnen angegebene lokale Endpoint-IP-Adresse ist der Loopback-Schnittstelle für das Tier-0-Gateway zugeordnet und wird auch als routingfähige IP-Adresse über die Uplink-Schnittstelle veröffentlicht. Damit der IPSec-VPN-Dienst auf einem Tier-1-Gateway läuft und die lokale Endpoint-IP-Adresse routingfähig ist, muss das Routen-Advertisement für lokale IPSec-Endpoints in der Tier-1-Gateway-Konfiguration aktiviert sein. Weitere Informationen hierzu finden Sie unter [Tier-1-Gateway hinzufügen](#).

- 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 (Optional) Optional können Sie eine **Beschreibung** hinzufügen.
- 8 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 Endpoint definiert sind, 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.
- 9 Wählen Sie aus den Dropdown-Menüs **Vertrauenswürdige CA-Zertifikate** und **Zertifikatswiderrufsliste** die entsprechenden Zertifikate aus, die für den lokalen Endpoint erforderlich sind.
  - 10 Geben Sie bei Bedarf ein Tag an.
  - 11 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-Profiles	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>

Anstelle der standardmäßig verwendeten IKE-Profile können Sie auch eine der ab NSX-T Data Center 2.5 unterstützten Compliance-Suites auswählen. Weitere Informationen finden Sie unter [Informationen zu unterstützten Compliance-Suites](#).

Wenn Sie sich gegen die Verwendung der bereitgestellten standardmäßigen IKE-Profile oder Compliance-Suites entscheiden, können Sie Ihr eigenes IKE-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 Klicken Sie auf die Registerkarte **Netzwerk > VPN > Profile**.
- 3 Wählen Sie den Profiltyp **IKE-Profil** 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**

<b>IKE-Version</b>	<b>Beschreibung</b>
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 standardmäßigen IPSec-Profile aufgeführt.

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

Name 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>

Anstelle des standardmäßigen IPSec-Profils können Sie auch eine der ab NSX-T Data Center 2.5 unterstützten Compliance-Suites auswählen. Weitere Informationen finden Sie unter [Informationen zu unterstützten Compliance-Suites](#).

Wenn Sie sich gegen die Verwendung der bereitgestellten standardmäßigen IPSec-Profile oder Compliance-Suites entscheiden, 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 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.

Tabelle 5-8. Verwendete Algorithmen

Art des Algorithmus	Gültige Werte	Beschreibung
Verschlüsselung	<ul style="list-style-type: none"> <li>■ AES GCM 128 (Standard)</li> <li>■ AES 128</li> <li>■ AES 256</li> <li>■ AES-GCM 192</li> <li>■ AES-GCM 256</li> <li>■ Keine Verschlüsselung Auth AES GMAC 128'</li> <li>■ Keine Verschlüsselung Auth AES GMAC 192</li> <li>■ Keine Verschlüsselung Auth AES GMAC 256</li> <li>■ Keine Verschlüsselung</li> </ul>	Der Verschlüsselungsalgorithmus, der während der IPSec(Internet Protocol Security)-Aushandlung verwendet wird.
Digest	<ul style="list-style-type: none"> <li>■ SHA 1</li> <li>■ SHA2 256</li> <li>■ SHA2 384</li> <li>■ SHA2 512</li> </ul>	Der sichere Hashing-Algorithmus, der während der IPSec-Aushandlung verwendet wird.
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> <li>■ Gruppe 16</li> <li>■ Gruppe 19</li> <li>■ Gruppe 20</li> <li>■ Gruppe 21</li> </ul>	Die Kryptografieschemata, die die Peer-Site und NSX Edge verwenden, um einen gemeinsamen geheimen Schlüssel über einen unsicheren Kommunikationskanal zu etablieren.

- 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 5-9. 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-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.

## 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-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 eines autonomen Edge als L2-VPN-Client

Sie können L2 VPN verwenden, um Ihre Netzwerke der Ebene 2 auf eine Site zu erweitern, die nicht von NSX-T Data Center verwaltet wird. Ein autonomer NSX Edge kann als L2-VPN-Client auf der Site bereitgestellt werden. Der autonome NSX Edge ist einfach bereitzustellen, einfach programmierbar und bietet Hochleistungs-VPN. Der autonome NSX Edge wird unter Verwendung einer OVF-Datei auf einem Host bereitgestellt, der nicht von NSX-T Data Center verwaltet wird. Sie können HA auch für VPN-Redundanz aktivieren, indem Sie primäre und sekundäre autonome L2-VPN-Edge-Clients bereitstellen.

### Voraussetzungen

- Erstellen Sie eine Portgruppe und binden Sie sie an den vSwitch auf Ihrem Host.
- Erstellen Sie eine Portgruppe für Ihren internen L2-Erweiterungsport.
- Rufen Sie die IP-Adressen für die lokale IP und die Remote-IP ab, die mit der hinzugefügten L2-VPN-Clientsitzung verwendet werden sollen.
- Rufen Sie den Peer-Code ab, der während der Konfiguration des L2-VPN-Servers generiert wurde.

### Verfahren

- 1** Melden Sie sich mit vSphere Web Client bei dem vCenter Server an, der die Nicht-NSX-Umgebung verwaltet.
- 2** Wählen Sie **Hosts und Cluster** aus und erweitern Sie die Cluster, um die verfügbaren Hosts anzuzeigen.

- 3 Klicken Sie mit der rechten Maustaste auf den Host, auf dem Sie das autonome NSX Edge installieren möchten und wählen Sie **OVF-Vorlage bereitstellen** aus.
- 4 Geben Sie die URL ein, um die OVF-Datei aus dem Internet herunterzuladen und zu installieren oder klicken Sie auf **Durchsuchen**, um nach dem Ordner auf Ihrem Computer zu suchen, der die OVF-Datei des autonomen NSX Edge enthält und klicken Sie auf **Weiter**.
- 5 Geben Sie auf der Seite **Name und Ordner auswählen** einen Namen für das autonome NSX Edge ein und wählen Sie den Ordner oder das Datacenter für die Bereitstellung aus. Klicken Sie anschließend auf **Weiter**.
- 6 Wählen Sie auf der Seite **Computing-Ressource auswählen** das Ziel der Computing-Ressource aus.
- 7 Überprüfen Sie auf der Seite „Einzelheiten zur OVF-Vorlage“ die Vorlagendetails und klicken Sie auf **Weiter**.
- 8 Wählen Sie auf der Seite **Konfiguration** eine Konfigurationsoption für die Bereitstellung aus.
- 9 Wählen Sie auf der Seite **Speicher auswählen** den Speicherort für die Dateien der Konfiguration und Datenträgerdateien aus.
- 10 Konfigurieren Sie auf der Seite **Netzwerke auswählen** die Netzwerke, die die bereitgestellte Vorlage verwenden muss. Wählen Sie die für die Uplink-Schnittstelle erstellte Portgruppe und die für den L2-Erweiterungsport erstellte Portgruppe aus und geben Sie eine HA-Schnittstelle ein. Klicken Sie auf **Weiter**.
- 11 Geben Sie auf der Seite **Vorlage anpassen** die folgenden Werte ein und klicken Sie auf **Weiter**.
  - a Geben Sie das CLI-Administratorkennwort ein und wiederholen Sie es.
  - b Geben Sie das CLI-Aktivierungskennwort ein und wiederholen Sie es.
  - c Geben Sie das CLI-Rootkennwort ein und wiederholen Sie es.
  - d Geben Sie die IPv4-Adresse für das Verwaltungsnetzwerk ein.
  - e Geben Sie unter **Externer Port** die Details für die VLAN-ID, die Exit-Schnittstelle, die IP-Adresse und die IP-Präfixlänge ein, sodass die Exit-Schnittstelle dem Netzwerk mit der Portgruppe Ihrer Uplink-Schnittstelle zugeordnet wird.  
  
Wenn die Exit-Schnittstelle mit einer Trunk-Portgruppe verbunden ist, geben Sie eine VLAN-ID an. Beispiel: **20,eth2,192.168.5.1,24**. Sie können Ihre Portgruppe auch mit einer VLAN-ID konfigurieren und VLAN 0 unter **Externer Port** verwenden.
  - f (Optional) Geben Sie zum Konfigurieren der Hochverfügbarkeit die Details für den **HA-Port** ein, wobei die Exit-Schnittstelle dem entsprechenden HA-Netzwerk zugeordnet wird.
  - g (Optional) Wählen Sie beim Bereitstellen eines autonomen NSX Edge als sekundären Knoten für HA die Option **Diesen autonomen Edge als sekundären Knoten bereitstellen** aus.

Verwenden Sie dieselbe OVF-Datei wie der primäre Knoten und geben Sie die IP-Adresse, den Benutzernamen, das Kennwort und den Fingerabdruck des primären Knotens ein.

Um den Fingerabdruck des primären Knotens abzurufen, melden Sie sich beim primären Knoten an und führen Sie den folgenden Befehl aus:

```
get certificate api thumbprint
```

Stellen Sie sicher, dass sich die VTEP-IP-Adressen der primären und sekundären Knoten im selben Subnetz befinden und dass Sie mit derselben Portgruppe verbunden sind.

Wenn Sie die Bereitstellung abschließen und den sekundären Edge starten, stellt er eine Verbindung zum primären Knoten her, um einen Edge-Cluster zu bilden.

- 12 Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Einstellungen des eigenständigen Edge und klicken Sie auf **Fertigstellen**.

---

**Hinweis** Wenn während der Bereitstellung Fehler auftreten, wird in der Befehlszeilenschnittstelle eine Meldung des Tages angezeigt. Sie können auch einen API-Aufruf verwenden, um nach Fehlern zu suchen:

```
GET https://<nsx-mgr>/api/v1/node/status
```

Die Fehler werden als behebbare Fehler und schwerwiegende Fehler kategorisiert. Verwenden Sie API-Aufrufe, um die behebbaren Fehler bei Bedarf zu beheben. Sie können die Meldung des Tages mithilfe eines API-Aufrufs löschen:

```
POST /api/v1/node/status?action=clear_bootup_error
```

- 
- 13 Schalten Sie die neue autonome NSX Edge-Appliance ein.
  - 14 Melden Sie sich beim autonomen NSX Edge-Client an.
  - 15 Wählen Sie **L2VPN > Sitzung hinzufügen** aus und geben Sie die folgenden Werte ein:
    - a Geben Sie einen Sitzungsnamen ein.
    - b Geben Sie die lokale IP-Adresse und die Remote-IP-Adresse ein.
    - c Geben Sie den Peer-Code vom L2VPN-Server ein. Einzelheiten zum Abrufen des Peer-Codes finden Sie unter [Herunterladen der L2-VPN-Konfigurationsdatei der Remotesite](#).
  - 16 Klicken Sie auf **Speichern**.
  - 17 Wählen Sie **Port > Port hinzufügen** aus, um einen L2-Erweiterungsport zu erstellen.
  - 18 Geben Sie einen Namen und ein VLAN ein und wählen Sie eine Exit-Schnittstelle aus.
  - 19 Klicken Sie auf **Speichern**.
  - 20 Wählen Sie **L2VPN > Port anhängen** aus und geben Sie die folgenden Werte ein:
    - a Wählen Sie die von Ihnen erstellte L2-VPN-Sitzung aus.
    - b Wählen Sie den von Ihnen erstellten L2-Erweiterungsport aus.

- c Geben Sie eine Tunnel-ID ein.

## 21 Klicken Sie auf **Anhängen**.

Sie können zusätzliche L2-Erweiterungsports erstellen und Sie an die Sitzung anhängen, wenn Sie mehrere L2-Netzwerke erweitern müssen.

## 22 Melden Sie sich über den Browser beim autonomen NSX Edge an oder verwenden Sie API-Aufrufe, um den Status der L2VPN-Sitzung anzuzeigen.

---

**Hinweis** Wenn sich die Konfiguration des L2VPN-Servers ändert, stellen Sie sicher, dass Sie den Peer-Code erneut herunterladen und die Sitzung mit dem neuen Peer-Code aktualisieren.

---

# 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.

---

**Hinweis** DNAT wird auf einem Gateway der Ebene 1 nicht unterstützt, bei dem richtlinienbasiertes IPsec-VPN konfiguriert ist.

---

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.
  - Für SNAT ist die externe Adresse die übersetzte Quelladresse, nachdem NAT abgeschlossen ist.
  - Für DNAT ist die externe Adresse die übersetzte Zieladresse, bevor NAT abgeschlossen ist.
  - Für REFLEXIV wird die Firewall für ausgehenden Datenverkehr auf die übersetzte Quelladresse angewendet, nachdem NAT abgeschlossen ist. Für eingehenden Datenverkehr wird die Firewall auf die ursprüngliche Zieladresse angewendet, bevor NAT abgeschlossen ist.
- **Interne Adresse abgleichen:** Das Paket wird von Firewallregeln verarbeitet, die der Kombination aus ursprünglicher IP-Adresse und ursprünglichem Port entsprechen.
  - Für SNAT ist die interne Adresse die ursprüngliche Quelladresse, bevor NAT abgeschlossen ist.
  - Für DNAT ist die interne Adresse die übersetzte Zieladresse, nachdem NAT abgeschlossen ist.
  - Für REFLEXIV wird für ausgehenden Datenverkehr die Firewall auf die ursprüngliche Quelladresse angewendet, bevor NAT abgeschlossen ist. Für eingehenden Datenverkehr wird die Firewall auf die übersetzte Zieladresse angewendet, nachdem NAT abgeschlossen ist.

- **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.

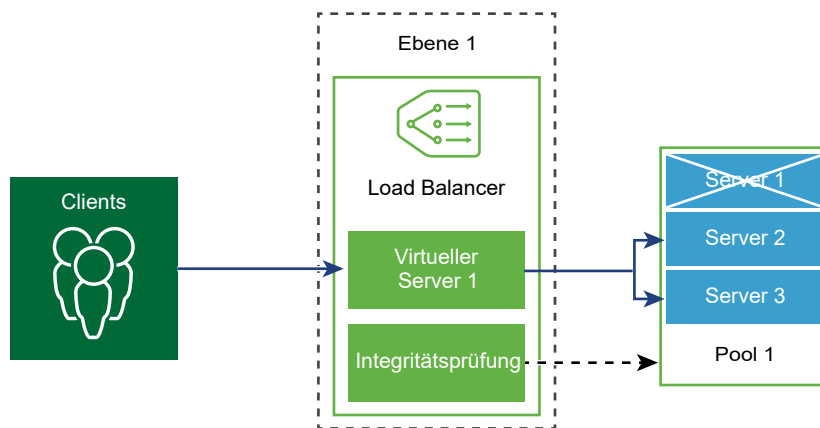
Ein niedrigerer Wert bedeutet eine höhere Priorität. Die Standardeinstellung ist 100.

15 Klicken Sie auf **Speichern**.

# Load Balancing

# 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. 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 auf dem Tier-1-Gateway unterstützt. Ein Load Balancer kann nur an ein Tier-1-Gateway angehängt werden.

---

Dieses Kapitel enthält die folgenden Themen:

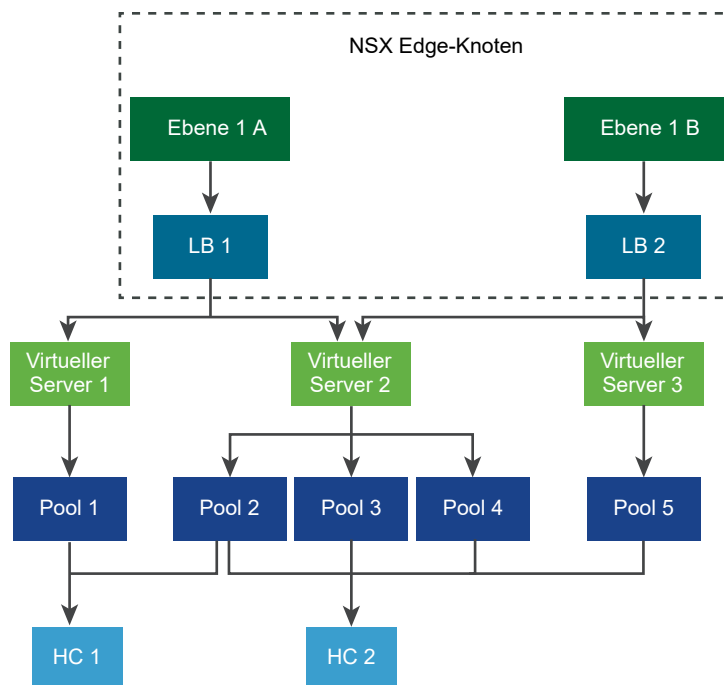
- Wichtige Load Balancer-Konzepte
- Einrichten von Load Balancer-Komponenten
- Für Serverpools und virtuelle Server erstellte Gruppen

## 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

Wenn Sie einen Load Balancer konfigurieren, können Sie eine Größe (klein, mittel oder groß) angeben. Die Größe bestimmt die Anzahl der virtuellen Server, Serverpools und Poolmitglieder, die der Load Balancer unterstützen kann.

Ein Load Balancer wird auf einem Tier-1-Gateway der ausgeführt, das sich im Aktiv/Standby-Modus befinden muss. Das Gateway wird auf NSX Edge Knoten ausgeführt. Der Formfaktor des NSX Edge-Knotens (Bare Metal, klein, mittel oder groß) bestimmt die Anzahl der Load Balancer, die der NSX Edge-Knoten unterstützen kann. Auf der Registerkarte **Netzwerk und Sicherheit – Erweitert** bezieht sich der Begriff „logischer Router“ auf ein Gateway.



Weitere Informationen darüber, welche Optionen die unterschiedlichen Load Balancer-Größen und NSX Edge-Formfaktoren unterstützen können, finden Sie unter <https://configmax.vmware.com>.

In einer Produktionsumgebung sollten keine kleinen NSX Edge-Knoten zur Ausführung eines kleinen Load Balancer verwendet werden.

Sie können eine API aufrufen, um die Load Balancer-Nutzungsinformationen für einen NSX Edge-Knoten abzurufen. Wenn Sie die Registerkarte **Netzwerk** verwenden, um das Load Balancing zu konfigurieren, führen Sie den folgenden Befehl aus:

```
GET /policy/api/v1/infra/lb-node-usage?node_path=<node-path>
```

Wenn Sie die Registerkarte **Netzwerk und Sicherheit – Erweitert** verwenden, um das Load Balancing zu konfigurieren, führen Sie den folgenden Befehl aus:

```
GET /api/v1/loadbalancer/usage-per-node/<node-id>
```

Die Nutzungsinformationen umfassen die Anzahl der Load Balancer-Objekte (z. B. Load Balancer-Dienste, virtuelle Server, Serverpools und Poolmitglieder), die auf dem Knoten konfiguriert sind. Weitere Informationen finden Sie im *Handbuch zur NSX-T Data Center-API*.

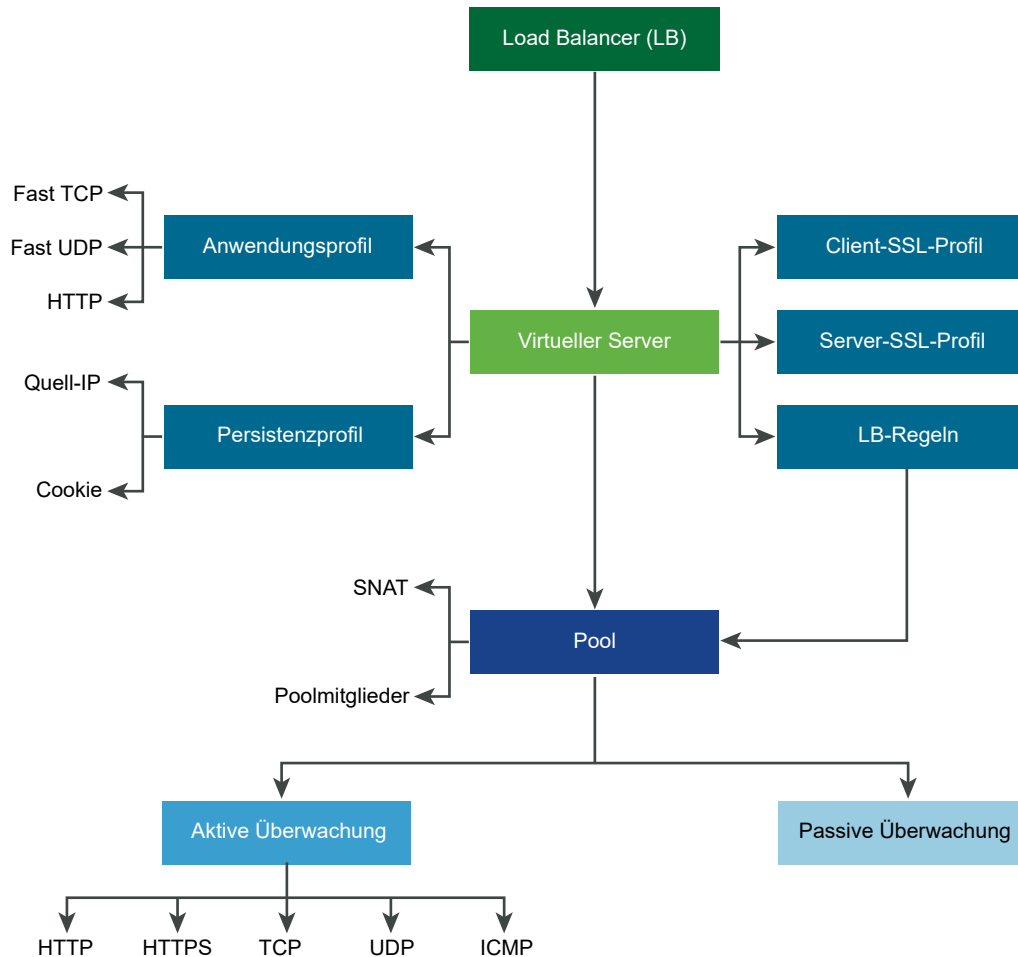
## Unterstützte Load Balancer-Funktionen

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.

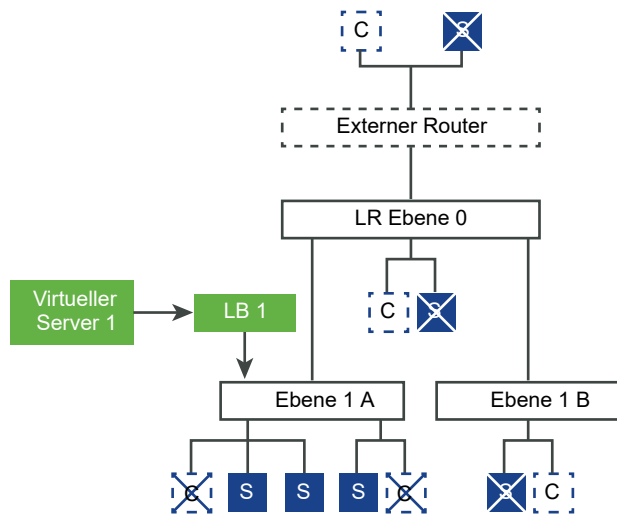


## Load Balancer-Topologien

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

### Inline-Topologie

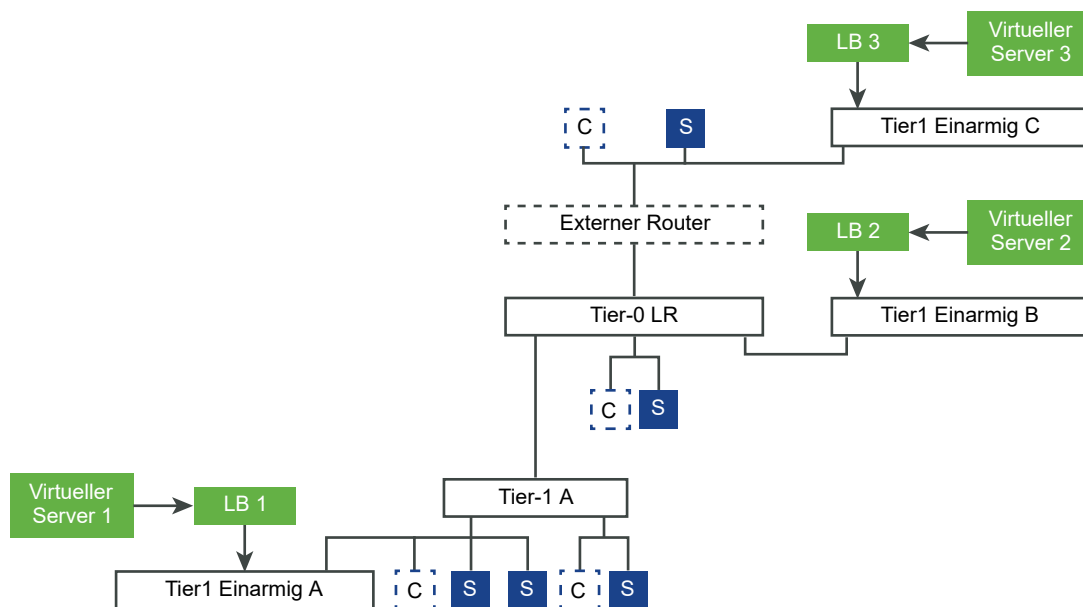
Im Inline-Modus befindet sich der Load Balancer im Datenverkehrspfad zwischen dem Client und dem Server. Clients und Server sollten nicht mit Überlagerungssegmenten auf demselben logischen Tier-1-Router verbunden sein, wenn SNAT auf dem Load Balancer nicht erwünscht ist. Wenn Clients und Server mit Überlagerungssegmenten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

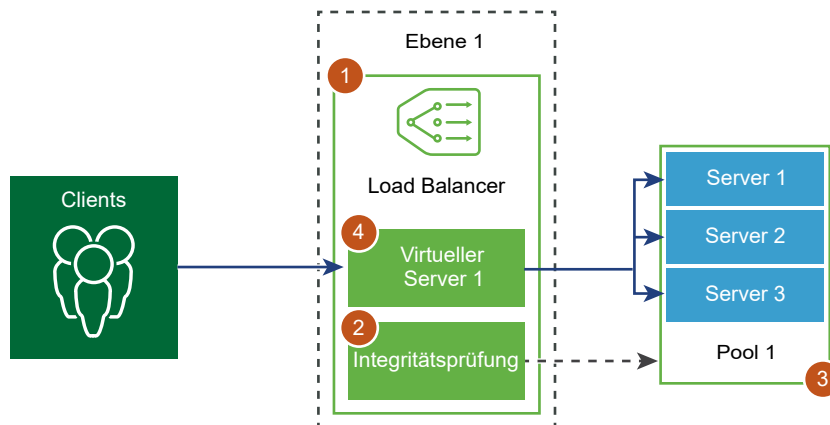
Zur Verwendung logischer Load Balancers müssen Sie zuerst einen Load Balancer konfigurieren und ihn dann an ein Tier-1-Gateway anhängen.

---

**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 Balancers

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

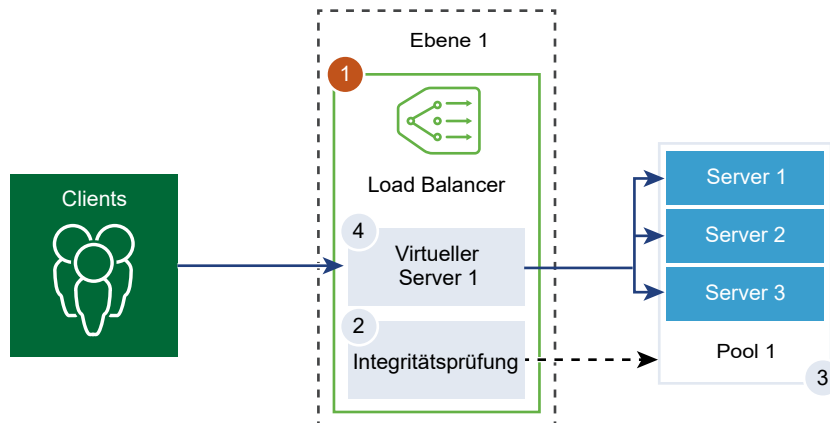
---

**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 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.

## 9 (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.

---

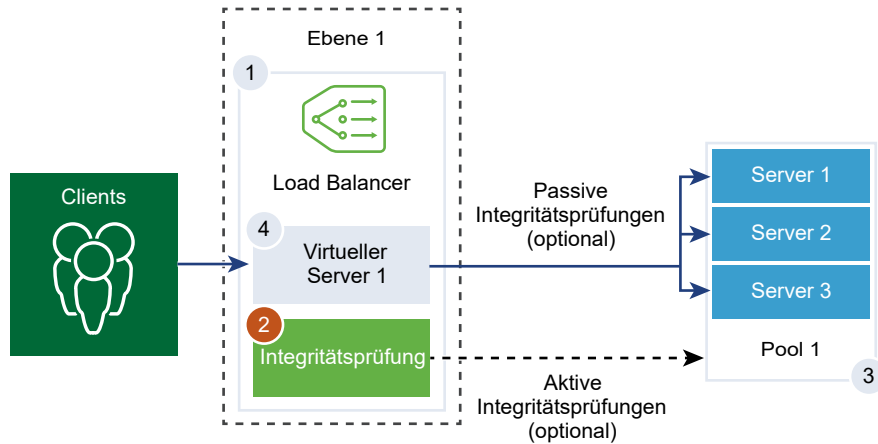
Server, die innerhalb eines bestimmten Zeitraums nicht oder mit Fehlern reagieren, werden solange aus der künftigen Verbindungsverarbeitung ausgeschlossen, bis durch eine nachträgliche regelmäßig durchgeführte Systemdiagnose sichergestellt wird, dass die betreffenden Server ordnungsgemäß ausgeführt werden.

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.
<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.

Option	Beschreibung
Anzahl bis zum erneuten Versuch	Legen Sie einen Wert fest, der angibt, nach welcher Zeit ein erneuter Verbindungsversuch mit dem Server unternommen wird, um herauszufinden, ob er verfügbar ist.
Tags	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
HTTP-Methode	Wählen Sie die Methode (GET, OPTIONS, POST, HEAD und PUT) zur Erkennung des Serverstatus im Dropdown-Menü aus.
HTTP-Anforderungs-URL	Geben Sie die Anforderungs-URI für die Methode ein.
HTTP-Anforderungsversion	Wählen Sie die unterstützte Anforderungsversion im Dropdown-Menü aus. Sie können auch die Standardversion HTTP_VERSION_1 übernehmen.
HTTP-Antwort-Header	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.
HTTP-Anforderungstext	Geben Sie den Anforderungstext ein. Gültig für die Methoden POST und PUT.
HTTP-Antwortcode	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.
HTTP-Antworttext	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
Gesendete UDP-Daten	Geben Sie die Zeichenfolge ein, die nach dem Verbindungsaufbau an den Server gesendet werden soll.
Erwartete UDP-Daten	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.

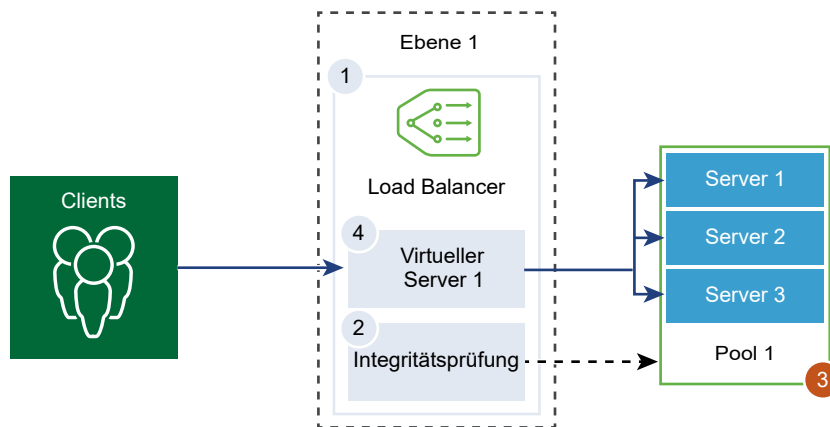
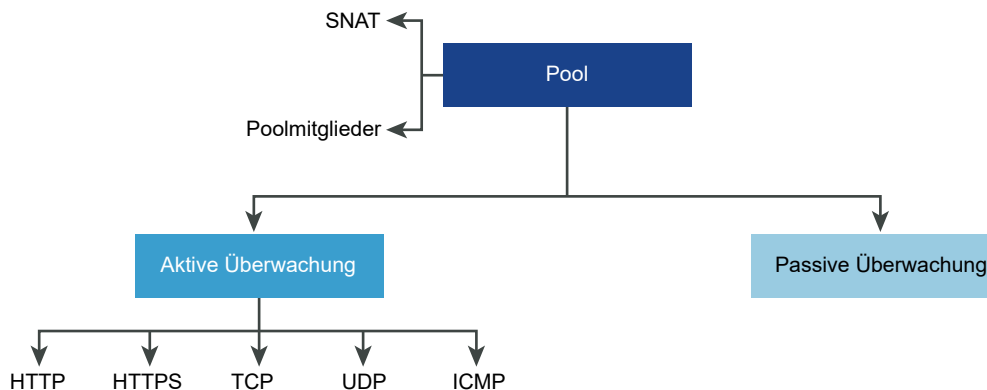


Abbildung 7-1. Konfiguration der Serverpool-Parameter



#### 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 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.

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 Load Balancing-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>	<p>Wählt einen Server auf der Basis eines Hash der Quell-IP-Adresse und der gesamten Gewichtung aller ausgeführten Server aus.</p>

## 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 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.</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.</p> <p>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 und optional eine Beschreibung ein.</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 Load Balancer 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 Load Balancer 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.

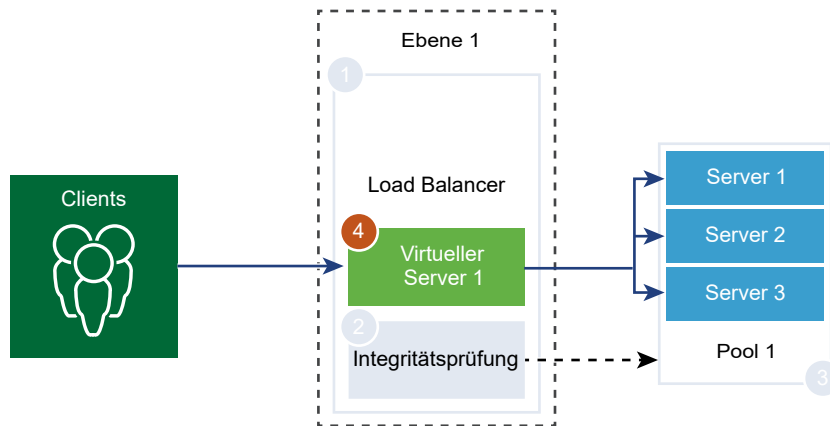
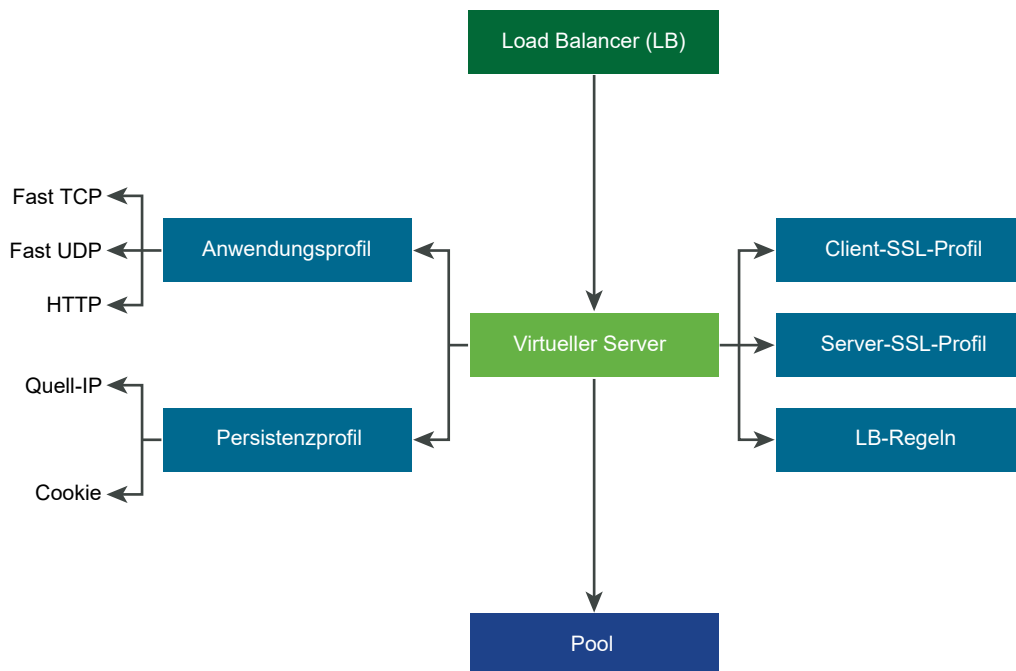


Abbildung 7-2. Komponenten des virtuellen Servers



## 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

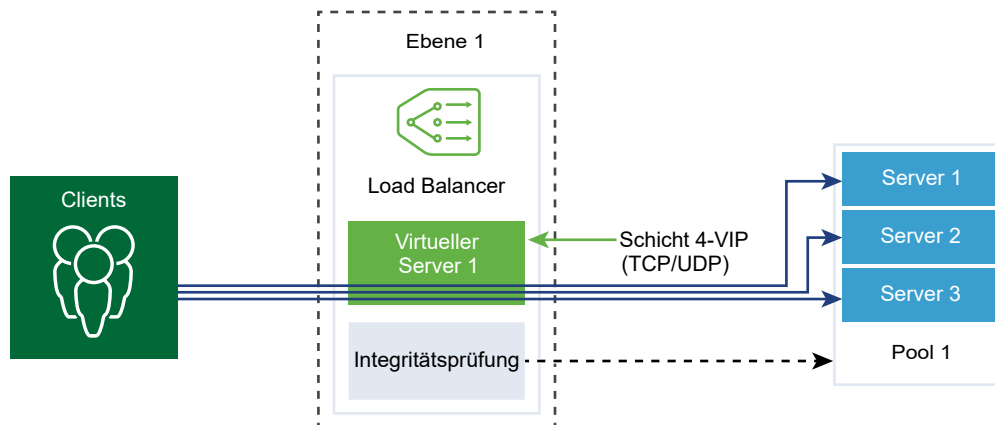
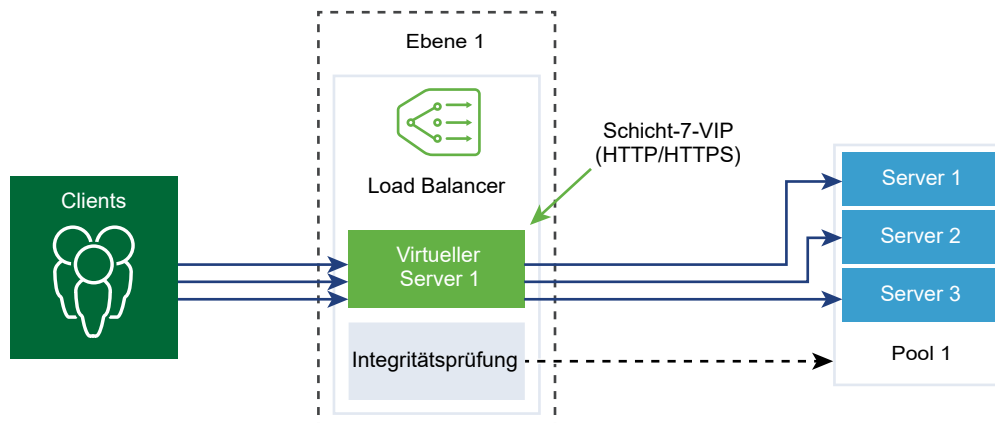


Abbildung 7-4. HTTPS-Anwendungsprofil der Schicht 7



## 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.</p> <p>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
Umleitung	<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

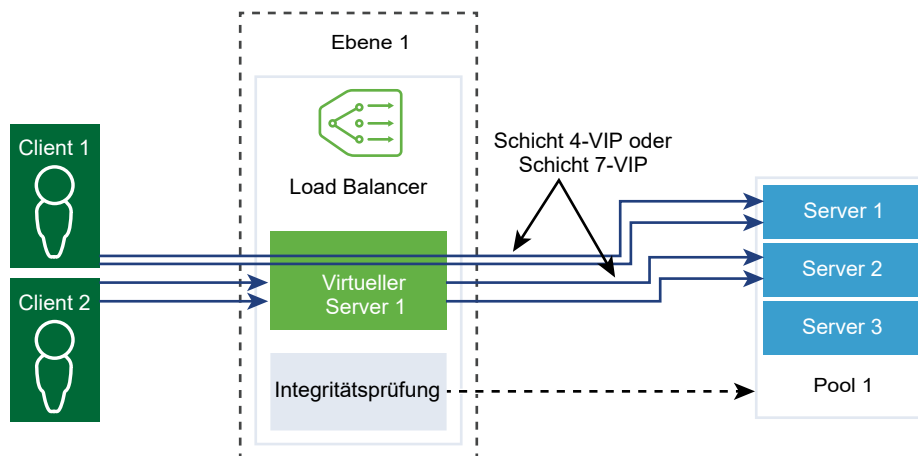
Zur Gewährleistung der Stabilität von statusbehafteten Anwendungen implementieren Load Balancer Persistenz, die alle zugehörigen Verbindungen an denselben Server weiterleitet. Es werden verschiedene Arten von Persistenz unterstützt, um die unterschiedlichen Anwendungsanforderungen zu erfüllen.

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. Beachten Sie, dass ein Leerzeichen in einem Cookienamen **nicht** unterstützt wird.

Das generische Persistenzprofil unterstützt die Persistenz basierend auf dem HTTP-Header, Cookie oder der URL in der HTTP-Anforderung. Aus diesem Grund unterstützt es die Persistenz von App-Sitzungen, wenn die Sitzungs-ID Teil der URL ist. Dieses Profil ist nicht direkt mit einem virtuellen Server verknüpft. Sie können dieses Profil angeben, wenn Sie eine Load Balancer-Regel für die Anforderungsweiterleitung und die Umschreibung der Antwort 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 > 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 Persistenztable des Load Balancers enthält Einträge, die die Weiterleitung von Clientanforderungen an denselben Server aufzeichnen. Bei der allerersten Verbindung von einer neuen Client-IP erfolgt ein Lastausgleich mit einem Poolmitglied. NSX speichert diesen Persistenzeintrag in der LB-Persistenztable, die auf dem Edge-Knoten, der den aktiven T1-LB hostet, mit folgendem CLI-Befehl angezeigt werden kann:</p> <pre>get load-balancer &lt;LB-UUID&gt; persistence-tables.</pre> <ul style="list-style-type: none"> <li>■ Wenn Verbindungen von diesem Client mit der VIP vorhanden sind, wird der Persistenzeintrag beibehalten.</li> <li>■ Wenn keine Verbindungen mehr zwischen diesem Client und der VIP vorhanden sind, wird der Timer für den Persistenzeintrag gemäß dem Wert unter „Zeitüberschreitung für Persistenzeintrag“ heruntergezählt. Wenn vor dem Ablauf des Timers keine neue Verbindung zwischen diesem Client und der VIP hergestellt wird, wird der Persistenzeintrag für diese Client-IP gelöscht. Wenn der Client nach dem Löschen des Eintrags wieder aktiv wird, erfolgt erneut ein Lastausgleich mit einem Poolmitglied gemäß dem Lastausgleichsalgorithmus.</li> </ul>
<b>Bei voller Tabelle Einträge löschen</b>	<p>Ein hoher Wert für die Zeitüberschreitung führt möglicherweise dazu, dass die Persistenztable sich schnell füllt, wenn der Datenverkehr hoch ist. Wenn diese Option aktiviert ist, wird für den aktuellen Eintrag der älteste Eintrag gelöscht.</p> <p>Wenn diese Option deaktiviert und die Quell-IP-Persistenztable voll ist, werden neue Clientverbindungen abgelehnt.</p>
<b>HA-Persistenzspiegelung</b>	<p>Schalten Sie die Schaltfläche um, um Persistenzeinträge mit dem HA-Peer zu synchronisieren. Wenn die HA-Persistenzspiegelung aktiviert ist, bleibt die Client-IP-Persistenz im Falle eines Failover-Vorgangs für den Load Balancer bestehen.</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>

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

Option	Beschreibung
<b>Name und Beschreibung</b>	<p>Geben Sie einen Namen und eine Beschreibung für das Cookie-Persistenzprofil ein.</p>
<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>	Wählen Sie im Dropdown-Menü einen Modus aus. <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>Cookieiname</b>	Geben Sie den Cookienamen ein. Ein Leerzeichen wird in einem Cookienamen <b>nicht</b> unterstützt.
<b>Cookiedomäne</b>	Geben Sie den Domännennamen ein. Die HTTP-Cookiedomäne kann nur im Modus EINFÜGEN konfiguriert werden.
<b>Cookie-Fallback</b>	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. 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.
<b>Cookiepfad</b>	Geben Sie den URL-Pfad des Cookies ein. Der HTTP-Cookiepfad kann nur im Modus EINFÜGEN festgelegt werden.
<b>Cookieverschlüsselung</b>	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. Verschlüsseln Sie die Informationen zu IP-Adresse und Port des Cookieservers.
<b>Cookie-Typ</b>	Wählen Sie im Dropdown-Menü einen Cookietyp aus. <b>Sitzungs-Cookie</b> – nicht gespeichert. Geht verloren, wenn der Browser geschlossen wird. <b>Persistenz-Cookie</b> – wird vom Browser gespeichert. Geht nicht verloren, wenn der Browser geschlossen wird.
<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>	Geben Sie Tags ein, um die Suche zu vereinfachen. Sie können ein Tag angeben, um einen Geltungsbereich des Tags festzulegen.

- 5 Wählen Sie **Generisch** aus, um ein generisches Persistenzprofil hinzuzufügen und geben Sie die Profildetails ein.

Option	Beschreibung
<b>Name und Beschreibung</b>	Geben Sie einen Namen und eine Beschreibung für das Quell-IP-Persistenzprofil ein.
<b>Persistenz freigeben</b>	Klicken Sie auf die Schaltfläche, um das Profil auf den virtuellen Servern freizugeben.

Option	Beschreibung
<b>Zeitüberschreitung für Persistenzeintrag</b>	<p>Geben Sie den Zeitraum für die Persistenz bis zum Ablauf in Sekunden ein. Die Persistenztafel des Load Balancers enthält Einträge, die die Weiterleitung von Clientanforderungen an denselben Server aufzeichnen. Bei der allerersten Verbindung von einer neuen Client-IP erfolgt ein Lastausgleich mit einem Poolmitglied. NSX speichert diesen Persistenzeintrag in der LB-Persistenztafel, die auf dem Edge-Knoten, der den aktiven T1-LB hostet, mit folgendem CLI-Befehl angezeigt werden kann:</p> <pre>get load-balancer &lt;LB-UUID&gt; persistence-tables.</pre> <ul style="list-style-type: none"> <li>■ Wenn Verbindungen von diesem Client mit der VIP vorhanden sind, wird der Persistenzeintrag beibehalten.</li> <li>■ Wenn keine Verbindungen mehr zwischen diesem Client und der VIP vorhanden sind, wird der Timer für den Persistenzeintrag gemäß dem Wert unter „Zeitüberschreitung für Persistenzeintrag“ heruntergezählt. Wenn vor dem Ablauf des Timers keine neue Verbindung zwischen diesem Client und der VIP hergestellt wird, wird der Persistenzeintrag für diese Client-IP gelöscht. Wenn der Client nach dem Löschen des Eintrags wieder aktiv wird, erfolgt erneut ein Lastausgleich mit einem Poolmitglied gemäß dem Lastausgleichsalgorithmus.</li> </ul>
<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. 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

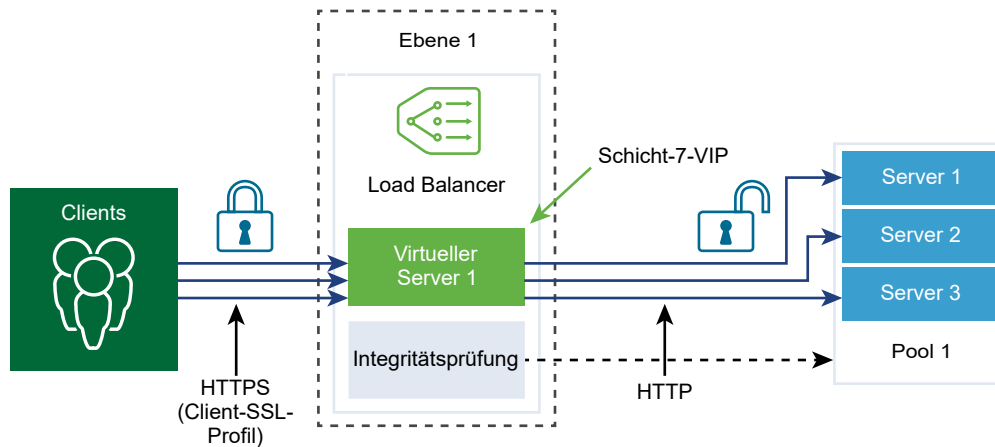
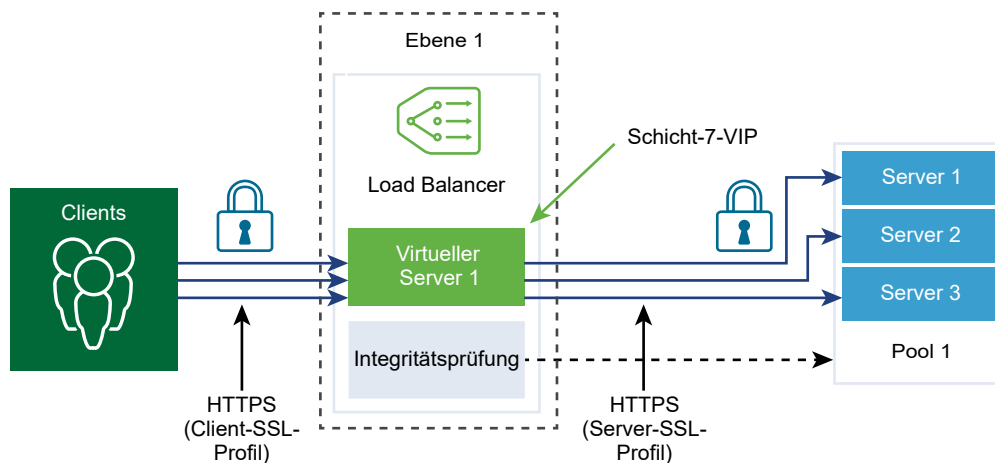


Abbildung 7-6. End-to-End-SSL



## 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>	<p>Wählen Sie die SSL-Verschlüsselungsgruppe im Dropdown-Menü aus, und die in das Client-SSL-Profil aufzunehmenden verfügbaren SSL-Verschlüsselungen und -Protokolle werden befüllt.</p> <p>Die SSL-Verschlüsselungsgruppe „Ausgeglichen“ stellt den Standardwert dar.</p>
<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>	<p>Geben Sie Tags ein, um die Suche zu vereinfachen.</p> <p>Sie können ein Tag angeben, um einen Geltungsbereich des Tags festzulegen.</p>
<b>Unterstützte SSL-Verschlüsselungen</b>	<p>Je nach zugewiesener SSL-Suite werden die unterstützten SSL-Verschlüsselungen hier aufgefüllt. Klicken Sie auf <b>Mehr anzeigen</b>, um die gesamte Liste anzuzeigen.</p> <p>Bei Auswahl von <b>Benutzerdefiniert</b> müssen Sie die SSL-Verschlüsselungen im Dropdown-Menü auswählen.</p>
<b>Unterstützte SSL-Protokolle</b>	<p>Je nach zugewiesener SSL-Suite werden die unterstützten SSL-Protokolle hier aufgefüllt. Klicken Sie auf <b>Mehr anzeigen</b>, um die gesamte Liste anzuzeigen.</p> <p>Bei Auswahl von <b>Benutzerdefiniert</b> müssen Sie die SSL-Verschlüsselungen im Dropdown-Menü auswählen.</p>
<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>	<p>Schalten Sie die Schaltfläche um, sodass der Server die erste unterstützte Verschlüsselung aus der Liste auswählen kann, die er unterstützen kann.</p> <p>Während eines SSL-Handshakes sendet der Client eine sortierte Liste der unterstützten Verschlüsselungen an den Server.</p>

### 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>	<p>Wählen Sie die SSL-Verschlüsselungsgruppe im Dropdown-Menü aus, und die in das Server-SSL-Profil aufzunehmenden verfügbaren SSL-Verschlüsselungen und -Protokolle werden befüllt.</p> <p>Die SSL-Verschlüsselungsgruppe „Ausgeglichen“ stellt den Standardwert dar.</p>
<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.

Option	Beschreibung
<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.
<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>	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. Sie können auf die vertikalen Punkte klicken, um einen Serverpool zu erstellen.
<b>Anwendungsprofil</b>	Je nach Protokolltyp wird das vorhandene Anwendungsprofil automatisch befüllt. Sie können auf die vertikalen Punkte klicken, um ein Anwendungsprofil zu erstellen.
<b>Persistenz</b>	Wählen Sie im Dropdown-Menü ein vorhandenes Persistenzprofil aus. Das Persistenzprofil kann auf einem virtuellen Server aktiviert werden, damit auf die Quell-IP bezogene Clientverbindungen an denselben Server gesendet werden können.
<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.

Option	Beschreibung
<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 Zielport gesendet.
<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>	Geben Sie Tags ein, um die Suche zu vereinfachen. Sie können ein Tag angeben, um einen Geltungsbereich des Tags festzulegen.

#### 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>	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. Sie können auf die vertikalen Punkte klicken, um einen Serverpool zu erstellen.
<b>Anwendungsprofil</b>	Je nach Protokolltyp wird das vorhandene Anwendungsprofil automatisch befüllt. Sie können auf die vertikalen Punkte klicken, um ein Anwendungsprofil zu erstellen.
<b>Persistenz</b>	Wählen Sie im Dropdown-Menü ein vorhandenes Persistenzprofil aus. Das Persistenzprofil kann auf einem virtuellen Server aktiviert werden, damit auf die Quell-IP bezogene Clientverbindungen an denselben Server gesendet werden können.

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 Zielport gesendet.
<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>	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.

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

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.

---

**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 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-Profiles](#).
- 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.
<b>Serverpool</b>	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. Sie können auf die vertikalen Punkte klicken, um einen Serverpool zu erstellen.
<b>Anwendungsprofil</b>	Je nach Protokolltyp wird das vorhandene Anwendungsprofil automatisch befüllt. Sie können auf die vertikalen Punkte klicken, um ein Anwendungsprofil zu erstellen.
<b>Persistenz</b>	Wählen Sie im Dropdown-Menü ein vorhandenes Persistenzprofil aus. 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.

- 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>	Klicken Sie auf den Schalter, um das Profil zu aktivieren. Clientseitige SSL-Profilbindung ermöglicht mehrere Zertifikate, damit verschiedene Hostnamen mit demselben virtuellen Server verbunden werden können.
<b>Standardzertifikat</b>	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.

Option	Beschreibung
<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.

Option	Beschreibung
<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 Zielport gesendet.
<b>Administrativer Zustand</b>	Klicken Sie auf den Schalter, um den administrativen Zustand des virtuellen Servers der Schicht 7 zu deaktivieren.
<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.

## 8 Klicken Sie auf **Speichern**.

### Anzeigen von Load Balancer-Regeln

Auf virtuellen HTTP-Servern der Schicht 7 können Sie optional Load Balancer-Regeln konfigurieren und das Load Balancing-Verhalten 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:s)`ensitive“, sondern stattdessen „Case `((?i:s)`ensitive)“.

- 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
- \$\_arg\_<name> - argument <name> in der Anforderungszeile
- \$\_cookie\_<name> – Wert des <name>-Cookies
- \$\_upstream\_cookie\_<name> – Cookie mit dem angegebenen Namen, der vom vorgeschalteten Server im Antwortheader-Feld „Set-Cookie“ gesendet wurde
- \$\_upstream\_http\_<name> – beliebiges Antwortheader-Feld; <name> ist der Feldname konvertiert in Kleinbuchstaben, wobei Bindestriche durch Unterstriche ersetzt wurden
- \$\_host – in der folgenden Rangfolge: der Hostname aus der Anforderungszeile oder der Hostname im Anforderungsheader-Feld „Host“ oder der mit einer Anforderung übereinstimmende Servername

- `$_http_<name>` – beliebiges Feld des Anforderungsheaders; `<name>` ist der Name des Felds, konvertiert in Kleinbuchstaben, in dem Bindestriche durch Unterstriche ersetzt wurden.
- `$_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
- `$_server_protocol` – Anforderungsprotokoll, in der Regel „HTTP/1.0“ oder „HTTP/1.1“
- (Nur NSX-T Data Center 2.5.0) `$_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.
- (Nur NSX-T Data Center 2.5.1 und höher) `$_Ssl_client_escaped_cert` – Gibt für eine hergestellte SSL-Verbindung das Clientzertifikat im PEM-Format zurück.
- `$_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 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
HTTP-Anforderungsmethode	Zuordnen einer HTTP-Anforderungsmethode. http_request.method – zuzuordnender Wert
HTTP-Anforderungs-URI	Zuordnen einer HTTP-Anforderungs-URI ohne Abfrageargumente. http_request.uri – zuzuordnender Wert
Argumente des HTTP-Anforderungs-URI	Zuordnen des Abfragearguments eines HTTP-Anforderungs-URI. http_request.uri_arguments – zuzuordnender Wert
HTTP-Anforderungsversion	Zuordnen einer HTTP-Anforderungsversion. http_request.version – zuzuordnender Wert
HTTP-Anforderungs-Header	Zuordnen eines beliebigen HTTP-Anforderungs-Headers. http_request.header_name – zuzuordnender Header-Name http_request.header_value – zuzuordnender Wert
HTTP-Anforderungs-Cookie	Zuordnung eines beliebigen HTTP-Anforderungs-Cookies. http_request.cookie_value – zuzuordnender Wert
HTTP-Anforderungstext	Zuordnen des Inhalts eines HTTP-Anforderungstexts. http_request.body_value – zuzuordnender Wert
Client-SSL	Zuordnen der Client-SSL-Profil-ID. ssl_profile_id – zuzuordnender Wert
Port des TCP-Headers	Zuordnen einer TCP-Quelle oder des Zielports. tcp_header.source_port – zuzuordnender Quellport tcp_header.destination_port – zuzuordnender Zielport
Quelle des IP-Headers	Zuordnen einer IP-Quelladresse oder -Zieladresse ip_header.source_address – zuzuordnende Quelladresse ip_header.destination_address – zuzuordnende Zieladresse
Variable	Erstellen einer Variablen und Zuweisen eines Wertes zu der Variablen.
Groß-/Kleinschreibung beachten	Festlegen eines Flags für den HTTP-Kopfzeilenwertvergleich. Bei dem Flag wird die Groß-/Kleinschreibung beachtet.

Aktionen	Beschreibung
HTTP-Anforderungs-URI umschreiben	Ändern eines URI. http_request.uri – zu schreibender URI (ohne Abfrageargumente) http_request.uri_args – zu schreibende URI-Abfrageargumente
HTTP-Anforderungs-Header umschreiben	Ändern des Werts eines HTTP-Headers. http_request.header_name – Name des Headers http_request.header_value – zu schreibender Wert
HTTP-Anforderungsheader löschen	Löschen des HTTP-Headers.

Aktionen	Beschreibung
	http_request.header_delete – Name des Headers http_request.header_delete – zu schreibender Wert

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

Alle Übereinstimmungswerte akzeptieren reguläre Ausdrücke.

Unterstützte Übereinstimmungsbedingung	Beschreibung
HTTP-Anforderungsmethode	Zuordnen einer HTTP-Anforderungsmethode. http_request.method – zuzuordnender Wert
HTTP-Anforderungs-URI	Zuordnen eines HTTP-Anforderungs-URI. http_request.uri – zuzuordnender Wert
HTTP-Anforderungsversion	Zuordnen einer HTTP-Anforderungsversion. http_request.version – zuzuordnender Wert
HTTP-Anforderungs-Header	Zuordnen eines beliebigen HTTP-Anforderungs-Headers. http_request.header_name – zuzuordnender Header-Name http_request.header_value – zuzuordnender Wert
HTTP-Anforderungs-Cookie	Zuordnung eines beliebigen HTTP-Anforderungs-Cookies. http_request.cookie_value – zuzuordnender Wert
HTTP-Anforderungstext	Zuordnen des Inhalts eines HTTP-Anforderungstexts. http_request.body_value – zuzuordnender Wert
Client-SSL	Zuordnen der Client-SSL-Profil-ID. ssl_profile_id – zuzuordnender Wert
Port des TCP-Headers	Zuordnen einer TCP-Quelle oder des Zielports. tcp_header.source_port – zuzuordnender Quellport tcp_header.destination_port – zuzuordnender Zielport
Quelle des IP-Headers	Zuordnen einer IP-Quelladresse oder -Zieladresse ip_header.source_address – zuzuordnende Quelladresse ip_header.destination_address – zuzuordnende Zieladresse
Variable	Erstellen einer Variablen und Zuweisen eines Wertes zu der Variablen.
Groß-/Kleinschreibung beachten	Festlegen eines Flags für den HTTP-Kopfzeilenwertvergleich. Bei dem Flag wird die Groß-/Kleinschreibung beachtet.

Aktion	Beschreibung
HTTP-Ablehnung	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
HTTP-Umleitung	Umleiten einer Anforderung. Statuscode muss auf 3xx gesetzt werden. http_forward.redirect_status – HTTP-Statuscode für Umleiten http_forward.redirect_url – HTTP-Umleitungs-URL



Aktion	Beschreibung
<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>Variablenpersistenz-Überprüfung</b>	Wählen Sie ein generisches Persistenz-Profil aus und geben Sie einen Variablennamen ein.  Sie können auch <b>Hash-Variable</b> aktivieren. Wenn der Variablenwert sehr lang ist, wird durch das Hashing der Variablen sichergestellt, dass sie ordnungsgemäß in der Persistenztafel gespeichert wird. Wenn <b>Hash-Variable</b> nicht aktiviert ist, wird nur der feste Präfixteil des Variablenwerts in der Persistenztafel gespeichert, wenn der Variablenwert sehr lang ist. Daher können zwei unterschiedliche Anforderungen mit langen Variablenwerten an denselben Backend-Server gesendet werden (weil ihre Variablenwerte denselben Präfixteil aufweisen), wenn Sie an verschiedene Backend-Server weitergeleitet werden sollen.
<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>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

Unterstützte Übereinstimmungsbedingung	Beschreibung
Quelle des IP-Headers	Zuordnen einer IP-Quelladresse oder -Zieladresse ip_header.source_address – zuzuordnende Quelladresse ip_header.destination_address – zuzuordnende Zieladresse
Variable	Erstellen einer Variablen und Zuweisen eines Wertes zu der Variablen.
Groß-/Kleinschreibung beachten	Festlegen eines Flags für den HTTP-Kopfzeilenwertvergleich. Bei dem Flag wird die Groß-/Kleinschreibung beachtet.

Aktion	Beschreibung
HTTP-Antwort-Header umschreiben	Ändern des Werts eines HTTP-Antwort-Headers. Http_response.header_name – Name des Headers Http_response.header_value – zu schreibender Wert
HTTP-Antwort-Header löschen	Löschen des HTTP-Headers. http_request.header_delete – Name des Headers http_request.header_delete – zu schreibender Wert
Variablenpersistenz-Lernvorgang	Wählen Sie ein generisches Persistenz-Profil aus und geben Sie einen Variablennamen ein.  Sie können auch <b>Hash-Variable</b> aktivieren. Wenn der Variablenwert sehr lang ist, wird durch das Hashing der Variablen sichergestellt, dass sie ordnungsgemäß in der Persistenztabelle gespeichert wird. Wenn <b>Hash-Variable</b> nicht aktiviert ist, wird nur der feste Präfixteil des Variablenwerts in der Persistenztabelle gespeichert, wenn der Variablenwert sehr lang ist. Daher können zwei unterschiedliche Anforderungen mit langen Variablenwerten an denselben Backend-Server gesendet werden (weil ihre Variablenwerte denselben Präfixteil aufweisen), wenn Sie an verschiedene Backend-Server weitergeleitet werden sollen.

## Für Serverpools und virtuelle Server erstellte Gruppen

NSX Manager erstellt automatisch Gruppen für Load Balancer-Serverpools und VIP-Ports.

Vom Load Balancer erstellte Gruppen werden unter **Bestand > Gruppen** angezeigt.

Serverpool-Gruppen werden mit dem NLB.PoolLB-Namen *Pool\_Name LB\_Name* mit zugewiesenen Gruppenmitglieder-IP-Adressen erstellt:

- Pool konfiguriert ohne LB-SNAT (transparent): 0.0.0.0/0
- Pool konfiguriert ohne automatische LB-SNAT-Zuordnung: T1-Uplink IP 100.64.x.y und T1-ServiceInterface IP
- Pool konfiguriert ohne LB-SNAT-IP-Pool: LB-SNAT IP-Pool

VIP-Gruppen werden mit dem NLB.VIP-Namen *Name des virtuellen Servers* erstellt, wobei die VIP-Gruppenmitglieder-IP-Adressen „VIP IP@“ lauten.

Für Serverpool-Gruppen können Sie eine Regel für eine verteilte Firewall für den Datenverkehr vom Load Balancer erstellen (NLB.PoolLB. *Pool\_Name LB\_Name*). Für die Tier-1-Gateway-Firewall können Sie Datenverkehr von Clients an LB VIP NLB.VIP.*Name des virtuellen Servers* zulassen.

# 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** Einzelheiten zur Verwaltung Ihrer Public Cloud-Arbeitslast-VMs mit NSX-T Data Center finden Sie unter [Kapitel 22 Verwenden von NSX Cloud](#).

---

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 Ein **Route zum Underlay** für den gesamten Datenverkehr innerhalb einer Transit-/Computing-VPC bzw. eines Transit-/Computing-VNet.
- 2 Eine weitere **Route zum Underlay** für den gesamten Datenverkehr an die Metadatendienste der Public Cloud.
- 3 Eine **Route zum Overlay** für den restlichen 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 weitergeleitet.

**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 geleitet 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.

## Unterstützte Weiterleitungsrichtlinien und häufige Anwendungsfälle

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

- Route zum Underlay
- Route vom Underlay
- Route zum Overlay

Dies sind die allgemeinen Szenarien, in denen Weiterleitungsrichtlinien nützlich sind:

- **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 Klicken Sie in der Spalte **Subnetze** auf **Festlegen**, um Subnetze hinzuzufügen.

- 6 Wählen Sie zum Angeben eines Adressblocks **Subnetz hinzufügen > IP-Block** aus.
  - a Wählen Sie einen IP-Block aus.
  - b Geben Sie eine Größe an.
  - c Klicken Sie auf den Umschalter **Gateway automatisch zuweisen**, um die automatische Gateway-IP-Zuweisung zu aktivieren oder zu deaktivieren.
  - d Klicken Sie auf **Hinzufügen**.
- 7 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**.
- 8 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
- Ost-West-Netzwerksicherheit – Verkettung von Drittanbieterdiensten
- Konfigurieren einer Gateway-Firewall
- Nord-Süd-Netzwerksicherheit – Einfügen eines Drittanbieterdiensts
- Endpoint-Schutz
- Sicherheitsprofile

## 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
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	<p>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.</p> <p>Beim Erstellen einer Gruppe müssen Sie eine Domäne einbeziehen, zu der die Gruppe gehört. Hierbei handelt es sich in der Regel um die Standarddomäne.</p> <p>Gruppen wurden zuvor als NSGroup oder Sicherheitsgruppe bezeichnet.</p>
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 Desktops (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 Zielseiter von der virtuellen Quellmaschine (VM), für die IDFW aktiviert ist. 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 Personal- und Konstruktionsabteilung mit demselben RDSH-Server verbinden und von diesem Server aus auf verschiedene Anwendungen zugreifen.

IDFW kann auch auf VMs verwendet werden, die über unterstützte Betriebssysteme verfügen. Siehe [Von der identitätsbasierten Firewall unterstützte Konfigurationen](#).

Ein Überblick auf oberster Ebene über den Workflow der IDFW-Konfiguration beginnt mit der Vorbereitung der Infrastruktur. Zur Vorbereitung gehört die Installation der Hostvorbereitungskomponenten 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 anzuwenden. 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 Kontext-Engine weiter. Diese Informationen werden verwendet, um die Erzwingung für die verteilte Firewall bereitzustellen.

IDFW verarbeitet die Benutzeridentität an der Quelle nur in Regeln für verteilte Firewalls. Identitätsbasierte Gruppen können in DFW-Regeln nicht als Ziel verwendet werden.

---

**Hinweis** IDFW vertraut auf die Sicherheit und Integrität des Gastbetriebssystems. Ein lokaler Administrator mit böswilligen Absichten hat mehrere Möglichkeiten, die Identität zu manipulieren und die Firewallregeln zu umgehen. Benutzeridentitätsinformationen werden vom NSX Guest Introspection Agent innerhalb der Gast-VMs bereitgestellt. Sicherheitsadministratoren müssen sicherstellen, dass Thin Agent auf jeder Gast-VM installiert ist und ausgeführt wird. Angemeldete Benutzer sollten nicht über die Berechtigung zum Entfernen oder Beenden des Agents verfügen.

---

Informationen zu unterstützten IDFW-Konfigurationen finden Sie unter [Von der identitätsbasierten Firewall unterstützte Konfigurationen](#).

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 Kontext-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.

Identitätsbasierte Firewallregeln werden von der Mitgliedschaft in einer Active Directory (AD)-Gruppe bestimmt. Siehe [Von der identitätsbasierten Firewall unterstützte Konfigurationen](#).

IDFW verarbeitet die Benutzeridentität an der Quelle nur in Regeln für verteilte Firewalls. Identitätsbasierte Gruppen können in DFW-Regeln nicht als Ziel verwendet werden.

---

**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.

---

### Voraussetzungen

Wenn die automatische Windows-Anmeldung auf VMs aktiviert ist, wechseln Sie zu **Lokale Computerrichtlinie > Computerkonfiguration > Administrative Vorlagen > System > Anmeldung** und aktivieren Sie die Option **Beim Starten des Computers und Anmelden immer auf das Netzwerk warten**.

Informationen zu unterstützten IDFW-Konfigurationen finden Sie unter [Von der identitätsbasierten Firewall unterstützte Konfigurationen](#).

### 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 **Sicherheit > Verteilte Firewall** aus.
- 2 Klicken Sie in der linken Ecke auf **Aktionen > Allgemeine Einstellung**.
- 3 Klicken Sie auf den Schalter „Status“, um IDFW zu aktivieren.  
Die verteilte Firewall muss ebenfalls aktiviert sein, damit IDFW funktioniert.
- 4 Wenn Sie IDFW auf eigenständigen Hosts oder Clustern aktivieren möchten, wählen Sie die Registerkarte **Einstellungen für die identitätsbasierte Firewall** aus.
- 5 Klicken Sie auf die Leiste **Aktivieren** und wählen Sie die eigenständigen Hosts aus; oder wählen Sie den Cluster aus, in dem der IDFW-Host aktiviert werden muss.
- 6 Klicken Sie auf **Speichern**.

## Best Practices für die identitätsbasierte Firewall

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

- IDFW unterstützt die folgenden Protokolle:
  - Einzelbenutzer (VDI oder Nicht-RDSH-Server) – TCP, UDP, ICMP
  - Mehrbenutzer (RDSH) – TCP, UDP
- Eine einzelne, ID-basierte Gruppe kann nur in einer DFW-Regel als Quelle verwendet werden. Wenn für die Quelle IP- und ID-basierte Gruppen benötigt werden, erstellen Sie zwei separate Firewallregeln.
- 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 lokale Domänencontroller bei der Active Directory-Synchronisation verwendet und sollten nicht über die Standardwerte bearbeitet werden.

## Von der identitätsbasierten Firewall unterstützte Konfigurationen

Die folgenden Konfigurationen werden für IDFW auf virtuellen Maschinen (VMs) unterstützt. IDFW für physische Geräte wird nicht unterstützt.

Gastbetriebssysteme	Erzwingungstyp
Windows 8	Desktop – unterstützt Anwendungsbeispiel für Desktop-Benutzer
Windows 10	Desktop – unterstützt Anwendungsbeispiel für Desktop-Benutzer

Gastbetriebssysteme	Erzwingungstyp
Windows 2012	Server – unterstützt Anwendungsbeispiel für Server Benutzer
Windows 2012R2	Server – unterstützt Anwendungsbeispiel für Server Benutzer
Windows 2016	Server – unterstützt Anwendungsbeispiel für Server Benutzer
Windows 2012R2	RDSH – unterstützt Remote Desktop-Sitzungshost
Windows 2016	RDSH – unterstützt Remote Desktop-Sitzungshost

Active Directory-Domänencontroller:

- Windows Server 2012
- Windows Server 2012R2
- Windows Server 2016
- Windows Server 2019

Hostbetriebssystem: ESXi

VMware Tools – Version 11

- VMCI-Treiber
- NSX Datei-Introspektion-Treiber
- NSX Netzwerk-Introspektion-Treiber

## Kontextprofil der Schicht 7

Die App-IDs der Schicht 7 werden im Rahmen eines Kontextprofils konfiguriert.

Ein Kontextprofil kann eine oder mehrere [Attribute](#) angeben und kann auch Unterattribute für die Verwendung in den Regeln der verteilten Firewall (DFW) und der Gateway-Firewall enthalten. Wenn ein Unterattribut, z. B. TLS Version 1.2, definiert ist, werden mehrere Anwendungsidentitätsattribute nicht unterstützt. Zusätzlich zu Attributen unterstützt DFW auch einen vollqualifizierten Domännennamen (FQDN) oder eine URL, die in einem Kontextprofil für die FQDN-Whitelist oder -Blacklist angegeben werden kann. Derzeit wird eine vordefinierte Liste der Domänen unterstützt. FQDN kann mit einem Attribut in einem Kontextprofil konfiguriert werden oder sie können jeweils in verschiedenen Kontextprofilen festgelegt werden. Nachdem ein Kontextprofil definiert wurde, kann es auf eine oder mehrere verteilte Firewallregeln angewendet werden.

Derzeit wird eine vordefinierte Liste der Domänen unterstützt. Sie können die Liste der FQDNs anzeigen, wenn Sie ein neues Kontextprofil mit dem Attributtyp *Domänenname (FQDN)* hinzufügen. Sie können auch eine Liste der FQDNs anzeigen, indem Sie den API-Aufruf / `policy/api/v1/infra/context-profiles/attributes?attribute_key=DOMAIN_NAME` ausführen.

---

### Hinweis

- Gateway-Firewallregeln unterstützen nicht die Verwendung von FQDN-Attributen oder anderen Unterattributen in Kontextprofilen.
  - Kontextprofile werden in der Tier-0-Gateway-Firewallrichtlinie nicht unterstützt. Gateway-Firewallregeln unterstützen nicht die Verwendung von FQDN-Attributen oder anderen Unterattributen.
- 

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 vDPI-Engine bezeichnet wird. Einige nachfolgende Pakete werden für jeden Flow an diese vDPI-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 erneut mit der Regeltabelle verglichen und mit einem 5-Tupel sowie auf der App-ID der Schicht 7 abgeglichen. Die entsprechende Aktion, wie in der Regel definiert, wird ausgeführt. Im Falle einer ALLOW-Regel werden alle nachfolgenden Pakete für den Flow im Kernel verarbeitet und mit der Verbindungstabelle abgeglichen. Für eine vollständig abgestimmte DROP-Regel wird ein Ablehnungspaket generiert. Von der verteilten Firewall generierte Protokolle enthalten die App-ID der Schicht 7 und die jeweilige URL, wenn dieser Flow an DPI weitergegeben wurde.

Regelverarbeitung für ein eingehendes Paket:

- 1 Nach dem Eingeben eines DFW- oder Gateway-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. Die erste vollständig übereinstimmende L4/L7-Regel wird verwendet. Die entsprechende Aktion wird ausgeführt (zulassen/verweigern/ablehnen) und der Eintrag in der Flowtabelle wird entsprechend aktualisiert.

## Workflow für Firewallregel der Schicht 7

App-IDs der Schicht 7 werden beim Erstellen von Kontextprofilen verwendet, die in Regeln für verteilte Firewalls oder in Gateway-Firewallregeln verwendet werden. Die auf Attributen basierende Regelerzwingung ermöglicht Benutzern, die Ausführung von Anwendungen auf einem beliebigen Port zuzulassen oder zu verweigern.

NSX-T bietet integrierte [Attribute](#) für gemeinsame Infrastruktur- und Unternehmensanwendungen. App-IDs umfassen Versionen (SSL/TLS und CIFS/SMB) sowie die Verschlüsselungs-Suite (SSL/TLS). Bei einer verteilten Firewall werden App-IDs über Kontextprofile in Regeln verwendet und können mit FQDN-Whitelists und -Blacklists kombiniert werden. App-IDs werden auf ESXi- und KVM-Hosts unterstützt.

---

### Hinweis

- Gateway-Firewallregeln unterstützen nicht die Verwendung von FQDN-Attributen oder anderen Unterattributen in Kontextprofilen.
  - Kontextprofile werden in der Tier-0-Gateway-Firewallrichtlinie nicht unterstützt. Gateway-Firewallregeln unterstützen nicht die Verwendung von FQDN-Attributen oder anderen Unterattributen.
- 

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.

Beachten Sie, dass Sie bei Verwendung einer Kombination aus Ebene 7 und ICMP oder anderen Protokollen die Firewallregeln der Ebene 7 zuletzt einfügen müssen. Regeln über einer Schicht 7-„any/any“-Regel werden nicht ausgeführt.

### Verfahren

- 1 Erstellen eines benutzerdefinierten Kontextprofils: [Hinzufügen eines Kontextprofils](#).

- 2 Verwenden Sie das Kontextprofil in einer Regel für verteilte Firewalls oder in einer Gateway-Firewallregel: [Hinzufügen einer verteilten Firewall](#) oder [Hinzufügen von Regeln und Richtlinien für eine Gateway-Firewall](#).

Mehrere App-ID-Kontextprofile können in einer Firewallregel mit Diensten verwendet werden, die auf **Beliebig** festgelegt sind. Für ALG-Profile (FTP, ORACLE, DCERPC, TFTP) wird pro Regel ein Kontextprofil unterstützt.

## Attribute

Durch Attribute der Schicht 7 (App-IDs) wird bestimmt, von welcher Anwendung ein bestimmtes Paket oder ein bestimmter Flow unabhängig vom verwendeten Port generiert wird.

Die auf App-IDs 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. vDPI ermöglicht die Abstimmung der Paketzustlast mit definierten Mustern. 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.

App-IDs der Schicht 7 werden in Kontextprofilen in verteilten Firewallregeln und Gateway-Firewallregeln verwendet und auf ESXi- und KVM-Hosts unterstützt.

---

**Hinweis** NFS Version 4 ist kein unterstütztes Attribut.

---

### Hinweis

- Gateway-Firewallregeln unterstützen nicht die Verwendung von FQDN-Attributen oder anderen Unterattributen in Kontextprofilen.
  - Kontextprofile werden in der Tier-0-Gateway-Firewallrichtlinie nicht unterstützt. Gateway-Firewallregeln unterstützen nicht die Verwendung von FQDN-Attributen oder anderen Unterattributen.
- 

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.

Attribut (App-ID)	Beschreibung	Typ
360ANTIV	360 Safeguard ist ein vom chinesischen IT-Unternehmen Qihoo 360 entwickeltes Programm.	Webdienste
ACTIVDIR	Microsoft Active Directory	Netzwerk
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.	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
CTRXGOTO	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
CTRIXICA	ICA (Independent Computing Architecture) ist ein von Citrix Systems entwickeltes proprietäres Protokoll für Anwendungsserver-Systeme.	Remotezugriff

Attribut (App-ID)	Beschreibung	Typ
DCERPC	Distributed Computing Environment / Remote Procedure Calls ist das für die Distributed Computing Environment (DCE) entwickelte Remoteprozeduraufruf-System.	Netzwerk
DIAMETER	Ein Authentifizierungs-, Autorisierungs- und Accounting-Protokoll für Computernetzwerke	Netzwerk
DHCP	Dynamic Host Configuration Protocol ist ein Protokoll, das für die Verwaltung der Verteilung von IP-Adressen innerhalb eines Netzwerks verwendet wird.	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

Attribut (App-ID)	Beschreibung	Typ
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.  <b>Hinweis</b> NFS Version 4 ist kein unterstütztes Attribut.	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
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
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
SIP	Das SIP (Session Initiation Protocol) ist ein allgemeines Steuerungsprotokoll für die Einrichtung und die Steuerung von Sprach- und Videoanrufen.	Streaming Media



Attribut (App-ID)	Beschreibung	Typ
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
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
SYMUPDAT	Symantec LiveUpdate-Datenverkehr; dies umfasst Spyware-Definitionen, Firewall-Regeln, Antivirus-Signaturdateien und Software-Updates.	Dateiübermittlung
SYSLOG	SYSLOG ist ein Protokoll, über das Netzwerkgeräte Ereignismeldungen an einen Protokollserver senden können.	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.

**Tabelle 10-2. Regelkategorien für verteilte Firewalls**

Kategorie	Beschreibung
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

Tabelle 10-2. Regelkategorien für verteilte Firewalls (Fortsetzung)

Kategorie	Beschreibung
Umgebung	Regeln zwischen den Zonen – Produktion bzw. Entwicklung, Regeln für geschäftseinheitsübergreifenden Datenverkehr
Anwendung	Regeln zwischen Anwendungen, Anwendungsebenen oder die Regeln zwischen Mikrodiensten

## Firewall-Entwürfe

Bei einem Entwurf handelt es sich um eine vollständige verteilte Firewall-Konfiguration mit Abschnitten zu Richtlinien und Regeln. Entwürfe können automatisch oder manuell gespeichert und sofort veröffentlicht oder für die Veröffentlichung zu einem späteren Zeitpunkt gespeichert werden.

Wenn Sie eine manuelle Entwurfs-Firewall-Konfiguration speichern möchten, navigieren Sie im Bildschirm „Verteilte Firewall“ nach oben rechts und klicken Sie auf **Aktionen > Speichern**. Nach dem Speichern kann die Konfiguration durch Auswahl von **Aktionen > Anzeigen** aufgerufen werden. Automatische Entwürfe sind standardmäßig aktiviert. Automatische Entwürfe können deaktiviert werden, indem Sie zu **Aktionen > Allgemeine Einstellungen** navigieren. Wenn automatische Entwürfe aktiviert sind, führt jede Änderung an einer Firewallkonfiguration zu einem vom System generierten automatischen Entwurf. Es können maximal 100 automatische Entwürfe und 10 manuelle Entwürfe gespeichert werden. Automatische Entwürfe können bearbeitet und als manueller Entwurf für die direkte oder spätere Veröffentlichung gespeichert werden. Um zu verhindern, dass mehrere Benutzer den Entwurf öffnen und bearbeiten, können manuelle Entwürfe gesperrt werden. Bei der Veröffentlichung eines Entwurfs wird die aktuelle Konfiguration durch die Konfiguration im Entwurf ersetzt.

### Speichern oder Anzeigen eines Firewall-Entwurfs

Ein Entwurf ist eine Konfiguration einer verteilten Firewall, die veröffentlicht oder für die Veröffentlichung zu einem späteren Zeitpunkt gespeichert wurde. Entwürfe werden automatisch oder manuell erstellt.

Manuelle Entwürfe können bearbeitet und gespeichert werden. Automatische Entwürfe können geklont, als manuelle Entwürfe gespeichert und anschließend bearbeitet werden. Die maximale Anzahl an Entwürfen, die gespeichert werden können, liegt bei 100 automatischen Entwürfen und 10 manuellen Entwürfen.

#### Verfahren

- 1 Klicken Sie auf **Sicherheit > Verteilte Firewall**.
- 2 Um eine Firewall-Konfiguration manuell zu speichern, gehen Sie zu **Aktionen > Speichern**.  
Ein manueller Entwurf kann gespeichert oder bearbeitet und dann gespeichert werden. Nach dem Speichern können Sie die ursprüngliche Konfiguration wiederherstellen.
- 3 Füllen Sie für die Konfiguration das Feld **Name** aus.

- 4 Um zu verhindern, dass mehrere Benutzer einen manuellen Entwurf öffnen und bearbeiten, **Sperren** Sie die Konfiguration und fügen Sie einen Kommentar hinzu.

- 5 Klicken Sie auf **Speichern**.

- 6 Um die gespeicherte Konfiguration anzuzeigen, klicken Sie auf **Aktionen > Anzeigen**.

Eine Zeitachse wird geöffnet, in der alle gespeicherten Konfigurationen angezeigt werden. Um Details wie den Namen des Entwurfs, das Datum, die Uhrzeit und die speichernde Person anzuzeigen, zeigen Sie auf das Punkt- oder Sternsymbol eines beliebigen Entwurfs. Gespeicherte Konfigurationen können nach Zeit gefiltert werden. Dabei werden alle Entwürfe angezeigt, die am letzten Tag, in der letzten Woche, in den letzten 30 Tagen oder in den letzten drei Monaten erstellt wurden. Sie können nach automatischem Entwurf und eigenen Speichervorgängen gefiltert werden. Über die Suche oben rechts können sie auch nach Name gefiltert werden.

- 7 Bewegen Sie den Mauszeiger über einen Entwurf, um den Namen, das Datum und die Uhrzeit der gespeicherten Konfiguration anzuzeigen. Klicken Sie auf den Namen, um Details zum Entwurf anzuzeigen.

Die detaillierte Entwurfsansicht zeigt die Änderungen an, die an der aktuellen Firewall-Konfiguration vorgenommen werden müssen, damit sie mit diesem Entwurf übereinstimmt. Wenn dieser Entwurf veröffentlicht wird, werden alle in dieser Ansicht angezeigten Änderungen auf die aktuelle Konfiguration angewendet.

Durch Klicken auf den abwärts gerichteten Pfeil werden die einzelnen Abschnitte erweitert und die Änderungen in jedem Abschnitt werden hinzugefügt, geändert und gelöscht. Der Vergleich zeigt hinzugefügte Regeln mit einem grünen Balken auf der linken Seite des Felds, geänderte Elemente (z. B. eine Namensänderung) mit einem gelben Balken und gelöschte Elemente mit einem roten Balken.

- 8 Um den Namen oder die Beschreibung eines ausgewählten Entwurfs zu bearbeiten, klicken Sie im Fenster **Entwurfsdetails anzeigen** auf das Menüsymbol (drei Punkte) und wählen **Bearbeiten** aus.

Manuelle Entwürfe können gesperrt werden. Wenn der Entwurf gesperrt wird, muss ein Kommentar dafür angegeben werden.

Einige Rollen wie Enterprise-Administrator verfügen über Anmeldedaten für den vollständigen Zugriff und können nicht gesperrt werden. Siehe [Rollenbasierte Zugriffssteuerung](#).

- 9 Automatische Entwürfe und manuelle Entwürfe können auch geklont und gespeichert werden, indem Sie auf **Klonen** klicken.

Im Fenster der gespeicherten Konfigurationen können Sie den Standardnamen übernehmen oder bearbeiten. Sie können die Konfiguration auch sperren. Wenn der Entwurf gesperrt wird, muss ein Kommentar dafür angegeben werden.

- 10 Um die geklonte Version der Entwurfskonfiguration zu speichern, klicken Sie auf **Speichern**. Der Entwurf ist jetzt im Abschnitt „Gespeicherte Konfigurationen“ enthalten.

## Nächste Schritte

Nachdem Sie einen Entwurf angezeigt haben, können Sie ihn laden und veröffentlichen. Er wird dann zur aktiven Firewall-Konfiguration.

## Veröffentlichen oder Wiederherstellen eines Firewall-Entwurfs

Sowohl automatische Entwürfe als auch gespeicherte manuelle Entwürfe können geladen und veröffentlicht werden, um zur aktiven Konfiguration zu werden.

Während der Veröffentlichung wird ein neuer automatischer Entwurf erstellt. Dieser automatische Entwurf kann veröffentlicht werden, um die vorherige Konfiguration wiederherzustellen.

### Verfahren

- 1 Um die gespeicherte Konfiguration anzuzeigen, klicken Sie auf **Aktionen > Anzeigen**.

Eine Zeitachse wird geöffnet, in der alle gespeicherten Konfigurationen angezeigt werden. Um Details wie z. B. den Namen des Entwurfs, das Datum, die Uhrzeit und die speichernde Person anzuzeigen, zeigen Sie auf das Punktsymbol eines beliebigen Entwurfs. Gespeicherte Konfigurationen werden nach Zeit gefiltert. Dabei werden alle Entwürfe angezeigt, die an einem Tag, in einer Woche, in 30 Tagen oder den letzten drei Monaten erstellt wurden.

- 2 Klicken Sie auf einen Entwurfsnamen, um das Fenster „Entwurfsdetails anzeigen“ zu öffnen.
- 3 Klicken Sie auf **Laden**. Die neue Firewall-Konfiguration wird im Hauptfenster angezeigt.

---

**Hinweis** Ein Entwurf kann nicht geladen werden, wenn Firewall-Filter verwendet werden oder wenn in der aktuellen Konfiguration nicht gespeicherte Änderungen vorhanden sind.

---

- 4 Um die Entwurfskonfiguration zu übernehmen und sie zu aktivieren, klicken Sie auf **Veröffentlichen**. Um zur vorherigen veröffentlichten Konfiguration zurückzukehren, klicken Sie auf **Wiederherstellen**.

Nach der Veröffentlichung sind die im Entwurf enthaltenen Änderungen in der aktiven Konfiguration vorhanden.

- 5 Um den Inhalt des ausgewählten Entwurfs vor der Veröffentlichung anzupassen, bearbeiten Sie die Konfiguration nach dem Klicken auf **Laden**.

- 6 Um die bearbeitete Version der Entwurfskonfiguration zu speichern, klicken Sie auf **Aktionen > Speichern**.

Manuelle Entwürfe können als neue Konfiguration oder als Aktualisierung der vorhandenen Konfiguration gespeichert werden. Automatische Entwürfe können nur als neue Konfiguration gespeichert werden.

- 7 Geben Sie einen **Namen** und optional eine **Beschreibung** ein. Sie können den Entwurf auch **Sperren**. Wenn der Entwurf gesperrt wird, muss ein Kommentar dafür angegeben werden.
- 8 Klicken Sie auf **Speichern**.

- 9 Um die Entwurfskonfiguration zu übernehmen und sie zu aktivieren, klicken Sie auf **Veröffentlichen**. Alternativ können Sie auf **Wiederherstellen** klicken, um zur zuvor veröffentlichten Konfiguration zurückzukehren.

## Hinzufügen einer verteilten Firewall

Eine verteilte Firewall (Distributed Firewall, DFW) überwacht den gesamten Ost-West-Datenverkehr auf Ihren virtuellen Maschinen.

### Voraussetzungen

Bei per DFW zu schützenden Gast-VMs muss ihr vNIC mit einem logischen N-VDS-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. 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.

---

Beachten Sie, dass Sie bei Verwendung einer Kombination aus Ebene 7 und ICMP oder anderen Protokollen die Firewallregeln der Ebene 7 zuletzt einfügen müssen. Regeln über einer Schicht 7-„any/any“-Regel werden nicht ausgeführt.

### 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 Aktivieren Sie die verteilte Firewall, indem Sie **Aktionen > Allgemeine Einstellungen** auswählen und den Status der verteilten Firewall wechseln. Klicken Sie auf **Speichern**.
- 4 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](#).
- 5 Geben Sie einen **Namen** für den Abschnitt mit der neuen Richtlinie ein.

- 6 (Optional) Klicken Sie zum Konfigurieren der folgenden Richtlinieneinstellungen auf das Zahnradsymbol:

Option	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 erkennt die verteilte Firewall (DFW) möglicherweise nicht den Dreizeige-Handshake für einen bestimmten Flow (aufgrund des asymmetrischen Datenverkehrs oder der aktivierten verteilten Firewall, während ein Flow vorhanden ist). Standardmäßig erzwingt die verteilte Firewall nicht die Notwendigkeit, einen Dreizeige-Handshake anzuzeigen und nimmt bereits eingerichtete 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 eine bestimmte DFW-Richtlinie 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 Richtlinienebene 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 wie Enterprise-Administrator verfügen über Anmeldeinformationen für vollständigen Zugriff 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 Quellfeld einer IDFW-Regel verwendet werden. Weitere Informationen hierzu finden Sie unter [Hinzufügen einer Gruppe](#).

IPv4-, IPv6- und Multicast-Adressen werden unterstützt.

Hinweis: IPv6-Firewall muss über die auf einem verbundenen Segment aktivierte IP Discovery für IPv6 verfügen. Weitere Informationen finden Sie unter [Grundlegendes zum Segmentprofil für die IP Discovery](#).

- 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**. Weitere Informationen hierzu finden Sie unter [Hinzufügen einer Gruppe](#). IPv4-, IPv6- und Multicast-Adresse werden unterstützt.
- 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 Die 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 oder klicken Sie auf **Neues Kontextprofil hinzufügen**. Siehe [Hinzufügen eines Kontextprofils](#).

Kontextprofile verwenden App-ID-Attribute der Ebene 7 für die Verwendung in Regeln für eine verteilte Firewall und in Gateway-Firewallregeln. Mehrere App-ID-Kontextprofile können in einer Firewallregel mit Diensten verwendet werden, die auf **Beliebig** festgelegt sind. Für ALG-Profil (FTP oder TFTP) wird pro Regel ein Kontextprofil unterstützt.

- 14 Klicken Sie auf **Anwenden**, um das Kontextprofil auf die Regel anzuwenden.
- 15 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.

## 16 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.

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

## 18 (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/dfwpklogs.log“ auf ESXi- und KVM-Hosts gespeichert.
<b>Richtung</b>	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>Protokollbezeichnung</b>	Die Protokollbezeichnung wird in das Firewallprotokoll übertragen, wenn die Protokollierung aktiviert ist.

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

## 20 Klicken Sie für jede Regel auf das Symbol **Info**, um die Regel-ID-Nummer und die Stelle anzuzeigen, an der sie erzwungen wird.

Dieses Symbol ist ausgegraut, bis Sie die Regel veröffentlichen. Sie können auch eine Regel-ID angeben, wenn Sie auf das Filtersymbol klicken, um nur Richtlinien und Regeln anzuzeigen, die die Filterkriterien erfüllen.



- 21 Die Umsetzungsstatus-API wurde auf Sicherheitsrichtlinienebene erweitert, um zusätzliche Informationen zum Status der Umsetzung bereitzustellen. Dies kann erreicht werden, indem der Abfrageparameter *include\_enforced\_status = true* zusammen mit *intent\_path* angegeben wird. Führen Sie den folgenden API-Aufruf aus:

```
GET https://<nsx>/policy/api/v1/infra/realized-state/status?intent_path=/
infra/domains/default/security-policies/<security-policy-
id>&include_enforced_status=true
```

## 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 Domänennamen 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. Navigieren Sie zum Festlegen einer Standard-Konnektivitätsstrategie zu **Verteilte Firewall**. Klicken Sie oben auf der Seite auf den Konnektivitätsstatus, um eine andere Option auszuwählen.

Firewallrichtlinien und -regeln müssen bereits erstellt worden sein, um die standardmäßig ausgewählte Konnektivitätsstrategie zu ändern und anzuwenden. Wenn keine Richtlinie oder Regeln erstellt werden, verbleibt die Standardkonnektivitätsstrategie, bis eine Richtlinie und Regeln erstellt 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.

## Verwalten einer Firewall-Ausschlussliste

Firewall-Ausschlusslisten bestehen aus Gruppen, die basierend auf der Gruppenmitgliedschaft von einer Firewallregel ausgeschlossen werden können.

Gruppen können von Firewallregeln ausgeschlossen werden und es können maximal 100 Gruppen in der Liste enthalten sein. IP-Sets, MAC-Sets und AD-Gruppen können nicht als Mitglieder in eine Gruppe eingeschlossen werden, die in einer Ausschlussliste für die Firewall verwendet wird.

---

**Hinweis** NSX-T Data Center fügt automatisch NSX Manager- und NSX Edge-Knoten-VMs zur Firewall-Ausschlussliste hinzu.

---

### Verfahren

- 1 Navigieren Sie zu **Sicherheit > Verteilte Firewall > Aktionen > Ausschlussliste**.  
Es wird ein Fenster mit verfügbaren Gruppen angezeigt.
- 2 Wenn Sie eine Gruppe der Ausschlussliste hinzufügen möchten, aktivieren Sie das Kontrollkästchen neben einer beliebigen Gruppe. Klicken Sie dann auf **Übernehmen**.
- 3 Klicken Sie zum Erstellen einer Gruppe auf **Gruppe hinzufügen**. Siehe [Hinzufügen einer Gruppe](#).
- 4 Wenn Sie eine Gruppe bearbeiten möchten, klicken Sie auf das Menü mit den drei Punkten neben einer Gruppe und wählen Sie **Bearbeiten** aus.
- 5 Wenn Sie eine Gruppe löschen möchten, klicken Sie auf das Menü mit den drei Punkten und wählen Sie **Löschen** aus.
- 6 Wenn Sie Gruppendetails anzeigen möchten, klicken Sie auf **Alle erweitern**.

## Filtern bestimmter Domänen (FQDN/URLs)

Richten Sie eine Regel für die verteilte Firewall ein, um bestimmte, mit FQDN/URLs identifizierte Domänen zu filtern, z. B. *\*.office365.com*.

Derzeit wird eine vordefinierte Liste der Domänen unterstützt. Sie können die Liste der FQDNs anzeigen, wenn Sie ein neues Kontextprofil mit dem Attributtyp *Domänenname (FQDN)* hinzufügen. Sie können auch eine Liste der FQDNs anzeigen, indem Sie den API-Aufruf /  
policy/api/v1/infra/context-profiles/attributes?attribute\_key=DOMAIN\_NAME ausführen.

Sie müssen zuerst eine DNS-Regel einrichten. Richten Sie dann unterhalb dieser Regel die FQDN-Positivlistenregel oder -Negativlistenregel ein. NSX-T Data Center verwendet in der DNS-Antwort (vom DNS-Server an die virtuelle Maschine) TTL (Time to live), um den Zuordnungs-Cache-Eintrag von DNS zu IP für die virtuelle Maschine (VM) beizubehalten. Informationen zum Überschreiben von DNS-TTL mithilfe eines DNS-Sicherheitsprofils finden Sie unter [Konfigurieren der DNS-Sicherheit](#). Damit die FQDN-Filterung wirksam ist, müssen virtuelle Maschinen für die Domänenauflösung einen DNS-Server verwenden (keine statischen DNS-Einträge) und die in der DNS-Antwort empfangene TTL-Information berücksichtigen. NSX-T Data Center verwendet DNS-Snooping, um eine Zuordnung zwischen der IP-Adresse und dem FQDN zu erhalten. SpoofGuard sollte Switch-übergreifend auf allen logischen Ports aktiviert werden, um sich vor dem Risiko von DNS-Spoofing-Angriffen zu schützen. Ein DNS-Spoofing-Angriff liegt vor, wenn eine bössartige VM gefälschte DNS-Antworten einfügen kann, um Datenverkehr an bössartige Endpoints umzuleiten oder die Firewall zu umgehen. Weitere Informationen zu SpoofGuard finden Sie unter [Grundlegendes zum Spoofguard-Segmentprofil](#).

Diese Funktion arbeitet auf Schicht 7 und bezieht sich nicht auf ICMP. Wenn ein Benutzer eine Negativlistenregel für alle Dienste auf `example.com` erstellt, arbeitet die Funktion ordnungsgemäß, wenn `ping example.com` antwortet, `curl example.com` jedoch nicht.

Die Auswahl eines Platzhalter-FQDNs wird als Best Practice empfohlen, da dieser Unterdomänen einbezieht. Wenn Sie z. B. `*example.com` auswählen, werden Unterdomänen wie `americas.example.com` und `emea.example.com` einbezogen. Wenn Sie `example.com` verwenden, werden keine Unterdomänen einbezogen.

FQDN-basierte Regeln werden während des vMotion-Vorgangs für ESXi-Hosts beibehalten.

---

**Hinweis** ESXi- und KVM-Hosts werden unterstützt. KVM-Hosts unterstützen nur die FQDN-Positivliste. FQDN-Filterung ist nur für TCP- und UDP-Datenverkehr verfügbar.

---

## 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 > Verteilte Firewall**.
- 3 Befolgen Sie die Schritte unter [Hinzufügen einer verteilten Firewall](#) und fügen Sie einen Abschnitt für eine Firewallrichtlinie hinzu. Es kann auch ein vorhandener Firewall-Richtlinienabschnitt verwendet werden.
- 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**. Geben Sie zudem die folgenden Details an:

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

- 6 Klicken Sie noch einmal auf **Regel hinzufügen**, um die FQDN-Positivlistenregel oder -Negativlistenregel einzurichten.
- 7 Benennen Sie die Regel mit einem aussagekräftigen Namen, beispielsweise **FQDN/URL-Positivliste**. 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> , <b>Ablegen</b> oder <b>Ablehnen</b> aus.

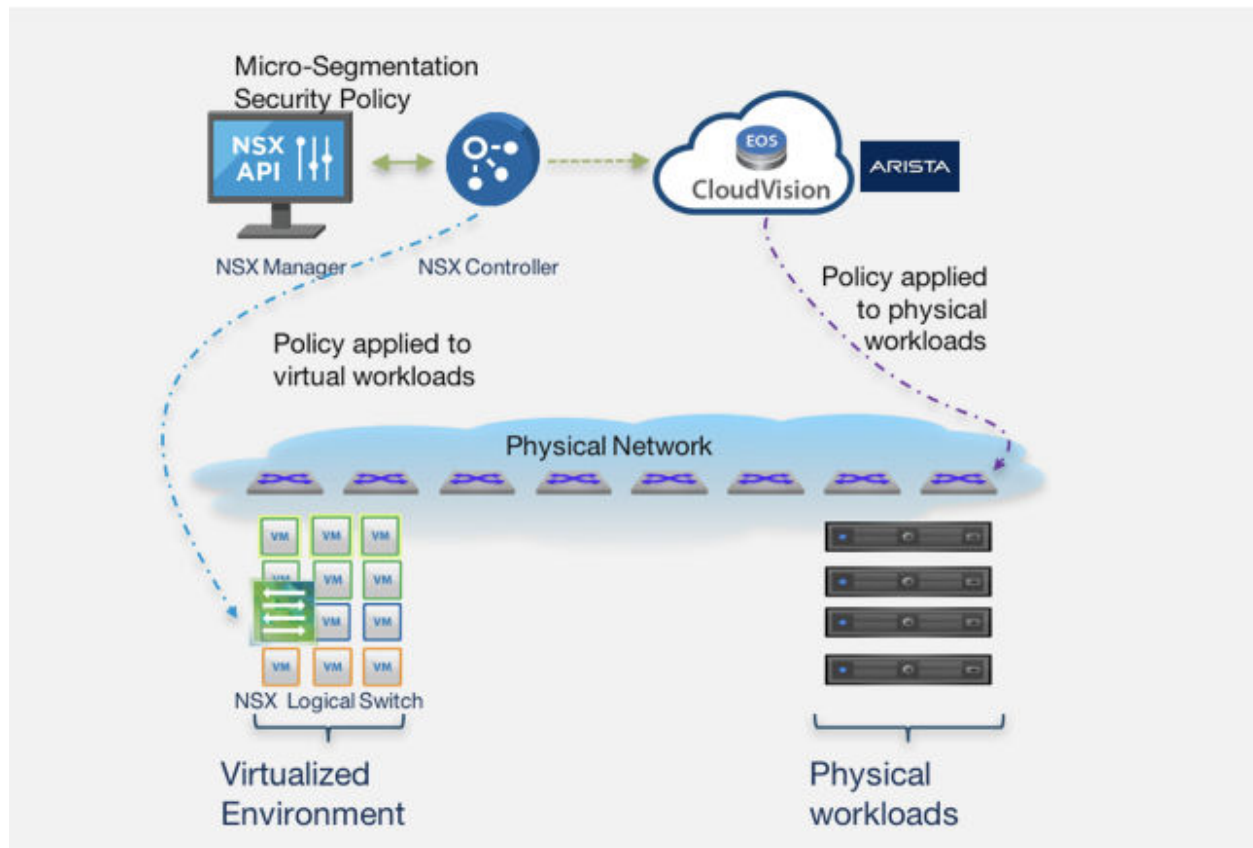
- 9 Klicken Sie auf **Veröffentlichen**.

## Erweitern von Sicherheitsrichtlinien auf physische Arbeitslasten

NSX-T Data Center kann sowohl für virtuelle als auch für physische Arbeitslasten als zentrale Verwaltungsstelle fungieren.

Ab NSX-T Data Center 2.5.1 wird die Integration in Arista CloudVision eXchange (CVX) unterstützt. Diese Integration vereinfacht unabhängig von Ihren Anwendungskonzepten oder physischen Netzwerkinfrastrukturen konsistente Netzwerk- und Sicherheitsdienste für virtuelle und physische Arbeitslasten. NSX-T Data Center programmiert den physischen Netzwerk-Switch oder -Router nicht direkt, sondern integriert sich auf der physischen SDN-Controller-Ebene, wodurch die Autonomie von Sicherheitsadministratoren und physischen Netzwerkadministratoren erhalten bleibt.

Ab NSX-T Data Center 2.5.1 wird die Integration in Arista EOS 4.22.1FX-PCS und höher unterstützt.



## Einschränkungen

- Bei den Arista-Switches muss der ARP-Datenverkehr vorhanden sein, bevor die Firewallregeln auf einen Endhost angewendet werden, der mit einem Arista-Switch verbunden ist. Pakete können daher durch den Switch geleitet werden, bevor Firewallregeln zum Blockieren des Datenverkehrs konfiguriert werden.
- Der zulässige Datenverkehr wird nicht fortgesetzt, wenn ein Switch abstürzt oder neu geladen wird. Die ARP-Tabellen müssen nach dem Start des Switches erneut aufgefüllt werden, damit die Firewallregeln auf dem Switch erzwungen werden.
- Firewallregeln können nicht auf den physischen Arista-Switch angewendet werden. Dies gilt für passive FTP-Clients, die eine Verbindung zum FTP-Server herstellen, der mit dem physischen Arista-Switch verbunden ist.
- In der CVX HA-Einrichtung, die die virtuelle IP für den CVX-Cluster verwendet, müssen der promiskuitive DVPF-Modus der CVX-VM und die gefälschten Übertragungen auf „Zulassen“ festgelegt sein. Für den Fall, dass Sie auf die Standardeinstellung (Ablehnen) festgelegt sind, ist die virtuelle CVX HA-IP-Adresse von NSX Manager nicht erreichbar.

## Konfigurieren von Arista CVX für die Interaktion mit NSX-T Manager

Führen Sie nach der Konfiguration von NSX-T Data Center den Konfigurationsvorgang auf Arista CloudVision eXchange (CVX) durch, um CVX die Interaktion mit NSX-T Data Center zu ermöglichen.

### Voraussetzungen

NSX-T Data Center hat CVX als Enforcement Point registriert.

### Verfahren

- 1 Melden Sie sich bei NSX Manager als Root-Benutzer an und führen Sie den folgenden Befehl aus, um für CVX einen Fingerabdruck für die Kommunikation mit NSX Manager zu erstellen:

```
openssl s_client -connect <IP address of nsx-manager>:443 | openssl x509 -pubkey -noout |
openssl rsa -pubin -outform der | openssl dgst -sha256 -binary | openssl base64
```

Beispielausgabe:

```
depth=0 C = US, ST = CA, L = Palo Alto, O = VMware Inc., OU = NSX, CN = nsx-mgr
verify error:num=18:self signed certificate
verify return:1
depth=0 C = US, ST = CA, L = Palo Alto, O = VMware Inc., OU = NSX, CN = nsx-mgr
verify return:1
writing RSA key
S+zwADluzeNf+dnffDpYvgs4YrS6QBgyeDry40bPgms=
```

- 2 Führen Sie die folgenden Befehle über die CVX-CLI aus:

```
cvx
no shutdown
service pcs
no shutdown
controller <IP address of nsx-manager>
username <NSX administrator user name>
password <NSX administrator password>
enforcement-point cvx-default-ep
pinned-public-key <thumbprint for CVX to communicate with NSX
                    Manager>
notification-id <notification ID created while registering CVX with NSX>
end
```

- 3 Führen Sie den folgenden Befehl über die CVX-CLI aus, um die Konfiguration zu überprüfen:

```
show running-config
```

Beispielausgabe:

```
cvx
    no shutdown
    source-interface Management1
    !
```



```

service hsc
  no shutdown

!
service pcs
  no shutdown
  controller 192.168.2.80
  username admin
  password 7 046D26110E33491F482F2800131909556B
  enforcement-point cvx-default-ep
  pinned-public-key sha256//S+zwADluzeNf+dnffDpYvgs4YrS6QBgyeDry40bPgms=
  notification-id a0286cb6-de4d-41de-99a0-294465345b80

```

- 4 Konfigurieren Sie tag an der Ethernet-Schnittstelle des physischen Switch, der eine Verbindung mit dem physischen Server herstellt. Führen Sie die folgenden Befehle auf dem physischen Switch aus, der von CVX verwaltet wird.

```

configure terminal
interface ethernet 4
tag phy_app_server
end
copy running-config startup-config
Copy completed successfully.

```

- 5 Führen Sie den folgenden Befehl aus, um die Tag-Konfiguration für den Switch zu überprüfen:

```
show running-config section tag
```

Beispielausgabe:

```

interface Ethernet4
  description connected-to-7150s-3
  switchport trunk allowed vlan 1-4093
  switchport mode trunk
  tag sx4_app_server

```

IP-Adressen, die mit ARP auf den getaggten Schnittstellen gelernt werden, werden mit NSX-T Data Center geteilt.

- 6 Melden Sie sich bei NSX Manager an, um Firewallregeln für die von CVX verwalteten physischen Arbeitslasten zu erstellen und zu veröffentlichen. Weitere Informationen zum Erstellen von Regeln finden Sie unter [Kapitel 10 Sicherheit](#). Beispiel:

<a href="#">+ RICHTLINIE HINZUFÜGEN</a> <a href="#">+ REGEL HINZUFÜGEN</a> <a href="#">📄 KLONEN</a> <a href="#">↶ RÜCKGÄNGIG MACHEN</a> <a href="#">🗑 LÖSCHEN</a> <a href="#">⋮</a>								
<input type="checkbox"/>	Name	Quellen	Ziele	Dienste	Profile	Angewendet auf	Aktion	
⋮	<input type="checkbox"/> Firewall_Services	(2)	Angewendet auf	DFW				● Aktiv <a href="#">🔄</a> <a href="#">🔍</a> <a href="#">🗑</a>
⋮	<input type="checkbox"/> vm_to_phy_server	🔗 vm	🔗 phy_server	Beliebig	Keine	DFW	● Zulassen ▾	🟢 <a href="#">🔄</a> <a href="#">🔍</a> <a href="#">🗑</a>
⋮	<input type="checkbox"/> phy_server_to_vm	🔗 phy_server	🔗 vm	Beliebig	Keine	DFW	● Zulassen ▾	🟢 <a href="#">🔄</a> <a href="#">🔍</a> <a href="#">🗑</a>

NSX-T Data Center-Richtlinien und -Regeln, die in NSX-T Data Center veröffentlicht werden, werden als dynamische ACLs auf dem physischen Switch angezeigt, der von CVX verwaltet wird.

```
prmh-nsx-tor-7050sx-4#show ip access-lists dynamic
IP Access List et4.v4.in [dynamic]
    10 permit ip host 71.1.1.3 host 27.1.1.11

IP Access List et4.v4.out [dynamic]
    10 permit ip host 27.1.1.11 host 71.1.1.3
```

Weitere Informationen finden Sie unter [CVX HA-Einrichtung](#), [Einrichtung der virtuellen CVX HA-IP](#) und [Mlag-Einrichtung für den physischen Switch](#)

## Konfigurieren von NSX-T Data Center für die Interaktion mit Arista CVX

Führen Sie den Konfigurationsvorgang in NSX-T Data Center aus, damit CVX als Enforcement Point in NSX-T Data Center hinzugefügt werden kann und NSX-T Data Center mit CVX interagieren kann.

### Voraussetzungen

Rufen Sie die virtuelle IP-Adresse für den Arista CVX-Cluster ab.

### Verfahren

- 1 Melden Sie sich bei NSX Manager als Root-Benutzer an und führen Sie den folgenden Befehl aus, um den Fingerabdruck für CVX abzurufen:

```
openssl s_client -connect <virtual IP address of CVX cluster> | openssl x509 -noout
-fingerprint -sha256
```

Beispielausgabe:

```
depth=0 CN = self.signed
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = self.signed
verify return:1
SHA256
Fingerprint=35:C1:42:BC:7A:2A:57:46:E8:72:F4:C8:B8:31:E3:13:5F:41:95:EF:D8:1E:E9:3D:F0:CC:3
B:09:A2:FE:22:DE
```

- 2 Bearbeiten Sie den abgerufenen Fingerabdruck, um nur Kleinbuchstaben zu verwenden und Doppelpunkte im Fingerabdruck auszuschließen.

Beispiel des bearbeiteten Fingerabdrucks für CVX:

```
35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de
```

- 3 Rufen Sie die `PATCH /policy/api/v1/infra/sites/default/enforcement-points-API` auf und erstellen Sie mithilfe des CVX-Fingerabdrucks einen Enforcement Endpoint für CVX. Beispiel:

```
PATCH https://<nsx-manager>/policy/api/v1/infra/sites/default/enforcement-points/cvx-
default-ep
{
  "auto_enforce": "false",
  "connection_info": {
    "enforcement_point_address": "<IP address of CVX>",
    "resource_type": "CvxConnectionInfo",
    "username": "cvpadmin",
    "password": "1q2w3e4rT",
    "thumbprint": "65a9785e88b784f54269e908175ada662be55f156a2dc5f3a1b0c339cea5e343"
  }
}
```

- 4 Rufen Sie die `GET /policy/api/v1/infra/sites/default/enforcement-points-API` auf, um die Endpoint-Informationen abzurufen. Beispiel:

```
https://<nsx-manager>/policy/api/v1/infra/sites/default/enforcement-points/cvx-default-ep
{
  "auto_enforce": "false",
  "connection_info": {
    "enforcement_point_address": "<IP address of CVX>",
    "resource_type": "CvxConnectionInfo",
    "username": "admin",
    "password": "1q2w3e4rT",
    "thumbprint": "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de"
  }
}
```

Beispielausgabe:

```
{
  "connection_info": {
    "thumbprint": "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de",
    "enforcement_point_address": "192.168.2.198",
    "resource_type": "CvxConnectionInfo"
  },
  "auto_enforce": false,
  "resource_type": "EnforcementPoint",
  "id": "cvx-default-ep",
  "display_name": "cvx-default-ep",
  "path": "/infra/sites/default/enforcement-points/cvx-default-ep",
  "relative_path": "cvx-default-ep",
  "parent_path": "/infra/sites/default",
  "marked_for_delete": false,
  "_system_owned": false,
  "_create_user": "admin",
  "_create_time": 1564036461953,
  "_last_modified_user": "admin",
}
```

```

    "_last_modified_time": 1564036461953,
    "_protection": "NOT_PROTECTED",
    "_revision": 0
}

```

- 5 Rufen Sie die POST `/api/v1/notification-watchers/-` API auf und erstellen Sie mithilfe des CVX-Fingerabdrucks eine Benachrichtigungs-ID. Beispiel:

```

POST https://<nsx-manager>/api/v1/notification-watchers/
{
  "server": "<virtual IP address of CVX cluster>",
  "method": "POST",
  "uri": "/pcs/v1/nsgroup/notification",
  "use_https": true,
  "certificate_sha256_thumbprint":
  "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de",
  "authentication_scheme": {
    "scheme_name": "BASIC_AUTH",
    "username": "cvpadmin",
    "password": "1q2w3e4rT"
  }
}

```

- 6 Rufen Sie GET `/api/v1/notification-watchers/` auf, um die Benachrichtigungs-ID abzurufen.

Beispielausgabe:

```

{
  "id": "a0286cb6-de4d-41de-99a0-294465345b80",
  "server": "192.168.2.198",
  "port": 443,
  "use_https": true,
  "certificate_sha256_thumbprint":
  "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de",
  "method": "POST",
  "uri": "/pcs/v1/nsgroup/notification",
  "authentication_scheme": {
    "scheme_name": "BASIC_AUTH",
    "username": "cvpadmin"
  },
  "send_timeout": 30,
  "max_send_uri_count": 5000,
  "resource_type": "NotificationWatcher",
  "display_name": "a0286cb6-de4d-41de-99a0-294465345b80",
  "_create_user": "admin",
  "_create_time": 1564038044780,
  "_last_modified_user": "admin",
  "_last_modified_time": 1564038044780,
  "_system_owned": false,
  "_protection": "NOT_PROTECTED",
  "_revision": 0
}

```

- 7 Rufen Sie die `PATCH /policy/api/v1/infra/domains/default/domain-deployment-maps/cvx-default-dmap-API` auf, um eine Bereitstellungszuordnung für die CVX-Domäne zu erstellen.  
Beispiel:

```
PATCH https://<nsx-manager>/policy/api/v1/infra/domains/default/domain-deployment-maps/cvx-default-dmap
{

  "display_name": "cvx-deployment-map",

  "id": "cvx-default-dmap",

  "enforcement_point_path": "/infra/sites/default/enforcement-points/cvx-default-ep"

}
```

- 8 Rufen Sie die `GET /policy/api/v1/infra/domains/default/domain-deployment-maps-API` auf, um die Bereitstellungszuordnungsinformationen abzurufen.

## Freigegebene Adresssätze

Sicherheitsgruppen, die auf dynamischen oder logischen Objekten basieren, können in den Regeln für verteilte Firewalls im Textfeld **Angewendet auf** erstellt und verwendet werden.

Da Adresssätze basierend auf dem Namen oder den Tags der virtuellen Maschine dynamisch aufgefüllt werden und für jeden Filter aktualisiert werden müssen, können Sie die verfügbare Menge an Heap-Speicher auf Hosts für die Speicherung von DFW-Regeln und IP-Adressen auf den Hosts erschöpfen.

In NSX-T Data Center Version 2.5 und höher werden mit der Funktion „Globale Adresssätze“ oder „Gemeinsam genutzte Adresssätze“ Adresssätze für alle Filter gemeinsam genutzt. Jeder Filter kann je nach Eingabe im Feld **Angewendet auf** unterschiedliche Regeln aufweisen. Die Mitglieder in den Adressätzen bleiben bei allen Filtern konstant. Diese Funktion ist standardmäßig aktiviert und verringert die Auslastung des Heap-Speichers. Sie kann nicht deaktiviert werden.

In NSX-T Data Center Version 2.4 und früher sind die globalen oder gemeinsam genutzten Adresssätze deaktiviert, und für Umgebungen mit umfangreichen Regeln für verteilte Firewalls kann der VSIP-Heap erschöpft sein.

## Ost-West-Netzwerksicherheit – Verkettung von Drittanbieterdiensten

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.

## Voraussetzungen

- Partner müssen Dienste bei NSX-T Data Center registrieren.
- ESXi-Hosts müssen mithilfe von Transportknotenprofilen als NSX-T Data Center-Transportknoten vorbereitet werden.

---

## Hinweis

- Dienst-VMs werden ausschließlich auf ESXi-Hosts unterstützt und nicht auf KVM-Hosts.
  - NSX-T Data Center schützt nur die auf ESXi-Hosts ausgeführten Gast-VMs.
  - NSX-T Data Center schützt keine auf KVM-Hosts ausgeführten Gast-VMs.
- 

## 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.

## NSX-T Data Center-Anforderungen für den Ost-West-Datenverkehr

In der NSX-T Data Center-Bereitstellung müssen Sie sicherstellen, dass eine Overlay-Transportzone und Overlay-gestützte logische Switches vorhanden sind.

Der Vorgang zum Einfügen des Ost-West-Diensts wird auf eine gesamte NSX-T-Bereitstellung angewendet. Sie können den Dienst nicht auf Cluster- oder Hostebene bereitstellen.

Alle Transportknoten müssen dem Typ „Overlay“ entsprechen, da der Dienst Datenverkehr auf GENEVE- oder Overlay-gestützten logischen Switches sendet. Ein Overlay-gestützter (GENEVE-gestützter) logischer Switch wird intern bereitgestellt und ist auf der Benutzeroberfläche nicht sichtbar.

Selbst wenn Sie eine Bereitstellung planen, in der nur VLAN-gestützte logische Switches verwendet werden, durchläuft der Ost-West-Datenverkehr Overlay-Transportzonen und Overlay-gestützte logische Switches. Stellen Sie daher sicher, dass Sie eine Overlay-Transportzone und GENEVE-gestützte logische Switches erstellen. Ohne diese Anforderungen kann während eines vMotion-Vorgangs die Gast-VM auf einem Host nicht zu einem anderen Transportknoten migriert werden. Die Gast-VM wechselt in den getrennten Zustand und verursacht dadurch Konfigurationsfehler im Ost-West-Dienst.

## Allgemeine Aufgaben für die Ost-West-Netzwerksicherheit

Führen Sie die folgenden Schritte aus, um die Netzwerksicherheit für den Ost-West-Datenverkehr einzurichten.

Tabelle 10-3. 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
Bereitstellen eines Diensts für die Selbstprüfung von Ost-West-Datenverkehr	Administrator	API und NSX Manager-Benutzeroberfläche
Hinzufügen eines Dienstprofils	Administrator	API und NSX Manager-Benutzeroberfläche
Hinzufügen einer Dienstkette	Administrator	API und NSX Manager-Benutzeroberfläche
Hinzufügen von Umleitungsregeln für Ost-West-Datenverkehr	Administrator	API und NSX Manager-Benutzeroberfläche

## 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 müssen 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 Verwaltungsvernetzwerks miteinander kommunizieren können.
- Host-basierte Dienstbereitstellung: bevor Sie Dienst-VMs auf den einzelnen Hosts bereitstellen, konfigurieren Sie jeden Host des Clusters mit NSX-T Data Center, indem Sie ein Transportknotenprofil anwenden.

### 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 „Compute Manager“ den vCenter Server zum Bereitstellen des Diensts aus.
- 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 und das 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. Gast-VMs, die mit einem Dienstsegment verbunden sind, erhalten einen Ost-West-Netzwerkdatenverkehrsschutz.
- 10 Wählen Sie im Feld „Bereitstellungstyp“ eine der folgenden Bereitstellungsoptionen aus: Je nach den Diensten, die vom Partner registriert werden, können mehrere Dienste als Teil einer einzelnen Dienst-VM bereitgestellt werden.
  - Geclustert: stellt den Dienst auf einem oder mehreren Hosts bereit, die zu einem Cluster gehören, der für das Hosten von Dienst-VMs vorgesehen ist.
  - Host-basiert: stellt den Dienst auf allen Hosts innerhalb eines Clusters bereit.
- 11 Wählen Sie im Feld „Bereitstellungsvorlage“ die Vorlage mit Attributen zum Schutz der Arbeitslast aus, die in Gast-VM-Gruppen ausgeführt werden soll.
- 12 (Nur Cluster-basierte Bereitstellung) Geben Sie unter „Anzahl der geclusterten Bereitstellung“ die Anzahl 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 [Hinzufügen eines Dienstprofils](#).

## Hinzufügen eines Dienstprofils

Ein Dienstprofil ist eine Instanz einer Partneranbietervorlage. Administratoren können die Attribute einer Anbietervorlage zum Erstellen einer Instanz der Vorlage anpassen.

---

**Hinweis** Sie können mehrere Dienstprofile für einen einzelnen Anbieter erstellen. Beispielsweise stellt das für den Weiterleitungspfad festgelegte Dienstprofil den IDS-Schutz bereit, wohingegen das für den umgekehrten Pfad festgelegte Dienstprofil den IPS-Schutz unterstützt. Ein einzelnes Dienstprofil kann jedoch sowohl für den Weiterleitungs- als auch für den umgekehrten Pfad festgelegt werden.

---

### 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 Das Feld „Umleitungsaktion“ erbt die Funktionalität der Anbietervorlage. Wenn z. B. COPY die von der Anbietervorlage bereitgestellte Funktionalität ist, lautet die Umleitungsaktion beim Erstellen eines Dienstprofils standardmäßig COPY.
- 6 (Optional) Definieren Sie Tags, um Dienstprofile zu filtern und zu verwalten.
- 7 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 „Umgekehrter Pfad“ **Weiterleitungspfad umkehren** für die Dienstebene aus, um das Dienstprofil zu verwenden, das Sie für den Weiterleitungspfad festgelegt haben.
- 10 Wenn Sie ein neues Dienstprofil für den umgekehrten Pfad festlegen möchten, klicken Sie auf **Reverse Path festlegen** und fügen Sie ein Dienstprofil hinzu.
- 11 Klicken Sie auf **Speichern**, um das Hinzufügen eines Reverse Path für die Dienstkette abzuschließen.
- 12 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.
- 13 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 Netzwerk-Introspektion 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-T Data Center-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 Netzwerk-Introspektion 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 Wählen Sie eine Dienstkette aus.
- 4 Klicken Sie zum Hinzufügen einer Richtlinie auf **Veröffentlichen**.
- 5 Klicken Sie auf die vertikalen Auslassungspunkte  in einem Abschnitt und dann auf **Regel hinzufügen**.

- 6 Bearbeiten Sie das Feld **Quelle**, um eine Gruppe hinzuzufügen, indem Sie Mitgliedschaftskriterien, statische Mitglieder, IP-/MAC-Adressen oder Active Directory-Gruppen festlegen.
  - a Definieren Sie die Mitgliedschaftskriterien mithilfe einer dieser Entitäten:
    - Virtuelle Maschine
    - Logischer Switch
    - Logischer Port
    - IP Set
  - b Definieren Sie die statische Mitgliederliste mit einer dieser Entitäten:
    - Gruppe
    - Segment
    - Segment-Port
    - Virtuelle Netzwerkschnittstelle
    - Virtuelle Maschine
- 7 Klicken Sie auf **Speichern**.
- 8 Bearbeiten Sie zum Hinzufügen einer Zielgruppe das Feld **Ziel**.
- 9 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.
- 10 Wählen Sie im Feld „Aktion“ die Option **Umleiten** aus, um Datenverkehr entlang der Dienstkette umzuleiten, oder die Option **Nicht umleiten**, um keine Netzwerk-Introspektion auf den Datenverkehr anzuwenden.
- 11 Klicken Sie auf **Veröffentlichen**.
- 12 Klicken Sie zum Wiederherstellen einer veröffentlichten Regel auf **Wiederherstellen**.
- 13 Klicken Sie zum Hinzufügen einer Richtlinie auf **+ Richtlinie hinzufügen**.
- 14 Wählen Sie eine zu klonende Richtlinie oder Regel aus und klicken Sie auf **Klonen**.
- 15 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**.
- 16 Nach dem Aktivieren bzw. Deaktivieren einer Regel klicken Sie auf **Veröffentlichen**, um die Regel durchzusetzen.

## Ergebnisse

Datenverkehr zur Quelle wird zum Zweck der Netzwerk-Introspektion 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 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 10-4. 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** aus.

- 3 Wenn Sie die Gateway-Firewall aktivieren möchten, wählen Sie **Aktionen > Allgemeine Einstellungen** aus und klicken Sie auf die Schaltfläche „Status“. Klicken Sie auf **Speichern**.
- 4 Klicken Sie auf **Richtlinie hinzufügen**. Weitere Informationen zu Kategorien finden Sie unter [Konfigurieren einer Gateway-Firewall](#).
- 5 Geben Sie einen **Namen** für den Abschnitt mit der neuen Richtlinie ein.
- 6 Wählen Sie das **Ziel** für die Richtlinie aus.
- 7 Klicken Sie auf das Zahnradsymbol, um die folgenden Richtlinieneinstellungen zu konfigurieren:

Einstellungen	Beschreibung
Strenges TCP	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 kann die Firewall den Dreizeige-Handshake für einen bestimmten Flow nicht erkennen (d. h., aufgrund des asymmetrischen Datenverkehrs). Standardmäßig erzwingt die Firewall nicht die Notwendigkeit, einen Dreizeige-Handshake anzuzeigen und nimmt bereits eingerichtete 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. 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 Ebene der Gateway-Firewallrichtlinie aktiviert. „Strenges TCP“ wird nicht für Pakete erzwungen, die mit einer standardmäßigen ANY-ANY-Zulassung übereinstimmen, wofür kein TCP-Dienst angegeben wurde.
Statusbehaftet	Eine statusbehaftete Firewall überwacht den Zustand der aktiven Verbindungen und verwendet diese Informationen, um zu ermitteln, welche Pakete die Firewall passieren dürfen.
Gesperrt	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.

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

Die neue Richtlinie wird auf dem Bildschirm angezeigt.

- 9 Wählen Sie einen Richtlinienabschnitt aus und klicken Sie auf **Regel hinzufügen**.
- 10 Geben Sie einen Namen für die Regel ein. IPv4-, IPv6- und Multicast-Adresse werden unterstützt.
- 11 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](#).
- 12 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](#).
- 13 Klicken Sie in der Spalte **Dienste** auf das Bleistiftsymbol und wählen Sie Dienste aus. Wenn nicht definiert, bezieht sich die Regel auf alle Dienste.
- 14 Klicken Sie in der Spalte **Profile** auf das Symbol „Bearbeiten“ und wählen Sie ein Kontextprofil aus oder klicken Sie auf **Neues Kontextprofil hinzufügen**. Siehe [Hinzufügen eines Kontextprofils](#).
  - Kontextprofile werden in der Tier-0-Gateway-Firewallrichtlinie nicht unterstützt.
  - Gateway-Firewallregeln unterstützen keine Kontextprofile mit FQDN-Attributen oder anderen Unterattributen.

Kontextprofile verwenden App-ID-Attribute der Ebene 7 für die Verwendung in Regeln für eine verteilte Firewall und in Gateway-Firewallregeln. Mehrere App-ID-Kontextprofile können in einer Firewallregel mit Diensten verwendet werden, die auf **Beliebig** festgelegt sind. Für ALG-Profil (FTP und TFTP) wird ein Kontextprofil pro Regel unterstützt.

- 15 Klicken Sie auf **Übernehmen**.
- 16 Die Spalte **Angewendet auf** definiert den Geltungsbereich der Erzwingung pro Regel und ermöglicht Benutzern die selektive Anwendung von Regeln auf eine oder mehrere Uplink-Schnittstellen oder Dienstschnittstellen. Standardmäßig werden Gateway-Firewallregeln auf alle verfügbaren Uplinks und Dienstschnittstellen auf einem ausgewählten Gateway angewendet.



17 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.
<b>Ablehnen</b>	Lehnt Pakete mit der angegebenen Quelle, dem angegebenen Ziel und Protokoll ab. Durch das Ablehnen eines Pakets wird eine Meldung über ein nicht erreichbares Ziel an den Absender gesendet. 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 sendende Anwendung wird nach einem Versuch benachrichtigt, dass die Verbindung nicht hergestellt werden kann.

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

19 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. Protokolle werden unter „/var/log/syslog“ auf dem Edge 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>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.
<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>Tag</b>	Tag, das der Regel hinzugefügt wurde.

**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.

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

21 Klicken Sie in jedem Richtlinienabschnitt auf das Symbol **Info**, um den aktuellen Status der Edge-Firewallregeln anzuzeigen, die an Edge-Knoten übertragen werden. Beim Übertragen von Regeln an Edge-Knoten generierte Alarmer werden ebenfalls angezeigt.

- 22** Wenn Sie den konsolidierten Status von Richtlinienregeln anzeigen möchten, die auf Edge-Knoten angewendet werden, führen Sie den API-Aufruf aus.

```
GET https://<policy-mgr>/policy/api/v1/infra/
realized-state/status?intent_path=/infra/domains/default/gateway-policies/
<GatewayPolicy_ID>&include_enforced_status=true
```

## Nord-Süd-Netzwerksicherheit – Einfügen eines Drittanbieterdiensts

NSX-T Data Center bietet die Funktionalität zum Einfügen von Drittanbieterdiensten auf einem Router der Ebene 0 oder 1 im Datacenter, um den Datenverkehr für die Introspektion an den Drittanbieterdienst umzuleiten. Nur ESXi-Hosts werden für die Bereitstellung von vertikalen Dienst-VMs unterstützt. KVM-Hosts werden nicht unterstützt.

### 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 Netzwerk-Introspektion 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 zugreifen.
- Der Hochverfügbarkeitsmodus für den logischen Router muss sich im Aktiv/Standby-Modus befinden.
- Aktivieren Sie das Dienstprogramm Distributed Resource Scheduler.

#### 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-O-Router bereitzustellen. Wählen Sie <b>Hochverfügbarkeit</b> aus, um mehrere Dienstinstanzen im Modus „Aktiv/Standby“ auf dem logischen Tier-O-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.
Netzwerk-ID	Geben Sie die Netzwerk-ID des logischen Switches ein, auf dem Sie das Verwaltungsnetzwerk verbinden möchten.
Compute Manager	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-O-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 > Netzwerk-Introspektion (vertikal) > Richtlinie hinzufügen.**  
Ein Richtlinienabschnitt gleicht einem Firewallabschnitt, in dem Regeln definiert werden, die die Flussrichtung des Datenverkehrs bestimmen.
- 3 Legen Sie für **Umleiten an** die Dienstinstanz fest, die bei NSX-T registriert ist, um eine Netzwerk-Introspektion des Datenverkehrs zwischen Quell- und Zieleinheit durchzuführen.
- 4 Klicken Sie zum Hinzufügen einer Richtlinie auf **Veröffentlichen**.
- 5 Klicken Sie auf die vertikalen Auslassungspunkte  in einem Abschnitt und dann auf **Regel hinzufügen**.

- 6 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.
- 7 Klicken Sie auf **Speichern**.
- 8 Bearbeiten Sie zum Hinzufügen einer Zielgruppe das Feld **Ziel**.
- 9 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.
- 10 Wählen Sie im Feld „Aktion“ die Option **Umleiten** aus, um den Datenverkehr der Dienstinstanz umzuleiten, oder die Option **Nicht umleiten**, um keine Netzwerk-Introspektion auf den Datenverkehr anzuwenden.
- 11 Klicken Sie auf **Veröffentlichen**.
- 12 Klicken Sie zum Wiederherstellen einer veröffentlichten Regel auf **Wiederherstellen**.
- 13 Klicken Sie zum Hinzufügen einer Richtlinie auf **+ Richtlinie hinzufügen**.
- 14 Wählen Sie eine zu klonende Richtlinie oder Regel aus und klicken Sie auf **Klonen**.
- 15 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**.
- 16 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 Netzwerk-Introspektion 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.

## Endpoint-Schutz

Mit NSX-T Data Center können Sie Drittanbieter-Partnerdienste als separate Dienst-VM einfügen, die Endpoint-Schutzdienste bereitstellt. Eine Partnerdienst-VM verarbeitet Datei-, Prozess- und Registrierungsereignisse von der Gast-VM basierend auf den vom NSX-T Data Center-Administrator angewendeten Regeln der Endpoint-Schutzrichtlinie.

## Grundlegendes zum Endpoint-Schutz

Lernen Sie den Anwendungsfall, den Workflow und die wichtigsten Konzepte des Endpoint-Schutzes kennen.

### Anwendungsfall für Endpoint-Schutz

Verwenden Sie in einer virtuellen Umgebung die Guest Introspection-Plattform, um den Virenschutz und den Antimalwareschutz für Gast-VMs bereitzustellen.

Als NSX-Administrator implementieren Sie eine Lösung zum Schutz vor Viren und Malware, die als Dienst-VM (SVM) bereitgestellt wird, um eine Datei-, Netzwerk- oder Prozessaktivität 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 legt dann fest, wie auf das Ereignis reagiert werden soll. Beispiel: zum Überprüfen der Datei auf Virensignaturen.

- 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, fordert Sie den Thin Agent auf der Gast-VM auf, eine der folgenden Methoden anzuwenden:
  - Löschen der infizierten Datei oder Verweigern des Zugriffs auf die Datei.
  - Infizierten VMs kann ein Tag von NSX zugewiesen werden. Darüber hinaus können Sie eine Regel definieren, die solche gekennzeichneten Gast-VMs automatisch in eine Sicherheitsgruppe verschiebt, die die infizierte VM für eine zusätzliche Prüfung und Isolierung vom Netzwerk unter Quarantäne stellt, bis die Infektion vollständig entfernt wurde.



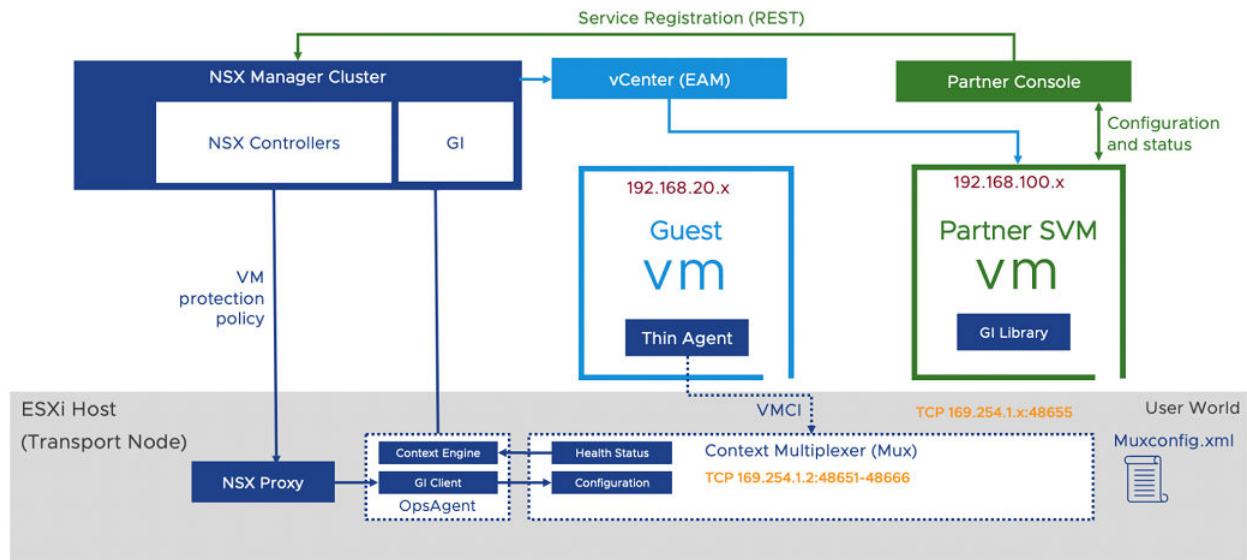
Die Vorteile der Verwendung der Guest Introspection-Plattform zum Schutz von Gast-VM-Endpoints:

- **Reduzierter Verbrauch von Computing-Ressourcen:** Guest Introspection verlagert Virensignaturen und die Sicherheits-Scan-Logik von jedem Endpoint auf einem Host zu einer Drittanbieter-Partnerdienst-VM auf dem Host. Da die Virenprüfung nur auf der Dienst-VM erfolgt, ist es nicht erforderlich, Computing-Ressourcen auf Gast-VMs auszugeben, um Virenprüfungen auszuführen.
- **Besseres Management:** Da Virenprüfungen an eine Dienst-VM ausgelagert werden, müssen die Virensignaturen auf nur ein Objekt pro Host aktualisiert werden. Ein solcher Mechanismus funktioniert besser als eine Agent-basierte Lösung, bei der dieselben Virensignaturen auf allen Gast-VMs aktualisiert werden müssen.
- **Fortlaufender Antiviren- und Antimalwareschutz:** Da die Dienst-VM kontinuierlich ausgeführt wird, ist eine Gast-VM nicht zur Ausführung der neuesten Virensignaturen verpflichtet. Beispiel: Eine Snapshot-VM führt möglicherweise eine ältere Version der Virensignatur aus, wodurch sie auf herkömmliche Weise anfällig für den Schutz von Endpoints wird. Mit der Guest Introspection-Plattform führt die Dienst-VM fortlaufend die neuesten Viren- und Malware-Signaturen aus, wodurch sichergestellt wird, dass jede neu hinzugefügte VM auch mit den neuesten Virensignaturen geschützt ist.
- **Ausgelagerte Virensignaturen zu einer Dienst-VM:** Der Virendatenbank-Lebenszyklus befindet sich außerhalb des Lebenszyklus der Gast-VM. Daher ist die Dienst-VM nicht von Gast-VM-Ausfällen betroffen.

## Guest Introspection-Architektur

Machen Sie sich mit der Architektur der Service Insertion- und Guest Introspection-Komponenten in NSX-T Data Center vertraut.

Abbildung 10-1. Guest Introspection-Architektur



## Wichtige Konzepte:

- Partnerkonsole: Es handelt sich hierbei um die vom Sicherheitsanbieter bereitgestellte Webanwendung, um mit der Guest Introspection-Plattform zu arbeiten.
- NSX Manager: Es handelt sich dabei um die Appliance auf Management Plane für NSX, die Kunden und Partnern API und grafische Benutzeroberfläche für die Konfiguration von Netzwerk- und Sicherheitsrichtlinien zur Verfügung stellt. Für Guest Introspection bietet NSX Manager auch API und GUI zur Bereitstellung und Verwaltung von Partner-Appliances.
- Guest Introspection SDK: von VMware bereitgestellte Bibliothek, die vom Sicherheitsanbieter genutzt wird.
- Dienst-VM: Dies ist die vom Sicherheitsanbieter bereitgestellte VM, die das von VMware bereitgestellte Guest Introspection SDK nutzt. Sie enthält die Logik zum Prüfen von Datei- oder Prozessereignissen, um Viren oder Malware auf dem Gastsystem zu erkennen. Nach dem Scannen einer Anforderung sendet sie ein Urteil oder eine Benachrichtigung über die Aktion zurück, die von der Gast-VM für die Anforderung vorgenommen wurde.
- Guest Introspection-Hostagent (Kontext-Multiplexer): verarbeitet die Konfiguration von Endpoint-Schutzrichtlinien. Darüber hinaus führt er Multiplex- und Weiterleitungsvorgänge für Nachrichten von geschützten VMs an die Dienst-VM aus. Er meldet den Systemzustand der Guest Introspection-Plattform und verwaltet Datensätze der Dienst-VM-Konfiguration in der muxconfig.xml-Datei.
- OPS-Agent (Kontext-Engine und Guest Introspection-Client): leitet die Guest Introspection-Konfiguration des Guest Introspection-Hostagents (Kontext-Multiplexer) weiter. Darüber hinaus wird der Systemzustand der Lösung an NSX Manager weitergeleitet.
- EAM: NSX Manager verwendet den ESXi Agent Manager zum Bereitstellen einer Partnerdienst-VM auf jedem Host des Clusters, der für den Schutz konfiguriert ist.

- **Thin Agent:** dies ist der Datei- oder Netzwerk-Introspektionsagent, der innerhalb der Gast-VMs ausgeführt wird. Darüber hinaus werden Datei- und Netzwerkaktivitäten abgefangen, die über den Hostagent an die Dienst-VM weitergeleitet werden. Dieser Agent gehört zu den VMware Tools. Er ersetzt den herkömmlichen Agent, der von Antivirus- oder Antimalware-Sicherheitsanbietern bereitgestellt wird. Es handelt sich um einen generischen und Lightweight-Agent, der die Auslagerung von Dateien und Prozessen für das Scannen auf der vom Anbieter bereitgestellten Dienst-VM erleichtert.

## Wichtige Konzepte des Endpoint-Schutzes

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 diesen Attributen: Name, Beschreibung, unterstützte Formfaktoren, Bereitstellungsattribute, die Netzwerkschnittstellen enthalten, und den Speicherort der Appliance-OVF-Pakete, die von der SVM verwendet werden sollen.
- **Service Insertion:** NSX stellt das Service Insertion-Framework bereit, mit dem Partner Netzwerk- und Sicherheitslösungen in die NSX-Plattform integrieren können. Die Guest Introspection-Lösung ist eine solche Form von Service Insertion.
- **Dienstprofile und Anbietervorlagen:** Partner registrieren Anbietervorlagen, die Schutzebenen für Richtlinien darstellen. Schutzebenen können beispielsweise als „Gold“, „Silber“ oder „Platin“ klassifiziert werden. Dienstprofile können anhand von Anbietervorlagen erstellt werden, mit denen die NSX-Administratoren die Anbietervorlagen wunschgemäß benennen können. Für andere Dienste als Guest Introspection ermöglichen die Dienstprofile eine weitere Anpassung mithilfe von Attributen. Die Dienstprofile können dann in den Regeln der Endpoint-Schutzrichtlinie verwendet werden, um den Schutz für in NSX definierte virtuelle Maschinengruppen zu konfigurieren. Als Administrator können Sie Gruppen basierend auf VM-Name, Tags oder Bezeichnungen erstellen. Optional können mehrere Dienstprofile aus einer einzelnen Anbietervorlage erstellt werden.
- **Endpoint-Schutzrichtlinie:** eine Richtlinie ist eine Sammlung von Regeln. Wenn Sie über mehrere Richtlinien verfügen, ordnen Sie sie in der Reihenfolge ihrer Ausführung an. Dasselbe gilt für Regeln, die innerhalb einer Richtlinie definiert sind. Beispielsweise enthält Richtlinie A drei Regeln und Richtlinie B weist vier Regeln auf, die so angeordnet sind, dass die Richtlinie A der Richtlinie B vorangestellt ist. Wenn die Guest Introspection mit der Ausführung von Richtlinien beginnt, werden die Regeln aus Richtlinie A vor den Regeln aus Richtlinie B ausgeführt.
- **Endpoint-Schutzregel:** als NSX-Administrator können Sie Regeln erstellen, die die zu schützenden VM-Gruppen angeben. Zudem können Sie die Schutzebene für diese Gruppen auswählen, indem Sie das Dienstprofil für jede Regel angeben.

- **Dienstinstanz:** bezieht sich auf die Dienst-VM auf einem Host. Die Dienst-VMs werden von vCenter als spezielle VMs behandelt und gestartet, bevor eine der Gast-VMs eingeschaltet wird. Sie werden angehalten, nachdem alle Gast-VMs ausgeschaltet wurden. Es gibt eine Dienstinstanz pro Dienst und Host.

---

**Wichtig** Die Anzahl Dienstinstanzen entspricht der Anzahl Hosts, auf denen der Dienst den Host ausführt. Wenn Sie beispielsweise über acht Hosts in einem Cluster verfügen und der Partnerdienst auf zwei Clustern bereitgestellt wurde, beträgt die Gesamtzahl der Dienstinstanzen 16 SVMs.

---

- **Dienstbereitstellung:** als Admin stellen Sie die Partnerdienst-VMs über NSX-T clusterweise bereit. Bereitstellungen werden auf Clusterebene verwaltet, sodass EAM automatisch die Dienst-VM auf ihnen bereitstellt, wenn ein beliebiger Host dem Cluster hinzugefügt wird.

Die automatische Bereitstellung des SVM ist wichtig, da vCenter bei erfolgter DRS-Dienstkonfiguration für ein vCenter-Cluster eine Neuverteilung oder Verteilung vorhandener VMs auf beliebigen Hosts durchführen kann, die nach der SVM-Bereitstellung und nach dem Starten auf dem neuen Host dem Cluster hinzugefügt wurden. Da Partnerdienst-VMs die NSX-T-Plattform benötigen, um Sicherheit für Gast-VMs zu gewährleisten, muss der Host als Transportknoten vorbereitet werden.

---

**Wichtig** Eine Dienstbereitstellung bezieht sich auf einen Cluster auf dem vCenter Server, der für die Bereitstellung und Konfiguration eines Partnerdiensts verwaltet wird.

---

- **Datei-Introspektionstreiber:** ist auf der Gast-VM installiert und fängt die Dateiaktivität auf der Gast-VM ab.
- **Netzwerk-Introspektionstreiber:** ist auf der Gast-VM installiert, fängt den Netzwerkdatenverkehr, den Prozess und die Benutzeraktivitäten auf der Gast-VM ab.

## Allgemeine Aufgaben für den Endpoint-Schutz

Dienste von Drittanbieterpartnern, die eine Sicherheits-Scan-Logik enthalten, sind bei NSX-T Data Center für den Schutz von Gast-VMs registriert. Der Partnerdienst wird erzwungen, wenn der NSX-Administrator die registrierten Dienste bereitstellt und Endpoint-Schutzrichtlinien auf Gast-VM-Gruppen anwendet.

Der Guest Introspection-Workflow für den Anwendungsfall des Endpoint-Schutzes lautet wie folgt:

**Abbildung 10-2. Workflow für Endpoint-Schutz**

Workflow-Aufgaben	Rolle/Persona	Implementierung
Registrieren eines Diensts bei NSX-T Data Center	Partneradministrator	Partnerkonsole
Registrieren eines Diensts bei NSX-T Data Center	Partneradministrator	Partnerkonsole

Workflow-Aufgaben	Rolle/Persona	Implementierung
<a href="#">Registrieren eines Diensts bei NSX-T Data Center</a>	Partneradministrator	Partnerkonsole
<a href="#">Bereitstellen eines Diensts</a>	NSX-Administrator	API und NSX Manager-Benutzeroberfläche
<a href="#">Anzeigen von Details der Dienstinstanz</a>	NSX-Administrator	API und NSX Manager-Benutzeroberfläche
<a href="#">Aktivieren der Dienstinstanz</a>	NSX-Administrator	API und NSX Manager-Benutzeroberfläche
<a href="#">Hinzufügen eines Dienstprofils</a>	NSX-Administrator	API und NSX Manager-Benutzeroberfläche
<a href="#">Verwenden der Guest Introspection-Richtlinie</a>	NSX-Administrator	API und NSX Manager-Benutzeroberfläche
<a href="#">Hinzufügen und Veröffentlichen von Regeln für Endpoint-Schutz</a>	NSX-Administrator	API und NSX Manager-Benutzeroberfläche
<a href="#">Überwachen des Endpoint-Schutzstatus</a>	NSX-Administrator	API und NSX Manager-Benutzeroberfläche

## Konfigurieren von Endpoint-Schutz

Schützen Sie die in einer NSX-T Data Center-Umgebung ausgeführten Gast-VMs mithilfe von Drittanbieter-Sicherheitsdiensten.

Übergeordnete Schritte zum Konfigurieren von Richtlinien für den Endpoint-Schutz:

- 1 Stellen Sie sicher, dass [Voraussetzungen für die Konfiguration des Endpoint-Schutzes](#) erfüllt sind, bevor Sie den Endpoint-Schutz auf Gast-VMs konfigurieren.
- 2 Unterstützte Software. Siehe [Unterstützte Software](#).
- 3 Installieren Sie den Datei-Introspektionstreiber für Linux-VMs. Siehe [Installieren von Guest Introspection Thin Agent auf virtuellen Linux-Maschinen](#).
- 4 Installieren Sie den Datei-Introspektionstreiber für Windows-VMs. Siehe [Installieren von Guest Introspection Thin Agent auf virtuellen Linux-Maschinen](#).
- 5 Installieren Sie den Netzwerk-Introspektionstreiber für Linux-VMs. Siehe [Installieren von Linux Thin Agent für die Netzwerk-Introspektion](#).
- 6 Erstellen Sie einen Benutzers mit der Rolle „Guest Introspection-Partner-Administrator“. Siehe [Erstellen eines Benutzers mit der Rolle „Guest Introspection-Partner-Administrator“](#).
- 7 Registrieren Sie den Partnerdienst mit NSX-T Data Center. Informationen dazu finden Sie in der Partner-Dokumentation.
- 8 Bereitstellen eines Diensts. Siehe [Bereitstellen eines Diensts](#).
- 9 Verwenden Sie die Guest Introspection-Richtlinie. Siehe [Verwenden der Guest Introspection-Richtlinie](#).

- 10 Fügen Sie Regeln für den Endpoint-Schutz hinzu und veröffentlichen Sie sie. Siehe [Hinzufügen und Veröffentlichen von Regeln für Endpoint-Schutz](#).
- 11 Überwachen Sie die Regeln für Endpoint-Schutz. Siehe [Überwachen des Endpoint-Schutzstatus](#).

## 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 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
```

## 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)
- Windows Server 2016
- Windows Server 2019

## 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 (vsepflt)- und Netzwerk-Introspektion (vnetflt)-Treiber.
Guest Introspection-Treiber	Installiert Datei-Introspektion (vsepflt)- und Netzwerk-Introspektion (vnetflt)-Treiber.
NSX File Introspection- und NSX Network Introspection-Treiber	Wählen Sie „NSX File Introspection-Treiber“, um vsepflt zu installieren. Wählen Sie optional „NSX-Netzwerk-Introspektion-Treiber“ aus, um vnetflt (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 `vsepflt` aufgelistet.

## 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

- Windows 7
- Windows 8/8.1
- Windows 10
- Windows 2008 Server R2

- Windows 2012 Server R2
- Windows 2016 Server
- CentOS 7.4 GA
- RHEL 7.4 GA
- Ubuntu 16.04.5 LTS (64 Bit)
- SLES 12 GA

### 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

Aktualisieren Sie eine Partnerdienst-VM.

## 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 Wählen Sie im Dropdown-Menü „Partnerdienst“ den Dienst aus, der bereitgestellt werden soll.
- 4 Klicken Sie auf **Bereitstellung** und dann auf **Dienst bereitstellen**.
- 5 Geben Sie den Namen der Dienstbereitstellung ein.
- 6 Wählen Sie im Feld „Compute Manager“ die Computing-Ressource auf dem vCenter Server aus, auf dem der Dienst bereitgestellt werden soll.
- 7 Wählen Sie im Feld „Cluster“ den Cluster aus, auf dem die Dienste bereitgestellt werden müssen.
- 8 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 dem Host angegeben** 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.

Informationen zur Konfiguration von EAM finden Sie in der vSphere-Dokumentation.
- 9 Klicken Sie in der Spalte „Netzwerk“ auf **Festlegen**.
- 10 Legen Sie die Verwaltungsnetzwerkschnittstelle auf **Auf dem Host angegeben** oder **DVPG** fest.

- 11 Legen Sie den Netzwerktyp auf „DHCP“ oder „Statischer IP-Pool“ fest. Wenn Sie den Netzwerktyp auf „Statischer IP-Pool“ festlegen, treffen Sie in der Liste der verfügbaren IP-Pools eine Auswahl.
- 12 Wählen Sie im Feld „Bereitstellungsspezifikation“ die Option Host-basierte Bereitstellung aus, um den Dienst auf allen Hosts bereitzustellen. Je nach den Diensten, die vom Partner registriert werden, können mehrere Dienste als Teil einer einzelnen Dienst-VM bereitgestellt werden.
- 13 Wählen Sie im Feld „Bereitstellungsvorlage“ die registrierte Bereitstellungsvorlage aus.
- 14 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	Der Name, den Sie bei der Bereitstellung des Diensts eingegeben haben.

Tabelle 10-9. (Fortsetzung)

Feld	Beschreibung
Bereitgestellt auf	Host-IP-Adresse oder FQDN
Bereitstellungsmodus	Cluster oder Eigenständig
Bereitstellungsstatus	Status „Aktiv“ zur Angabe einer erfolgreichen Bereitstellung
Systemzustand	<p>Wenn die Dienstinstanz bereitgestellt wird, lautet der Systemzustand <code>Bereit</code>. Um den Systemzustand von <code>Bereit</code> in <code>Aktiv</code> zu ändern, führen Sie die erforderlichen Konfigurationsänderungen durch. Siehe <a href="#">Aktivieren der Dienstinstanz</a>.</p> <p>Nachdem die folgenden Parameter von NSX-T Data Center erfolgreich umgesetzt wurden, ändert sich der Systemzustand von <code>Bereit</code> in <code>Aktiv</code>.</p> <ul style="list-style-type: none"> <li>■ Lösungsstatus: <code>Aktiv</code></li> <li>■ Konnektivität zwischen NSX-T Data Center Guest Introspection-Agent und NSX-T Data Center Ops-Agent: <code>Aktiv</code></li> <li>■ Systemzustand empfangen um: &lt;Tag, Datum, Uhrzeit&gt;</li> </ul>

### Nächste Schritte

Rufen Sie die Dienstinstanz auf. Siehe [Aktivieren der Dienstinstanz](#).

## 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](#).

## Hinzufügen eines Dienstprofils

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 > Regeln für Endpoint-Schutz > Dienstprofile** aus.
- 3 Wählen Sie im Feld „Partnersdienst“ 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. Siehe [Verwenden der Guest Introspection-Richtlinie](#).

## 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 Ausführen eines Sicherheitsdiensts in einer VM-Gruppe müssen Sie folgende Schritte durchführen:

### Verfahren

- 1 Definieren einer Richtlinie und von Regeln.
- 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 neuen Regel den Regelnamen ein.
- 4 Klicken Sie im Feld „Gruppen auswählen“ auf das Symbol „Bearbeiten“.
- 5 Treffen Sie im Fenster „Gruppen festlegen“ in der vorhandenen Liste der Gruppen eine Auswahl oder fügen Sie eine neue Gruppe hinzu.
  - a Klicken Sie zum Hinzufügen einer neuen Gruppe auf **Gruppe hinzufügen**, geben Sie die Details ein und klicken Sie auf **Speichern**.  
 Siehe [Hinzufügen einer Gruppe](#).
- 6 Wählen Sie in der Spalte „Gruppe“ die VM-Gruppe aus.

7 Wählen Sie in der Spalte „Dienstprofile“ das Dienstprofil aus, das den Gast-VMs in der Gruppe die gewünschte Schutzebene bereitstellt.

- a Klicken Sie zum Hinzufügen eines neuen Dienstprofils auf **Dienstprofil hinzufügen**, geben Sie die Details ein und klicken Sie auf **Speichern**.

Siehe [Hinzufügen eines Dienstprofils](#).

8 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 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 [Beheben von Problemen mit Partnerdiensten](#).

### Anzeigen des Kapazitätsstatus, der für den Endpoint-Schutz festgelegt wurde

Zeigen Sie den Kapazitätsstatus des Endpoint-Schutzdienstes 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.

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%

- 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.
- 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.

## Verwalten des Endpoint-Schutzes

Beheben Sie Richtlinienkonflikte, Integritätsprobleme mit Dienst-VMs und erfahren Sie, wie die Endpoint-Schutzrichtlinie funktioniert.

### Beheben von Problemen mit Partnerdiensten

Wenn die virtuelle Maschine für Partnerdienste nicht funktionsfähig ist, sind die Gast-VMs nicht vor Malware geschützt.

Stellen Sie sicher, dass auf jedem Host die folgenden Dienste oder Prozesse ausgeführt werden:

- Der EAM-Dienst ( ESXi Agency Manager) muss ausgeführt werden. Es muss Zugriff auf die folgende URL bestehen.

```
https://<vCenter_Server_IP_Address>/eam/mob
```

Stellen Sie sicher, dass der Agency Manager von ESXi online ist.

```
root> service-control --status vmware-eam
```

- Portgruppen mit SVMs dürfen nicht gelöscht werden, da diese Portgruppen erforderlich sind, um sicherzustellen, dass SVM weiterhin Gast-VMs schützt.

```
https://<vCenter_Server_IP_Address>/ui
```

- Navigieren Sie in vCenter Server zur virtuellen Maschine, klicken Sie 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.
- Die Verwaltungsschnittstelle, auf der NSX-T Data Center mit der Partnerdienstkonsole kommuniziert, muss aktiviert sein.
- Die Steuerungsschnittstelle, die die Kommunikation zwischen MUX und SVM ermöglicht, muss aktiv sein. Eine Portgruppe zur Verbindung von MUX mit SVM muss erstellt werden. Sowohl Schnittstelle als auch Portgruppe sind erforderlich, 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 10-10. Probleme bei ESXi Agency Manager

Problem	Kategorie	Beschreibung	Lösung
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 kann daran liegen, dass der Webserver, der das OVF-Paket bereitstellt, nicht verfügbar ist. Der Webserver gehört oft zur Lösung, die die Agency erstellt hat.	Der Agency Manager (EAM)-Dienst von ESXi wiederholt den OVF-Downloadvorgang. Überprüfen Sie den Status der Partnerverwaltungskonsole. Klicken Sie auf <b>Auflösen</b> .
Nicht kompatible Hostversion	VM nicht bereitgestellt	Es wird erwartet, dass eine virtuelle Agent-Maschine auf einem Host bereitgestellt wird. Aufgrund von Kompatibilitätsproblemen wurde der Agent jedoch nicht auf dem Host bereitgestellt.	Aktualisieren Sie entweder den Host oder die Lösung, damit der Agent mit dem Host kompatibel ist. Überprüfen Sie die Kompatibilität des SVM. Klicken Sie auf <b>Auflösen</b> .
Nicht genügend Ressourcen	VM nicht bereitgestellt	Es wird erwartet, dass eine virtuelle Agent-Maschine auf einem Host bereitgestellt wird. Allerdings hat der Agency Manager (EAM)-Dienst von ESXi die virtuelle Agent-Maschine nicht bereitgestellt, da der Host weniger CPU- oder Arbeitsspeicherressourcen aufweist.	Der Agency Manager (EAM)-Dienst von ESXi versucht, die virtuelle Maschine erneut bereitzustellen. Stellen Sie sicher, dass CPU- und Arbeitsspeicherressourcen verfügbar sind. Überprüfen Sie den Host und geben Sie einige Ressourcen frei. Klicken Sie auf <b>Auflösen</b> .
Nicht genügend Speicherplatz	VM nicht bereitgestellt	Es wird erwartet, dass eine virtuelle Agent-Maschine auf einem Host bereitgestellt wird. Die virtuelle Agent-Maschine wurde jedoch nicht bereitgestellt, da der Agent-Datenspeicher auf dem Host nicht über genügend freien Speicherplatz verfügte.	Der Agency Manager (EAM)-Dienst von ESXi versucht, die virtuelle Maschine erneut bereitzustellen. Geben Sie Speicherplatz im Datenspeicher frei. Klicken Sie auf <b>Auflösen</b> .

Tabelle 10-10. Probleme bei ESXi Agency Manager (Fortsetzung)

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.	Fügen Sie dem Host eines der unter „customAgentVmNetwork“ aufgelisteten Netzwerke hinzu. Das Problem wird automatisch aufgelöst, sobald der Datenspeicher verfügbar ist.
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.	Der Agency Manager (EAM)-Dienst von ESXi versucht, SVM erneut bereitzustellen. Schlagen Sie in der Dokumentation der Partnerlösung nach oder führen Sie ein Upgrade der Partnerlösung durch, um das gültige OVF-Paket zu erhalten. Klicken Sie auf <b>Auflösen</b> .
Fehlender Agent-IP-Pool	VM ausgeschaltet	Es wird erwartet, dass eine virtuelle Agent-Maschine eingeschaltet ist. Die virtuelle Agent-Maschine wird jedoch ausgeschaltet, weil im VM-Netzwerk des Agents keine IP-Adressen definiert sind.	Definieren Sie die IP-Adresse im Netzwerk der virtuellen Maschine. Klicken Sie auf <b>Auflösen</b> .
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.	Fügen Sie dem Host einen der unter „customAgentVmDatastore“ aufgelisteten Datenspeicher hinzu. Das Problem wird automatisch aufgelöst, sobald der Datenspeicher verfügbar ist.
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.	Fügen Sie den Host einem der Netzwerke hinzu, die in einem benutzerdefinierten Agent-VM-Netzwerk aufgelistet sind. Das Problem wird automatisch aufgelöst, sobald ein benutzerdefiniertes VM-Netzwerk verfügbar ist.



**Tabelle 10-10. Probleme bei ESXi Agency Manager (Fortsetzung)**

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.	Fügen Sie den Host einem der Datenspeicher hinzu, die in einem benutzerdefinierten Agent-VM-Datenspeicher aufgelistet sind. Das Problem wird automatisch aufgelöst.
Verwaiste Agency	Agency-Fehler	Die Lösung, die die Agency erstellt hat, ist nicht mehr mit dem vCenter Server registriert.	Registrieren Sie die Lösung mit vCenter Server.
Verwaister DvFilter-Switch	Hostfehler	Auf einem Host ist ein dvFilter-Switch vorhanden, aber keine Agents auf dem Host benötigen den dvFilter. Dieser Fall tritt ein, wenn eine Hostverbindung bei Änderung einer Agency-Konfiguration getrennt wird.	Klicken Sie auf <b>Auflösen</b> . Der Agency Manager (EAM)-Dienst von ESXi versucht, den Host zu verbinden, bevor die Agency-Konfiguration aktualisiert 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.	Klicken Sie auf <b>Auflösen</b> . Der Agency Manager (EAM)-Dienst von ESXi versucht, die virtuelle Maschine in der Bestandsliste zu platzieren, zu der sie gehört.
Ungültige OVF-Eigenschaft	VM-Fehler	Eine Agent-VM muss eingeschaltet werden, aber eine OVF-Eigenschaft fehlt oder weist einen ungültigen Wert auf.	Klicken Sie auf <b>Auflösen</b> . Der Agency Manager (EAM)-Dienst von ESXi versucht, die korrekte OVF-Eigenschaft erneut zu konfigurieren.
VM beschädigt	VM-Fehler	Eine Agent-VM ist beschädigt.	Klicken Sie auf <b>Auflösen</b> . Der Agency Manager (EAM)-Dienst von ESXi versucht, die virtuelle Maschine zu reparieren.
VM verwaist	VM-Fehler	Ein Agent-VM ist auf einem Host vorhanden, der Host gehört aber nicht mehr zum Bereich für die Agency. Dieser Fall tritt ein, wenn eine Hostverbindung bei Änderung der Agency-Konfiguration getrennt wird.	Klicken Sie auf <b>Auflösen</b> . Der Agency Manager (EAM)-Dienst von ESXi versucht, den Host wieder mit der Agency-Konfiguration zu verbinden.

Tabelle 10-10. Probleme bei ESXi Agency Manager (Fortsetzung)

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.	Klicken Sie auf <b>Auflösen</b> . Der Agency Manager (EAM)-Dienst von ESXi versucht, die virtuelle Agent-Maschine vom Host zu entfernen.
VM ausgeschaltet	VM-Fehler	Eine Agent-VM soll eingeschaltet werden, wurde aber ausgeschaltet.	Klicken Sie auf <b>Auflösen</b> . Der Agency Manager (EAM)-Dienst von ESXi versucht, die virtuelle Maschine einzuschalten.
VM eingeschaltet	VM-Fehler	Eine Agent-VM soll ausgeschaltet werden, wurde aber eingeschaltet.	Klicken Sie auf <b>Auflösen</b> . Der Agency Manager (EAM)-Dienst von ESXi versucht, die virtuelle Maschine auszuschalten.
VM angehalten	VM-Fehler	Eine Agent-VM soll eingeschaltet werden, wurde aber angehalten.	Klicken Sie auf <b>Auflösen</b> . Der Agency Manager (EAM)-Dienst von ESXi versucht, die virtuelle Maschine einzuschalten.
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.	Klicken Sie auf <b>Auflösen</b> . Der Agency Manager (EAM)-Dienst von ESXi versucht, die virtuelle Agent-Maschine im vorgesehenen Ordner zu platzieren.

**Tabelle 10-10. Probleme bei ESXi Agency Manager (Fortsetzung)**

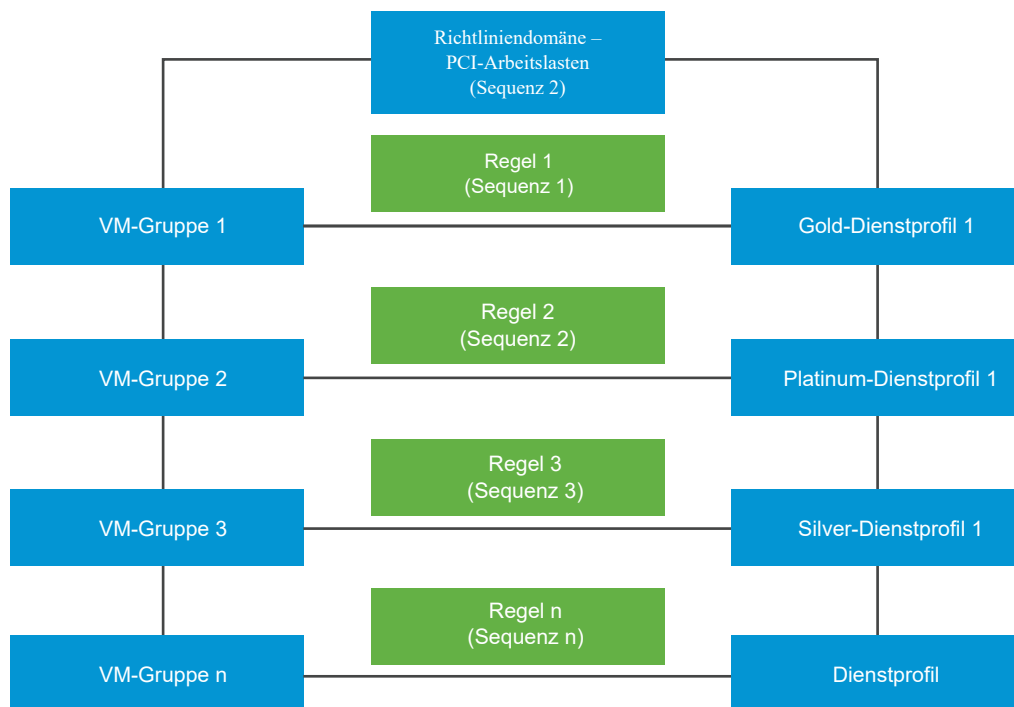
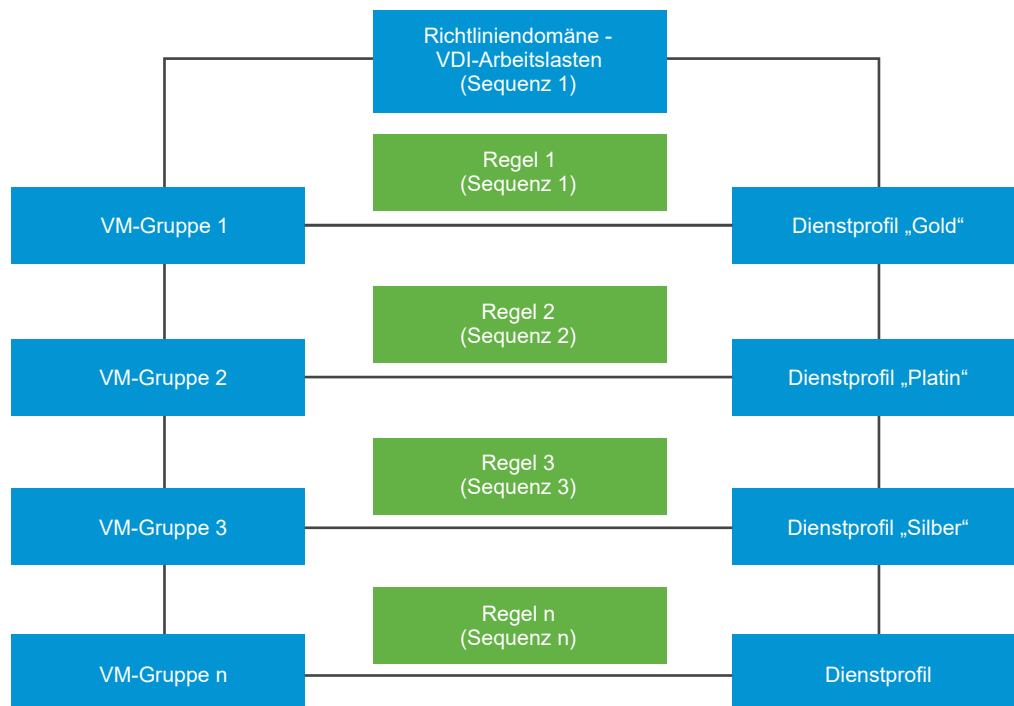
Falscher VM-Ressourcenpool	VM-Fehler	Eine Agent-VM soll in einem bestimmten Ressourcenpool der Agent-VM gespeichert sein, befindet sich aber in einem anderen Ressourcenpool.	Klicken Sie auf <b>Auflösen</b> . Der Agency Manager (EAM)-Dienst von ESXi versucht, die virtuelle Agent-Maschine in einem vorgesehenen Ressourcenpool zu platzieren.
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.	Klicken Sie zum Bereitstellen der virtuellen Agent-Maschine auf <b>Auflösen</b> .

Im nächsten Schritt konfigurieren Sie den Endpoint-Schutz für VM-Gruppen. Siehe [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.

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 10-11. NSX-T Data Center-APIs, die zum Definieren von Regeln verwendet werden, die Dienstprofile auf VM-Gruppen anwenden**

API	Details
Abrufen aller Details der Dienstkongfiguration.	<pre>GET /api/v1/service-configs</pre> <p>Die Dienstkongfigurations-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 Dienstkongfiguration.	<pre>POST /api/v1/service-configs</pre> <p>Die Dienstkongfigurations-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 Dienstkongfiguration.	<pre>DELETE /api/v1/service-configs/ &lt;config-set-id&gt;</pre> <p>Die Dienstkongfigurations-API löscht die auf die VM-Gruppe angewendete Konfiguration.</p>
Abrufen der Details einer bestimmten Konfiguration.	<pre>GET /api/v1/service-configs/ &lt;config-set-id&gt;</pre> <p>Abrufen der Details einer bestimmten Konfiguration</p>
Aktualisieren einer Dienstkongfiguration.	<pre>PUT /api/v1/service-configs/ &lt;config-set-id&gt;</pre> <p>Aktualisieren einer Dienstkongfiguration.</p>
Abrufen der effektiven Profile.	<pre>GET /api/v1/service-configs/ effective-profiles?resource_id=&lt;resource-id&gt; &amp;resource_type=&lt;resource-type&gt;</pre> <p>Die Dienstkongfigurations-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.

## Konfliktlösung bei Endpoint-Richtlinien

Stellen Sie sich ein Szenario vor, in dem zwei Richtliniendomänen vorhanden sind, die beide aus mehreren Regeln bestehen. Als Admin 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.

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 Admin 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 <code>Inaktiv</code> oder <code>Nicht verfügbar</code> .	<ol style="list-style-type: none"> <li>1 Stellen Sie sicher, dass der Status der Dienstbereitstellung <code>Aktiv</code> ist (grüne Statusanzeige). Bei Fehlern finden Sie weiterführende Informationen unter <a href="#">Beheben von Problemen mit Partnerdiensten</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 <code>Inaktiv</code> .	<ol style="list-style-type: none"> <li>1 Stellen Sie sicher, dass der Status der Dienstbereitstellung <code>Aktiv</code> ist (grüne Statusanzeige). Bei Fehlern finden Sie weiterführende Informationen unter <a href="#">Beheben von Problemen mit Partnerdiensten</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="#">Beheben von Problemen mit Partnerdiensten</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*.

# Sicherheitsprofile

Dieser Abschnitt enthält Profile zur Feinabstimmung von Firewall-Vorgängen: Sitzungs-Timer, Flood Protection und DNS-Sicherheit

## Erstellen eines Sitzungs-Timers

Mithilfe von Sitzungs-Timern wird definiert, wie lange eine Sitzung nach Inaktivität in der Sitzung an der Firewall beibehalten wird.

Wenn die Sitzungszeitüberschreitung für das Protokoll abläuft, wird die Sitzung geschlossen. An der Firewall können verschiedene Zeitüberschreitungen für TCP-, UDP- und ICMP-Sitzungen angegeben werden, die auf eine benutzerdefinierte Gruppe oder ein Tier-0- oder Tier-1-Gateway angewendet werden. Die Standardwerte für die Sitzung können je nach Netzwerkanforderungen geändert werden. Hinweis: Wenn Sie einen zu niedrigen Wert festlegen, können häufige Zeitüberschreitungen die Folge sein. Die Festlegung zu hoher Werte kann dagegen die Fehlererkennung verzögern.

### Verfahren

- 1 Navigieren Sie zu **Sicherheit > Einstellungen > Sicherheitsprofile > Sitzungs-Timer**.
- 2 Klicken Sie auf **Profil hinzufügen** .  
Der Bildschirm **Profil** wird mit den Standardwerten gefüllt angezeigt.
- 3 Geben Sie einen **Namen** und eine **Beschreibung** (optional) für das Timer-Profil ein.
- 4 Klicken Sie auf **Festlegen**, um das Tier-0- oder Tier-1-Gateway oder die Gruppe auszuwählen, auf die das Timer-Profil angewendet wird.
- 5 Wählen Sie das Protokoll aus. Übernehmen Sie die Standardwerte, oder geben Sie eigene Werte ein.

TCP-Variablen	Beschreibung
Erstes Paket	Der Zeitüberschreitungswert für die Verbindung nach dem Senden des ersten Pakets. Die Standardeinstellung ist 120 Sekunden.
Öffnen	Der Zeitüberschreitungswert für die Verbindung nach dem Übertragen des zweiten Pakets. Die Standardeinstellung ist 30 Sekunden.
Hergestellt	Der Zeitüberschreitungswert für die Verbindung, nachdem die Verbindung vollständig hergestellt wurde.
Wird geschlossen	Der Zeitüberschreitungswert für die Verbindung nach dem Senden des ersten FIN. Die Standardeinstellung ist 120 Sekunden.
Fin Wait	Der Zeitüberschreitungswert für die Verbindung, nachdem beide FINs ausgetauscht wurden und die Verbindung geschlossen ist. Die Standardeinstellung ist 45 Sekunden.
Geschlossen	Der Zeitüberschreitungswert für die Verbindung, nachdem ein Endpoint ein RST gesendet hat. Die Standardeinstellung ist 20 Sekunden.

UDP-Variablen	Beschreibung
Erstes Paket	Der Zeitüberschreitungswert für die Verbindung nach dem Senden des ersten Pakets. Dies ist die initiale Zeitüberschreitung für den neuen UDP-Fluss. Die Standardeinstellung ist 60 Sekunden.
Einzel	Der Zeitüberschreitungswert für die Verbindung, wenn der Quellhost mehrere Pakete sendet und der Zielhost kein Paket zurückgesendet hat. Die Standardeinstellung ist 30 Sekunden.
Mehrere	Der Zeitüberschreitungswert für die Verbindung, wenn beide Hosts Pakete gesendet haben. Die Standardeinstellung ist 60 Sekunden.

ICMP-Variablen	Beschreibung
Erstes Paket	Der Zeitüberschreitungswert für die Verbindung nach dem Senden des ersten Pakets. Dies ist die initiale Zeitüberschreitung für den neuen ICMP-Fluss. Die Standardeinstellung ist 20 Sekunden.
Fehlerantwort	Der Zeitüberschreitungswert für die Verbindung nach dem Zurückgeben eines ICMP-Fehlers in Reaktion auf ein ICMP-Paket. Die Standardeinstellung ist 10 Sekunden.

## 6 Klicken Sie auf **Speichern**.

### Nächste Schritte

Klicken Sie nach dem Speichern auf [Gruppen-zu-Profil-Vorrang verwalten](#), um die Bindungspriorität zwischen Gruppe und Profil zu verwalten.

## Sitzungs-Timer-Standardwerte

Das Sitzungs-Timer-Profil wendet die Zeitüberschreitungswerte auf Routerschnittstellen der Ebene 0 oder 1 oder auf Gruppen mit Segmenten an. Die Zeitüberschreitungswerte legen fest, wie lange eine Protokollsitzung nach dem Schließen der Sitzung aktiv bleibt.

### Sitzungs-Timer-Werte

- Das mit der API und auf der Benutzeroberfläche angezeigte Standard-Timer-Profil gilt nur für die verteilte Firewall (DFW).
- Die Standard-Sitzungs-Timer der Gateway-Firewall (GFW) unterscheiden sich von den Standard-Profil-Timern, die bei Verwendung der API und der Benutzeroberfläche angezeigt werden. Die Standard-Sitzungs-Timer von GFW sind für horizontalen Datenverkehr optimiert und standardmäßig niedriger.
- FW-Sitzungs-Timer können sowohl für DFW als auch für GFW über die API und die Benutzeroberfläche geändert werden.
- Dasselbe nicht standardmäßige Timer-Profil kann bei Bedarf sowohl auf DFW als auch auf GFW angewendet werden.

Wenn Sie die Timer-Werte nicht anpassen, verwendet das Gateway Standardwerte. Standard-Timer-Werte der Gateway-Firewall:

Timer-Eigenschaft	Edge-Standardwert (Sek.)	Minimum (Sekunden)	Maximum (Sekunden)
ICMP-Fehlerantwort	6	10	4320000
Erstes ICMP-Paket	6	10	4320000

Timer-Eigenschaft	Edge-Standardwert (Sek.)	Minimum (Sekunden)	Maximum (Sekunden)
TCP geschlossen	2	10	4320000
TCP wird geschlossen	900	10	4320000
TCP eingerichtet	7200	120	4320000
TCP FIN-wait	4	10	4320000
Erstes TCP-Paket	120	10	4320000
TCP wird geöffnet	30	10	4320000
Erstes UDP-Paket	30	10	4320000
UDP mehrfach	30	10	4320000
UDP einfach	30	10	4320000

Sitzungs-Timer-Standardwerte der verteilten Firewall:

Timer-Eigenschaft	DFW-Standardwert (Sek.)	Minimum (Sekunden)	Maximum (Sekunden)
ICMP-Fehlerantwort	10	10	4320000
Erstes ICMP-Paket	20	10	4320000
TCP geschlossen	20	10	4320000
TCP wird geschlossen	120	10	4320000
TCP eingerichtet	43200	120	4320000
TCP FIN-wait	45	10	4320000
Erstes TCP-Paket	120	10	4320000
TCP wird geöffnet	30	10	4320000
Erstes UDP-Paket	60	10	4320000
UDP mehrfach	60	10	4320000
UDP einfach	30	10	4320000

## Flood Protection

Flood Protection hilft beim Schutz vor Denial-of-Service-Angriffen (DDoS).

DDoS-Angriffe zielen darauf ab, einen Server für legitimen Datenverkehr nicht verfügbar zu machen, indem alle verfügbaren Serverressourcen verbraucht werden – der Server wird mit Anforderungen überflutet. Beim Erstellen eines Flood Protection-Profiles werden aktive Sitzungsgrenzwerte für ICMP-, UDP- und halboffene TCP-Flows festgelegt. Die verteilte Firewall kann Flow-Einträge im SYN\_SENT- und SYN\_RECEIVED-Status zwischenspeichern und jeden Eintrag auf einen TCP-Status heraufstufen, nachdem eine Bestätigung vom Initiator empfangen wurde, um den Drei-Wege-Handshake abzuschließen.

## Verfahren

- 1 Navigieren Sie zu **Sicherheit > Sicherheitsprofile > Flood Protection**.
- 2 Klicken Sie auf **Profil hinzufügen** und wählen Sie **Edge-Gateway-Profil hinzufügen** oder **Firewall-Profil hinzufügen** aus.
- 3 Vervollständigen Sie die Parameter für das Flood Protection-Profil:

**Tabelle 10-15. Parameter für Firewall- und Edge Gateway-Profile**

Parameter	Mindest- und Höchstwerte	Standard	
Grenzwert für halboffene TCP-Verbindung – TCP SYN-Flood-Angriffe werden verhindert, indem die Anzahl der aktiven, nicht vollständig eingerichteten TCP-Flows begrenzt wird, die von der Firewall zugelassen werden.	1–1.000.000	Firewall – keine Edge-Gateway – 1.000.000	Legen Sie dieses Textfeld fest, um die Anzahl der aktiven halboffenen TCP-Verbindungen zu begrenzen. Wenn dieses Textfeld leer ist, wird dieser Grenzwert auf ESX-Knoten deaktiviert und auf den Standardwert für Edge-Gateways festgelegt.
Grenzwert für aktiven UDP-Flow – UDP-Flood-Angriffe werden verhindert, indem die Anzahl der aktiven UDP-Flows begrenzt wird, die von der Firewall zugelassen werden. Sobald der festgelegte UDP-Flow-Grenzwert erreicht ist, werden nachfolgende UDP-Pakete, die einen neuen Flow generieren können, verworfen.	1–1.000.000	Firewall – keine Edge-Gateway – 1.000.000	Legen Sie dieses Textfeld fest, um die Anzahl der aktiven UDP-Verbindungen zu begrenzen. Wenn dieses Textfeld leer ist, wird dieser Grenzwert auf ESX-Knoten deaktiviert und auf den Standardwert für Edge-Gateways festgelegt.

Tabelle 10-15. Parameter für Firewall- und Edge Gateway-Profil (Fortsetzung)

Parameter	Mindest- und Höchstwerte	Standard	
Grenzwert für aktiven ICMP-Flow – ICMP-Flood-Angriffe werden verhindert, indem die Anzahl der aktiven ICMP-Flows begrenzt wird, die von der Firewall zugelassen werden. Nachdem der festgelegte Flow-Grenzwert erreicht wurde, werden nachfolgende ICMP-Pakete, die einen neuen Flow generieren können, verworfen.	1–1.000.000	Firewall – keine Edge-Gateway – 10.000	Legen Sie dieses Textfeld fest, um die Anzahl der aktiven offenen ICMP-Verbindungen zu begrenzen. Wenn dieses Textfeld leer ist, wird dieser Grenzwert auf ESX-Knoten deaktiviert und auf den Standardwert für Edge-Gateways festgelegt.
Grenzwert für andere aktive Verbindung	1–1.000.000	Firewall – keine Edge-Gateway – 10.000	Legen Sie dieses Textfeld fest, um die Anzahl der aktiven Verbindungen zu begrenzen, bei denen es sich nicht um halboffene ICMP-, TCP- und UDP-Verbindungen handelt. Wenn dieses Textfeld leer ist, wird dieser Grenzwert auf ESX-Knoten deaktiviert und auf den Standardwert für Edge-Gateways festgelegt.



Tabelle 10-15. Parameter für Firewall- und Edge Gateway-Profil (Fortsetzung)

Parameter	Mindest- und Höchstwerte	Standard	
SYN-Cache – SYN-Cache wird verwendet, wenn auch ein Grenzwert für halboffene TCP-Verbindungen konfiguriert wurde. Die Anzahl der aktiven halboffenen Verbindungen wird durch die syncache-Beibehaltung der nicht vollständig eingerichteten TCP-Sitzungen erzwungen. Dieser Cache verwaltet die Flow-Einträge, die sich im SYN_SENT- und SYN_RECEIVED-Status befinden. Jeder syncache-Eintrag wird auf einen vollständigen TCP-Statuseintrag heraufgestuft, nachdem eine Bestätigung vom Initiator empfangen wurde, um den Dreiwege-Handshake abzuschließen.		Nur für Firewall-Profil verfügbar.	Ein- und ausschalten. Das Aktivieren des SYN-Caches ist nur wirksam, wenn ein Grenzwert für halboffene TCP-Verbindungen konfiguriert ist.
RST-Spoofing – Generiert manipuliertes RST auf dem Server, wenn halboffene Zustände aus dem SYN-Cache gelöscht werden. Ermöglicht dem Server, Zustände in Verbindung mit einer SYN-Flood zu bereinigen (halboffen).		Nur für Firewall-Profil verfügbar.	Aktivieren und deaktivieren. SYN-Cache muss ausgewählt werden, damit diese Option verfügbar ist

4 Wenn Sie das Profil auf Edge-Gateways und Firewall-Gruppen anwenden möchten, klicken Sie auf **Festlegen**.

5 Klicken Sie auf **Speichern**.

#### Nächste Schritte

Klicken Sie nach dem Speichern auf [Gruppen-zu-Profil-Vorrang verwalten](#), um die Bindungspriorität zwischen Gruppe und Profil zu verwalten.

## Konfigurieren der DNS-Sicherheit

Das Erstellen eines DNS-Sicherheitsprofils hilft beim Schutz vor DNS-bezogenen Angriffen.

Nach der Einrichtung des DNS-Sicherheitsprofils können Sie Folgendes tun:

- Führen Sie einen Snooping-Vorgang auf DNS-Antworten für eine VM oder eine Gruppe von VMs auf dem Transportknoten aus, um FQDN mit IP-Adressen zu verknüpfen.
- Fügen Sie globale und standardmäßige DNS-Serverinformationen hinzu und wenden Sie sie auf alle VMs an, die DFW-Regeln verwenden.
- Geben Sie die ausgewählten DNS-Serverinformationen für ausgewählte VMs an.
- Wenden Sie DNS-Profile auf Gruppen an.

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

#### Verfahren

- 1 Navigieren Sie zu **Sicherheit > Einstellungen > Sicherheitsprofile > DNS-Sicherheit**.
- 2 Klicken Sie auf **Profil hinzufügen**.
- 3 Geben Sie die folgenden Werte ein:

Option	Beschreibung
Profilname	Geben Sie einen Profilnamen an.
TTL	<p>In diesem Feld wird die Lebenszeit für den DNS-Cache-Eintrag in Sekunden erfasst. Sie haben die folgenden Optionen:</p> <p>TTL 0 – zwischengespeicherter Eintrag läuft nie ab.</p> <p>TTL 1 bis 3599 – ungültig</p> <p>TTL 3600 bis 864000 – gültig</p> <p>TTL leer gelassen – automatische TTL, festgelegt im DNS-Antwortpaket.</p> <p><b>Hinweis</b> Das DNS-Sicherheitsprofil verfügt über eine standardmäßige DNS-Cache-Zeitüberschreitung von 24 Stunden.</p>
Angewendet auf	<p>Sie können eine Gruppe basierend auf beliebigen Kriterien auswählen, um das DNS-Sicherheitsprofil darauf anzuwenden.</p> <p><b>Hinweis</b> Nur ein DNS-Serverprofil wird auf eine VM angewendet.</p>
Tags	<p>Optional Weisen Sie dem DNS-Profil ein Tag und einen Geltungsbereich zu, um die Suche zu vereinfachen. Weitere Informationen hierzu finden Sie unter <a href="#">Hinzufügen von Tags zu einem Objekt</a>.</p>

- 4 Klicken Sie auf **Speichern**.

#### Nächste Schritte

Klicken Sie nach dem Speichern auf [Gruppen-zu-Profil-Vorrang verwalten](#), um die Bindungspriorität zwischen Gruppe und Profil zu verwalten.

## Gruppen-zu-Profil-Vorrang verwalten

Sie können mehrere Gruppen an ein Sicherheitsprofil binden. NSX-T Data Center wendet das Sicherheitsprofil auf die Gruppe mit der höchsten Prioritätsstufe an.

Wenn Sie ein Sicherheitsprofil an mehrere Gruppen binden, weist NSX-T Data Center der neuesten Gruppe aus dieser Liste die höchste Priorität zu. Sie können jedoch die Prioritätsstufe für Gruppen ändern.

So weisen Sie Gruppen eine Priorität zu:

#### Voraussetzungen

- Sitzungs-Timer-Gruppen dürfen nur Segmente, Segment-Ports und VMs als Mitglieder enthalten. Andere Kategorietypen werden nicht unterstützt.
- DNS-Sicherheitsgruppen dürfen nur VMs als Mitglieder enthalten. Andere Kategorietypen werden nicht unterstützt.

#### 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 > Sicherheitsprofile**.
- 3 Klicken Sie auf **Gruppen-zu-Profil-Vorrang verwalten**
- 4 Wenn Sie einer Gruppe die höchste Prioritätsstufe zuweisen möchten, verschieben Sie sie an den Anfang der Liste.
- 5 Klicken Sie auf **Schließen**.

#### Ergebnisse

Das Sicherheitsprofil wird auf die Gruppe mit der höchsten Prioritätsstufe angewendet.

Sie können Dienste, Gruppen, Kontextprofile und virtuelle Maschinen für den NSX-T Data Center-Bestand konfigurieren.

Wenn Sie auf die Registerkarte **Bestand** klicken, wird eine Übersicht über die Bestandsobjekte mit der Anzahl Gruppen, Dienste, virtuelle Maschinen und Kontextprofile angezeigt, die sich im Bestand befinden. Darüber hinaus werden die folgenden Informationen zu Gruppen angezeigt:

- die Anzahl der Gruppen, die in Richtlinien verwendet werden
- die Anzahl der Gruppen, die nicht in Richtlinien verwendet werden
- die Anzahl der Gruppen mit Mitgliedern
- die Anzahl der Gruppen ohne Mitglieder
- die Anzahl der Identitätsgruppen
- die Anzahl der in Richtlinien verwendeten Identitätsgruppen
- die Anzahl der Identitätsgruppen, die nicht in Richtlinien verwendet werden

Dieses Kapitel enthält die folgenden Themen:

- [Hinzufügen eines Diensts](#)
- [Hinzufügen einer Gruppe](#)
- [Hinzufügen eines Kontextprofils](#)

## 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. Einige 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**. 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) Fügen Sie ein oder mehrere Tags hinzu.
- 9 (Optional) Geben Sie eine Beschreibung ein.
- 10 Klicken Sie auf **Speichern**.

## Hinzufügen einer Gruppe

Gruppen enthalten verschiedene Objekte, die sowohl statisch als auch dynamisch hinzugefügt werden und als Quelle und Ziel einer Firewallregel verwendet werden können.

Gruppen können so konfiguriert werden, dass sie eine Kombination aus virtuellen Maschinen, IP Sets, MAC Sets, Segment-Ports, Segmenten, AD-Benutzergruppen und anderen Gruppen enthalten. Gruppen können auf Basis von Tags, Maschinen-, Betriebssystem- oder Computernamen dynamisch aufgenommen werden. Gruppen, die auf dynamischen oder logischen Objekten basieren, können nicht im Textfeld „Angewendet auf“ für Regeln für verteilte Firewalls verwendet werden.

Bei Tags in NSX wird die Groß-/Kleinschreibung beachtet, aber für eine Gruppe, die auf Tags basiert, wird „die Groß-/Kleinschreibung beachtet“. Wenn z. B. das Kriterium der dynamischen Gruppierungsmitgliedschaft `VM Tag Equals 'quarantine'` ist, enthält die Gruppe alle VMs, die das Tag „Quarantäne“ bzw. „QUARANTÄNE“ enthalten.

Gruppen können von Firewallregeln auch ausgeschlossen werden und es können maximal 100 Gruppen in der Liste enthalten sein. IP-Sets, MAC-Sets und AD-Gruppen können nicht als Mitglieder in eine Gruppe eingeschlossen werden, die in einer Ausschlussliste für die Firewall verwendet wird. Weitere Informationen hierzu finden Sie unter [Verwalten einer Firewall-Ausschlussliste](#).

---

**NSX Cloud-Hinweis** Bei Verwendung von NSX Cloud finden Sie unter [Gruppen-VMs mit NSX-T Data Center und Public-Cloud-Tags](#) Informationen zur Verwendung von Public Cloud-Tags zur Gruppierung Ihrer Arbeitslast-VMs in NSX Manager.

---

Eine einzelne, ID-basierte Gruppe kann nur in einer DFW-Regel als Quelle verwendet werden. Wenn für die Quelle IP- und ID-basierte Gruppen 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 (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 Mitgliedschaftskriterium kann auf Folgendes angewendet werden:

- **Segment-Port** – kann ein Tag und optional den Geltungsbereich angeben.
- **Segment** – 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.
- **IP Set** – kann ein Tag und optional den Geltungsbereich angeben.

- 5 (Optional) Klicken Sie auf **Mitglieder**, um Mitglieder auszuwählen.

Die verfügbaren Mitgliedstypen sind:

- **Gruppe**
- **Segment**
- **Segment-Port**
- **Virtuelle Netzwerkschnittstelle**
- **Virtuelle Maschine**

- 6 (Optional) Klicken Sie auf **IP-/MAC-Adressen**, um IP- und MAC-Adressen als Gruppenmitglieder hinzuzufügen.

IPv4-, IPv6- und Multicast-Adressen werden unterstützt.

**7** (Optional) Klicken Sie auf **AD-Gruppen**, um Active Directory-Gruppen hinzuzufügen. Gruppen mit Active Directory-Mitgliedern können im Quellfeld einer verteilten Firewallregel verwendet werden. Gruppen können sowohl AD- als auch Computing-Mitglieder enthalten.

**8** (Optional) Geben Sie eine Beschreibung und ein Tag ein.

**9** Klicken Sie auf **Anwenden**.

Gruppen werden mit einer Option zum Anzeigen der Mitglieder und einer Angabe zu deren Verwendungsort aufgeführt.

## Hinzufügen eines Kontextprofils

Kontext Profile ermöglichen das Erstellen von Attributschlüssel-Wert-Paaren wie App-ID der Schicht 7 und Domännennamen. Nach der Definition eines Kontextprofils kann es in einer oder mehreren Regeln für verteilte Firewalls und Gateway-Firewallregeln verwendet werden.

Es gibt zwei Attribute für die Verwendung in Kontextprofilen: App-ID und Domänenname (FQDN). Die Auswahl von App-IDs kann ein oder mehrere unter Attribute aufweisen, z. B. TLS\_Version und CIPHER\_SUITE. 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.

Derzeit wird eine vordefinierte Liste der Domänen unterstützt. Sie können die Liste der FQDNs anzeigen, wenn Sie ein neues Kontextprofil mit dem Attributtyp *Domänenname (FQDN)* hinzufügen. Sie können auch eine Liste der FQDNs anzeigen, indem Sie den API-Aufruf / `policy/api/v1/infra/context-profiles/attributes?attribute_key=DOMAIN_NAME` ausführen.

---

### Hinweis

- Gateway-Firewallregeln unterstützen nicht die Verwendung von FQDN-Attributen oder anderen Unterattributen in Kontextprofilen.
  - Kontextprofile werden in der Tier-0-Gateway-Firewallrichtlinie nicht unterstützt. Gateway-Firewallregeln unterstützen nicht die Verwendung von FQDN-Attributen oder anderen Unterattributen.
- 

### 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 verteilte Firewall-Regel der Schicht 7 (für Schicht 7 oder Domänenname) oder eine Gateway-Firewallregel (für Schicht 7) an.



Es gibt mehrere Möglichkeiten, die NSX-T-Umgebung sowie den Netzwerkdatenverkehr zu überwachen.

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](#)
- [Simple Network Management-Protokoll \(SNMP\)](#)
- [Verwenden von vRealize Log Insight für die Systemüberwachung](#)
- [Verwenden von vRealize Operations Manager für die Systemüberwachung](#)
- [Verwenden von vRealize Network Insight Cloud für die Systemüberwachung](#)
- [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 **Planen und Fehler beheben > Empfehlungen** aus.
- 3 Klicken Sie auf die Registerkarte **Firewall-IPFIX-Profile**.
- 4 Klicken Sie auf **Firewall-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.
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.
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 im Dropdown-Menü einen Collector aus.
Angewendet auf	Klicken Sie auf <b>Festlegen</b> und wählen Sie eine Gruppe aus, auf die der Filter angewendet werden soll, oder erstellen Sie eine neue Gruppe.
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 **Speichern**.

## Hinzufügen eines Switch-IPFIX-Profiles

Sie können IPFIX-Profile für Switches (auch als „Segmente“ bezeichnet) konfigurieren.

Die Flow-basierte Netzwerküberwachung ermöglicht Netzwerkadministratoren einen Einblick in den Datenverkehr, der über das Netzwerk übermittelt 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 **Planen und Fehler beheben > Empfehlungen** aus.
- 3 Klicken Sie auf die Registerkarte **Switch-IPFIX-Profile**.
- 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.
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 im Dropdown-Menü einen Collector aus.
Angewendet auf	Wählen Sie eine Kategorie aus: Segment, Segmentport oder Gruppen. Das-IPFIX-Profil wird auf das ausgewählte Objekt angewendet.
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.
Overlay-Flow exportieren	Dieser Parameter legt fest, ob die Overlay-Flows in Uplink- und Tunnel-Ports abgetastet und exportiert werden. Sowohl der vNIC-Flow als auch der Overlay-Flow sind im Beispiel enthalten. Der Standardwert lautet <b>aktiviert</b> . Wenn diese Option deaktiviert ist, werden nur vNIC-Flows abgetastet und exportiert.
Tags	Geben Sie ein Tag ein, um die Suche zu vereinfachen.

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 **Planen und Fehler beheben > Empfehlungen** aus.
- 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 **Planen und Fehler beheben > Port-Mirroring** aus.
- 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 **Quelle**, um eine Quelle festzulegen.

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**.

## 7 Klicken Sie auf **Festlegen** in der Spalte **Ziel**, um ein Ziel festzulegen.

## 8 Klicken Sie auf **Speichern**.

# Simple Network Management-Protokoll (SNMP)

Sie können SNMP (Simple Network Management Protocol) verwenden, um Ihre NSX-T Data Center-Komponenten zu überwachen. Der SNMP-Dienst wird nach der Installation nicht standardmäßig gestartet.

## Verfahren

### 1 Melden Sie sich bei der NSX Manager- oder NSX Edge-CLI an.

### 2 Führen Sie die folgenden Befehle aus

#### ■ Für SNMPv1/SNMPv2:

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

Die maximale Zeichenbeschränkung für **community-string** lautet 64.

#### ■ Für SNMPv3

```
set snmp v3-users <user_name> auth-password <auth_password> priv-password
<priv_password>

start service snmp
```

Die maximale Zeichenbeschränkung für **user\_name** lautet 32. Stellen Sie sicher, dass Ihre Kennwörter die PAM-Einschränkungen erfüllen. Wenn Sie die Standard-Engine-ID ändern möchten, verwenden Sie den folgenden Befehl:

```
set snmp v3-engine-id <v3-engine-id>

start service snmp
```

**v3-engine-id** ist eine hexadezimale Zeichenfolge, die 10 bis 64 Zeichen lang ist.

NSX-T Data Center unterstützt SHA1 und AES128 als Authentifizierungs- und Datenschutzprotokolle. Sie können auch API-Aufrufe zum Einrichten von SNMPv3 verwenden. Weitere Informationen finden Sie im *Handbuch zur NSX-T Data Center-API*.

## Beispiel:

## Verwenden von vRealize Log Insight für die Systemüberwachung

Sie können Ihre NSX-T Data Center-Umgebung mithilfe des Log Insight NSX-T-Inhaltspakets überwachen.

Dieses Inhaltspaket weist die folgenden Warnungen auf:

Warnungsname	Beschreibung
SysCpuUsage	Die CPU-Auslastung liegt seit mehr als 10 Minuten über 95 %.
SysMemUsage	Die Arbeitsspeichernutzung liegt seit mehr als 10 Minuten über 95 %.
SysDiskUsage	Die Festplattennutzung für mindestens eine Partition liegt seit mehr als 10 Minuten über 89 %.
PasswordExpiry	Das Kennwort für das Benutzerkonto der Appliance läuft demnächst ab oder ist abgelaufen.
CertificateExpiry	Mindestens ein von der Zertifizierungsstelle signiertes Zertifikat ist abgelaufen.
ClusterNodeStatus	Der lokale Edge-Clusterknoten ist ausgefallen.
BackupFailure	Fehler beim geplanten NSX-Sicherungsvorgang.
VipLeadership	Die VIP des NSX Management-Clusters ist nicht verfügbar.
ApiRateLimit	Für die Client-API wurde der konfigurierte Schwellenwert erreicht.
CorfuQuorumLost	Zwei Knoten sind im Cluster ausgefallen und das Quorum für Corfu ging verloren.
DfwHeapMem	Der für den DFW-Heap-Speicher konfigurierte Schwellenwert wurde überschritten.
ProcessStatus	Der Status des wichtigen Prozesses wurde geändert.
ClusterFailoverStatus	Der Status der SR-Hochverfügbarkeit wurde geändert oder es gab ein Failover bei aktiven Diensten/Standby-Diensten.
DhcpPoolUsageOverloadedEvent	Der DHCP-Pool hat den konfigurierten Nutzungsschwellenwert erreicht.

Warnungsname	Beschreibung
FabricCryptoStatus	Der Edge Crypto MUX-Treiber ist aufgrund eines Fehlers bei Known_Answer_Tests (KAT) ausgefallen.
VpnTunnelState	Der VPN-Tunnel ist ausgefallen.
BfdTunnelStatus	Der Status des BFD-Tunnels wurde geändert.
RoutingBgpNeighborStatus	Der BGP-Nachbarstatus ist nicht verfügbar.
VpnL2SessionStatus	Die L2 VPN-Sitzung ist inaktiv.
VpnIkeSessionStatus	Die IKE-Sitzung ist inaktiv.
RoutingStatus	Das Routing (BGP/BFD) ist nicht verfügbar.
DnsForwarderStatus	Der Ausführungsstatus der DNS-Weiterleitung ist nicht verfügbar.
TnConnDown_15min	Die Verbindung des Transportknotens mit einem Controller/Manager ist mindestens 15 Minuten lang inaktiv.
TnConnDown_5min	Die Verbindung des Transportknotens mit einem Controller/Manager ist mindestens 5 Minuten lang inaktiv.
ServiceDown	Mindestens ein Service ist nicht verfügbar.
IpNotAvailableInPool	Im Pool ist keine IP verfügbar oder der konfigurierte Schwellenwert wurde erreicht.
LoadBalancerError	Der NSX Load Balancer-Servicestatus lautet „FEHLER“.
LoadBalancerDown	Der NSX Load Balancer-Servicestatus lautet „INAKTIV“.
LoadBalancerVsDown	VS-Status: Alle Poolmitglieder sind ausgefallen.
LoadBalancerPoolDown	Poolstatus: Alle Poolmitglieder sind ausgefallen.
ProcessCrash	Prozess oder Daemon stürzt im Datenpfad oder in einem anderen LB-Prozess wie Disponenten usw. ab.

## Verwenden von vRealize Operations Manager für die Systemüberwachung

Sie können Ihre NSX-T Data Center-Umgebung mithilfe von vRealize Operations Manager überwachen.

**Tabelle 12-1. Warnungen im Management Pack für NSX-T**

Warnung	Beschreibung	Empfehlung
NSX-T-Managementdienst ist fehlgeschlagen	Wird ausgelöst, wenn der Managementdienst auf dem NSX-T Data Center-Host nicht ausgeführt wird.	Melden Sie sich bei NSX-T Manager an und starten Sie den fehlgeschlagenen Managementdienst neu.
Administrativer Zustand des logischen Switches ist nicht „AKTIV“	Wird ausgelöst, wenn der administrative Zustand auf dem logischen Switch deaktiviert ist.	Melden Sie sich bei NSX-T an und aktivieren Sie den administrativen Zustand, sofern dies so vorgesehen ist.

Tabelle 12-1. Warnungen im Management Pack für NSX-T (Fortsetzung)

Warnung	Beschreibung	Empfehlung
Konnektivität des Edge-Knoten-Controllers/Managers ist nicht „AKTIV“	Wird ausgelöst, wenn der Konnektivitätsstatus des Edge-Knotens in NSX-T Data Center nicht verfügbar ist.	Überprüfen Sie den Konnektivitätsstatus des Edge-Knotens mit dem Controller-Cluster und dem Manager-Cluster und beheben Sie die unterbrochene Verbindung.
Zustand des Edge-Hostknotens ist „Fehlgeschlagen“/„Fehler“	Wird ausgelöst, wenn der Hostknoten in NSX-T Data Center aus einem der folgenden Gründe den Status „Fehler“ oder „Fehlgeschlagen“ hat: <ul style="list-style-type: none"> <li>■ Fehler in der Edge-Konfiguration</li> <li>■ Fehler bei Installation</li> <li>■ Fehler bei Deinstallation</li> <li>■ Fehler beim Upgrade</li> <li>■ Fehler bei der Bereitstellen der virtuellen Maschine</li> <li>■ Fehler beim Ausschalten der virtuellen Maschine</li> <li>■ Fehler beim Einschalten der virtuellen Maschine</li> <li>■ Fehler beim Aufheben der Bereitstellung der virtuellen Maschine</li> </ul>	Der Edge-Hostknoten befindet sich im Zustand „Fehlgeschlagen“/„Fehler“. Überprüfen Sie den Status des Hostknotens und beheben Sie das Problem.
BFD-Dienst ist deaktiviert	Wird ausgelöst, wenn der BFD-Dienst auf dem logischen Router nicht aktiviert ist.	Der BFD-Dienst für einen TIER0-Router ist nicht aktiviert, obwohl die Nachbarn konfiguriert sind. Aktivieren Sie den BFD-Dienst bei Bedarf.
NAT-Regel nicht konfiguriert	Wird ausgelöst, wenn die NAT-Regel auf dem logischen Router nicht konfiguriert ist.	Melden Sie sich bei NSX-T Manager an und fügen Sie die NAT-Regeln für den logischen Router hinzu.
Statische Route nicht konfiguriert	Wird ausgelöst, wenn die statische Route auf dem logischen Router nicht konfiguriert ist.	Melden Sie sich bei NSX-T Manager an und fügen Sie die statische Route für den logischen Router bei Bedarf hinzu.
Routenankündigungs-Dienst deaktiviert	Wird ausgelöst, wenn der Routenankündigungs-Dienst auf dem logischen Router nicht aktiviert ist.	Der Routenankündigungs-Dienst für einen TIER1-Router ist nicht aktiviert, obwohl Routenankündigungen konfiguriert sind. Melden Sie sich bei NSX-T Manager an und aktivieren Sie den Dienst.



Tabelle 12-1. Warnungen im Management Pack für NSX-T (Fortsetzung)

Warnung	Beschreibung	Empfehlung
Route Redistribution-Dienst deaktiviert	Wird ausgelöst, wenn der Route Redistribution-Dienst auf dem logischen Router nicht aktiviert ist.	Der Route Redistribution-Dienst für einen TIER0-Router ist nicht aktiviert, obwohl Route Redistributions konfiguriert sind. Melden Sie sich bei NSX-T Manager an und aktivieren Sie den Dienst.
ECMP-Dienst für den logischen Router deaktiviert	Wird ausgelöst, wenn der ECMP-Dienst auf dem logischen Router nicht aktiviert ist.	Der BGP-ECMP-Dienst für einen TIER0-Router ist nicht aktiviert, obwohl die Nachbarn konfiguriert sind. Melden Sie sich bei NSX-T Manager an und aktivieren Sie den Dienst.
Konnektivität des Controller-Knotens unterbrochen	Wird ausgelöst, wenn der Konnektivitätsstatus des Controller-Knotens in NSX-T Data Center nicht verfügbar ist	Melden Sie sich bei NSX-T Manager an und überprüfen Sie die Konnektivität des Controller-Knotens mit dem Verwaltungsknoten und dem Controller-Cluster.
Weniger als 3 Controller-Knoten bereitgestellt	Wird ausgelöst, wenn der NSX-T Data Center-Server über weniger als drei Controller-Knoten verfügt.	Stellen Sie mindestens 3 Controller-Knoten im Cluster bereit.
Status des Controller-Clusters nicht stabil	Wird ausgelöst, wenn alle Controller-Knoten in NSX-T Data Center ausgefallen sind.	Überprüfen Sie den Status des Controller-Clusters.
Managementzustand nicht stabil	Wird ausgelöst, wenn der Status eines beliebigen Knotens im Verwaltungsknoten ausgefallen ist.	Überprüfen Sie den Status des Verwaltungsknotens.
Dateisystemnutzung beträgt mehr als 85 Prozent	Wird ausgelöst, wenn die Nutzung des Gastdateisystems der virtuellen Maschine des Controllers mehr als 85 Prozent beträgt.	Die Dateisystemnutzung beträgt mehr als 85 Prozent. Prüfen und bereinigen Sie das Dateisystem, um mehr Speicherplatz freizugeben.
Dateisystemnutzung beträgt mehr als 75 Prozent	Wird ausgelöst, wenn die Nutzung des Gastdateisystems der virtuellen Maschine des Controllers mehr als 75 Prozent beträgt.	Die Dateisystemnutzung beträgt mehr als 75 Prozent. Prüfen und bereinigen Sie das Dateisystem, um mehr Speicherplatz freizugeben.
Dateisystemnutzung über 70 Prozent	Wird ausgelöst, wenn die Nutzung des Gastdateisystems der virtuellen Maschine des Controllers mehr als 70 Prozent beträgt.	Die Dateisystemnutzung beträgt mehr als 70 Prozent. Prüfen und bereinigen Sie das Dateisystem, um mehr Speicherplatz freizugeben.

Tabelle 12-1. Warnungen im Management Pack für NSX-T (Fortsetzung)

Warnung	Beschreibung	Empfehlung
Edge-Cluster-Status ist „Inaktiv“	Wird ausgelöst, wenn der Status des Edge-Clusters „Inaktiv“ ist.	Überprüfen Sie den Status des Edge Clusters und befolgen Sie bei Bedarf die in der NSX-T-Dokumentation und der VMware-Dokumentation empfohlenen Standardschritte zur Fehlerbehebung.
Zustand des logischen Switches ist „Fehlgeschlagen“	Wird ausgelöst, wenn der Zustand des logischen Switches „Fehlgeschlagen“ ist.	Überprüfen Sie den Status des logischen Switches und befolgen Sie bei Bedarf die in der NSX-T-Dokumentation und der VMware-Dokumentation empfohlenen Standardschritte zur Fehlerbehebung.
Betriebszustand des Load-Balancer-Dienst ist „Inaktiv“	Wird ausgelöst, wenn der Betriebsstatus des Load-Balancer-Diensts „Inaktiv“ ist.	Überprüfen Sie den Betriebsstatus des Load-Balancer-Diensts und befolgen Sie bei Bedarf die in der NSX-T-Dokumentation und der VMware-Dokumentation empfohlenen Standardschritte zur Fehlerbehebung.
Betriebszustand des Load-Balancer-Dienst ist „Fehler“	Wird ausgelöst, wenn der Betriebsstatus des Load-Balancer-Diensts „Fehler“ enthält.	Überprüfen Sie den Betriebsstatus des Load-Balancer-Diensts und befolgen Sie bei Bedarf die in der NSX-T-Dokumentation und der VMware-Dokumentation empfohlenen Standardschritte zur Fehlerbehebung.
Betriebszustand des virtuellen Load-Balancer-Servers ist „Inaktiv“	Wird ausgelöst, wenn der Betriebszustand des virtuellen Load-Balancer-Servers „Inaktiv“ ist.	Überprüfen Sie den Betriebszustand des virtuellen Load-Balancer-Servers und befolgen Sie bei Bedarf die in der NSX-T-Dokumentation und der VMware-Dokumentation empfohlenen Standardschritte zur Fehlerbehebung.

Tabelle 12-1. Warnungen im Management Pack für NSX-T (Fortsetzung)

Warnung	Beschreibung	Empfehlung
Betriebszustand des virtuellen Load-Balancer-Servers ist „Getrennt“	Wird ausgelöst, wenn der Betriebsstatus des virtuellen Load-Balancer-Servers „Getrennt“ ist.	Überprüfen Sie den Betriebszustand des virtuellen Load-Balancer-Servers und befolgen Sie bei Bedarf die in der NSX-T-Dokumentation und der VMware-Dokumentation empfohlenen Standardschritte zur Fehlerbehebung.
Konfigurationsstatus des Edge-Knotens ist „Fehlgeschlagen“	Wird ausgelöst, wenn der Konfigurationszustand des Edge-Knotens „Fehlgeschlagen“ ist.	Überprüfen Sie den Konfigurationszustand des Edge-Knotens und befolgen Sie bei Bedarf die in der NSX-T-Dokumentation und der VMware-Dokumentation empfohlenen Standardschritte zur Fehlerbehebung.
Überwachungs-Laufzeitzustand des Managementdiensts ist „Fehlgeschlagen“	Wird ausgelöst, wenn der Überwachungs-Laufzeitzustand des Managementdiensts nicht mehr ausgeführt wird.	Melden Sie sich bei der NSX-T Manager-VA an und starten Sie den fehlgeschlagenen Managementdienst neu.
Managementzustand des Management-Clusters ist „Nicht stabil“	Wird ausgelöst, wenn der Managementzustand eines Verwaltungsclusters „Nicht stabil“ ist.	Überprüfen Sie den Status des Verwaltungsclusters.
Weniger als 3 Manager-Knoten bereitgestellt	Wird ausgelöst, wenn für den NSX-T-Server weniger als drei Manager-Knoten bereitgestellt sind.	Stellen Sie mindestens 3 Manager-Knoten im Cluster bereit.
Konnektivität des Manager-Knotens unterbrochen	Wird ausgelöst, wenn der Manager-Verbindungsstatus des Manager-Knotens nicht verfügbar ist.	Melden Sie sich bei NSX-T Manager an, überprüfen Sie die Manager-Konnektivität des Manager-Knotens und befolgen Sie die in der NSX-T-Dokumentation und der VMware-Dokumentation empfohlenen Standardschritte zur Fehlerbehebung.
Dateisystemnutzung des Manager-Knotens beträgt mehr als 85 Prozent	Wird ausgelöst, wenn die Nutzung des Gastdateisystems des Manager-Knotens mehr als 85 Prozent beträgt.	Die Dateisystemnutzung beträgt mehr als 85 Prozent. Prüfen und bereinigen Sie das Dateisystem, um mehr Speicherplatz freizugeben.

Tabelle 12-1. Warnungen im Management Pack für NSX-T (Fortsetzung)

Warnung	Beschreibung	Empfehlung
Dateisystemnutzung des Manager-Knotens beträgt mehr als 75 Prozent	Wird ausgelöst, wenn die Nutzung des Gastdateisystems des Manager-Knotens mehr als 75 Prozent beträgt.	Die Dateisystemnutzung beträgt mehr als 75 Prozent. Prüfen und bereinigen Sie das Dateisystem, um mehr Speicherplatz freizugeben.
Dateisystemnutzung des Manager-Knotens beträgt mehr als 70 Prozent	Wird ausgelöst, wenn die Nutzung des Gastdateisystems des Manager-Knotens mehr als 70 Prozent beträgt.	Die Dateisystemnutzung beträgt mehr als 70 Prozent. Prüfen und bereinigen Sie das Dateisystem, um mehr Speicherplatz freizugeben.

## Verwenden von vRealize Network Insight Cloud für die Systemüberwachung

Sie können Ihre NSX-T Data Center-Umgebung mithilfe von vRealize Network Insight Cloud überwachen.

Tabelle 12-2. Von vRealize Network Insight berechnete NSX-T Ereignisse

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80205	NSXTNoUplinkConnectivityEvent	Warnung	Logischer NSX-T-Tier-1-Router getrennt (Ereignis)	Der logische Router der NSX-T-Ebene 1 wurde vom Router der Ebene 0 getrennt. Netzwerke unter diesem Router sind von außen und umgekehrt nicht erreichbar.
1.3.6.1.4.1.6876.100.1.0.80206	NSXTRoutingAdvertisementEvent	Warnung	Routing-Ankündigung deaktiviert	Die Routing-Ankündigung wurde für den logischen Router der NSX-T-Ebene 1 deaktiviert. Netzwerke unter diesem Router sind von außerhalb nicht erreichbar.
1.3.6.1.4.1.6876.100.1.0.80207	NSXTManagerConnectivityDownEvent	Kritisch	NSX-T Edge-Knoten verfügt über keine Manager-Konnektivität	Der NSX-T Edge-Knoten hat die Konnektivität mit dem Manager verloren.

Tabelle 12-2. Von vRealize Network Insight berechnete NSX-T Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80208	NSXTControllerConnectivityDegradedEvent	Warnung	Controller-Konnektivität für NSX-T Edge-Knoten herabgestuft	Der NSX-T Edge-Knoten kann nicht mit einem oder mehreren Controllern kommunizieren.
1.3.6.1.4.1.6876.100.1.0.80209	NSXTControllerConnectivityDownEvent	Kritisch	NSX-T Edge-Knoten verfügt über keine Controller-Konnektivität	Der NSX-T-Edge Knoten kann nicht mit einem der Controller kommunizieren.
1.3.6.1.4.1.6876.100.1.0.80210	NSXTMTuMismatchEvent	Warnung	MTU-Nichtübereinstimmung zwischen NSX-T-Tier-0- und Uplink-Switch/Router	Die MTU, die in Schnittstellen des logischen Routers der Ebene 0 konfiguriert ist, stimmt nicht mit den Schnittstellen des Uplink-Switches/-Routers desselben L2-Netzwerks überein. Dies kann sich auf die Netzwerkleistung auswirken.
1.3.6.1.4.1.6876.100.1.0.80211	NSXTExcludedVmFlowEvent	Info	Eine oder mehrere VMs sind von der NSX-T DFW-Firewall ausgeschlossen.	Eine oder mehrere VMs werden nicht durch NSX-T-DFW-Firewall geschützt. vRealize Network Insight empfängt keine IPFix-Flows für diese VMs.
1.3.6.1.4.1.6876.100.1.0.80212	NSXTDoubleVlanTaggingEvent	Warnung	Fehlkonfiguration des Uplink-VLAN	Die Kommunikation wird unterbrochen, da sich das VLAN auf dem Uplink-Port des Routers der Ebene vom VLAN im externen Gateway unterscheidet.
1.3.6.1.4.1.6876.100.1.0.80213	NSXTNoTzAttachedOnTnEvent	Warnung	An den Transportknoten ist keine Transportzone angehängt	Keine Transportzone ist an den Transportknoten angehängt. Die VMs verlieren möglicherweise aus diesem Grund die Konnektivität.

Tabelle 12-2. Von vRealize Network Insight berechnete NSX-T Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80214	NSXTVtepDeleteEvent	Warnung	Kein VTEP auf dem Transportknoten verfügbar.	Alle VTEPs wurden aus dem Transportknoten gelöscht. Die VMs verlieren möglicherweise aus diesem Grund die Konnektivität.
1.3.6.1.4.1.6876.100.1.0.80225	NSXTControllerNodeToControlClusterConnectivityEvent	Kritisch	Der NSX-T-Controller-Knoten ist nicht mit dem Steuerungscluster verbunden	Der NSX-T-Controller-Knoten hat die Konnektivität mit dem Controller-Cluster verloren.
1.3.6.1.4.1.6876.100.1.0.80226	NSXTControllerNodeToMgmtPlaneConnectivityEvent	Kritisch	NSX-T-Controller-Knoten ist nicht mit der Managementebene verbunden	Der NSX-T-Controller-Knoten hat die Managementebenenkonnektivität verloren.
1.3.6.1.4.1.6876.100.1.0.80227	NSXTMPNodeToMgmtClusterConnectivityEvent	Kritisch	NSX-T-Verwaltungsknoten ist nicht mit dem Verwaltungscluster verbunden	Der NSX-T-Verwaltungsknoten hat die Verwaltungsclusterkonnektivität verloren.
1.3.6.1.4.1.6876.100.1.0.80246	NSXTHostNodeMgmtConnectivityStatusDownEvent	Warnung	NSX-T-Hostknoten verfügt über keine Manager-Konnektivität	Desynchronisierung zwischen dem Konnektivitätszustand von NSX Manager mit den Hosttransportknoten
1.3.6.1.4.1.6876.100.1.0.80247	NSXTEdgeNodeCtrlConnectivityStatusUnknownEvent	Kritisch	Controller-Konnektivität für NSX-T Edge-Knoten ist „Unbekannt“.	Die Controller-Konnektivität des NSX-T Edge-Knotens ist „Unbekannt“.
1.3.6.1.4.1.6876.100.1.0.80248	NSXTHostNodeCtrlConnectivityStatusDownEvent	Warnung	NSX-T-Hostknoten verfügt über keine Controller-Konnektivität	Der NSX-T-Hostknoten kann nicht mit einem der Controller kommunizieren.
1.3.6.1.4.1.6876.100.1.0.80249	NSXTHostNodeCtrlConnectivityStatusDegradedEvent	Warnung	Controller-Konnektivität für NSX-T-Hostknoten herabgestuft	Der NSX-T-Hostknoten kann nicht mit einem oder mehreren Controllern kommunizieren.
1.3.6.1.4.1.6876.100.1.0.80250	NSXTHostNodeCtrlConnectivityStatusUnknownEvent	Warnung	Controller-Konnektivität für NSX-T-Hostknoten ist „Unbekannt“.	Die Controller-Konnektivität des NSX-T-Hostknotens ist „Unbekannt“.

Tabelle 12-2. Von vRealize Network Insight berechnete NSX-T Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80228	NSXTHostNodePnicStatusDownEvent	Warnung	Der pNIC-Status des NSX-T-Host-Transportknotens ist „Nicht verfügbar“.	Der pNIC-Status des NSX-T-Host-Transportknotens ist „Nicht verfügbar“.
1.3.6.1.4.1.6876.100.1.0.80229	NSXTHostNodePnicStatusDegradedEvent	Warnung	Der pNIC-Status des NSX-T-Host-Transportknotens ist „Beeinträchtigt“.	Der pNIC-Status des NSX-T-Host-Transportknotens ist „Beeinträchtigt“.
1.3.6.1.4.1.6876.100.1.0.80230	NSXTHostNodePnicStatusUnknownEvent	Warnung	Der pNIC-Status des NSX-T-Host-Transportknotens ist „Unbekannt“.	Der pNIC-Status des NSX-T-Host-Transportknotens ist „Unbekannt“.
1.3.6.1.4.1.6876.100.1.0.80237	NSXTEdgeNodePnicStatusDownEvent	Kritisch	Der pNIC-Status des NSX-T Edge-Transportknotens ist „Nicht verfügbar“.	Der pNIC-Status des NSX-T Edge-Transportknotens ist „Nicht verfügbar“.
1.3.6.1.4.1.6876.100.1.0.80238	NSXTEdgeNodePnicStatusDegradedEvent	Kritisch	Der pNIC-Status des NSX-T Edge-Transportknotens ist „Beeinträchtigt“.	Der pNIC-Status des NSX-T Edge-Transportknotens ist „Beeinträchtigt“.
1.3.6.1.4.1.6876.100.1.0.80239	NSXTEdgeNodePnicStatusUnknownEvent	Kritisch	Der pNIC-Status des NSX-T Edge-Transportknotens ist „Unbekannt“.	Der pNIC-Status des NSX-T Edge-Transportknotens ist „Unbekannt“.
1.3.6.1.4.1.6876.100.1.0.80231	NSXTHostNodeTunnelStatusDownEvent	Warnung	Der Tunnelstatus des NSX-T-Host-Transportknotens ist „Nicht verfügbar“.	Der Tunnelstatus des NSX-T-Host-Transportknotens ist „Nicht verfügbar“.
1.3.6.1.4.1.6876.100.1.0.80232	NSXTHostNodeTunnelStatusDegradedEvent	Warnung	Der Tunnelstatus des NSX-T-Host-Transportknotens ist „Beeinträchtigt“.	Der Tunnelstatus des NSX-T-Host-Transportknotens ist „Beeinträchtigt“.
1.3.6.1.4.1.6876.100.1.0.80233	NSXTHostNodeTunnelStatusUnknownEvent	Warnung	Der Tunnelstatus des NSX-T-Host-Transportknotens ist „Unbekannt“.	Der Tunnelstatus des NSX-T-Host-Transportknotens ist „Unbekannt“.
1.3.6.1.4.1.6876.100.1.0.80240	NSXTEdgeNodeTunnelStatusDownEvent	Kritisch	Der Tunnelstatus des NSX-T Edge-Transportknotens ist „Nicht verfügbar“.	Der Tunnelstatus des NSX-T Edge-Transportknotens ist „Nicht verfügbar“.
1.3.6.1.4.1.6876.100.1.0.80241	NSXTEdgeNodeTunnelStatusDegradedEvent	Kritisch	Der Tunnelstatus des NSX-T Edge-Transportknotens ist „Beeinträchtigt“.	Der Tunnelstatus des NSX-T Edge-Transportknotens ist „Beeinträchtigt“.

Tabelle 12-2. Von vRealize Network Insight berechnete NSX-T Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80242	NSXTEdgeNodeTunnelStatusUnknownEvent	Kritisch	Der Tunnelstatus des NSX-T Edge-Transportknotens ist „Unbekannt“.	Der Tunnelstatus des NSX-T Edge-Transportknotens ist „Unbekannt“.
1.3.6.1.4.1.6876.100.1.0.80234	NSXTHostNodeStatusDownEvent	Warnung	Der Status des NSX-T-Host-Transportknotens ist „Nicht verfügbar“.	Der Status des NSX-T-Host-Transportknotens ist „Nicht verfügbar“.
1.3.6.1.4.1.6876.100.1.0.80235	NSXTHostNodeStatusDegradedEvent	Warnung	Der Status des NSX-T-Host-Transportknotens ist „Beeinträchtigt“.	Der Status des NSX-T-Host-Transportknotens ist „Beeinträchtigt“.
1.3.6.1.4.1.6876.100.1.0.80236	NSXTHostNodeStatusUnknownEvent	Warnung	Der Status des NSX-T-Host-Transportknotens ist „Unbekannt“.	Der Status des NSX-T-Host-Transportknotens ist „Unbekannt“.
1.3.6.1.4.1.6876.100.1.0.80243	NSXTEdgeNodeStatusDownEvent	Kritisch	Der Status des NSX-T Edge-Transportknotens ist „Nicht verfügbar“.	Der Status des NSX-T Edge-Transportknotens ist „Nicht verfügbar“.
1.3.6.1.4.1.6876.100.1.0.80244	NSXTEdgeNodeStatusDegradedEvent	Kritisch	Der Status des NSX-T Edge-Transportknotens ist „Beeinträchtigt“.	Der Status des NSX-T Edge-Transportknotens ist „Beeinträchtigt“.
1.3.6.1.4.1.6876.100.1.0.80245	NSXTEdgeNodeStatusUnknownEvent	Kritisch	Der Status des NSX-T Edge-Transportknotens ist „Unbekannt“.	Der Status des NSX-T Edge-Transportknotens ist „Unbekannt“.
1.3.6.1.4.1.6876.100.1.0.80252	NSXTLogicalSwitchAdminStatusDownEvent	Warnung	Der Administratorstatus des logischen NSX-T-Switches ist „Nicht verfügbar“.	Der Administratorstatus des logischen NSX-T-Switches ist „Nicht verfügbar“.



Tabelle 12-2. Von vRealize Network Insight berechnete NSX-T Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80253	NSXTLogicalPortOperationalStatusDownEvent	Kritisch	Der Betriebsstatus des logischen NSX-T-Ports ist „Nicht verfügbar“.	Der Betriebsstatus des logischen NSX-T-Ports ist „Nicht verfügbar“. Dies kann zu einem Kommunikationsfehler zwischen zwei virtuellen Schnittstellen (VIFs) führen, die mit demselben logischen Switch verbunden sind. Sie können beispielsweise keinen Ping von einer VM an eine andere senden.
1.3.6.1.4.1.6876.100.1.0.80254	NSXTLogicalPortOperationalStatusUnknownEvent	Warnung	Der Betriebsstatus des logischen NSX-T-Ports ist „Unbekannt“.	Der Betriebsstatus des logischen NSX-T-Ports ist „Unbekannt“. Dies kann zu einem Kommunikationsfehler zwischen zwei virtuellen Schnittstellen (VIFs) führen, die mit demselben logischen Switch verbunden sind. Sie können beispielsweise keinen Ping von einer VM an eine andere senden.
1.3.6.1.4.1.6876.100.1.0.80255	NSXTComputeManagerConnectionStatusNotUpEvent	Warnung	Verbindungsstatus von NSX-T-Berechnungsmanager ist nicht „Verfügbar“.	Verbindungsstatus von NSX-T-Berechnungsmanager ist nicht „Verfügbar“.
1.3.6.1.4.1.6876.100.1.0.80256	NSXTClusterBackupDisabledEvent	Warnung	NSX-T Manager-Sicherung ist nicht geplant.	NSX-T Manager-Sicherung ist nicht geplant.
1.3.6.1.4.1.6876.100.1.0.80257	NSXTDFWFirewallDisabledEvent	Kritisch	NSX-T DFW-Firewall ist deaktiviert.	Die verteilte Firewall ist in NSX-T Manager deaktiviert.

Tabelle 12-2. Von vRealize Network Insight berechnete NSX-T Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80258	NSXTLogicalPortReceivedPacketDropEvent	Warnung	Empfangene Pakete des logischen NSX-T-Ports werden gelöscht.	Die empfangenen Pakete werden auf dem logischen NSX-T-Port gelöscht und dies kann sich auf die zugehörigen Entitäten auswirken.
1.3.6.1.4.1.6876.100.1.0.80259	NSXTLogicalPortTransmittedPacketDropEvent	Warnung	Übertragene Pakete des logischen NSX-T-Ports werden gelöscht.	Die übertragenen Pakete werden auf dem logischen NSX-T-Port gelöscht und dies kann sich auf die zugehörigen Entitäten auswirken.
1.3.6.1.4.1.6876.100.1.0.80260	NSXTLogicalSwitchReceivedPacketDropEvent	Warnung	Empfangene Pakete des logischen NSX-T-Switches werden gelöscht.	Die empfangenen Pakete werden auf dem logischen NSX-T-Switch gelöscht und dies kann sich auf die zugehörigen Entitäten auswirken.
1.3.6.1.4.1.6876.100.1.0.80261	NSXTLogicalSwitchTransmittedPacketDropEvent	Warnung	Übertragene Pakete des logischen NSX-T-Switches werden gelöscht.	Die übertragenen Pakete werden auf dem logischen NSX-T-Switch gelöscht und dies kann sich auf die zugehörigen Entitäten auswirken.
1.3.6.1.4.1.6876.100.1.0.80262	NSXTRxPacketDropOnMPNicEvent	Warnung	Empfangene Pakete werden auf der Netzwerkschnittstelle des NSX-T-Verwaltungsknotens gelöscht.	Die empfangenen Pakete werden an der Netzwerkschnittstelle des NSX-T-Verwaltungsknotens gelöscht. Dies kann sich auf den Netzwerkdatenverkehr im Zusammenhang mit dem NSX-T Verwaltungscluster auswirken.

Tabelle 12-2. Von vRealize Network Insight berechnete NSX-T Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80263	NSXTRxPacketDropOnEdgeTnNicEvent	Kritisch	Empfangene Pakete werden auf der Netzwerkschnittstelle des NSX-T Edge-Knotens gelöscht.	Die empfangenen Pakete werden an der Netzwerkschnittstelle des NSX-T Edge-Knotens gelöscht. Dies kann sich auf den Netzwerkdatenverkehr des Edge-Clusters auswirken.
1.3.6.1.4.1.6876.100.1.0.80264	NSXTRxPacketDropOnHostTnNicEvent	Warnung	Empfangene Pakete werden auf der Netzwerkschnittstelle des NSX-T-Host-Knotens gelöscht.	Die empfangenen Pakete werden an der Netzwerkschnittstelle des NSX-T-Hostknotens gelöscht. Dies kann sich auf den Netzwerkdatenverkehr auf dem ESXi-Host auswirken.
1.3.6.1.4.1.6876.100.1.0.80265	NSXTTxPacketDropOnMPNicEvent	Warnung	Übertragene Pakete werden auf der Netzwerkschnittstelle des NSX-T-Verwaltungsknotens gelöscht.	Die übertragenen Pakete werden an der Netzwerkschnittstelle des NSX-T-Verwaltungsknotens gelöscht. Dies kann sich auf den Netzwerkdatenverkehr im Zusammenhang mit dem NSX-T Verwaltungscluster auswirken.
1.3.6.1.4.1.6876.100.1.0.80266	NSXTTxPacketDropOnEdgeTnNicEvent	Kritisch	Übertragene Pakete werden auf der Netzwerkschnittstelle des NSX-T Edge-Knotens gelöscht.	Die übertragenen Pakete werden an der Netzwerkschnittstelle des NSX-T Edge-Knotens gelöscht. Dies kann sich auf den Netzwerkdatenverkehr des Edge-Clusters auswirken.

Tabelle 12-2. Von vRealize Network Insight berechnete NSX-T Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80267	NSXTTxPacketDropOnHostTnNicEvent	Warnung	Übertragene Pakete werden auf der Netzwerkschnittstelle des NSX-T-Host-Knotens gelöscht.	Die übertragenen Pakete werden an der Netzwerkschnittstelle des NSX-T-Hostknotens gelöscht. Dies kann sich auf den Netzwerkdatenverkehr auf dem ESXi-Host auswirken.
1.3.6.1.4.1.6876.100.1.0.80402	NSXTMPNodeServiceCmInventoryStatusEvent	Warnung	Die Ausführung des CM-Bestandsdiensts wurde beendet	Der Status des CM-Bestandsdiensts wurde in „Gestoppt“ geändert.
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeServiceControllerStatusEvent	Warnung	Der Controller-Dienst wird nicht mehr ausgeführt.	Der Status des Controller-Diensts wurde in „Gestoppt“ geändert.
1.3.6.1.4.1.6876.100.1.0.80404	NSXTMPNodeServiceDataStoreStatusEvent	Warnung	Der DataStore-Dienst wird nicht mehr ausgeführt.	Der Status des DataStore-Diensts wurde in „Gestoppt“ geändert.
1.3.6.1.4.1.6876.100.1.0.80405	NSXTMPNodeServiceHttpStatusEvent	Warnung	Der HTTP-Dienst wird nicht mehr ausgeführt.	Der Status des HTTP-Diensts wurde in „Gestoppt“ geändert.
1.3.6.1.4.1.6876.100.1.0.80406	NSXTMPNodeServiceInstallUpgradeEvent	Warnung	Der Upgradedienst für die Installation wird nicht mehr ausgeführt.	Der Status des Upgradediensts für die Installation wurde in „Gestoppt“ geändert.
1.3.6.1.4.1.6876.100.1.0.80407	NSXTMPNodeServiceLiagentStatusEvent	Warnung	Die Ausführung des liagent-Diensts wurde beendet.	Der Status des liagent-Diensts wurde in „Gestoppt“ geändert.
1.3.6.1.4.1.6876.100.1.0.80408	NSXTMPNodeServiceManagerStatusEvent	Warnung	Der Managerdienst wird nicht mehr ausgeführt.	Der Status des Managerdiensts wurde in „Gestoppt“ geändert.
1.3.6.1.4.1.6876.100.1.0.80409	NSXTMPNodeServiceMgmtPlaneBusStatusEvent	Warnung	Die Ausführung des Management Plane-Diensts wurde beendet.	Der Status des Management Plane-Diensts wurde in „Gestoppt“ geändert.

Tabelle 12-2. Von vRealize Network Insight berechnete NSX-T Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80410	NSXTMPNodeServiceMigrationCoordinatorStatusEvent	Warnung	Der Migrationskoordinatordienst wird nicht mehr ausgeführt.	Der Status des Migrationskoordinatordiensts wurde in „Gestoppt“ geändert.
1.3.6.1.4.1.6876.100.1.0.80411	NSXTMPNodeServiceNodeMgmtStatusEvent	Warnung	Der Knotenmanagementdienst wird nicht mehr ausgeführt.	Der Status des Knotenmanagementdiensts wurde in „Gestoppt“ geändert.
1.3.6.1.4.1.6876.100.1.0.80412	NSXTMPNodeServiceNodeStatsStatusEvent	Warnung	Der Knotenstatistikdienst wird nicht mehr ausgeführt.	Der Status des Knotenstatistikdiensts wurde in „Gestoppt“ geändert.
1.3.6.1.4.1.6876.100.1.0.80413	NSXTMPNodeServiceNSXMessageBusStatusEvent	Warnung	Der Nachrichtenbusdienst wird nicht mehr ausgeführt.	Der Status des Nachrichtenbus-Clientdiensts wurde in „Gestoppt“ geändert.
1.3.6.1.4.1.6876.100.1.0.80414	NSXTMPNodeServiceNSXPlatformClientStatusEvent	Warnung	Der Plattform-Client-Dienst wird nicht mehr ausgeführt.	Der Status des Plattform-Client-Diensts wurde in „Gestoppt“ geändert.
1.3.6.1.4.1.6876.100.1.0.80415	NSXTMPNodeServiceNSXUpgradeAgentStatusEvent	Warnung	Der Upgrade-Agent-Dienst wird nicht mehr ausgeführt.	Der Status des Upgrade-Agent-Diensts wurde in „Gestoppt“ geändert.
1.3.6.1.4.1.6876.100.1.0.80416	NSXTMPNodeServiceNTPStatusEvent	Warnung	Der NTP-Dienst wird nicht mehr ausgeführt.	Der Status des NTP-Diensts wurde in „Gestoppt“ geändert.
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeServicePolicyStatusEvent	Warnung	Der Richtliniendienst wird nicht mehr ausgeführt.	Der Status des Richtliniendiensts wurde in „Gestoppt“ geändert.
1.3.6.1.4.1.6876.100.1.0.80418	NSXTMPNodeServiceSearchStatusEvent	Warnung	Der Suchdienst wird nicht mehr ausgeführt.	Der Status des Suchdiensts wurde in „Gestoppt“ geändert.
1.3.6.1.4.1.6876.100.1.0.80419	NSXTMPNodeServiceSNMPStatusEvent	Warnung	Der SNMP-Dienst wird nicht mehr ausgeführt.	Der Status des SNMP-Diensts wurde in „Gestoppt“ geändert.
1.3.6.1.4.1.6876.100.1.0.80420	NSXTMPNodeServiceSSHStatusEvent	Warnung	Der SSH-Dienst wird nicht mehr ausgeführt.	Der Status des SSH-Diensts wurde in „Gestoppt“ geändert.

Tabelle 12-2. Von vRealize Network Insight berechnete NSX-T Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80421	NSXTMPNodeService SyslogStatusEvent	Warnung	Der Syslog-Dienst wird nicht mehr ausgeführt.	Der Status des Syslog-Diensts wurde in „Gestoppt“ geändert.
1.3.6.1.4.1.6876.100.1.0.80422	NSXTMPNodeService TelemetryStatusEvent	Warnung	Der Telemetrie-Dienst wird nicht mehr ausgeführt.	Der Status des Telemetrie-Diensts wurde in „Gestoppt“ geändert.
1.3.6.1.4.1.6876.100.1.0.80423	NSXTMPNodeService UIServiceStatusEvent	Warnung	Der UI-Dienst wird nicht mehr ausgeführt.	Der Status des UI-Diensts wurde in „Gestoppt“ geändert.
1.3.6.1.4.1.6876.100.1.0.80402	NSXTMPNodeService CmlInventoryStatusEvent	Kritisch	CM-Bestandsdienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens – der CM-Bestandsdienst – wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeService ControllerStatusEvent	Kritisch	Controller-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens – der Controller-Dienst – wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80404	NSXTMPNodeService DataStoreStatusEvent	Kritisch	DataStore-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens – der DataStore-Dienst – wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80405	NSXTMPNodeService HttpStatusEvent	Kritisch	HTTP-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens – der HTTP-Dienst – wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80406	NSXTMPNodeService InstallUpgradeEvent	Warnung	Dienst für die Installation von Upgrades wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens – der Dienst für die Installation von Upgrades – wird nicht mehr ausgeführt.

Tabelle 12-2. Von vRealize Network Insight berechnete NSX-T Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80407	NSXTMPNodeServiceLiagentStatusEvent	Warnung	liagent-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens – der liagent-Dienst – wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80408	NSXTMPNodeServiceManagerStatusEvent	Kritisch	Manager-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens – der Manager-Dienst – wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80409	NSXTMPNodeServiceMgmtPlaneBusStatusEvent	Warnung	Management Plane-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens – der Management Plane-Dienst – wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80410	NSXTMPNodeServiceMigrationCoordinatorStatusEvent	Warnung	Migrationskoordinator-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens – der Migrationskoordinator-Dienst – wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80411	NSXTMPNodeServiceNodeMgmtStatusEvent	Kritisch	Knotenmanagementdienst wurde beendet	Einer der Dienste des NSX-T-Managementknotens – der Knotenmanagementdienst – wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80412	NSXTMPNodeServiceNodeStatsStatusEvent	Kritisch	Knotenstatistikdienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens – der Knotenstatistikdienst – wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80413	NSXTMPNodeServiceNSXMessageBusStatusEvent	Warnung	Nachrichtenbusdienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens – der Nachrichtenbusdienst – wird nicht mehr ausgeführt.

Tabelle 12-2. Von vRealize Network Insight berechnete NSX-T Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80414	NSXTMPNodeService NSXPlatformClientStatusEvent	Kritisch	Plattform-Client-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens – der Plattform-Client-Dienst – wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80415	NSXTMPNodeService NSXUpgradeAgentStatusEvent	Warnung	Upgrade-Agent-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens – der Upgrade-Agent-Dienst – wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80416	NSXTMPNodeService NTPStatusEvent	Kritisch	NTP-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens – der NTP-Dienst – wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeService PolicyStatusEvent	Kritisch	Richtliniendienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens – der Richtliniendienst – wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80418	NSXTMPNodeService SearchStatusEvent	Kritisch	Suchdienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens – der Suchdienst – wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80419	NSXTMPNodeService SNMPStatusEvent	Warnung	SNMP-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens – der SNMP-Dienst – wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80420	NSXTMPNodeService SSHStatusEvent	Kritisch	SSH-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens – der SSH-Dienst – wird nicht mehr ausgeführt.



Tabelle 12-2. Von vRealize Network Insight berechnete NSX-T Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80421	NSXTMPNodeServiceSyslogStatusEvent	Kritisch	Syslog-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens – der Syslog-Dienst – wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80422	NSXTMPNodeServiceTelemetryStatusEvent	Warnung	Telemetriedienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens – der Telemetriedienst – wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80423	NSXTMPNodeServiceUIServiceStatusEvent	Kritisch	UI-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens – der UI-Dienst – wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80424	NSXTMPNodeServiceClusterManagerStatusEvent	Kritisch	Cluster Manager-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens – der Cluster Manager-Dienst – wird nicht mehr ausgeführt.

## NSX-T-Systemereignisse

Nachfolgend finden Sie eine Liste der in vRealize Network Insight unterstützten Ereignisse von NSX-T 2.2 bis 2.5. Die Objekt-ID (OID) für alle diese NSX-T-Systemereignisse ist

1.3.6.1.4.1.6876.100.1.0.80203.

Tabelle 12-3. NSX-T-Systemereignisse

Ereignisname	Beschreibung
vmwNSXPlatformSysCpuUsage	CPU-Auslastung auf Manager- und Edge-Appliances (NSX-T 2.2).
vmwNSXPlatformSysDiskUsage	Festplattenspeichernutzung auf der Manager- Edge-Appliance für die Partition „/var/log“ (NSX-T 2.2).
vmwNSXPlatformSysMemUsage	Arbeitsspeichernutzung auf der Manager- Edge-Appliance (NSX-T 2.2).
vmwNSXPlatformSysConfigDiskUsage	Festplattennutzung auf Manager- und Edge-Appliances für die Partition „/config“ (NSX-T 2.4).
vmwNSXPlatformSysVarDumpDiskUsage	Festplattennutzung auf Manager- und Edge-Appliances für die Partition „/var/dump“ (NSX-T 2.5).

Tabelle 12-3. NSX-T-Systemereignisse (Fortsetzung)

Ereignisname	Beschreibung
vmwNSXPlatformSysRepositoryDiskUsage	Festplattennutzung auf Manager- und Edge-Appliances für die Partition „/repository“ (NSX-T 2.5).
vmwNSXPlatformSysRootDiskUsage	Festplattennutzung auf Manager- und Edge-Appliances für die Partition „root“ (NSX-T 2.5).
vmwNSXPlatformSysTmpDiskUsage	Festplattennutzung auf Manager- und Edge-Appliances für die Partition „tmp“ (NSX-T 2.5).
vmwNSXPlatformSysImageDiskUsage	Festplattennutzung auf Manager- und Edge-Appliances für die Partition „/image“ (NSX-T 2.5).
vmwNSXDhcpPoolUsageOverloadedEvent	DHCP-Pool überlastet/normal (NSX-T 2.5).
vmwNSXDhcpPoolLeaseAllocationFailedEvent	Fehler/Erfolg bei der Lease-Zuteilung des DHCP-Pools (NSX-T 2.5).
vmwNSXPlatformPasswordExpiryStatus	Kennwortablauf für Manager (NSX-T 2.4).
vmwNSXPlatformCertificateExpiryStatus	Zertifikatsablauf für Manager (NSX-T 2.4).
vmwNSXRoutingBgpNeighborStatus	BGP-Nachbarstatus (NSX-T 2.2)
vmwNSXVpnTunnelState	VPN-Tunnel aktiv/inaktiv (NSX-T 2.2)
vmwNSXVpnL2TunnelStatus	L2 VPN-Sitzung aktiv/inaktiv (NSX-T 2.2)
vmwNSXVpnIkeSessionStatus	IKE-Sitzung aktiv/inaktiv (NSX-T 2.2)
vmwNSXDnsForwarderStatus	DNS-Weiterleitungsstatus (NSX-T 2.4)
vmwNSXClusterNodeStatus	Cluster-Knotenstatus (NSX-T 2.4)
vmwNSXFabricCryptoStatus	Edge Crypto MUX-Treiber hat Known_Answer_Tests(KAT) bestanden/nicht bestanden (NSX-T 2.4).
Manager-Festplattennutzung ist nicht OK	
Der BGP-Nachbar ist inaktiv.	Eine Warnung ist erforderlich, wenn der BGP-Nachbar nicht verfügbar ist.
BGP-Nachbar verfügbar	Alarm löschen, wenn ein Nachbar zur Verfügung steht.
Speichernutzung über X	Alarm für Speicher über X – Ereignis wird für alle Appliance-VMs (MP, CCP) oder Transportknoten (Edge, Host) ausgelöst.
Arbeitsspeichernutzung über X	Alarm für Arbeitsspeicher über X – Ereignis wird für alle Appliance-VMs (MP, CCP) oder Transportknoten (Edge, Host) ausgelöst.
CPU-Auslastung über X	Alarm für CPU über X – Ereignis wird für alle Appliance-VMs (MP, CCP) oder Transportknoten (Edge, Host) ausgelöst.

## 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 ein markiertes Paket, während es das Overlay-Netzwerk durchläuft. Jedes Paket wird überwacht, während es das Overlay-Netzwerk durchläuft, bis es eine Ziel-Gast-VM oder einen Edge-Uplink erreicht. Beachten Sie, dass das injizierte Traceflow-Paket selbst nie an die Ziel-Gast-VM übermittelt wird.

Traceflow kann auf Transportknoten verwendet werden und unterstützt sowohl IPv4- als auch IPv6-Protokolle, einschließlich: ICMP, TCP, UDP, DHCP, DNS und ARP/NDP.

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 Zielpunkt 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.

Wenn das NSX-Bridging konfiguriert ist, werden Pakete mit unbekannten MAC-Zieladressen 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.

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.

Hinweis: Multi- und Broadcast werden in einer VMware Cloud(VMC)-Umgebung nicht unterstützt.

## 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 oben.	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
Frame-Größe	Die Standardeinstellung ist 128.
TTL	Die Standardeinstellung ist 64.
Zeitüberschreitung (ms)	Die Standardeinstellung ist 10000.
Ethernet-Typ	Die Standardeinstellung ist 2048.

Option	Beschreibung
Nutzlasttyp	Wählen Sie <b>Base64</b> , <b>Hex</b> , <b>Klartext</b> , <b>Binär</b> oder <b>Dezimal</b> aus.
Nutzlastdaten	Formatierte Nutzlast auf Basis des ausgewählten Typs.

- 8 (Optional) Wählen Sie ein Protokoll aus und stellen Sie verwandte Informationen bereit.

Protokoll	Parameter
TCP	Geben Sie einen Quellport, Zielport und TCP-Flags an.
UDP	Geben Sie einen Quellport und einen Zielport an.
ICMPv6	Geben Sie eine ICMP-ID und eine Sequenz 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 [NSX-T Data Center-Funktionen mit Support in NSX 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</b> <b>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 [NSX-T Data Center-Funktionen mit Support in NSX 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-Profil**.
- 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.
Overlay-Flow exportieren	Einstellung zur Festlegung, ob das Beispielergebnis Overlay-Flow-Informationen enthält.
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 **Hinzufügen**.

## 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
888	egressInterfaceAttr	unsigned16	2 Byte
889	vxlانExportRole	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.

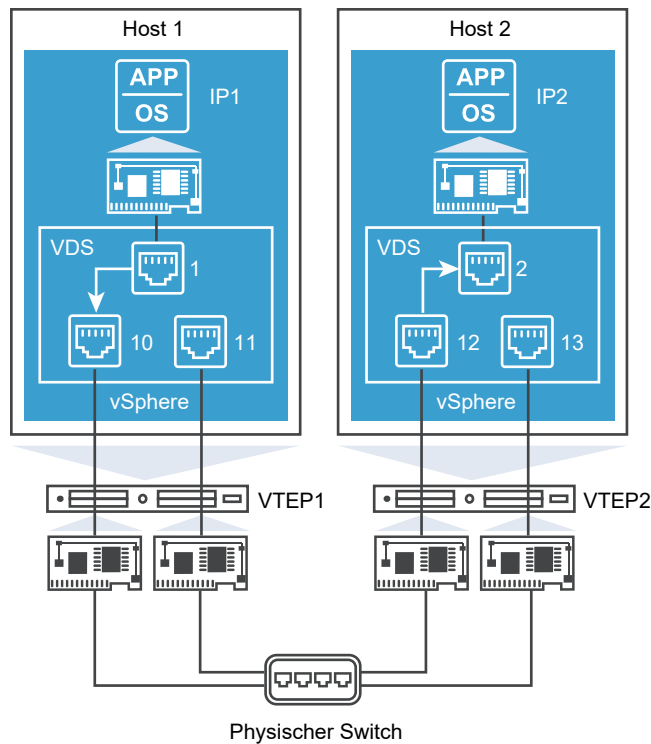
Element-ID	Parametername	Datentyp	Einheit
950	ruleId	unsigned32	4 Byte
951	vmUuid	string	16 Byte
952	vnidIndex	unsigned32	4 Byte
953	sessionFlags	unsigned8	1 Byte
954	flowDirection	unsigned8	1 Byte
955	algControlFlowId	unsigned64	8 Byte
956	algType	unsigned8	1 Byte
957	algFlowType	unsigned8	1 Byte
958	averageLatency	unsigned32	4 Byte
959	retransmissionCount	unsigned32	4 Byte

Element-ID	Parametername	Datentyp	Einheit
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)

```

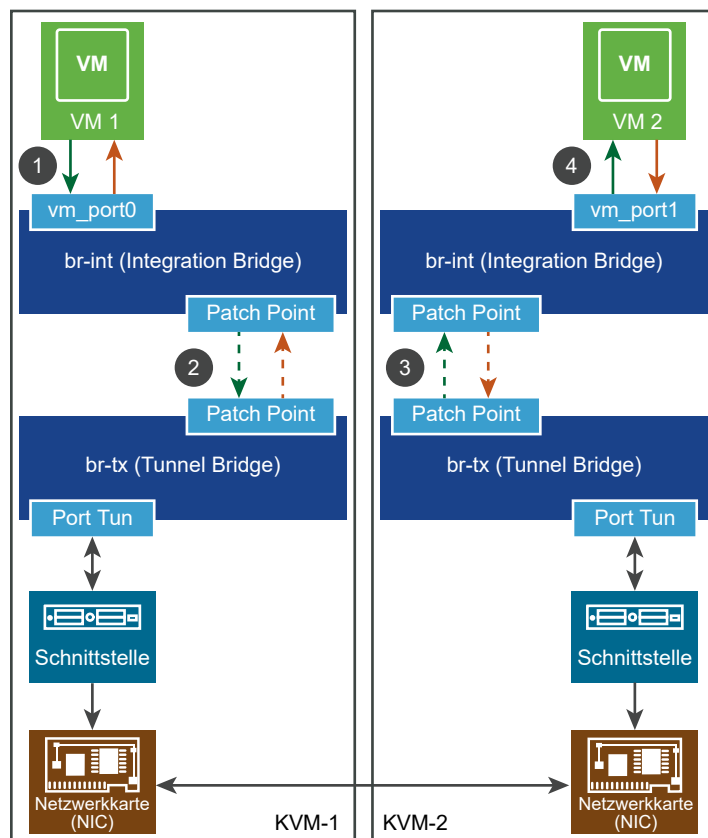
## IPFIX-Vorlagen für KVM

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](#).

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](#).

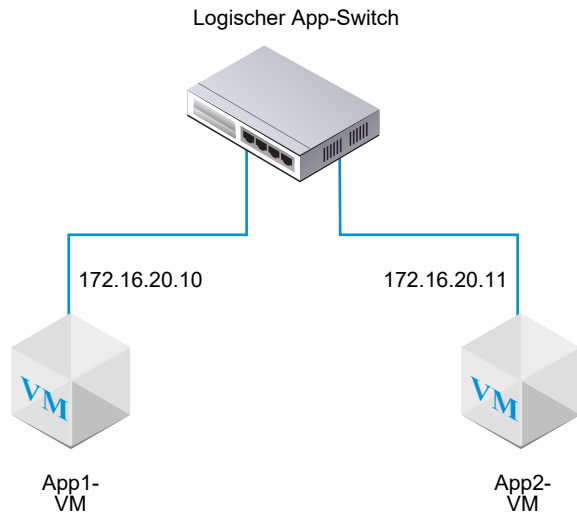
---

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 [NSX-T Data Center-Funktionen mit Support in NSX 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](#)
- [Erweiterter Netzwerkstapel](#)
- [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

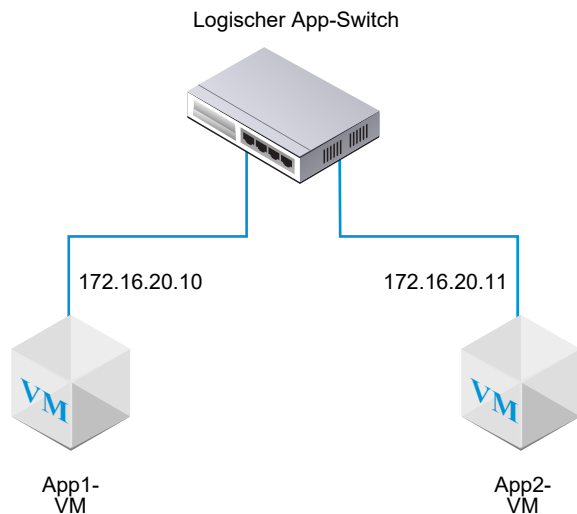
Die Konfiguration zum Verbinden einer VM mit einem logischen Switch ist vom jeweiligen Host abhängig.

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. Sie können Ports für logische Switches und die VIF-Anhangs-ID auf dem NSX Manager in **Netzwerk und Sicherheit – Erweitert > Netzwerk > Switching > Ports** anzeigen.

Verwenden Sie den GET <https://<mgr-ip>/api/v1/logical-ports/-API-Aufruf>, um die Port-Details und den Adminstatus für die entsprechende VIF-Anhangs-ID anzuzeigen. Verwenden Sie zum Anzeigen des Betriebsstatus den <https://<mgr-ip>/api/v1/logical-ports/<logical-port-id>/status-API-Aufruf> mit der entsprechenden logischen Port-ID.

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*.

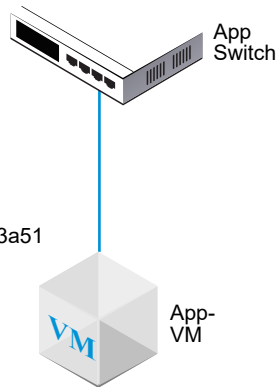
## Verknüpfen einer auf eigenständigem ESXi gehosteten VM mit einem logischen NSX-T Data Center-Switch

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' section is expanded, showing the following configuration:

- Neues Netzwerk:** VM Network
- Status:** ☒ Beim Einschalten verbinden
- Adapertyp:** VMXNET 3
- DirectPath I/O:** ☐ Aktivieren
- MAC-Adresse:** Automatisch
- Neues CD-/DVD-Laufwerk:** Clientgerät ☐ Verbinden...
- Neues Diskettenlaufwerk:** Clientgerät ☐ Verbinden...

At the bottom, the 'Neues Gerät' button is active, with 'Netzwerk' selected in the dropdown menu.

- 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-fe77-08c5-5bf7-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**

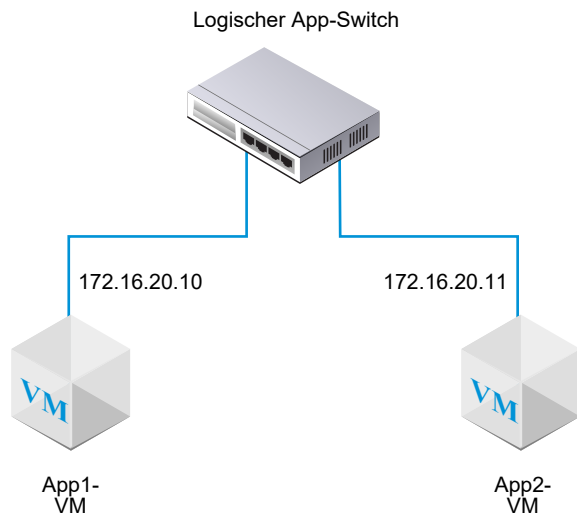
Fügen Sie einen logischen Router hinzu.

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
Name und Beschreibung	Geben Sie einen Namen und optional eine Beschreibung ein.
Logischer Switch	Wählen Sie im Dropdown-Menü einen logischen Switch aus.
Administrativer Status	Wählen Sie <b>Aktiv</b> oder <b>Inaktiv</b> aus.
Anhangstyp	Wählen Sie <b>Keine</b> oder <b>VIF</b> aus.
Anhangs-ID	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.

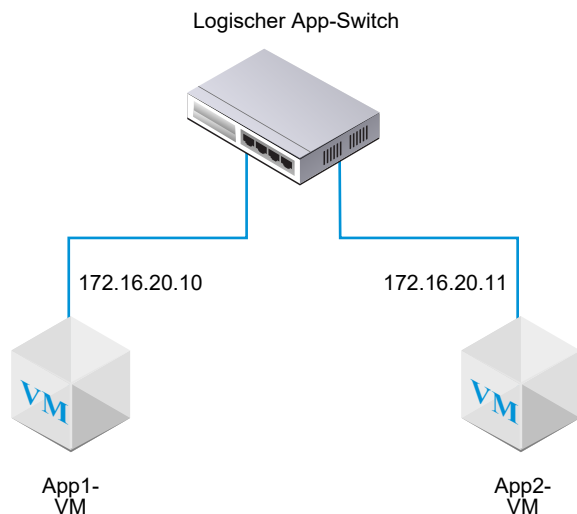
- 4 (Optional) Wählen Sie auf der Registerkarte **Switching-Profile** Switching-Profile aus.
- 5 Klicken Sie auf **Speichern**.

## 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
<code>get logical-switch &lt;vni-oder-uuid&gt; arp-table</code>	<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>
<code>get logical-switch &lt;vni-oder-uuid&gt; connection-table</code>	<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>
<code>get logical-switch &lt;vni-oder-uuid&gt; mac-table</code>	<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>
<code>get logical-switch &lt;vni-oder-uuid&gt; stats</code>	<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>
<code>get logical-switch &lt;vni-oder-uuid&gt; stats-sample</code>	<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>

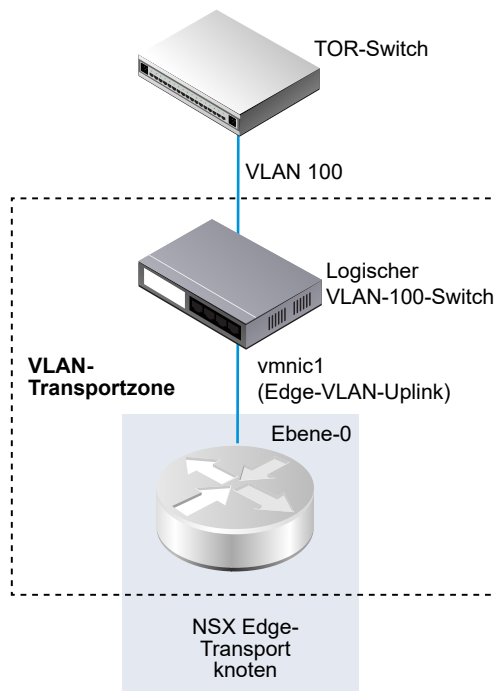
## Ergebnisse

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-Profiles

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 **Netzwerk und Sicherheit – Erweitert > Netzwerk > Switching > Switching-Profile > Hinzufügen** auswählen
- 3 Wählen Sie **QoS** aus und ergänzen Sie die Details des QoS-Switching-Profiles.

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
Dienstklasse	<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>
Ingress	<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>
Ingress Broadcast	<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>
Egress	<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.

Es wird empfohlen, das Port-Mirroring nur zur Fehlerbehebung zu verwenden.

---

**Hinweis** Das Port-Mirroring wird für die Überwachung nicht empfohlen, da die Leistung bei längerer Verwendung beeinflusst wird.

---

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-Profils für die Portspiegelung](#).

## Überprüfen eines benutzerdefinierten Switching-Profils 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-Profils 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 und 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 Prüfung wird für Ports durchgeführt, die sich im selben Segment befinden. Wenn eine doppelte Adresse erkannt wird, wird die neu ermittelte Adresse der erkannten Liste, aber nicht der realisierten Bindungsliste hinzugefügt. Allen doppelten IPs ist ein Ermittlungszeitstempel zugeordnet. Wenn die IP, die sich in der realisierten Bindungsliste befindet, entweder durch Hinzufügen zur Ignorieren-Bindungsliste 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 erkannt und der Liste der realisierten Bindungen hinzugefügt wird, bleibt diese Bindung für immer in der realisierten Liste. TOFU wird auf die ersten 'n' eindeutigen <IP-, MAC-, VLAN >-Bindungen angewendet, 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 erkannt wird, wird sie der Liste der realisierten Bindungen hinzugefügt und wenn sie gelöscht oder abgelaufen ist, wird sie aus der Liste der realisierten Bindungen entfernt. DHCP-Snooping und VM-Tools werden immer im TOEU-Modus betrieben.

NSX Manager verwaltet für jeden Port eine Ignorieren-Bindungsliste, die IP-Adressen enthält, die nicht an den Port gebunden werden können. Durch Navigieren zu **Netzwerk und Sicherheit – Erweitert > Switching > Ports** und Auswählen eines Ports können Sie erkannte Bindungen der Liste der ignorierten Bindungen hinzufügen. Sie können auch eine vorhandene erkannte oder realisierte Bindung löschen, indem Sie sie nach **Ignorierte Bindungen** kopieren.

**Hinweis** TOFU ist nicht identisch mit SpoofGuard und blockiert den Datenverkehr nicht auf dieselbe Weise wie SpoofGuard. Weitere Informationen finden Sie unter [Grundlegendes zum Spoofguard-Segmentprofil](#).

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 IP Discovery

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

### Voraussetzungen

Machen Sie sich mit dem Konzept des Switching-Profiles für die IP Discovery 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-Profile > Hinzufügen** aus.
- 3 Wählen Sie **IP-Ermittlung** aus und geben Sie die Details der Switching-Profile für die IP Discovery 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. Der zulässige Mindestwert ist 1 (Standard), der maximale Wert 256.
<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.

Option	Beschreibung
<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 IP Discovery 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, ihre vorhandene IP-Adresse zu verändern. 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 auf der Registerkarte **Übersicht** die Einträge **Adressbindungen > Manuelle Bindungen**.
- 4 Klicken Sie auf **Hinzufügen**.

Das Dialogfeld „Adressbindungen hinzufügen“ wird angezeigt.

- 5 Geben Sie IP-Adresse (IPv4-Adresse, IPv6-Adresse oder IPv6-Subnetz) und die MAC-Adresse des logischen Ports an, auf den Sie die Adressbindung anwenden möchten. Für IPv6 ist z. B. 2001::/64 ein IPv6-Subnetz, 2001::1 eine Host-IP-Adresse, wohingegen 2001::1/64 eine ungültige Eingabe ist. 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 eine 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 BPDU (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 BPDU-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** aus.
- 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.

Option	Beschreibung
DHCP-Filter	<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>
DHCPv6-Filter	<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>
Nicht-IP-Datenverkehr blockieren	<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>
RA-Guard	<p>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.</p>
Ratenbegrenzungen	<p>Legen Sie eine Ratenbegrenzung für Broadcast- und Multicast-Datenverkehr fest. Diese Option ist standardmäßig aktiviert.</p> <p>Ratenbegrenzungen können verwendet werden, um den logischen Switch oder VMs vor Ereignissen wie Broadcast-Stürmen zu schützen.</p> <p>Um Konnektivitätsprobleme zu vermeiden, muss die Mindestrate größer oder gleich 10 PPS sein.</p>

## 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-Profile > 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.
<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-Profilen einem logischen Switch zugeordnet werden, setzen sie vorhandene Standard-Switching-Profilen 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-Profils 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-Profilen 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*.

## Erweiterter Netzwerkstapel

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

Der N-VDS-Switch kann im Modus „Erweiterter Datenpfad“ nur auf einem ESXi-Host konfiguriert werden. ENS unterstützt zudem den Datenverkehr, der durch Edge-VMs fließt. Im erweiterten Datenpfadmodus können Sie Overlay-Datenverkehr und VLAN-Datenverkehr konfigurieren.

## Automatisches Zuweisen von logischen ENS-Kernen

Weisen Sie vNICs automatisch logische Kerne zu, sodass dedizierte logische Kerne den eingehenden Datenverkehr zu und ausgehenden Datenverkehr von vNICs verwalten.

Wenn der N-VDS-Switch im erweiterten Datenpfadmodus konfiguriert und ein einzelner logischer Kern einer vNIC zugeordnet ist, verarbeitet dieser logische Kern den bidirektionalen Datenverkehr, der an eine vNIC übermittelt wird oder von ihr stammt. Wenn mehrere logische Kerne konfiguriert sind, bestimmt der Host automatisch, welcher logische Kern den Datenverkehr eines vNIC verarbeiten muss.

Weisen Sie vNICs basierend auf einem dieser Parameter logische Kerne zu.

- **vNIC-count:** Host geht davon aus, dass für die Übertragung des ein- oder ausgehenden Datenverkehrs für eine vNIC-Richtung dieselben CPU-Ressourcen erforderlich sind. Jedem logischen Kern wird die gleiche Anzahl vNICs basierend auf dem verfügbaren Pool logischer Kerne zugewiesen. Dies ist der Standardmodus. Der vNIC-count-Modus ist zuverlässig, aber für einen asymmetrischen Datenverkehr nicht optimal.
- **CPU-usage:** Host prognostiziert die CPU-Nutzung zur Übertragung des ein- oder ausgehenden Datenverkehrs in jede vNIC-Richtung mithilfe interner Statistiken. Basierend auf der CPU-Nutzung zur Übertragung von Datenverkehr ändert der Host die logischen Kernzuweisungen, um die Last unter logischen Kernen auszugleichen. Der CPU-usage-Modus ist besser als der vNIC-count-Modus. Er ist jedoch unzuverlässig, wenn der Datenverkehr nicht stabil ist.

Wenn der Datenverkehr im CPU-usage-Modus häufig geändert wird, werden die erforderlichen prognostizierten CPU-Ressourcen und die vNIC-Zuweisung möglicherweise ebenfalls häufig geändert. Zu häufige Zuweisungsänderungen können zu Paket-Auslassungen führen.

Wenn die Datenverkehrsmuster unter vNICs symmetrisch sind, bietet die Option „vNIC-count“ ein zuverlässiges Verhalten, das weniger anfällig für häufige Änderungen ist. Wenn die Datenverkehrsmuster jedoch asymmetrisch sind, kann die Option „vNIC-count“ zu Paket-Auslassungen führen, da sie bei den vNICs nicht die Unterschiede zwischen dem Datenverkehr berücksichtigt.

Im vNIC-count-Modus wird empfohlen, eine geeignete Anzahl logischer Kerne zu konfigurieren, sodass jeder logische Kern derselben Anzahl vNICs zugewiesen wird. Wenn die Anzahl vNICs, die jedem logischen Kern zugeordnet sind, unterschiedlich ist, ist die CPU-Zuweisung unfair und die Leistung ist nicht deterministisch.

Wenn ein vNIC verbunden oder getrennt ist oder wenn ein logischer Kern hinzugefügt oder entfernt wird, erkennen Hosts automatisch die Änderungen und die Neuverteilung.

### Verfahren

- ◆ Führen Sie zum Wechseln zwischen den Modi den folgenden Befehl aus.

```
set ens lcore-assignment-mode <host-switch-name> <ens-lc-mode>
```

Dabei kann *<ens-lc-mode>* auf den Modus **vNIC-count** oder **cpu-usage** festgelegt werden.

**vNIC-count** ist eine logische Kernzuweisung, die auf der vNIC/Richtungsanzahl basiert.

**cpu-usage** ist eine CPU-auslastungsbasierte, logische Kernzuweisung.

## Konfigurieren von Inter-VLAN-Routing für Gäste

In Overlay-Netzwerken unterstützt NSX-T das Routing von Inter-VLAN-Datenverkehr für eine L3-Domäne. Während des Routings verwendet der virtuelle verteilte Router (Virtual Distributed Router, VDR) die VLAN-ID, um Pakete zwischen VLAN-Subnetzen weiterzuleiten.

Das Inter-VLAN-Routing überwindet die Beschränkung von 10 vNICs, die pro VM verwendet werden können. Das NSX-T unterstützende Inter-VLAN-Routing stellt sicher, dass viele VLAN-Unterschnittstellen in der vNIC erstellt und für verschiedene Netzwerkdienste verwendet werden können. Beispielsweise kann eine vNIC einer VM in mehrere Unterschnittstellen aufgeteilt werden. Jede Unterschnittstelle gehört zu einem Subnetz, das einen Netzwerkdienst wie SNMP oder DHCP hosten kann. Mit Inter-VLAN-Routing kann beispielsweise eine Unterschnittstelle in VLAN-10 eine Unterschnittstelle in VLAN-10 oder ein beliebiges anderes VLAN erreichen.

Jede vNIC auf einer VM ist mit dem N-VDS über den übergeordneten logischen Port verbunden, der nicht gekennzeichnete Pakete verwaltet.

Zum Erstellen einer Unterschnittstelle erstellen Sie auf dem erweiterten N-VDS-Switch einen untergeordneten Port unter Verwendung der API mit einem zugeordneten VIF unter Verwendung des API-Aufrufs, der im Verfahren beschrieben wird. Die mit einer VLAN-ID gekennzeichnete Unterschnittstelle ist mit einem neuen logischen Switch verknüpft, z. B. ist VLAN10 an den logischen Switch LS-VLAN-10 angehängt. Alle Unterschnittstellen von VLAN10 müssen an LS-VLAN-10 angehängt werden. Diese 1-1-Zuordnung zwischen der VLAN-ID der Unterschnittstelle

und dem zugehörigen logischen Switch ist eine wichtige Voraussetzung. Wenn Sie beispielsweise einen untergeordneten Port mit VLAN20 zum logischen Switch LS-VLAN-10 hinzufügen, der VLAN-10 zugeordnet ist, ist das Routing von Paketen zwischen VLANs nicht funktionsfähig. Durch solche Konfigurationsfehler ist das Inter-VLAN-Routing nicht funktionsfähig.

### Voraussetzungen

- Bevor Sie eine VLAN-Teil Schnittstelle einem logischen Switch zuordnen, stellen Sie sicher, dass der logische Switch keine anderen Zuordnungen mit einer anderen VLAN-Unterschnittstelle aufweist. Wenn eine Abweichung vorliegt, funktioniert das Inter-VLAN-Routing in Overlay-Netzwerken möglicherweise nicht.
- Stellen Sie sicher, dass Hosts ESXi 6.7 U2 oder höhere Versionen ausführen.

### Verfahren

- 1 Um Unterschnittstellen für eine vNIC zu erstellen, stellen Sie sicher, dass die vNIC auf einen übergeordneten Port aktualisiert wird. Führen Sie den folgenden REST-API-Aufruf aus:

```
PUT https://<nsx-mgr-ip>/api/v1/logical-ports/<Logical-Port UUID-of-the-vNIC>
{
  "resource_type" : "LogicalPort",
  "display_name" : "parentport",
  "attachment" : {
    "attachment_type" : "VIF",
    "context" : {
      "resource_type" : "VifAttachmentContext",
      "vif_type": "PARENT"
    },
    "id" : "<Attachment UUID of the vNIC>"
  },
  "admin_state" : "UP",
  "logical_switch_id" : "UUID of Logical Switch to which the vNIC is connected",
  "_revision" : 0
}
```

- 2 Um untergeordnete Ports für einen übergeordneten vNIC-Port auf dem N-VDS zu erstellen, der den Unterschnittstellen auf einer VM zugeordnet ist, führen Sie den API-Aufruf aus. Bevor Sie den API-Aufruf durchführen, stellen Sie sicher, dass ein logischer Switch vorhanden ist, um untergeordnete Ports mit den Unterschnittstellen auf der VM zu verbinden.

```
POST https://<nsx-mgr-ip>/api/v1/logical-ports/
{
  "resource_type" : "LogicalPort",
  "display_name" : "<Name of the Child PORT>",
  "attachment" : {
    "attachment_type" : "VIF",
    "context" : {
      "resource_type" : "VifAttachmentContext",
      "parent_vif_id" : "<UUID of the PARENT port from Step 1>",
      "traffic_tag" : <VLAN ID>,
      "app_id" : "<ID of the attachment>", ==> display id(can give any string). Must be
```

```

unique.
    "vif_type" : "CHILD"
  },
  "id" : "<ID of the CHILD port>"
},

  "logical_switch_id" : "<UUID of the Logical switch(not the PARENT PORT's logical switch)
to which Child port would be connected to>",
  "address_bindings" : [ { "mac_address" : "<vNIC MAC address>", "ip_address" : "<IP
address to the corresponding VLAN>", "vlan" : <VLAN ID> } ],
  "admin_state" : "UP"
}

```

## Ergebnisse

NSX-T Data Center erstellt Unterschnittstellen auf VMs.

## 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-Profil. 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 Edge-Bridge-Profiles

Ein Edge-Bridge-Profil ermöglicht es einem NSX Edge-Cluster, Schicht-2-Bridging für einen logischen Switch bereitzustellen.

Wenn Sie ein Edge-Bridge-Profil erstellen, den Failover-Modus als präventiv festlegen und ein Failover auftritt, wird der Standby-Knoten zum aktiven Knoten. Nachdem der ausgefallene Knoten wiederhergestellt wurde, wird er wieder zum aktiven Knoten. Wenn Sie den Failover-Modus als nicht präventiv festlegen und ein Failover auftritt, wird der Standby-Knoten zum aktiven Knoten. Nachdem der ausgefallene Knoten wiederhergestellt wurde, wird er zum Standby-Knoten. Sie können den Standby-Edge-Knoten manuell auf den aktiven Knoten festlegen, indem Sie den CLI-Befehl `set l2bridge-port <uuid> state active` auf dem Standby-Edge-Knoten ausführen.

Der Befehl kann nur im nicht präventiven Modus angewendet werden. Andernfalls tritt ein Fehler auf. Im nicht präventiven Modus löst der Befehl ein HA-Failover aus, wenn er auf einen Standby-Knoten angewendet wird. Er wird ignoriert, wenn er auf einen aktiven Knoten angewendet wird. Weitere Informationen finden Sie in der *Referenz zur NSX-T Data Center Command-Line Interface*.

### 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-Profiles 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">AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=</opaqueData>
    </opaqueData>
</opaqueDataSpec>

```

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="vmobl.Binary">AAABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=</opaqueData>
    </opaqueData>
  </opaqueDataSpec>

```

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="vmobl.Binary">AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=</opaqueData>
    </opaqueData>
  </opaqueDataSpec>

```

- 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 ein Edge-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** aus.
- 3 Klicken Sie auf den Namen eines Overlay-Switches (Datenverkehrstyp: Overlay).
- 4 Klicken Sie auf **Zugehörig > Edge-Bridge-Profile**.
- 5 Klicken Sie auf **Anhängen**.
- 6 Gehen Sie wie folgt vor, um ein Edge-Bridge-Profil anzuhängen:
  - a Wählen Sie ein Edge-Bridge-Profil aus.
  - b Wählen Sie eine Transportzone aus.
  - c Geben Sie eine VLAN-ID ein.
  - d Klicken Sie auf **Speichern**.
- 7 Verbinden Sie VMs mit dem logischen Switch, wenn diese noch nicht verbunden sind.  
Die VMs müssen sich auf Transportknoten in derselben Transportzone wie das Edge-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:

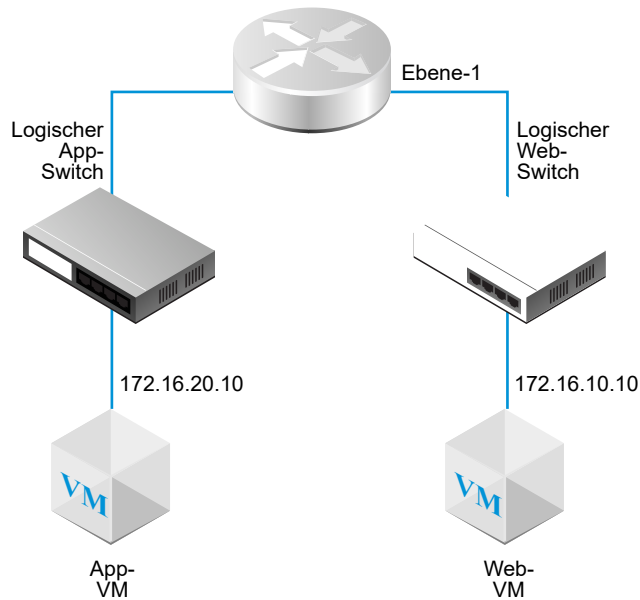
- [Logischer Tier-1-Router](#)
- [Logischer Tier-0 Router](#)

## 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

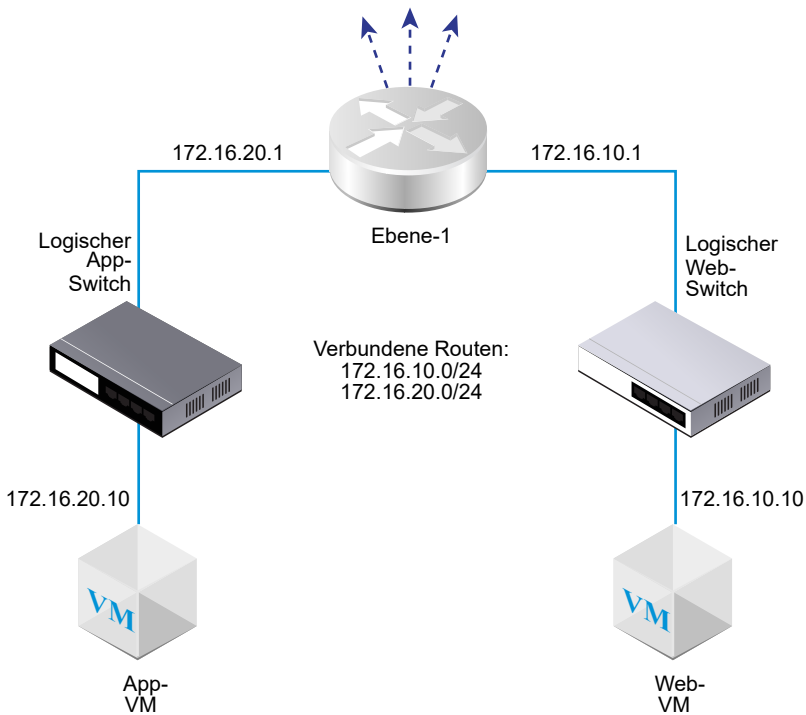
- 1 Melden Sie sich in Ihrem Browser mit Administratorrechten bei einem NSX Manager unter <https://<nsx-manager-ip-address>> an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Router > Netzwerk**.
- 3 Klicken Sie auf den Namen eines Routers.
- 4 Klicken Sie auf die Registerkarte **Konfiguration** 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](#).

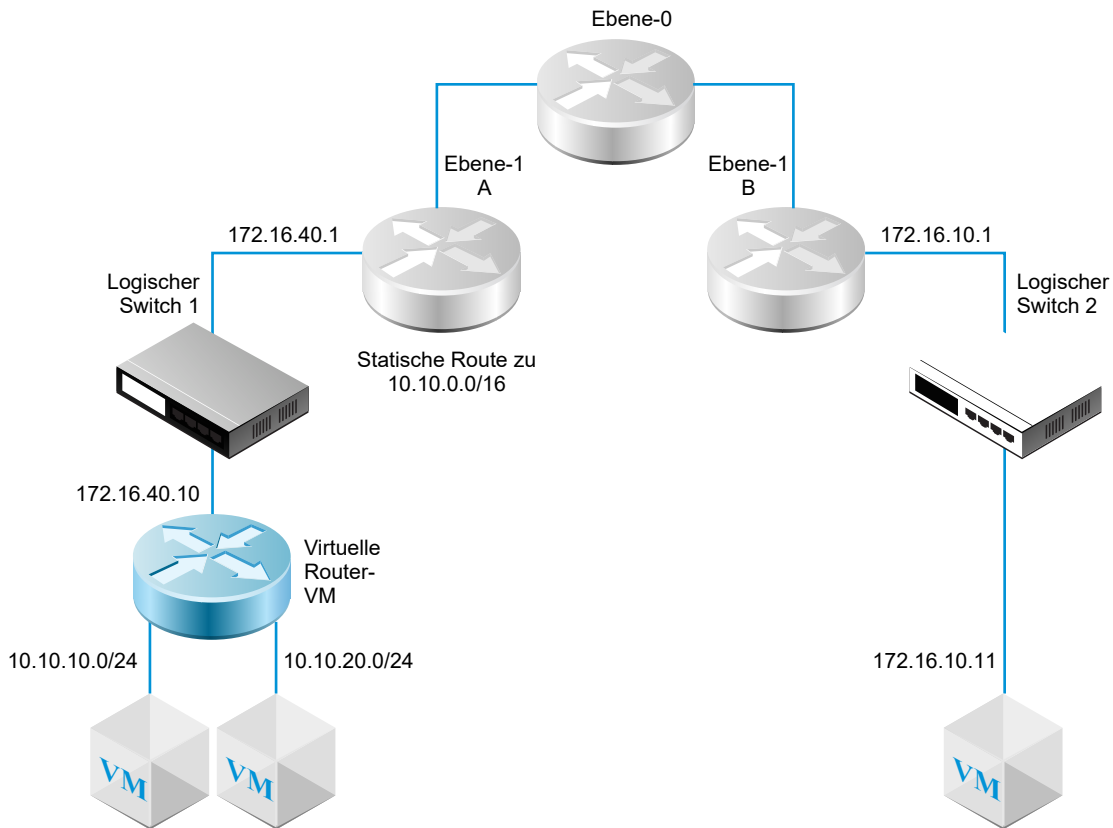
Wenn bereits ein logischer Tier-0 Router mit dem logischen Tier-1 Router verbunden ist, müssen Sie sicherstellen, dass der Tier-0 Router die Informationen über die mit dem Tier-1 Router verbundenen Routen abrufen. Siehe [Überprüfen des Abrufs von Routen von einem Tier-1-Router für einen Tier-0-Router](#).

## 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

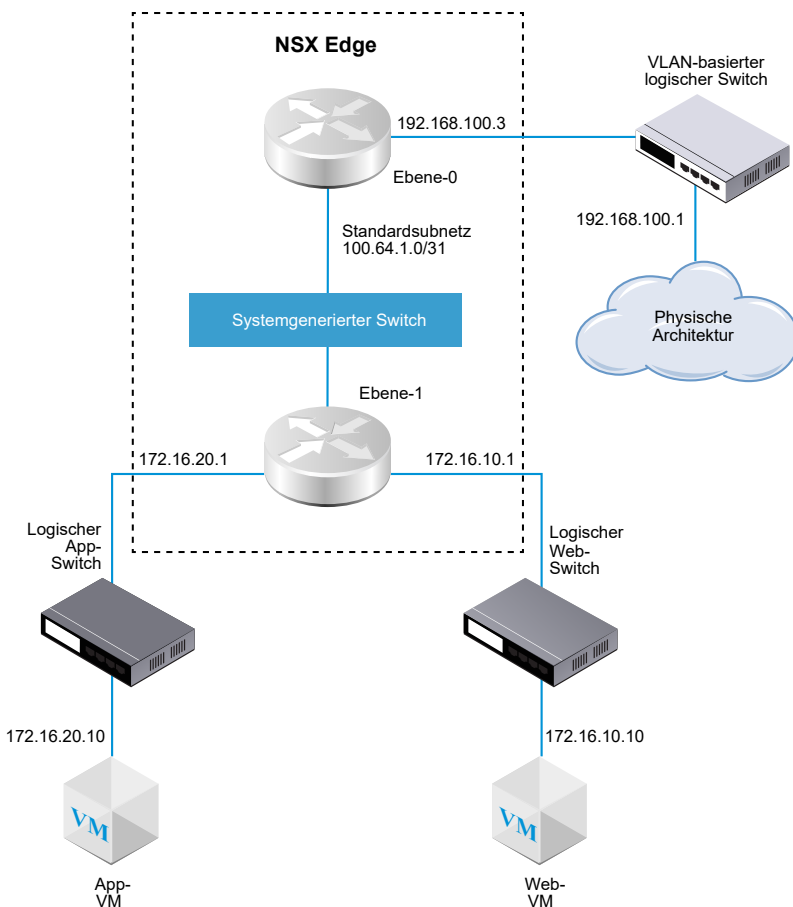
Ein logischer Tier-0 Router bietet einen Gateway-Dienst zwischen dem logischen und dem physischen Netzwerk.

**NSX Cloud-Hinweis** Wenn Sie NSX Cloud verwenden, finden Sie unter [NSX-T Data Center-Funktionen mit Support in NSX 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.

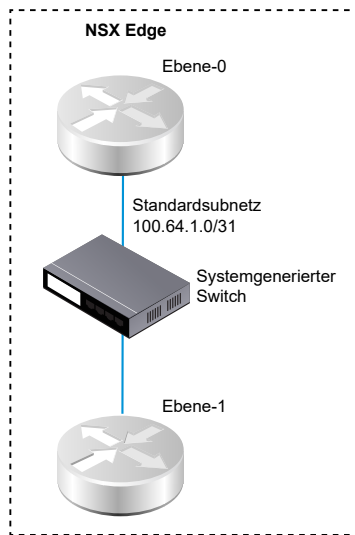
Konfigurieren Sie den logischen Tier-0-Router für dessen Verbindung mit einem logischen VLAN-Switch zum Erstellen eines Uplinks zu einem externen Netzwerk. Siehe [Verbinden eines logischen Tier-0 Routers mit einem logischen VLAN-Switch für den NSX Edge-Uplink](#).

## 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-O-Router aus.

- 11 Klicken Sie auf die Registerkarte **Konfiguration** des Tier-O-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-O-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-O-Router

Wenn ein logischer Tier-1 Router Routen für einen logischen Tier-O Router ankündigt, werden die Routen in der Routing-Tabelle des Tier-O 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-O-Dienstrouters abzurufen.

```
nsx-edge-1> get logical-routers
Logical Router
UUID          : 736a80e3-23f6-5a2d-81d6-bbfeb2786666
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

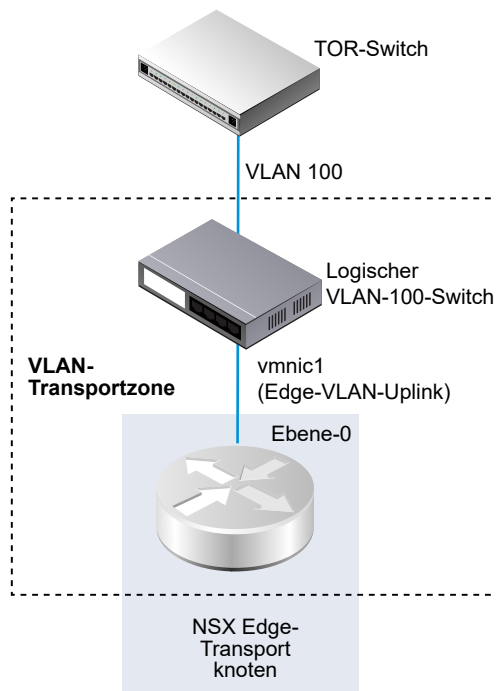
b   10.10.10.0/24      [20/0]      via 192.168.100.254
rl  100.91.176.0/31   [0/0]      via 169.254.0.1
c   169.254.0.0/28    [0/0]      via 169.254.0.2
ns  172.16.10.0/24    [3/3]      via 169.254.0.1
ns  172.16.20.0/24    [3/3]      via 169.254.0.1
c   192.168.100.0/24  [0/0]      via 192.168.100.2

```

## 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-bbfeb2786666
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 BGP 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**.

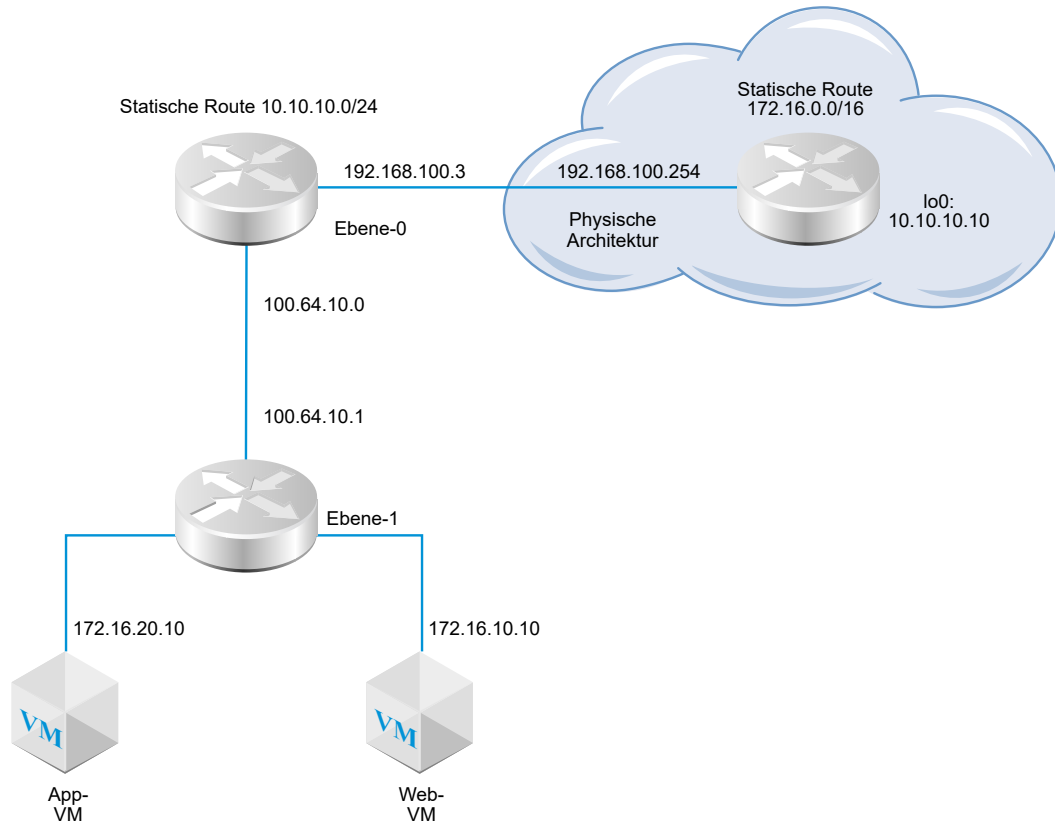
- 6 Geben Sie für den Router-Port einen Namen und optional eine Beschreibung ein.
- 7 Wählen Sie im Feld **Typ** die Option **Zentral** aus.
- 8 Wählen Sie als **URPF-Modus** entweder **Streng** oder **Keine** aus.  
URPF (Unicast Reverse Path Forwarding) ist eine Sicherheitsfunktion.
- 9 (Erforderlich) 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.

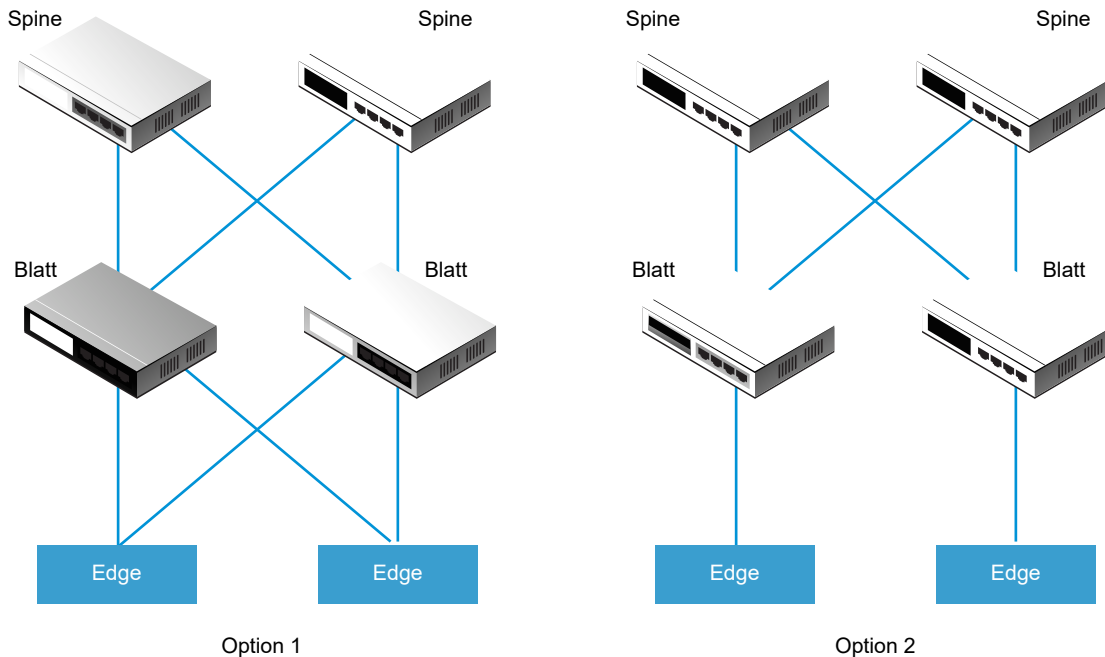
```
ping 10.10.10.10
```

```
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 BGP 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.

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.

Wenn Sie BGP 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 konfigurieren. EBGP-Nachbarn müssen direkt verbunden sein und sich im selben Subnetz wie der Tier-0-Uplink befinden. Wenn Sie sich nicht im selben Subnetz befinden, sollte BGP-Multi-Hop verwendet werden.

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.

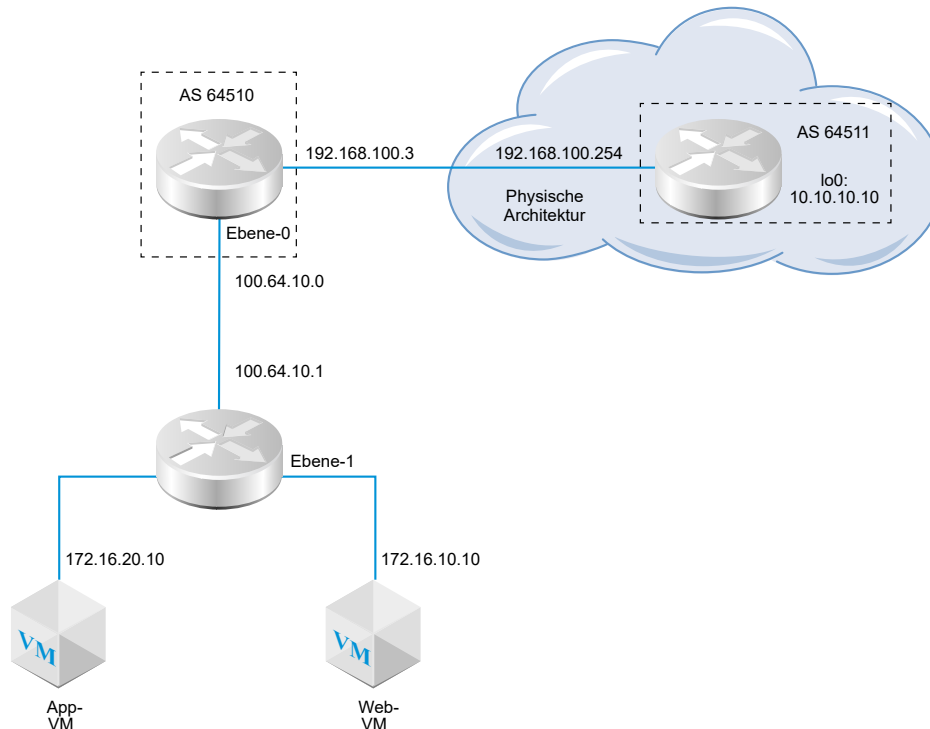
In einer Topologie mit einem logischen Tier-0-Router im Aktiv/Aktiv-Modus, der an einen logischen Tier-1-Router im Aktiv/Standby-Modus angehängt ist, müssen Sie Inter-SR-Routing aktivieren, um das asymmetrische Routing zu verarbeiten. Sie haben asymmetrisches Routing, wenn Sie eine statische Route auf 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 (eBGP-Nachbar) oder 64510 (iBGP-Nachbar).
- 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](#).

### Überprüfen von BGP-Verbindungen von einem Tier-O-Dienstrouter aus

Mit der Befehlszeilenschnittstelle (CLI) können Sie vom Tier-O-Dienstrouter aus überprüfen, ob eine BGP-Verbindung mit einem Nachbarn eingerichtet ist.

#### Voraussetzungen

Stellen Sie sicher, dass BGP konfiguriert ist. Siehe [Konfigurieren von BGP auf einem logischen Tier-O-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-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-0-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-O-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>■ TO Verbunden</li> <li>■ TO Uplink</li> <li>■ TO Downlink</li> <li>■ TO CSP</li> <li>■ TO Loopback</li> <li>■ TO Statisch</li> <li>■ TO NAT</li> <li>■ TO DNS-Weiterleitungs-IP</li> <li>■ TO Lokale IPSec-IP</li> <li>■ T1 Verbunden</li> <li>■ T1 CSP</li> <li>■ T1 Downlink</li> <li>■ T1 Statisch</li> <li>■ T1 LB-SNAT</li> <li>■ T1 NAT</li> <li>■ T1 LB-VIP</li> <li>■ T1 DNS-Weiterleitungs-IP</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 BGP 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-edgel(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

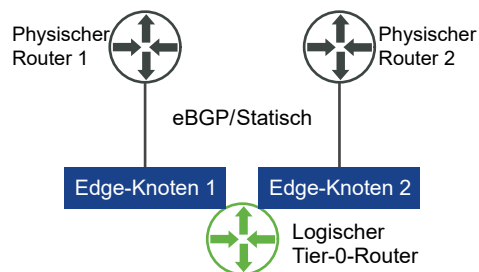
Konfigurieren Sie weitere Routing-Funktionen, wie ECMP.

## 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. Die Implementierung von ECMP auf NSX Edge basiert auf dem 5-Tupel der Protokollnummer, der Quelladresse, der Zieladresse sowie dem Quellport und dem Zielport. Der Algorithmus, der zum Verteilen der Daten auf die ECMP-Pfade verwendet wird, ist kein Round Robin. Aus diesem Grund führen einige Pfade möglicherweise mehr Datenverkehr als andere. Beachten Sie, dass ECMP nur auf den Quell- und Zieladressen basiert, wenn es sich bei dem Protokoll um IPv6 handelt und der IPv6-Header mehr als einen Erweiterungsheader aufweist.

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-0-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-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-0-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-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-0-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-O-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 EBGP-Peers.</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-O 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 individuellem 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 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:

- [Netzwerkadressübersetzung \(NAT\)](#)

## Netzwerkadressübersetzung (NAT)

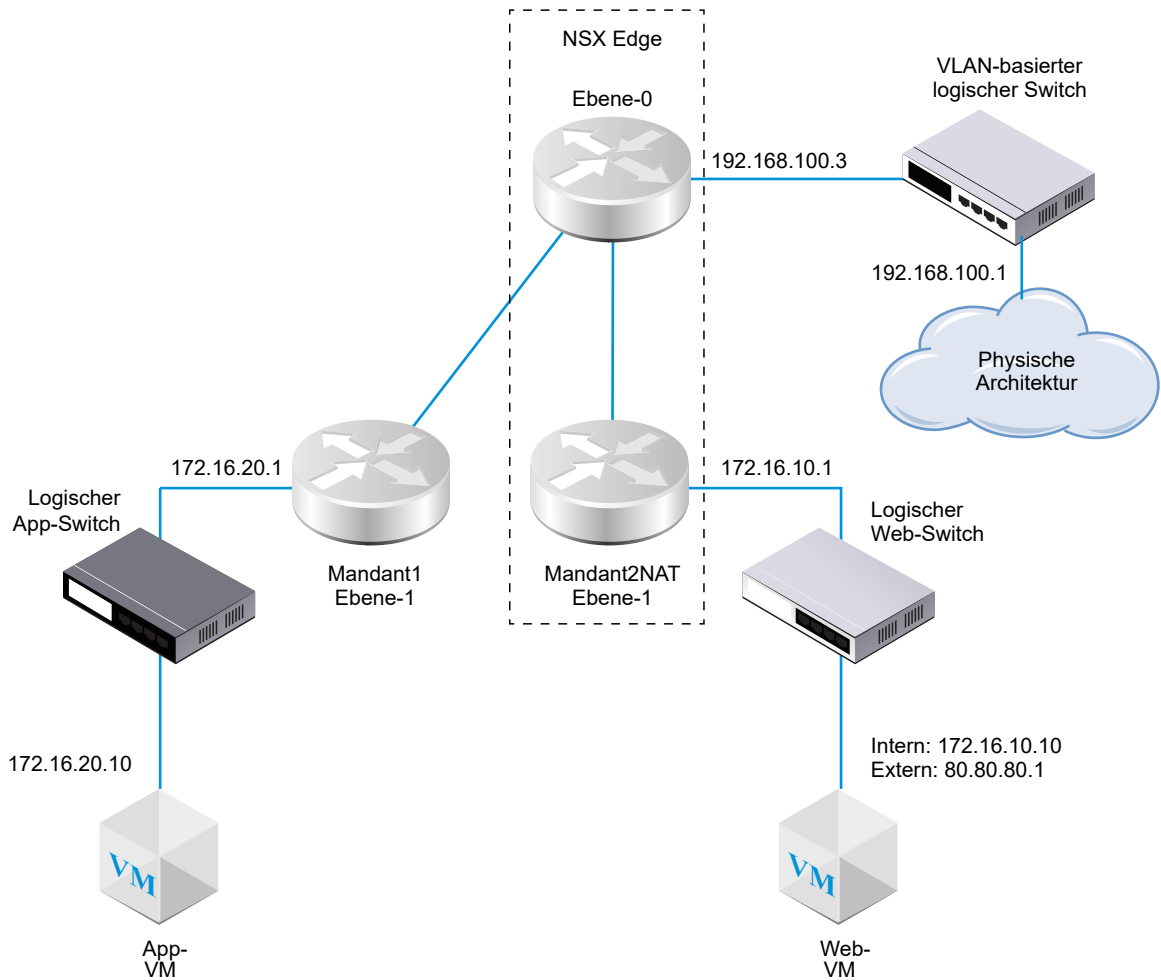
Die Netzwerkadressübersetzung (NAT, Network Address Translation) in NSX-T Data Center kann auf logischen Tier-0 und Tier-1 Routern konfiguriert werden.

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.

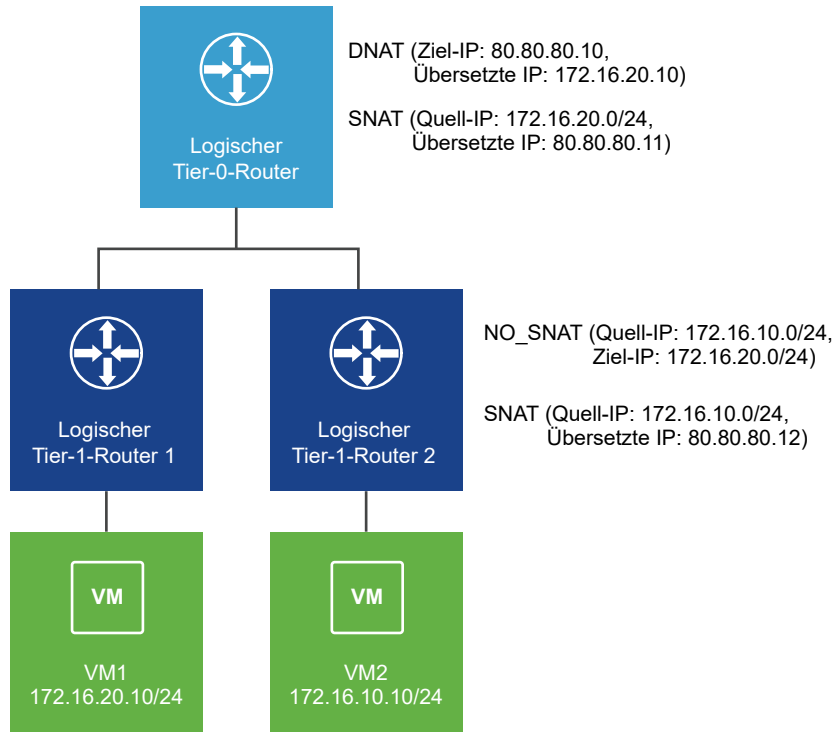
Die NAT wird für den Uplink des logischen Routers Mandant2NAT auf seiner Verbindung mit dem logischen Tier-0 Router erzwungen.

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



Hinweis: NAT-Hairpinning wird im folgenden Szenario nicht unterstützt. Für den logischen Tier-0-Router sind DNAT und SNAT konfiguriert. Für den logischen Tier-1-Router 2 sind NO\_SNAT und SNAT konfiguriert. VM2 kann über die externe Adresse 80.80.80.10 von VM1 nicht auf VM1 zugreifen.



In den folgenden Abschnitten wird beschrieben, wie Sie mithilfe der Manager-Benutzeroberfläche NAT-Regeln erstellen. Sie können auch einen API-Aufruf (`POST /api/v1/logical-routers/<logical-router-id>/nat/rules?action=create_multiple`) durchführen, um mehrere NAT-Regeln gleichzeitig zu erstellen. Weitere Informationen finden Sie im *Handbuch zur NSX-T Data Center-API*.

## 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 BGP 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 BGP 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>■ TO Verbunden</li> <li>■ TO Uplink</li> <li>■ TO Downlink</li> <li>■ TO CSP</li> <li>■ TO Loopback</li> <li>■ TO Statisch</li> <li>■ TO NAT</li> <li>■ TO DNS-Weiterleitungs-IP</li> <li>■ TO Lokale IPSec-IP</li> <li>■ T1 Verbunden</li> <li>■ T1 CSP</li> <li>■ T1 Downlink</li> <li>■ T1 Statisch</li> <li>■ T1 LB-SNAT</li> <li>■ T1 NAT</li> <li>■ T1 LB-VIP</li> <li>■ T1 DNS-Weiterleitungs-IP</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-0-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-0-NAT

Ein logischer Tier-0-Router im Modus „Aktiv/Standby“ unterstützt Quell-NAT (SNAT), Ziel-NAT (DNAT) und reflexive NAT. Ein logischer Tier-0-Router im Modus „Aktiv/Aktiv“ unterstützt nur reflexive NAT.

### Konfigurieren der Quell- und Ziel-NAT auf einem logischen Tier-0 Router

Sie können eine Quell- und Ziel-NAT auf einem logischen Tier-0 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-0 Routers konfigurierte SNAT verarbeitet den Datenverkehr von einem logischen Tier-1 Router sowie von einem anderen Uplink auf dem logischen 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 Klicken Sie auf einen logischen Tier-0 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.

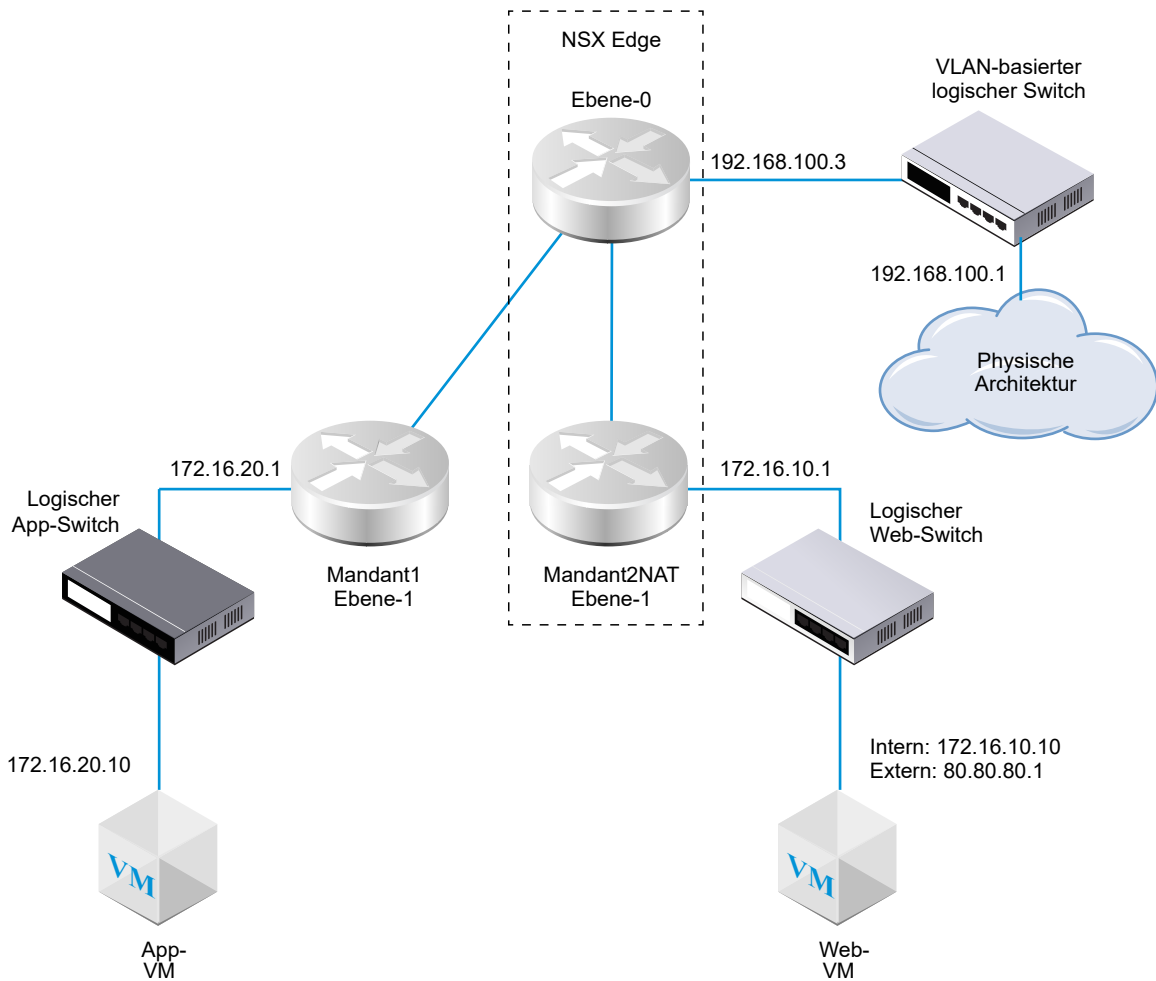
- 16 (Optional) Ändern Sie die Einstellung für die Firewall-Umgehung.

Diese Funktion ist standardmäßig aktiviert.

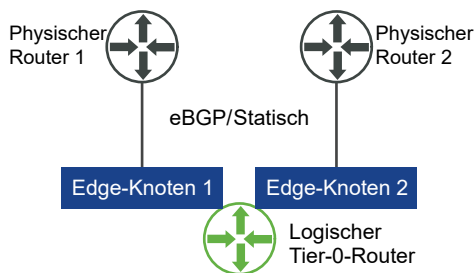
## Reflexive NAT

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

☒ Aktive Sitzungen
 ☐ Paketanzahl
 ☐ 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 kommasetrennten 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 NSGroups 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 [NSX-T Data Center-Funktionen mit Support in NSX 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.

- **IP Set** – kann ein Tag und optional den Geltungsbereich angeben.

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 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:

- [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** aus.
- 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-Server:

- 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

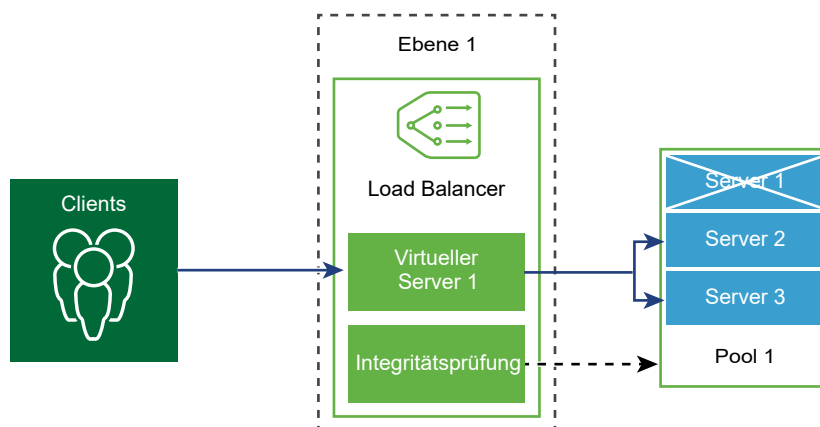
# 19

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 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](#).

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:

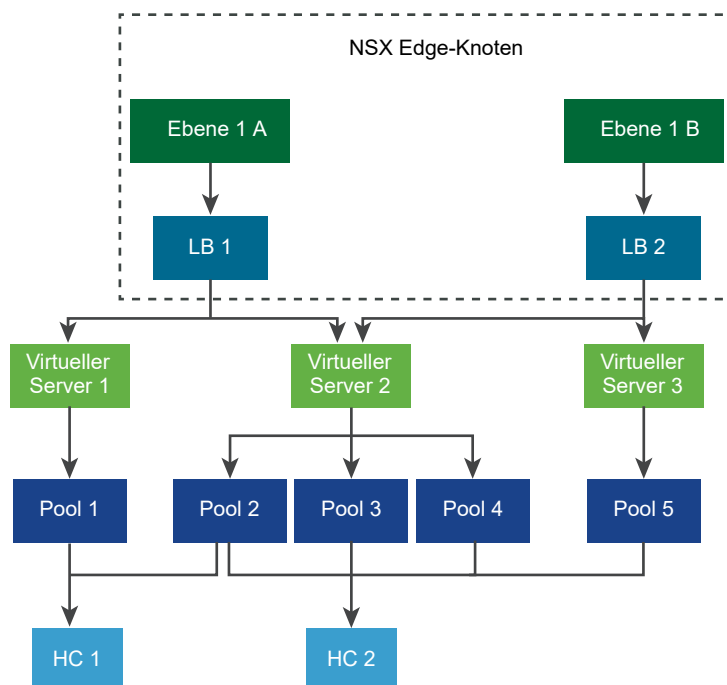
- [Wichtige Load Balancer-Konzepte](#)
- [Konfigurieren von Load Balancer-Komponenten](#)

## 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.

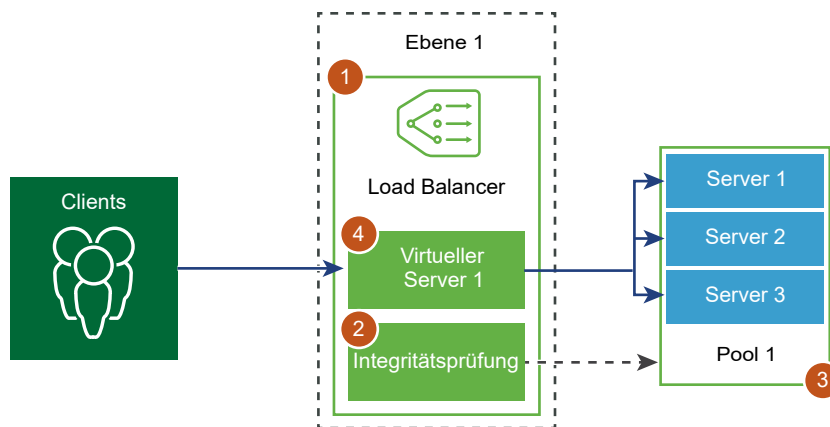
Wenn Sie die ordnungsgemäße Ausführung der Anwendung auf jedem Server prüfen möchten, können Sie Systemdiagnoseüberwachungen hinzufügen, die den Systemzustand eines Servers überprüfen.



## 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.

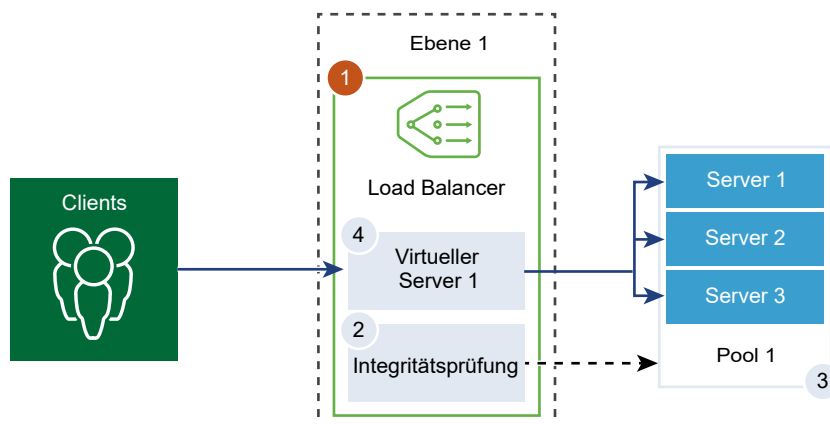


## Erstellen eines Load Balancers

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.

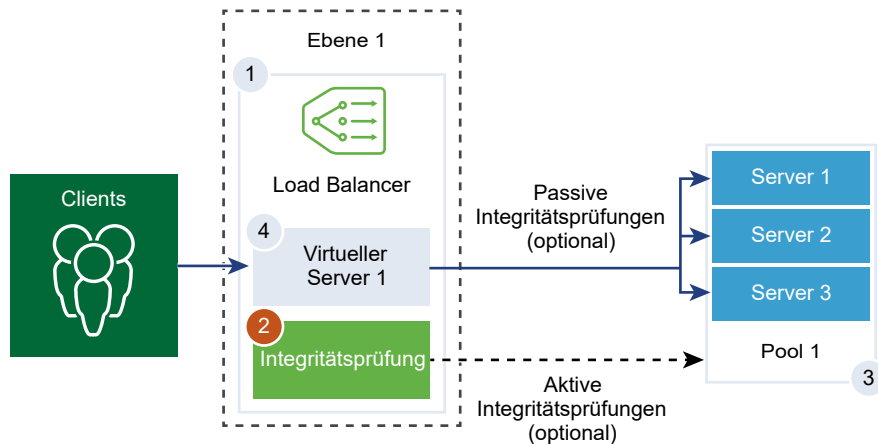
Aktive Systemdiagnosen werden auf Serverpoolmitgliedern durchgeführt, nachdem das Poolmitglied an einen virtuellen Server und dieser virtuelle Server dann an ein Tier-1-Gateway (zuvor als logischer Tier-1-Router bezeichnet) angehängt wurde.

Wenn das Tier-1-Gateway mit einem Tier-O-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-O-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 Dreiwege-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
Gesendete UDP-Daten	Geben Sie die Zeichenfolge ein, die nach dem Verbindungsaufbau an den Server gesendet werden soll.
Erwartete UDP-Daten	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.

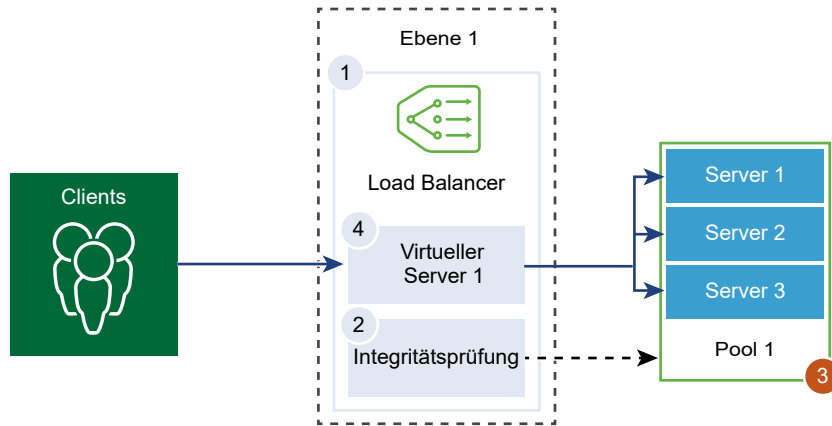
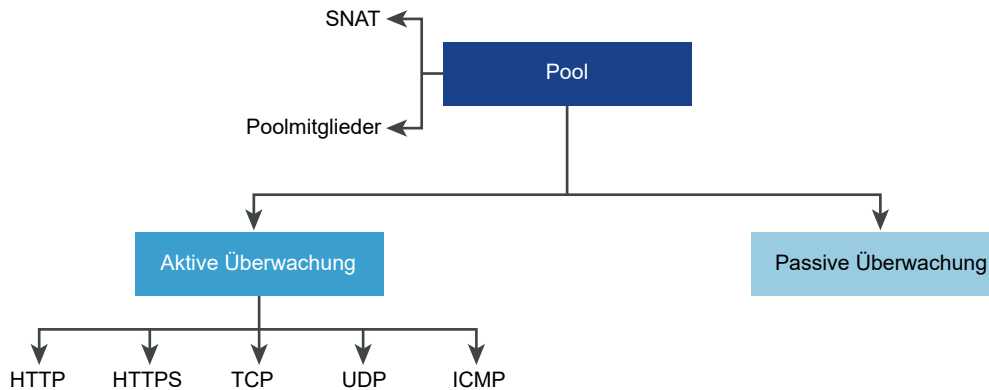


Abbildung 19-1. Konfiguration der Serverpool-Parameter



### 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
Statisch	Klicken Sie auf <b>Hinzufügen</b> , um ein statisches Poolmitglied hinzuzufügen. Sie können auch ein vorhandenes statisches Poolmitglied klonen.
Dynamisch	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.

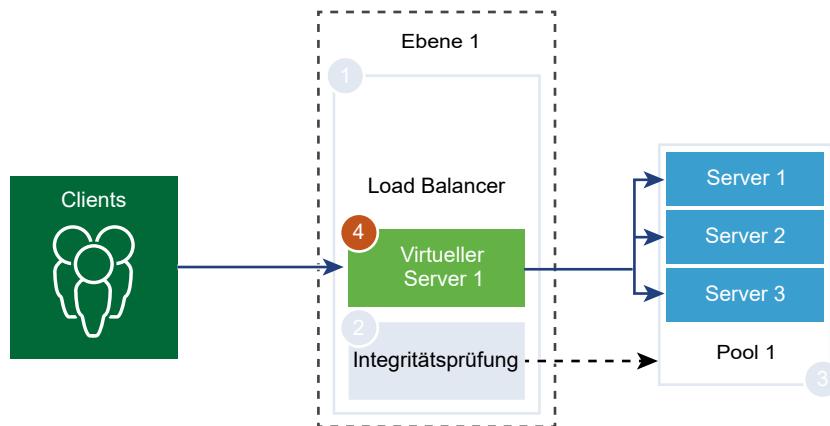
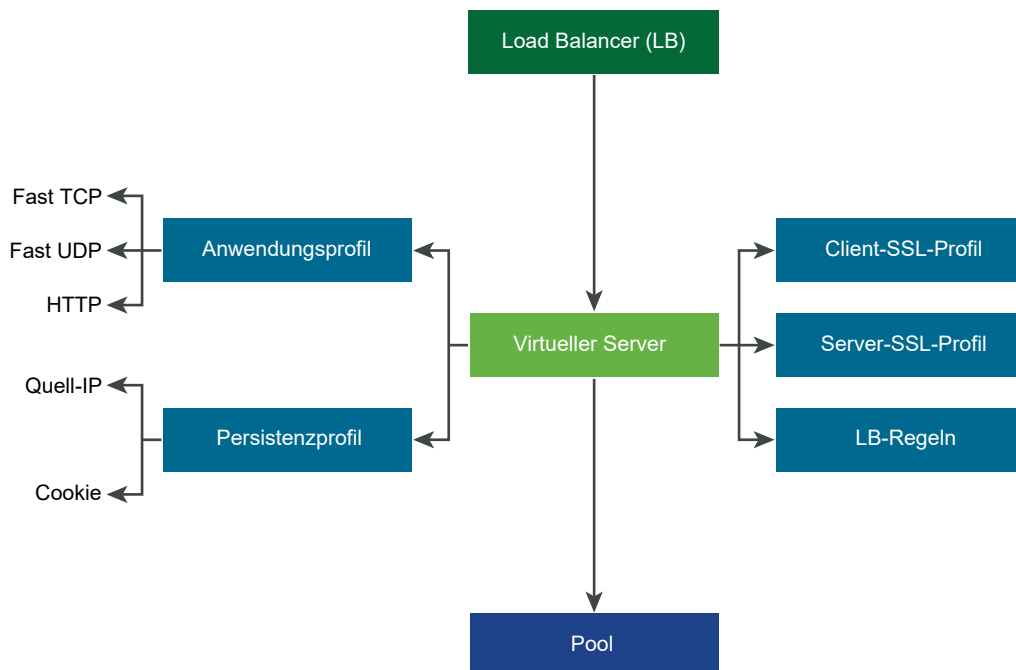


Abbildung 19-2. Komponenten des virtuellen Servers



## 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

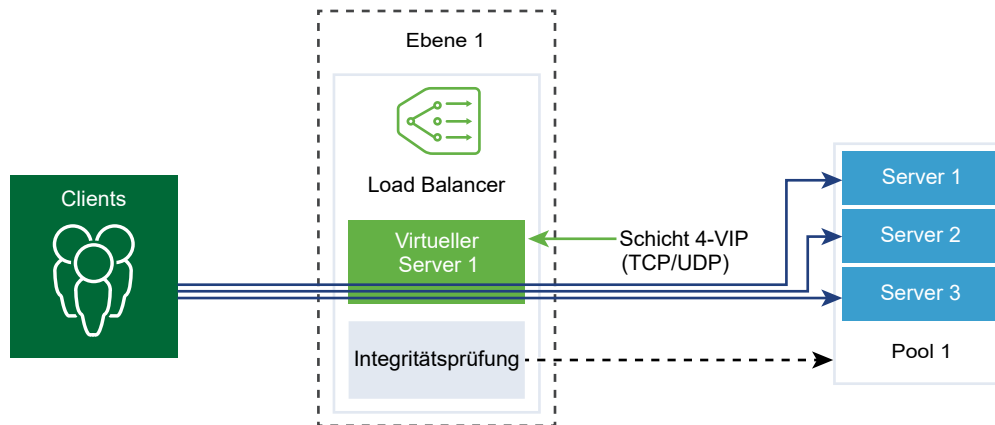
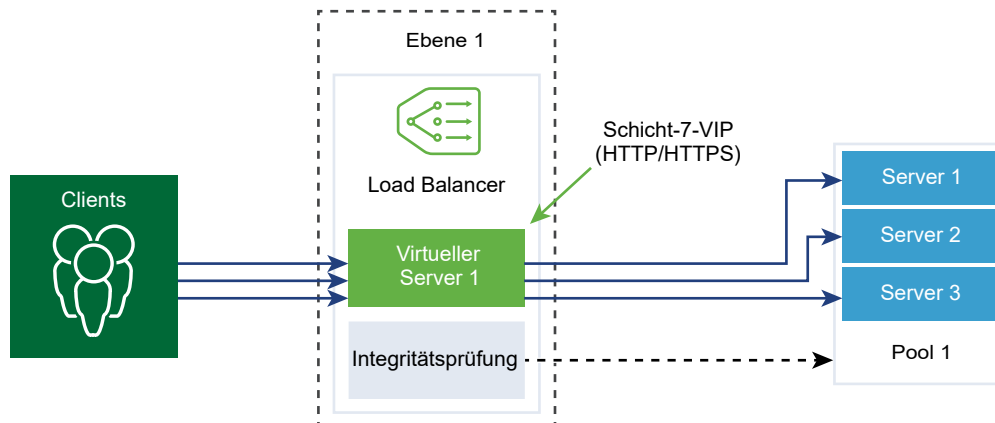


Abbildung 19-4. HTTPS-Anwendungsprofil der Schicht 7



## 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
Umleitung	<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>
XFF (X-Forwarded-For)	<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.</p> <p>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>

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**.

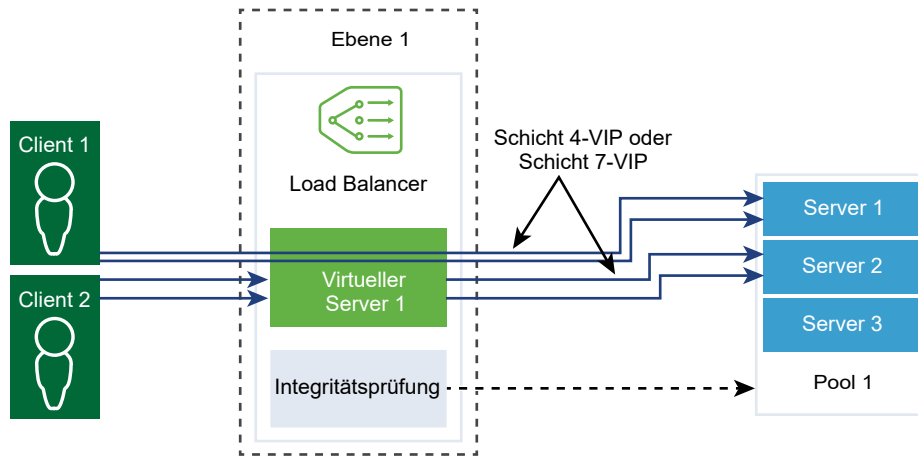
## Konfigurieren von persistenten Profilen

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. Beachten Sie, dass ein Leerzeichen in einem Cookienamen **nicht** 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 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 Persistenztafel 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 Persistenztafel.</p>
<b>Zeitüberschreitung für Persistenzeintrag</b>	<p>Geben Sie den Zeitraum für die Persistenz bis zum Ablauf in Sekunden ein.</p> <p>Die Persistenztafel 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 Persistenztafel voll ist.</p> <p>Ein hoher Wert für die Zeitüberschreitung führt möglicherweise dazu, dass die Persistenztafel sich schnell füllt, wenn der Datenverkehr hoch ist. Wenn die Persistenztafel 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>	<p>Wählen Sie im Dropdown-Menü einen Modus aus.</p> <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>Cookieiname</b>	Geben Sie den Cookienamen ein. Beachten Sie, dass ein Leerzeichen in einem Cookienamen <b>nicht</b> unterstützt wird.
<b>Cookieidomäne</b>	<p>Geben Sie den Domänennamen ein.</p> <p>Die HTTP-Cookieidomäne kann nur im Modus EINFÜGEN konfiguriert werden.</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>Verschlüsseln Sie die Informationen zu IP-Adresse und Port des Cookieservers.</p> <p>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.</p>
<b>Cookie-Fallback</b>	<p>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.</p> <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>

- f Geben Sie die Details zum Ablauf des Cookies an.

Option	Beschreibung
Cookiezeittyp	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.
Maximale Leerlaufzeit	Geben Sie die Zeit in Sekunden ein, die das Cookie im Leerlauf sein kann, bevor es abläuft.
Maximales Cookiealter	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

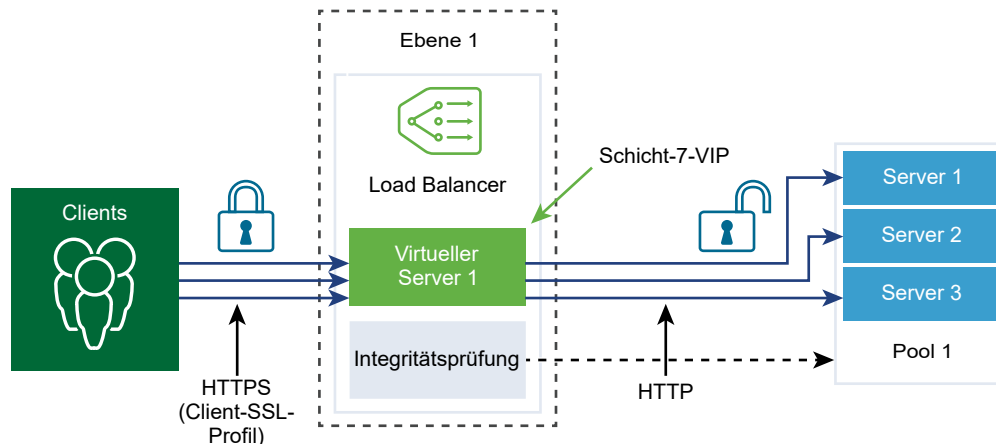
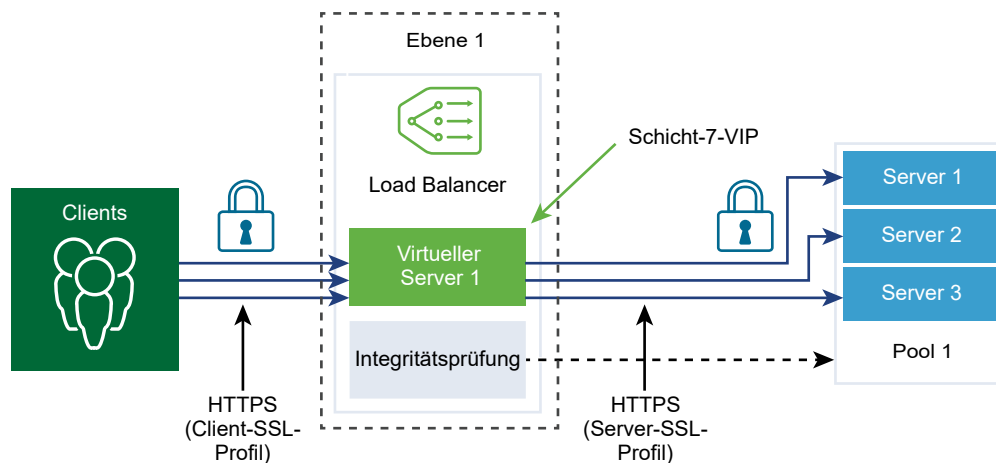


Abbildung 19-6. End-to-End-SSL



## 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-Profilen 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 Load Balancing-Verhalten 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 Load Balancing-Verhalten 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:s)ensitive“, sondern stattdessen „Case ((?i:s)ensitive)“.
- 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
- \$\_arg\_<name> - argument <name> in der Anforderungszeile
- \$\_cookie\_<name> – Wert des <name>-Cookies
- \$\_upstream\_cookie\_<name> – Cookie mit dem angegebenen Namen, der vom vorgeschalteten Server im Antwortheader-Feld „Set-Cookie“ gesendet wurde
- \$\_upstream\_http\_<name> – beliebiges Antwortheader-Feld; <name> ist der Feldname konvertiert in Kleinbuchstaben, wobei Bindestriche durch Unterstriche ersetzt wurden

- `$_host` – in der folgenden Rangfolge: der Hostname aus der Anforderungszeile oder der Hostname im Anforderungsheader-Feld „Host“ oder der mit einer Anforderung übereinstimmende Servername
- `$_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



Unterstützte Übereinstimmungsbedingung	Beschreibung
HTTP-Anforderungsnutzlast	Zuordnen des Inhalts eines HTTP-Anforderungstexts. http_request.body_value – zuzuordnender Wert
Felder des TCP-Headers	Zuordnen einer TCP-Quelle oder des Zielports. tcp_header.source_port – zuzuordnender Quellport tcp_header.destination_port – zuzuordnender Zielport
Felder des IP-Headers	Zuordnen einer IP-Quelladresse oder -Zieladresse ip_header.source_address – zuzuordnende Quelladresse ip_header.destination_address – zuzuordnende Zieladresse

Aktion	Beschreibung
HTTP-Anforderungs-URI umschreiben	Ändern eines URI. http_request.uri – zu schreibender URI (ohne Abfrageargumente) http_request.uri_args – zu schreibende URI-Abfrageargumente
HTTP-Anforderungs-Header umschreiben	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.

Unterstützte Übereinstimmungsbedingung	Beschreibung
HTTP-Anforderungsmethode	Zuordnen einer HTTP-Anforderungsmethode. http_request.method – zuzuordnender Wert
HTTP-Anforderungs-URI	Zuordnen eines HTTP-Anforderungs-URI. http_request.uri – zuzuordnender Wert
Argumente des HTTP-Anforderungs-URI	Zuordnen des Abfragearguments eines HTTP-Anforderungs-URI. http_request.uri_args – zuzuordnender Wert
HTTP-Anforderungsversion	Zuordnen einer HTTP-Anforderungsversion. http_request.version – zuzuordnender Wert
HTTP-Anforderungs-Header	Zuordnen eines beliebigen HTTP-Anforderungs-Headers. http_request.header_name – zuzuordnender Header-Name http_request.header_value – zuzuordnender Wert
HTTP-Anforderungsnutzlast	Zuordnen des Inhalts eines HTTP-Anforderungstexts. http_request.body_value – zuzuordnender Wert

Unterstützte Übereinstimmungsbedingung	Beschreibung
Felder des TCP-Headers	Zuordnen einer TCP-Quelle oder des Zielports. tcp_header.source_port – zuzuordnender Quellport tcp_header.destination_port – zuzuordnender Zielport
Felder des IP-Headers	Zuordnen einer IP-Quelladresse ip_header.source_address – zuzuordnende Quelladresse
Aktion	Beschreibung
Ablehnen	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
Umleiten	Umleiten einer Anforderung. Statuscode muss auf 3xx gesetzt werden. http_forward.redirect_status – HTTP-Statuscode für Umleiten http_forward.redirect_url – HTTP-Umleitungs-URL
Pool auswählen	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
HTTP-Antwort-Header	Zuordnen eines beliebigen HTTP-Antwort-Headers. http_response.header_name – zuzuordnender Header-Name http_response.header_value – zuzuordnender Wert
Aktion	Beschreibung
HTTP-Antwort-Header umschreiben	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 Balancing-Profilen 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-Profilen konfigurieren.

**Hinweis** SSL-Profilen 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 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:

- [Hinzufügen oder Löschen einer Firewallregel zu bzw. von einem logischen Router](#)
- [Konfigurieren der Firewall für den Bridge-Port eines logischen Switches](#)
- [Firewallabschnitte und Firewallregeln](#)
- [Informationen über Firewallregeln](#)

## 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.

---

## 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.

## 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.

---

## 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 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 Stateless Firewall zu erzwingen, wählen Sie die Option **Stateless Firewall aktivieren** aus. Diese Option steht nur für L3 zur Verfügung.

Stateless Firewalls überwachen den Netzwerkdatenverkehr und beschränken oder blockieren Pakete auf der Grundlage von Quell- und Zieladressen oder anderen statischen Werten. Für TCP- und UDP-Flows wird nach dem ersten Paket ein Cache für das Verkehrstupel in beide Richtungen erstellt und beibehalten, wenn das Firewall-Ergebnis ZULASSEN lautet. Das bedeutet, dass der Datenverkehr nicht mehr mit den Firewall-Regeln abgeglichen werden muss, was zu einer geringeren Latenz führt. Statusfreie Firewalls sind daher in der Regel schneller und bieten eine bessere Leistung bei höherem Datenverkehrsaufkommen.

Zustandsbehaftete Firewalls ermöglichen eine End-to-End-Überwachung von Datenverkehrs-Streams. Die Firewall wird für jedes Paket konsultiert, um den Status und die Sequenznummern zu validieren. 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 NSGroups. Wenn Sie eine NSGroup auswählen, muss sie einen oder mehrere logische Switches oder logische Ports enthalten. Wenn die NSGroup 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**.

## 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.

---

**Hinweis** NSX-T Data Center fügt automatisch NSX Manager- und NSX Edge-Knoten-VMs zur Firewall-Ausschlussliste hinzu.

---

### 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**.

## 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 keine 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> .
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 bösartige 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 Dienstregелеlements 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.
Containere objekt	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	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.
Containerelemente	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
Diensttyp	<ul style="list-style-type: none"> <li>■ ALG</li> <li>■ ICMP</li> <li>■ IGMP</li> <li>■ IP</li> <li>■ L4-Port-Satz</li> </ul>
Protokoll	Wählen Sie eines der verfügbaren Protokolle aus.
Quellports	Geben Sie den Quellport ein.
Zielpports	Wählen Sie den Zielpport 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.

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:

- Anzeigen von Überwachungs-Dashboards
- Nutzung und Kapazität von Objektkategorien anzeigen
- Überprüfen des Umsetzungsstatus einer Konfigurationsänderung
- Suchen nach Objekten
- Filtern nach Objektattributen
- 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
- Ersetzen eines NSX Edge-Transportknotens in einem NSX Edge-Cluster
- Wiederherstellen von NSX-T, wenn vCenter Server verlorengeht und nicht wiederhergestellt werden kann
- Bereitstellung von NSX-T Data Center für mehrere Sites
- Konfigurieren von Appliances

- Hinzufügen eines Lizenzschlüssels und Generieren eines Lizenznutzungsberichts
- Einrichten von Zertifikaten
- Übereinstimmungsbasierte Konfiguration
- Erfassen von Support-Paketen
- Protokollmeldungen und Fehlercodes
- 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
- Konfigurieren eines externen Load Balancer

## Anzeigen von Überwachungs-Dashboards

Die NSX Manager-Schnittstelle bietet zahlreiche Überwachungs-Dashboards mit Details zu Systemstatus, Netzwerk und Sicherheit sowie Konformitätsberichten. Diese Informationen werden in der NSX Manager-Schnittstelle angezeigt oder sind dort zugänglich, aber sie können gemeinsam auf der Seite **Startseite > Überwachungs-Dashboards** aufgerufen werden.

Sie können über die Startseite der NSX Manager-Schnittstelle auf die Überwachungs-Dashboards zugreifen. Über die-Dashboards können Sie auf die Quellseiten klicken und zugreifen, von denen die Dashboard-Daten abgerufen werden.

### Verfahren

- 1 Melden Sie sich als Administrator bei der NSX Manager-Schnittstelle an.
- 2 Klicken Sie auf **Startseite**, wenn Sie sich noch nicht auf der Startseite befinden.
- 3 Klicken Sie auf „Überwachungs-Dashboards“ und wählen Sie im Dropdown-Menü die gewünschte Dashboard-Kategorie aus.

Auf der Seite werden die Dashboards in den ausgewählten Kategorien angezeigt. Die Dashboard-Grafiken sind farblich codiert, wobei der Farb-Codeschlüssel direkt über den Dashboards angezeigt wird.

- 4 Um auf eine tiefere Detailebene zuzugreifen, klicken Sie auf den Titel des Dashboards oder eines der Elemente des Dashboards, sofern aktiviert.

In den folgenden Tabellen werden die Standard-Dashboards und ihre Quellen beschrieben.

Tabelle 21-1. System-Dashboards

Dashboard	Quellen	Beschreibung
System	<b>System &gt; Appliances &gt; Übersicht</b>	Zeigt den Nutzungsstatus der NSX Manager-Cluster und -Ressourcen (CPU, Arbeitsspeicher, Festplatte) an.
Fabric	<b>System &gt; Fabric &gt; Knoten</b> <b>System &gt; Fabric &gt; Transportzonen</b> <b>System &gt; Fabric &gt; Compute Managers</b>	Zeigt den Status der NSX-T-Fabric einschließlich der Host- und Edge-Transportknoten, Transportzonen und Compute Managers an.
Sicherungen	<b>System &gt; Sichern und Wiederherstellen</b>	Zeigt den Status von NSX-T-Sicherungen an, sofern konfiguriert. Es wird dringend empfohlen, geplante Sicherungen zu konfigurieren, die per Remote-Verbindung auf einer SFTP-Site gespeichert sind.
Endpoint-Schutz	<b>System &gt; Dienstbereitstellungen</b>	Zeigt den Status der Endpoint-Schutzbereitstellung an.

Tabelle 21-2. Dashboards für Netzwerk und Sicherheit

Dashboard	Quellen	Beschreibung
Sicherheit	<b>Bestand &gt; Gruppen</b> <b>Sicherheit &gt; Verteilte Firewall</b>	Zeigt den Status von Gruppen und Sicherheitsrichtlinien an. Eine Gruppe ist eine Sammlung von Arbeitslasten, Segmenten, Segment-Ports und IP-Adressen, in denen Sicherheitsrichtlinien, einschließlich der Regeln für die Ost-West-Firewalls, angewendet werden können.
Gateways	<b>Netzwerk &gt; Tier-0-Gateways</b> <b>Netzwerk &gt; Tier-1-Gateways</b>	Zeigt den Status von Tier-0- und Tier-1-Gateways an.
Segmente	<b>Netzwerk &gt; Segmente</b>	Zeigt den Status von Netzwerksegmenten an.
Load Balancers	<b>Netzwerk &gt; Load Balancing</b>	Zeigt den Status der Load Balancer-VMs an.
VPNs	<b>Netzwerk &gt; VPN</b>	Zeigt den Status von virtuellen privaten Netzwerken an.

Tabelle 21-3. Dashboards für Netzwerk und Sicherheit – Erweitert

Dashboard	Quellen	Beschreibung
Load Balancers	<b>Netzwerk und Sicherheit – Erweitert &gt; Load Balancers</b>	Zeigt den Status der Load Balancers, virtuellen Load Balancer-Server und Load Balancer-Server-Pools an. Ein Load Balancer kann einen oder mehrere virtuelle Server hosten. Ein virtueller Server ist an einen Serverpool gebunden, der Mitglieder enthält, die Anwendungen hosten.
Firewall	<b>Netzwerk und Sicherheit – Erweitert &gt; Sicherheit &gt; Verteilte Firewall</b> <b>Netzwerk und Sicherheit – Erweitert &gt; Sicherheit &gt; Bridge-Firewall</b> <b>Netzwerk und Sicherheit – Erweitert &gt; Netzwerk &gt; Router</b>	Gibt an, ob die Firewall aktiviert ist und zeigt die Anzahl Richtlinien, Regeln und Ausschlusslistenmitglieder an. <hr/> <b>Hinweis</b> Jedes detaillierte Element, das in diesem Dashboard angezeigt wird, wird von einer bestimmten Unterregisterkarte auf der zitierten Quellseite abgerufen.
VPN	Nicht anwendbar.	Zeigt den Status von virtuellen privaten Netzwerken und die Anzahl der geöffneten IPSec- und L2-VPN-Sitzungen an.
Switching	<b>Netzwerk und Sicherheit – Erweitert &gt; Switching</b>	Zeigt den Status logischer Switches und logischer Ports an, einschließlich VM- und Container-Ports.

Tabelle 21-4. Dashboard für Konformitätsbericht

Spalte	Beschreibung
Code für Nicht-Konformität	Zeigt den jeweiligen Code für die Nicht-Konformität an.
Beschreibung	Spezifische Ursache des nicht Nicht-Konformitätsstatus.
Ressourcenname	Die NSX-T-Ressource (Knoten, Switch und Profil) der Nicht-Konformität.
Ressourcentyp	Ressourcentyp der Ursache.
Betroffene Ressourcen	Anzahl der betroffenen Ressourcen. Klicken Sie auf den Zahlenwert, um eine Liste anzuzeigen.

Weitere Informationen zu jedem Konformitätsberichtscode finden Sie unter [Codes für Compliance-Statusberichte](#).

## Nutzung und Kapazität von Objektkategorien anzeigen

Sie können die Nutzung und Kapazität verschiedener Objektkategorien in Ihrer NSX-T Data Center-Umgebung anzeigen. Sie können auch Warnungen festlegen, um zu sehen, wann bestimmte Schwellenwerte bei der Nutzung erreicht werden.

Klicken Sie auf eine der folgenden Registerkarten, um die Nutzung und Kapazität verschiedener Objektkategorien anzuzeigen:

### ■ **Netzwerk > Netzwerkübersicht > Kapazität**

- **Sicherheit > Sicherheitsübersicht > Kapazität**
- **Bestand > Bestandsübersicht > Kapazität**
- **System > Systemübersicht > Kapazität**

Sie können auch zu **Planen und Fehler beheben > Konsolidierte Kapazität** navigieren, um alle Objektkategorien auf einer Seite anzuzeigen.

Auf jeder „Kapazität“-Seite werden für jede Objektkategorie die folgenden Informationen angezeigt:

- Maximale Kapazität – dieser Wert basiert auf der Kapazität einer großen Appliance.
- Aktueller Bestand (realisiert) – die Anzahl der Objekte, die erfolgreich erstellt oder konfiguriert wurden. Diese Zahl gibt die NSX Manager-Objekte an, die auf der Registerkarte **Netzwerk und Sicherheit – Erweitert** angezeigt werden. In diesen Objekten können einige enthalten sein, die Sie in den Registerkarten **Netzwerk**, **Sicherheit**, **Bestand** oder **System** erstellen. Zur Angabe des Nutzungsprozentsatzes wird eine farbcodierte Leiste angezeigt. Wenn die Nutzung unterhalb der Warnstufe „Warnung“ liegt, ist die Farbe grün. Wenn die Nutzung über der Warnstufe „Warnung“, aber unterhalb der Warnstufe „Kritisch“ liegt, ist die Farbe orange. Wenn die Nutzung die Warnstufe „Kritisch“ erreicht oder diese übersteigt, ist die Farbe rot.
- Warnstufe „Warnung“ – dies ist die Nutzungsstufe, bei der die oben erwähnte Nutzungsleiste orange ist. Sie können diesen Wert ändern.
- Warnstufe „Kritisch“ – dies ist die Nutzungsstufe, bei der die oben erwähnte Nutzungsleiste rot ist. Sie können diesen Wert ändern.

Wenn Sie den Wert für die Warnstufen „Warnung“ oder „Kritisch“ ändern, können Sie auf **Wiederherstellen** klicken, um zum zuletzt gespeicherten Wert zurückzukehren. Sie können auf **Werte zurücksetzen** klicken, um die Standardwerte für alle Objektkategorien wiederherzustellen.

Auf der Seite „Netzwerkkapazität“ werden die folgenden Objektkategorien angezeigt:

- Logischer Tier-0 Router
- Logischer Tier-1 Router
- Präfixlisten
- Systemweite NAT-Regeln
- DHCP-Server-Instanzen
- Systemweite DHCP-Bereiche und -Pools
- Logische Tier-1 Router mit aktivierter NAT
- Logische Switches
- Systemweite logische Switch Ports

Auf der Seite „Sicherheitskapazität“ werden die folgenden Objektkategorien angezeigt:

- Hosts, bei denen systemweiter Endpoint-Schutz aktiviert ist

- VMs, bei denen systemweiter Endpoint-Schutz aktiviert ist
- Active Directory-Gruppen
- Active Directory-Domänen
- Regeln für die verteilte Firewall
- Regeln für die systemweite Firewall
- Abschnitte der systemweiten Firewall
- Abschnitte der verteilten Firewall

Auf der Seite „Bestandskapazität“ werden die folgenden Objektkategorien angezeigt:

- Netzwerk- und Sicherheitsgruppen
- IP Sets
- Gruppen basierend auf IP Sets
- vCenter-Cluster
- Hypervisor-Hosts

Auf der Seite „Systemkapazität“ werden die folgenden Objektkategorien angezeigt:

- Systemweite virtuelle Schnittstellen
- Edge-Cluster
- Systemweite Edge-Knoten

## 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/mps
```

## 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>

DhcpServer
  POST /dhcp/servers
  PUT /dhcp/servers/<server-id>
  DELETE /dhcp/servers/<server-id>

DhcpStaticBinding
  POST /dhcp/servers/static-bindings
  PUT /dhcp/servers/<server-id>/static-bindings/<binding-id>
  DELETE /dhcp/servers/<server-id>/static-bindings/<binding-id>

DhcpIpPool
  POST /dhcp/servers/ip-pools
  PUT /dhcp/servers/<server-id>/ip-pools/<pool-id>
  DELETE /dhcp/servers/<server-id>/ip-pools/<pool-id>

DnsForwarder
  POST /dns/forwarders
  PUT /dns/forwarders/<forwarder-id>
  DELETE /dns/forwarders/<forwarder-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.

IPSecVPNIKEProfile / IPSecVPNDPDProfile / IPSecVPNTunnelProfile / IPSecVPNLocalEndpoint /

IPSecVPNPeerEndpoint / IPSecVPNService / IPSecVPNSession

Request - GET /vpn/ipsec/sessions/<session-id>/state?request\_id=<request-id>

Response - An instance of IPSecVPNSessionStateDto 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 IPSecVPNService is disabled, IKE itself is down and it does not respond. It will return unknown state in such a case.

DhcpServer

Request - GET /dhcp/servers/<server-id>/state?request\_id=<request-id>

Response - An instance of ConfigurationState.

DhcpStaticBinding

Request - GET /dhcp/servers/<server-id>/static-bindings/<binding-id>/state?

request\_id=<request-id>

Response - An instance of ConfigurationState.

DhcpIpPool

Request - GET /dhcp/servers/<server-id>/ip-pools/<pool-id>/state?request\_id=<request-id>

Response - An instance of ConfigurationState.

DnsForwarder

Request - GET /dns/forwarders/<forwarder-id>/state?request\_id=<request-id>

Response - An instance of ConfigurationState.

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
Objekte mit „Logical“ als Name oder Eigenschaft	Logical
Exakter Name des logischen Switches	display_name:LSP-301
Namen mit Sonderzeichen wie !	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.

## Filtern nach Objektattributen


Wenn Sie Objekte in NSX Manager anzeigen, können Sie diese nach einem oder mehreren der Attribute filtern. Wenn Sie beispielsweise Details von Tier-0-Gateways anzeigen, können Sie nach **Status** filtern und nur die Gateways anzeigen, die **Inaktiv** sind.

Die folgenden Filtertypen sind verfügbar:

- Vordefinierte Filter – eine Liste häufig verwendeter Filter, die Sie auf Ihre Objekte anwenden können.
- Textbasierte Filter – ein Filter basierend auf dem von Ihnen eingegebenen Attributwert. Dieser Filter gilt nur für die Attribute **Name**, **Tag**, **Pfad** und **Beschreibung** der Objekte.
- Attribut-Wert-Paare – ein Dropdown-Menü für Attribute, über das Sie Attribut-Wert-Paare für das Filtern angeben können.

Sie können Objekte entweder anhand mehrerer Attribute eines Objekts oder mehrerer Werte eines einzelnen Attributs filtern. Der Operator „AND“ wird angewendet, wenn Sie mehrere Attribute auswählen, während der Operator „OR“ verwendet wird, wenn Sie mehrere Werte eines einzelnen Attributs angeben.

### 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 der Registerkarte, auf der die Objekte angezeigt werden, die Sie anzeigen möchten.
- 3 Geben Sie die Attribute an, anhand derer Sie die Objekte filtern möchten.
  - Klicken Sie auf  und wählen Sie aus einer Liste vordefinierter Filter aus.
  - Geben Sie einen Wert für die Attribute **Name**, **Tag**, **Pfad** oder **Beschreibung** ein.
  - Wählen Sie ein Attribut aus dem Dropdown-Menü aus und geben Sie einen Wert dafür an.  
Beispiel: **Status: Inaktiv**

Objekte, die Ihren Filterkriterien entsprechen, werden angezeigt.

- 4 (Optional) Klicken Sie auf **Löschen**, um Ihre Filter zurückzusetzen.

## Hinzufügen eines Compute Managers

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

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

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

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

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

### Voraussetzungen

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

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

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

## Verfahren

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

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

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

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

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

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

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

Wenn eine bestehende Registrierung vorhanden ist, wird sie ersetzt.

## Ergebnisse

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

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



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

## 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 das Active Directory mit NSX Manager synchronisiert ist, können Sie Sicherheitsgruppen auf Basis der Benutzeridentität 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. 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 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 die Domäne abzurufen, geben Sie `nbstat -n` in einem Befehlsfenster auf einer Windows-Workstation ein, die Teil einer Domäne ist oder die sich auf einem Domänencontroller befindet. In der lokalen NetBIOS-Namenstabelle ist der Eintrag mit einem Präfix <00> und dem Typ „Gruppe“ der NetBIOS-Name.

Ein Basisdefinierter Name (Basis-DN) ist erforderlich, um eine Active Directory-Domäne hinzuzufügen. Ein-Basis-DN ist der Startpunkt, den ein LDAP-Server bei der Suche nach Benutzerauthentifizierung innerhalb einer Active Directory-Domäne verwendet. Wenn Ihr Domänenname z. B. „corp.local“ lautet, wird der DN für den Basis-DN für Active Directory auf „DC=corp, DC=local“ angegeben.

- 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.

### Voraussetzungen

Das Domänenkonto muss über AD-Leseberechtigung für alle Objekte in der Domänenstruktur verfügen. Das Konto des Ereignisprotokolllesers muss über Leseberechtigungen für Sicherheits-Ereignisprotokolle verfügen.

Wenn ein Cluster von NSX Managern vorhanden ist, müssen alle Knoten den LDAP-Server erreichen können.

### 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 Wenn LDAPS ausgewählt wurde, wählen Sie den von NSX Manager vorgeschlagenen SHA-256-Fingerabdruck aus oder geben Sie einen SHA-256-Fingerabdruck ein.

- 9 Geben Sie unter **Port** die Nummer des LDAP-Servers ein.

Der standardmäßige LDAP-Port 389 und der LDAPS-Port 636 werden für lokale Domänencontroller bei der Active Directory-Synchronisation verwendet und sollten nicht über die Standardwerte bearbeitet werden.

- 10 Geben Sie den **Benutzernamen** und das **Kennwort** eines Active Directory-Kontos ein, das mindestens Lesezugriff auf die Active Directory-Domänen besitzt.
- 11 Klicken Sie auf **Speichern**.
- 12 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.

Wenn Sie die API verwenden, um eine vollständige Synchronisierung manuell zu beenden, nachdem sie gestartet wurde, wird die Synchronisierungsstatistik nicht ordnungsgemäß aktualisiert.

---

**Hinweis** IDFW vertraut auf die Sicherheit und Integrität des Gastbetriebssystems. Ein lokaler Administrator mit böswilligen Absichten hat mehrere Möglichkeiten, die Identität zu manipulieren und die Firewallregeln zu umgehen. Benutzeridentitätsinformationen werden vom Guest Introspection Agent innerhalb der Gast-VMs bereitgestellt. Sicherheitsadministratoren müssen sicherstellen, dass auf jeder Gast-VM der NSX Guest Introspection Agent installiert ist und ausgeführt wird. Angemeldete Benutzer sollten nicht über die Berechtigung zum Entfernen oder Beenden des Agents verfügen.

---

### 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:

Menüelement	Beschreibung
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 NSX Manager- und NSX Edge-Appliance verfügt über drei lokale Konten: admin, audit und root. Sie können zwar das Kennwort für diese Benutzer verwalten, aber keine Benutzer hinzufügen oder löschen.

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.

Standardmäßig laufen Benutzerkennwörter nach 90 Tagen ab. Sie können den Kennwortablauf für jeden Benutzer ändern oder deaktivieren.

Wenn das Kennwort eines lokalen Benutzers auf dem NSX Manager innerhalb von 30 Tagen abläuft, zeigt die NSX Manager-Webschnittstelle eine Benachrichtigung zum Ablauf des Kennworts an. Wenn Sie den Kennwortablauf eines lokalen Benutzers auf 30 Tage oder weniger festlegen, ist die Benachrichtigung immer vorhanden.

Ab NSX-T Data Center 2.5.1 enthält die Benachrichtigung den Link „Kennwort ändern“. Klicken Sie auf den Link, um das Kennwort des lokalen Benutzers über die Webschnittstelle zu ändern.

#### 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 admin 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 admin 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 admin password-expiration
nsx>
```

## Zurücksetzen der Kennwörter einer Appliance

Die folgende Vorgehensweise gilt für NSX Manager-, NSX Edge- und Cloud-Service Manager-Appliances.

**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. Beachten Sie, dass die Synchronisierung des Kennworts mehrere Minuten oder länger dauern kann.

Wenn Sie den `admin`- oder den `audit`-Benutzer umbenannt haben, verwenden Sie den neuen Namen bei den folgenden Verfahren.

Wenn Sie eine Appliance neu starten, wird das GRUB-Startmenü nicht standardmäßig angezeigt. Die folgende Vorgehensweise erfordert die GRUB-Konfiguration für die Anzeige des GRUB-Startmenüs. Weitere Informationen zur GRUB-Konfiguration und zum Ändern des GRUB-`root`-Kennworts finden Sie unter „Konfigurieren von NSX-T Data Center zum Anzeigen des GRUB-Menüs während des Startvorgangs“ im *NSX-T Data Center-Installationshandbuch*.

Wenn Sie NSX-T Data Center 2.5.2 oder höher ausführen und das Kennwort für `root` kennen, das Kennwort für `admin` oder `audit` jedoch vergessen haben, können Sie es mit dem folgenden Verfahren zurücksetzen:

- 1 Melden Sie sich bei der Appliance als `root` an.
- 2 Führen Sie für NSX Edge den Befehl `/etc/init.d/nsx-edge-api-server stop` aus. Führen Sie ansonsten den Befehl `/etc/init.d/nsx-mp-api-server stop` aus.
- 3 Führen Sie zum Zurücksetzen des Kennworts für `admin` den Befehl `passwd admin` aus.
- 4 Führen Sie zum Zurücksetzen des Kennworts für `audit` den Befehl `passwd audit` aus.
- 5 Führen Sie den Befehl `touch /var/vmware/nsx/reset_cluster_credentials` aus.
- 6 Führen Sie für NSX Edge den Befehl `/etc/init.d/nsx-edge-api-server start` aus. Führen Sie ansonsten den Befehl `/etc/init.d/nsx-mp-api-server start` aus.

Wenn Sie das Kennwort des `root`-Benutzers vergessen haben, können Sie es über das folgende Verfahren zurücksetzen. Verwenden Sie das folgende Verfahren auch, wenn Sie NSX-T Data Center 2.5.0 oder 2.5.1 ausführen und das Kennwort für `admin` und `audit` zurücksetzen möchten. Wenn Sie NSX-T Data Center 2.5.2 oder höher ausführen, können Sie mit dem obigen Verfahren das Kennwort für `admin` oder `audit` zurücksetzen, nachdem Sie das Kennwort für `root` zurückgesetzt haben.

#### Verfahren

- 1 Stellen Sie eine Verbindung mit der Appliance-Konsole her.
- 2 Starten Sie das System neu.
- 3 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.
- 4 Drücken Sie **e**, um das Menü zu bearbeiten.  
  
Geben Sie den Benutzernamen (`root`) und das GRUB-Kennwort für `root` ein (nicht identisch mit dem `root`-Benutzer der Appliance).
- 5 Halten Sie den Cursor auf der Ubuntu-Auswahl.
- 6 Drücken Sie **e**, um die ausgewählte Option zu bearbeiten.
- 7 Suchen Sie nach der Zeile, die mit `linux` beginnt.
- 8 Wenn Sie NSX-T Data Center 2.5.0 oder 2.5.1 ausführen, führen Sie die folgenden Schritte aus:
  - a Entfernen Sie alle Optionen nach `root=UUID=<ID number>` und fügen nach der UUID `rw single init=/bin/bash` hinzu.
  - b Drücken Sie zum Starten auf **Strg+X**.

- c Drücken Sie die Eingabetaste, wenn die Protokollmeldungen stoppen.  
Sie sehen die Aufforderung `root@ (none) :/#`.
  - d 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.
  - e Geben Sie das neue Passwort ein und bestätigen Sie es durch nochmalige Eingabe.
  - f Wenn Sie das Kennwort auf einem NSX Manager zurücksetzen, führen Sie den Befehl `touch /var/vmware/nsx/reset_cluster_credentials` aus.
  - g Führen Sie den Befehl `sync` aus.
  - h Führen Sie den Befehl `reboot -f` aus.
- 9 Wenn Sie NSX-T Data Center 2.5.2 oder höher ausführen, führen Sie die folgenden Schritte aus:
- a Fügen Sie am Ende der Zeile `systemd.wants=PasswordRecovery.service` hinzu.
  - b Drücken Sie zum Starten auf **Strg+X**.
  - c Geben Sie ein neues Kennwort für `root` ein und bestätigen Sie es durch nochmalige Eingabe.  
Nach Abschluss des Startvorgangs können Sie die Änderung des Kennworts überprüfen, indem Sie sich als `root` mit dem neuen Kennwort anmelden.

## 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. Auf dem vIDM-Host führt der Befehl `openssl` eine ältere OpenSSL-Version aus. Daher müssen Sie den Befehl `openssl1` auf dem 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, per SSH als Benutzer **sshuser** beim vIDM-Host oder bei einem Server an, der den vIDM-Host anpingen kann.
- 2 Führen Sie einen der folgenden Befehle aus, um den Fingerabdruck des vIDM-Hosts abzurufen.
  - Wenn Sie beim vIDM-Host angemeldet sind, führen Sie den Befehl `openssl1` aus, um den Fingerabdruck abzurufen:

```
openssl1 s_client -connect <FQDN of vIDM host>:443 < /dev/null 2> /dev/null | openssl
x509 -sha256 -fingerprint -noout -in /dev/stdin
```

Wenn beim Ausführen des Befehls ein Fehler angezeigt wird, müssen Sie möglicherweise `openssl1` mit dem Befehl `sudo` ausführen, d. h. `sudo openssl1 ...`.



- Wenn Sie bei einem Server angemeldet sind, der den vIDM-Host anpingen kann, führen Sie den Befehl `openssl` 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. Bei der vIDM-Bereitstellung kann es sich um einen eigenständigen vIDM-Host oder einen vIDM-Cluster handeln.

Der vIDM-Host oder alle vIDM-Cluster-Komponenten sollten über ein von einer Zertifizierungsstelle 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 Domännennamen (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.

Wenn NSX-T-API-Zugriff erforderlich ist, muss eine der folgenden Konfigurationen wahr sein:

- vIDM verfügt über ein bekanntes, von der Zertifizierungsstelle signiertes Zertifikat.
- vIDM hat das Connector-CA-Zertifikat auf der vIDM-Dienstseite als vertrauenswürdig eingestuft.

- vIDM verwendet den ausgehenden Connector-Modus.

---

**Hinweis** NSX Manager und vIDM müssen sich in derselben Zeitzone befinden. Die empfohlene Vorgehensweise ist die Verwendung von UTC.

Sie müssen Ihre DNS-Server so konfigurieren, dass sie über PTR-Datensätze verfügen, wenn Sie keine virtuelle IP oder einen externen Load Balancer verwenden. (Dies bedeutet, dass der Manager mit der physischen IP-Adresse oder dem FQDN des Knotens konfiguriert ist).

Wenn Sie vIDM so konfigurieren, dass er in einen externen Load Balancer integriert wird, müssen Sie die Sitzungspersistenz im Load Balancer aktivieren, um Probleme zu vermeiden, wie Seiten, die nicht geladen werden, oder Benutzer, die unerwartet abgemeldet werden.

Wenn es sich bei der vIDM-Bereitstellung um einen vIDM-Cluster handelt, muss der vIDM-Load Balancer für die SSL-Beendigung und die erneute Verschlüsselung konfiguriert werden.

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://<csm-ip-address>/login.jsp?local=true` separat bei CSM anmelden.

---

### Voraussetzungen

- Stellen Sie sicher, dass Sie den Zertifikatfingerabdruck vom vIDM-Host oder vom vIDM-Load Balancer haben, je nach Typ der vIDM-Bereitstellung (ein eigenständiger vIDM-Host oder ein vIDM-Cluster). Der Befehl zum Abrufen des Fingerabdrucks ist in beiden Fällen identisch. 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-Workspace-ONE-Access/3.3/idm-administrator/GUID-AD4B6F91-2D68-48F2-9212-5B69D40A1FAE.html>. Wenn Sie den Client erstellen, müssen Sie nur Folgendes durchführen:
  - Legen Sie für das Feld **Zugriffstyp** die Option **Service-Client-Token** fest.
  - Geben Sie eine Client-ID an.
  - Erweitern Sie das Feld **Erweitert** und klicken Sie auf **Gemeinsamen geheimen Schlüssel generieren**.

- Klicken Sie auf **Hinzufügen**.

---

**Hinweis zu NSX Cloud** Wenn Sie NSX Cloud verwenden, stellen Sie außerdem sicher, dass CSM als OAuth-Client für vIDM 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 oder des vIDM-Load Balancers, je nach Typ der vIDM-Bereitstellung (ein eigenständiger vIDM-Host oder ein vIDM-Cluster).
<b>OAuth-Client-ID</b>	Die ID, die beim Registrieren von NSX Manager für vIDM erstellt wird.
<b>OAuth-Client-Secret</b>	Der geheime Schlüssel, der beim Registrieren von NSX Manager für vIDM erstellt wird.
<b>SSL-Fingerabdruck</b>	Der Certificate Thumbprint 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.

## Validieren der VMware Identity Manager-Funktionalität

Nach dem Konfigurieren von VMware Identity Manager validieren Sie die Funktionalität. Sofern VMware Identity Manager nicht ordnungsgemäß konfiguriert und validiert ist, erhalten einige Benutzer beim Anmeldeversuch möglicherweise die Fehlermeldung „Nicht autorisiert“ (Fehlercode 98).

Sofern VMware Identity Manager nicht ordnungsgemäß konfiguriert und validiert ist, erhalten einige Benutzer beim Anmeldeversuch möglicherweise die Fehlermeldung „Nicht autorisiert“ (Fehlercode 98).

### Verfahren

1 Erstellen Sie eine Base64-Kodierung des Benutzernamens und des Kennworts.

Führen Sie den folgenden Befehl aus, um die Kodierung abzurufen und das nachgestellte „\n“-Zeichen zu entfernen. Beispiel:

```
echo -n 'sfadmin@ad.node.com:password1234!' | base64 | tr -d '\n'
c2ZhZG1pbkZhZC5ub2RlLmNvbTpwYXNzd29yZDEyMzQhCg==
```

2 Stellen Sie sicher, dass jeder Benutzer einen API-Aufruf für jeden Knoten durchführen kann.

Verwenden Sie einen curl-Befehl für die Remote-Autorisierung: `curl -k -H 'Authorization: Remote <base64 encoding string>' https://<node FQDN>/api/v1/node/aaa/auth-policy`.  
Beispiel:

```
curl -k -H 'Authorization: Remote c2ZhZG1pbkZhZC5ub2RlLmNvbTpwYXNzd29yZDEyMzQhCg==' /
https://tmgr1.cptroot.com/api/v1/node/aaa/auth-policy
```

Dadurch werden die Autorisierungsrichtlinieneinstellungen zurückgegeben, z. B.:

```
{
  "_schema": "AuthenticationPolicyProperties",
  "_self": {
    "href": "/node/aaa/auth-policy",
    "rel": "self"
  },
  "api_failed_auth_lockout_period": 900,
  "api_failed_auth_reset_period": 900,
  "api_max_auth_failures": 5,
  "cli_failed_auth_lockout_period": 900,
  "cli_max_auth_failures": 5,
  "minimum_password_length": 12
}
```

Wenn der Befehl keinen Fehler zurückgibt, funktioniert VMware Identity Manager ordnungsgemäß. Es sind keine weiteren Schritte erforderlich. Wenn der curl-Befehl einen Fehler zurückgibt, ist der Benutzer möglicherweise gesperrt.

**Hinweis** Kontosperrungsrichtlinien werden festgelegt und knotenweise erzwungen. Wenn ein Knoten im Cluster einen Benutzer gesperrt hat, ist dies für andere Knoten möglicherweise nicht der Fall.

### 3 So setzen Sie eine Benutzersperre auf einem Knoten zurück:

- a Rufen Sie die Autorisierungsrichtlinie mit dem lokalen NSX Manager-Admin-Benutzer ab:

```
curl -k -u 'admin:<password>' https://nsxmgr/api/v1/node/aaa/auth-policy
```

- b Speichern Sie die Ausgabe in einer JSON-Datei im aktuellen Arbeitsverzeichnis.  
c Ändern Sie die Datei, um die Einstellungen für den Sperrzeitraum zu ändern.

Viele der Standardeinstellungen wenden z. B. Sperr- und Reset-Zeiträume von 900 Sekunden an. Ändern Sie diese Werte, um das sofortige Zurücksetzen zu aktivieren, z. B.:

```
{
  "_schema": "AuthenticationPolicyProperties",
  "_self": {
    "href": "/node/aaa/auth-policy",
    "rel": "self"
  },
  "api_failed_auth_lockout_period": 1,
  "api_failed_auth_reset_period": 1,
  "api_max_auth_failures": 5,
  "cli_failed_auth_lockout_period": 1,
  "cli_max_auth_failures": 5,
  "minimum_password_length": 12
}
```

- d Wenden Sie die Änderung auf den betroffenen Knoten an.

```
curl -k -u 'admin:<password>' -H 'Content-Type: application/json' -d \
@<modified_policy_setting.json> https://nsxmgr/api/v1/node/aaa/auth-policy
```

- e (Optional) Setzen Sie die Einstellungsdateien der Autorisierungsrichtlinie auf die vorherigen Einstellungen zurück.

Dadurch sollte das Sperrproblem behoben werden. Wenn Sie weiterhin Remote-Authentifizierungs-API-Aufrufe durchführen können, sich aber weiterhin nicht über den Browser anmelden können, hat der Browser möglicherweise einen ungültigen Cache oder ein ungültiges Cookie gespeichert. Löschen Sie den Cache und die Cookies und versuchen Sie es erneut.

## 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 time.nist.gov
server pool.ntp.org
server time.is dynamic
restrict 192.168.100.0 netmask 255.255.255.0 nomodify notrap
```

- 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
- 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 21-5. Rollen und Berechtigungen](#) und [Tabelle 21-6. Rollen und Berechtigungen für erweiterte Netzwerke und Sicherheit](#) zeigen 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
- 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 21-5. Rollen und Berechtigungen**

Vorgang	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud	VPN Adm	GI Adm	NI Adm
Netzwerk > Tier-0-Gateways	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
Netzwerk > Netzwerkschnittstelle	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R



Tabelle 21-5. 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
Netzwerk > statische Netzwerkrouten	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
Netzwerk > lokale Dienste	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
Netzwerk > statische ARP-Konfiguration	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
Netzwerk > Segmente	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
Netzwerk > Segmente > Segmentprofile	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
Netzwerk > IP-Adresspools	FA	R	FA	FA	R	R	FA	R	R	R	Keine	Keine	Keine
Netzwerk-Weiterleitungsrichtlinie	FA	R	FA	R	FA	R	FA	R	Keine	Keine	Keine	Keine	Keine
Netzwerk > DNS	FA	R	FA	FA	R	R	FA	R	R	R	Keine	Keine	Keine
Netzwerk > Load Balancing	FA	R	Keine	Keine	R	Keine	FA	R	FA	R	Keine	Keine	Keine
Netzwerk > NAT	FA	R	FA	R	FA	R	FA	R	R	R	Keine	Keine	Keine

Tabelle 21-5. 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
Netzwerk->VPN	FA	R	FA	R	FA	R	FA	R	Keine	Keine	FA	Keine	Keine
Netzwerk > IPv6-Profile													
Sicherheit > Verteilte Firewall	FA	R	R	R	FA	R	FA	R	R	R	R	R	R
Sicherheit > Gateway-Firewall	FA	R	R	R	FA	R	FA	R	Keine	Keine	Keine	Keine	FA
Sicherheit > Netzwerk-Introspektion	FA	R	R	R	R	R	FA	R	Keine	Keine	Keine	Keine	FA
Sicherheit > Regeln für Endpunkt-Schutz	FA	R	R	R	R	R	FA	R	Keine	Keine	Keine	FA	Keine
Bestand > Kontextprofile	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
Planen und Fehler beheben > Port-Mirroring	FA	R	FA	R	R	R	FA	R	Keine	Keine	Keine	Keine	Keine

Tabelle 21-5. 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
Planen und Fehler beheben > Port-Mirroring-Bindung	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
Planen und Fehler beheben > Überwachungsprofilbindung	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
Planen und Fehler beheben > Firewall-IPFIX-Profil	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
Planen und Fehler beheben > Switch-IPFIX-Profil	FA	R	FA	R	R	R	FA	R	R	R	R	R	R
System > Fabric > Knoten > Hosts	FA	R	R	R	R	R	R	R	Keine	Keine	Keine	Keine	Keine
System > Fabric > Knoten > Knoten	FA	R	FA	R	FA	R	R	R	R	R	Keine	Keine	Keine

Tabelle 21-5. 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
System > Fabric > Knoten > Edges	FA	R	FA	R	R	R	R	R	Keine	Keine	Keine	Keine	Keine
System > Fabric > Knoten > Edge- Cluster	FA	R	FA	R	R	R	R	R	Keine	Keine	Keine	Keine	Keine
System > Fabric > Knoten > Bridges	FA	R	FA	R	R	R	Keine	Keine	R	R	Keine	Keine	Keine
System > Fabric > Knoten > Transportknoten	FA	R	R	R	R	R	R	R	R	R	Keine	Keine	Keine
System > Fabric > Knoten > Tunnel	R	R	R	R	R	R	R	R	R	R	Keine	Keine	Keine
System > Fabric > Profile > Uplink- Profile	FA	R	R	R	R	R	R	R	R	R	Keine	Keine	Keine
System > Fabric > Profile > Edge- Clusterprofile	FA	R	FA	R	R	R	R	R	R	R	Keine	Keine	Keine

Tabelle 21-5. 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
System > Fabric > Profile > Konfiguration	FA	R	Keine	Keine	Keine	Keine	R	R	Keine	Keine	Keine	Keine	Keine
System > Fabric > Transportzonen > Transportzonen	FA	R	R	R	R	R	R	R	R	R	Keine	Keine	Keine
System > Fabric > Transportzonen > Transportzonen profile	FA	R	R	R	R	R	R	R	Keine	Keine	Keine	Keine	Keine
System > Fabric > Compute Managers	FA	R	R	R	R	R	R	R	Keine	Keine	Keine	R	R
System > Zertifikate	FA	R	Keine	Keine	FA	R	Keine	Keine	FA	R	FA	Keine	Keine
System > Dienstbereitstellungen > Dienstinstanzen	FA	R	R	R	FA	R	FA	R	Keine	Keine	Keine	FA	FA

Tabelle 21-5. 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
System > Dienstprogramm me > Support-Paket	FA	R	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine
System > Dienstprogramm me > Sicherheit	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 > Rollenzuweisungen	FA	R	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine
System > Active Directory	FA	R	FA	R	FA	FA	R	R	R	R	R	R	R
System > Benutzer > Konfiguration	FA	R	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine

Tabelle 21-5. 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
System > Lizenz	FA	R	R	R	R	R	Keine	Keine	Keine	Keine	Keine	Keine	Keine
System > Systemadministration	FA	R	R	R	R	R	R	R	Keine	Keine	Keine	Keine	Keine
Benutzerdefinierte Dashboard-Konfiguration	FA	R	R	R	R	R	FA	R	R	R	R	R	R
System > Lebenszyklusverwaltung > Migrieren	FA	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine

Tabelle 21-6. Rollen und Berechtigungen für erweiterte Netzwerke und Sicherheit

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 > Port-Mirrorin	FA	R	FA	R	R	R	FA	R	Keine	Keine	Keine	Keine	Keine
Tools > IPFIX	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R

Tabelle 21-6. Rollen und Berechtigungen für erweiterte Netzwerke und Sicherheit (Fortsetzung)

Vorgang	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud	VPN Adm	GI Adm	NI Adm
Firewall > Verteilte Firewall > Allgemein	FA	R	R	R	FA	R	FA	R	Keine	Keine	Keine	Keine	R
Firewall > Verteilte Firewall > Konfiguration	FA	R	R	R	FA	R	FA	R	Keine	Keine	Keine	Keine	Keine
Firewall > Edge-Firewall	FA	R	R	R	FA	R	FA	R	Keine	Keine	Keine	Keine	FA
Routing > Router	FA	R	FA	FA	R	R	FA	R	R	R	R	Keine	R
Routing > NAT	FA	R	FA	R	FA	R	FA	R	R	R	Keine	Keine	Keine
DHCP > Serverprofile	FA	R	FA	R	Keine	Keine	FA	R	Keine	Keine	Keine	Keine	Keine
DHCP > Server	FA	R	FA	R	Keine	Keine	FA	R	Keine	Keine	Keine	Keine	Keine
DHCP > Relay-Profile	FA	R	FA	R	Keine	Keine	FA	R	Keine	Keine	Keine	Keine	Keine
DHCP > Relay-Dienste	FA	R	FA	R	Keine	Keine	FA	R	Keine	Keine	Keine	Keine	Keine
DHCP > Metadaten- Proxys	FA	R	FA	R	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine
IPAM	FA	R	FA	FA	R	R	Keine	Keine	R	R	Keine	Keine	Keine



Tabelle 21-6. Rollen und Berechtigungen für erweiterte Netzwerke und Sicherheit (Fortsetzung)

Vorgang	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud	VPN Adm	GI Adm	NI Adm
Switching > Switches	FA	R	FA	FA	R	R	FA	R	R	R	R	Keine	R
Switching > Ports	FA	R	FA	FA	R	R	FA	R	R	R	R	Keine	R
Switching > Switching-Profile	FA	R	FA	FA	R	R	FA	R	R	R	Keine	Keine	Keine
Netzwerk > Load Balancers	FA	R	Keine	Keine	R	Keine	FA	R	FA	R	Keine	Keine	Keine
Load Balancing > Profile > SSL-Profile	FA	R	Keine	Keine	FA	R	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
Bestand > IP-Pools	FA	R	FA	R	Keine	Keine	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

Tabelle 21-6. Rollen und Berechtigungen für erweiterte Netzwerke und Sicherheit (Fortsetzung)

Vorgang	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud	VPN Adm	GI Adm	NI Adm
Bestand > Virtuelle Maschinen	R	R	R	R	R	R	R	R	R	R	R	R	R
Bestand > Virtuelle Maschinen > Konfigurieren von Tags	FA	Keine	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 Durch Aktivieren von **NSX-Konfigurationsänderung erkennen** wird eine nicht geplante vollständige Konfigurationssicherung ausgelöst, wenn sie laufzeitbezogene oder nicht konfigurationsbezogene Änderungen oder eine Änderung der Benutzerkonfiguration erkennt.

Sie können das Intervall zwischen den Sicherungen festlegen, die durch die Konfigurationsänderungen ausgelöst werden. Die Standardeinstellung ist 5 Minuten.

---

**Hinweis** Diese Option kann potenziell eine große Anzahl von Sicherungen generieren. Verwenden Sie sie mit Vorsicht.

---

- 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 die Sicherung auf einer neuen NSX Manager-Appliance wiederherstellen.

Wurde zum Zeitpunkt der Sicherung ein NSX Manager-Cluster verwendet, sollte 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.

---

**Wichtig** Wenn im NSX Manager-Cluster noch Knoten verfügbar sind, müssen Sie sie ausschalten, bevor Sie die Wiederherstellung starten.

---



## 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.
- Identifizieren Sie die wiederherzustellende Sicherung, indem Sie das Verfahren unter [Auflisten der verfügbaren Sicherungen](#) anwenden. Notieren Sie sich die IP-Adresse oder den FQDN des NSX Manager-Knotens, der die Sicherung vorgenommen hat.
- Wenn Sie die NSX Manager-Knoten für die Veröffentlichung ihres FQDN konfigurieren, müssen Sie die Forward- und Reverse-Sucheinträge für die NSX Manager-Knoten auf dem DNS-Server konfigurieren.

## Verfahren

- 1 Schalten Sie alle Knoten in dem NSX Manager-Cluster aus, den Sie wiederherstellen.
- 2 Installieren Sie einen neuen NSX Manager-Knoten, auf dem die Sicherung wiederhergestellt werden soll.

- Wenn die Sicherungsliste für die von Ihnen wiederhergestellte Sicherung eine IP-Adresse enthält, müssen Sie den neuen NSX Manager-Knoten mit derselben IP-Adresse bereitstellen. Konfigurieren Sie den NSX Manager-Knoten nicht, um den zugehörigen FQDN zu veröffentlichen.

```
2019-01-22;09:01:52 10.196.196.77 35163642-6623-8f6d-7af0-52e03f16faed
```

- Wenn die Sicherungsliste für die von Ihnen wiederhergestellte Sicherung einen FQDN enthält, müssen Sie den neuen NSX Manager-Knoten mit diesem FQDN konfigurieren. (Weitere Informationen finden Sie im Abschnitt „Veröffentlichen von FQDNs von NSX Manager“ unter dem Thema „NSX Manager-Installation“ im *Installationshandbuch für NSX-T Data Center*). Wenn der neue NSX Manager-Knoten jedoch eine andere IP-Adresse als die ursprüngliche aufweist, müssen Sie die Forward- und Reverse-Sucheinträge des DNS-Server für den NSX Manager-Knoten mit der neuen IP-Adresse aktualisieren.

```
2019-01-22;09:16:43 nsxmgr.example.com 41893642-597b-915f-5117-7da576df4ff2
```

Sobald der neue NSX Manager-Knoten ausgeführt wird und online ist, können Sie mit der Wiederherstellung fortfahren.

- 3 Melden Sie sich über Ihren Browser mit Administratorrechten bei dem neuen NSX Manager an.
- 4 Wählen Sie **System > Sichern und Wiederherstellen**.
- 5 Klicken Sie auf die Registerkarte **Wiederherstellen**.
- 6 Um den Sicherungsdateiserver zu konfigurieren, klicken Sie auf **Bearbeiten**.

- 7 Geben Sie die IP-Adresse oder den Hostnamen ein.
- 8 Ändern Sie die Portnummer, falls erforderlich.  
Die Standardeinstellung ist 22.
- 9 Um sich beim Server anzumelden, geben Sie den Benutzernamen und das Kennwort ein.
- 10 Geben Sie im Textfeld **Zielverzeichnis** den absoluten Verzeichnispfad ein, unter dem die Sicherungen gespeichert werden.
- 11 Geben Sie die zur Verschlüsselung der Sicherungsdaten verwendete Passphrase ein.
- 12 Geben Sie den SSH-Fingerabdruck des Servers ein, auf dem die Sicherungen gespeichert sind.
- 13 Klicken Sie auf **Speichern**.
- 14 Wählen Sie eine Sicherung aus.
- 15 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.

Nach dem Fertigstellen des Wiederherstellungsvorgangs 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 ermitteln, ob beim Wiederherstellen von Clustern oder Knoten ein Fehler aufgetreten ist, indem Sie die Protokolldateien prüfen. Führen Sie `get log-file syslog` aus, um die Systemprotokolldatei anzuzeigen und nach den Zeichenfolgen `Cluster-Wiederherstellung fehlgeschlagen` und `Knotenwiederherstellung fehlgeschlagen` zu suchen.

Führen Sie zum Neustarten des Managers den Befehl `restart service manager` aus.

Führen Sie zum Neustarten des Managers den Befehl `reboot` aus.

- 16** Wenn Sie nur einen Knoten bereitgestellt haben, können Sie, sobald der wiederhergestellte NSX Manager-Knoten aktiv und funktionsfähig ist, zusätzliche Knoten bereitstellen, um einen NSX Manager-Cluster zu bilden.

Anweisungen hierzu finden Sie im *Installationshandbuch für NSX-T Data Center*.

- 17** Nachdem der neue NSX Manager-Cluster bereitgestellt wurde, löschen Sie die ursprünglichen NSX Manager-Cluster-VMs, die Sie in Schritt 1 heruntergefahren haben.

Sie müssen außerdem die Zertifikate auf dem zweiten und dritten Knoten des Clusters ersetzen.

## Ergebnisse

Wenn Sie nach der Sicherung einen Compute Manager hinzugefügt haben und versuchen, den Compute Manager nach der Wiederherstellung erneut hinzuzufügen, erhalten Sie eine Fehlermeldung mit dem Hinweis darauf, dass die Registrierung fehlgeschlagen ist. 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.

## Sicherung und Wiederherstellung während Upgrades

Die Management Plane reagiert während des Upgrade-Vorgangs nicht mehr und Sie müssen eine Sicherung wiederherstellen, die während des Upgrades erstellt wurde.

### Problem

Der Upgrade-Koordinator wurde aktualisiert und die Management Plane reagiert nicht mehr. Sie verfügen über eine Sicherung, die während des Upgrades erstellt wurde.

### Lösung

- 1** Stellen Sie den Knoten Ihrer Management Plane mit derselben IP-Adresse bereit, aus der die Sicherung erstellt wurde.
- 2** Laden Sie das Upgrade-Paket hoch, das Sie zu Beginn des Upgrade-Vorgangs verwendet haben.
- 3** Führen Sie ein Upgrade des Upgrade-Koordinators durch.
- 4** Stellen Sie die Sicherungsaufnahme während des Upgrade-Vorgangs wieder her.
- 5** Laden Sie bei Bedarf ein neues Upgrade-Paket hoch.
- 6** Setzen Sie den Upgrade-Vorgang fort.

## 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	ADDRESS	PORT	FQDN	UUID	IP
HTTPS	10.160.71.225	443	ychin-nsxmanager-ob-12065118-1-F5	5c8d01f1-f3ee-4f94-b517-a093d8fbfad3	
CONTROLLER	10.160.71.225	-	ychin-nsxmanager-ob-12065118-1-F5	06fd0574-69c0-432e-a8af-53d140dbef8f	
CLUSTER_BOOT_MANAGER	10.160.71.225	-	ychin-nsxmanager-ob-12065118-1-F5	da8d535e-7a0c-4dd8-8919-d88bdde006b8	
DATASTORE	10.160.71.225	-	ychin-nsxmanager-ob-12065118-1-F5	3c9c4ec1-afef-47bd-aadb-1ed6a5536bc4	
MANAGER	10.160.71.225	9000	ychin-nsxmanager-ob-12065118-1-F5	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:		
IP	UUID	FQDN
10.160.71.225	43cd0642-275c-af1d-fe46-1f5200f9e5f9	ychin-nsxmanager-ob-12065118-1-F5
10.160.93.240	8ebb0642-201e-6a5f-dd47-a1e38542e672	ychin-nsxmanager-ob-12065118-2-F5
10.160.76.33	2e7e0642-df4a-b2ec-b9e8-633d1469f1ea	ychin-nsxmanager-ob-12065118-3-F5
	UP	

## Herunterfahren und Einschalten des NSX Manager-Clusters

Wenn Sie den NSX Manager-Cluster herunterfahren müssen, gehen Sie wie folgt vor.

### Verfahren

- 1 Wenn Sie einen NSX Manager-Cluster herunterfahren möchten, fahren Sie die Manager-Knoten einzeln nacheinander herunter. Sie können sich bei der Befehlszeilenschnittstelle (CLI) eines Manager-Knotens als `admin` anmelden und den Befehl `shutdown` ausführen oder die VM des Manager-Knotens aus vCenter Server herunterfahren.

Stellen Sie sicher, dass die VM in vCenter Server ausgeschaltet ist, bevor Sie mit der nächsten fortfahren.

- 2 Wenn Sie einen NSX Manager-Cluster einschalten möchten, schalten Sie die Manager-Knoten einzeln nacheinander in vCenter Server ein.

Stellen Sie sicher, dass der Knoten aktiv ist und ausgeführt wird, bevor Sie mit dem nächsten fortfahren.

## 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 der Registerkarte **Systeme** auf **NSX-Verwaltungsknoten**.
 

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.

## Hinzufügen und Entfernen eines ESXi-Host-Transportknotens zu und von vCenter Servern

Sie können einen ESXi-Host-Transportknoten von einem vCenter Server (VC) auf einen anderen und auch von einem NSX Manager-Cluster in einen anderen verschieben.

### Szenario 1: VC1 ist verbunden mit NSX Manager-Cluster 1 und VC2 ist verbunden mit NSX Manager-Cluster 2

Angenommen, der ESXi-Host-Transportknoten ESX1 befindet sich in VC1, dann können Sie ihn in VC2 verschieben, indem Sie die folgenden Schritte ausführen:

- 1 Deinstallieren Sie NSX von ESX1.
- 2 Verschieben Sie ESX1 zu VC2.
- 3 Wenden Sie ein Transportknotenprofil auf ESX1 an.

## Szenario 2: Sowohl VC1 als auch VC2 sind verbunden mit dem NSX Manager-Cluster

Angenommen, der ESXi-Host-Transportknoten ESX1 befindet sich in VC1, dann können Sie ihn in VC2 verschieben, indem Sie die folgenden Schritte ausführen:

- 1 Deinstallieren Sie NSX von ESX1.
- 2 Verschieben Sie ESX1 zu VC2.
- 3 Wenden Sie ein Transportknotenprofil auf ESX1 an.

## Szenario 3: VC1 ist verbunden mit NSX Manager-Cluster 1

Angenommen, der ESXi-Host-Transportknoten ESX1 befindet sich in VC1, dann können Sie ihn als eigenständigen Host in den NSX Manager-Cluster 2 verschieben, indem Sie die folgenden Schritte ausführen:

- 1 Deinstallieren Sie NSX von ESX1.
- 2 Fügen Sie ESX1 zum NSX Manager-Cluster 2 hinzu.

## Ersetzen eines NSX Edge-Transportknotens in einem NSX Edge-Cluster

Sie können einen NSX Edge-Transportknoten in einem NSX Edge-Cluster mithilfe der NSX Manager-Benutzeroberfläche oder -API ersetzen.

### Ersetzen eines NSX Edge-Transportknotens über die NSX Manager-Benutzeroberfläche

Das folgende Verfahren beschreibt das Ersetzen eines NSX Edge-Transportknotens in einem NSX Edge-Cluster über die NSX Manager-Benutzeroberfläche. Sie können den Edge-Transportknoten unabhängig davon ersetzen, ob er ausgeführt wird oder nicht.

Sofern der zu ersetzende Edge-Knoten nicht ausgeführt wird, kann der neue Edge-Knoten dieselbe Management-IP-Adresse und TEP-IP-Adresse besitzen. Wenn der zu ersetzende Edge-Knoten ausgeführt wird, muss der neue Edge-Knoten eine andere Management-IP-Adresse und TEP-IP-Adresse besitzen.

#### Voraussetzungen

Machen Sie sich mit der Vorgehensweise zum Installieren eines NSX Edge-Knotens vertraut, verbinden Sie den Edge-Knoten mit der Management Plane und erstellen Sie einen NSX Edge-Transportknoten. Weitere Informationen finden Sie im *Installationshandbuch zu NSX-T Data Center*.

## Verfahren

- 1 Wenn Sie möchten, dass der neue Edge-Transportknoten dieselben Konfigurationen wie der zu ersetzende Edge-Transportknoten besitzt, führen Sie den folgenden API-Aufruf aus, um die Konfigurationen zu finden:

```
GET https://<nsx-manager-IP>/api/v1/transport-nodes/<tn-id>
```

- 2 Befolgen Sie die im *Installationshandbuch für NSX-T Data Center* beschriebenen Verfahren, um einen Edge-Transportknoten zu installieren und zu konfigurieren.

Wenn Sie möchten, dass dieser Edge-Transportknoten dieselben Konfigurationen wie der zu ersetzende Edge-Transportknoten aufweist, verwenden Sie die Konfigurationen, die Sie in Schritt 1 erhalten haben.

- 3 Wählen Sie in NSX Manager **System > Fabric > Knoten > Edge-Cluster** aus.
- 4 Wählen Sie einen Edge-Cluster aus, indem Sie auf das Kontrollkästchen in der ersten Spalte klicken.
- 5 Klicken Sie auf **Aktionen > Edge-Clustermitglied ersetzen**.

Es wird empfohlen, den zu ersetzenden Transportknoten in den Wartungsmodus zu versetzen. Wenn der Transportknoten nicht ausgeführt wird, können Sie diese Empfehlung ignorieren.

- 6 Wählen Sie den zu ersetzenden Knoten in der Dropdown-Liste aus.
- 7 Wählen Sie den Ersatzknoten in der Dropdown-Liste aus.
- 8 Klicken Sie auf **Speichern**.

## Ersetzen eines NSX Edge-Transportknotens mithilfe der API

Im folgenden Verfahren wird beschrieben, wie Sie einen NSX Edge-Transportknoten in einem NSX Edge-Cluster mithilfe der NSX-T-API ersetzen. Sie können den Edge-Transportknoten unabhängig davon ersetzen, ob er ausgeführt wird oder nicht.

Sofern der zu ersetzende Edge-Knoten nicht ausgeführt wird, kann der neue Edge-Knoten dieselbe Management-IP-Adresse und TEP-IP-Adresse besitzen. Wenn der zu ersetzende Edge-Knoten ausgeführt wird, muss der neue Edge-Knoten eine andere Management-IP-Adresse und TEP-IP-Adresse besitzen.

### Voraussetzungen

Machen Sie sich mit der Vorgehensweise zum Installieren eines NSX Edge-Knotens vertraut, verbinden Sie den Edge-Knoten mit der Management Plane und erstellen Sie einen NSX Edge-Transportknoten. Weitere Informationen finden Sie im *Installationshandbuch zu NSX-T Data Center*.

## Verfahren

- 1 Wenn Sie möchten, dass der neue Edge-Transportknoten dieselben Konfigurationen wie der zu ersetzende Edge-Transportknoten besitzt, führen Sie den folgenden API-Aufruf aus, um die Konfigurationen zu finden:

```
GET https://<nsx-manager-IP>/api/v1/transport-nodes/<tn-id>
```

- 2 Befolgen Sie die im Installationshandbuch für NSX-T Data Center beschriebenen Verfahren, um einen Edge-Transportknoten zu installieren und zu konfigurieren.

Wenn Sie möchten, dass dieser Edge-Transportknoten dieselben Konfigurationen wie der zu ersetzende Edge-Transportknoten aufweist, verwenden Sie die Konfigurationen, die Sie in Schritt 1 erhalten haben.

- 3 Führen Sie einen API-Aufruf durch, um die ID des neuen Transportknotens und den zu ersetzenden Transportknoten abzurufen. Das Feld `id` enthält die Transportknoten-ID. Beispiel:

```
GET https://<nsx-manager-IP>/api/v1/transport-nodes
...
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "73cb00c9-70d0-4808-abfe-a12a43251133",
  "display_name": "TN-edgenode-01a",
  ...
  {
    "resource_type": "TransportNode",
    "description": "",
    "id": "890f0e3c-aa81-46aa-843b-8ac25fe30bd3",
    "display_name": "TN-edgenode-03a",
```

- 4 Führen Sie einen API-Aufruf aus, um die ID des NSX Edge-Clusters abzurufen. Das Feld `id` enthält die NSX Edge-Cluster-ID. Rufen Sie die Mitglieder des NSX Edge-Clusters vom Array `members` ab. Beispiel:

```
GET https://<nsx-manager-IP>/api/v1/edge-clusters
....
{
  "resource_type": "EdgeCluster",
  "description": "",
  "id": "9a302df7-0833-4237-af1f-4d826c25ad78",
  "display_name": "Edge-Cluster-1",
  ...
  "members": [
    {
      "member_index": 0,
      "transport_node_id": "73cb00c9-70d0-4808-abfe-a12a43251133"
    },
    {
```

```

    "member_index": 1,
    "transport_node_id": "e5d17b14-cdeb-4e63-b798-b23a0757463b"
  }
],

```

- 5 Führen Sie einen API-Aufruf aus, um einen Transportknoten in einem NSX Edge-Cluster zu ersetzen. Der `member_index` muss mit dem Index des zu ersetzenden Transportknotens übereinstimmen.

Beispiel: Der Transportknoten `TN-edgenode-01a (73cb00c9-70d0-4808-abfe-a12a43251133)` ist fehlgeschlagen und wird durch den Transportknoten `TN-edgenode-03a (890f0e3c-aa81-46aa-843b-8ac25fe30bd3)` im NSX Edge-Cluster `Edge-Cluster-1 (9a302df7-0833-4237-af1f-4d826c25ad78)` ersetzt.

```

POST http://<nsx-manager-IP>/api/v1/edge-clusters/9a302df7-0833-4237-af1f-4d826c25ad78?
action=replace_transport_node
{
  "member_index": 0,
  "transport_node_id" : "890f0e3c-aa81-46aa-843b-8ac25fe30bd3"
}

```

## Wiederherstellen von NSX-T, wenn vCenter Server verlorenght und nicht wiederhergestellt werden kann

Wenn vCenter Server (VC) verlorenght und nicht wiederhergestellt werden kann (möglicherweise weil keine Sicherung vorliegt oder die Sicherung beschädigt ist), verwenden Sie das folgende Verfahren, um die NSX-T-Umgebung wiederherzustellen, nachdem Sie VC erneut bereitstellen.

Der neue VC muss denselben FQDN und dieselbe IP-Adresse wie der ursprüngliche VC aufweisen. Außerdem müssen dieselben Cluster vorhanden sein, die dieselben Hosts enthalten. Seien Sie vorsichtig mit Hosts, die über eingeschaltete VMs verfügen, wenn Sie sie zu VC hinzufügen. Stellen Sie sicher, dass sie zu den richtigen Clustern und nicht zum VC-Datencenter hinzugefügt werden.

### Compute Manager

Löschen Sie in NSX Manager den alten Computermanager. Fügen Sie dann den neuen VC als Computermanager hinzu.

### Host-Transportknoten

In NSX Manager werden die Hosts in den richtigen VC-Clustern angezeigt. Es ist keine Aktion erforderlich.

## Edge-Knoten

Sie müssen Edge-Knoten ersetzen, die über die NSX Manager-Benutzeroberfläche bereitgestellt wurden.

- 1 Befolgen Sie das Verfahren in [Ersetzen eines NSX Edge-Transportknotens über die NSX Manager-Benutzeroberfläche](#), um einen Edge-Knoten zu ersetzen.
- 2 Stellen Sie sicher, dass die Gateways (oder logischen Router) und Tunnel auf der neuen Edge-VM konfiguriert sind.
- 3 Löschen Sie den alten Edge-Knoten, indem Sie zu **System > Fabric > Edge-Transportknoten** wechseln. Wählen Sie den Edge-Knoten aus und klicken Sie auf **Aktionen > Löschen**. Fehler wie „Ausschalten fehlgeschlagen“ können ignoriert werden.
- 4 Schalten Sie in VC die alte Edge-VM aus und löschen Sie sie.
- 5 Wiederholen Sie die obigen Schritte für jeden Edge-Knoten.

## NSX Manager

Sie müssen NSX Manager ersetzen, die über die NSX Manager-Benutzeroberfläche bereitgestellt wurden. In der Regel werden die zweiten und dritten NSX Manager auf diese Weise bereitgestellt.

- 1 Melden Sie sich bei der Benutzeroberfläche des ersten NSX Managers an.
- 2 Navigieren Sie zu **System > Appliances** und wählen Sie den dritten NSX Manager aus. Klicken Sie auf **Aktionen > Löschen**. Dies schlägt fehl, da die Manager-VM nicht ausgeschaltet werden kann. Die Option „Löschen erzwingen“ ist jetzt verfügbar. Wählen Sie **Aktionen > Löschen erzwingen** aus.
- 3 Wenn der erzwungene Löschvorgang nicht funktioniert, gehen Sie wie folgt vor:
  - a Melden Sie sich bei der CLI des ersten NSX Managers an.
  - b Führen Sie den Befehl `get cluster status` aus, um die UID des dritten NSX Managers abzurufen.
  - c Führen Sie den Befehl `detach node <node-uid>` aus, um den dritten NSX Manager vom Cluster zu trennen.
  - d Führen Sie den folgenden API-Aufruf aus, um das Löschen des dritten NSX Manager zu erzwingen:

```
POST : https://<nsx-manager-1>/api/v1/cluster/nodes/deployments/<node-uid>?
      action=delete&force_delete=true
```

- 4 Schalten Sie in VC den dritten NSX Manager aus und löschen Sie ihn.
- 5 Stellen Sie einen neuen NSX Manager mit derselben Konfiguration wie den dritten NSX Manager bereit.
- 6 Wiederholen Sie die obigen Schritte, um den zweiten NSX Manager zu löschen.
- 7 Stellen Sie zwei neue NSX Manager bereit.



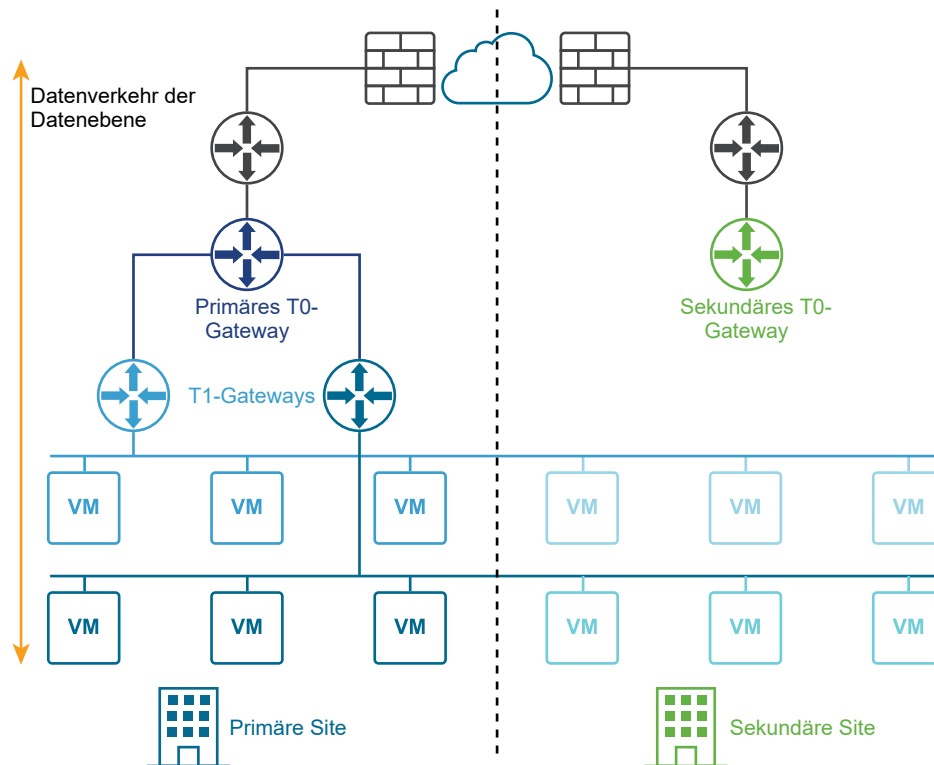
## Bereitstellung von NSX-T Data Center für mehrere Sites

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:

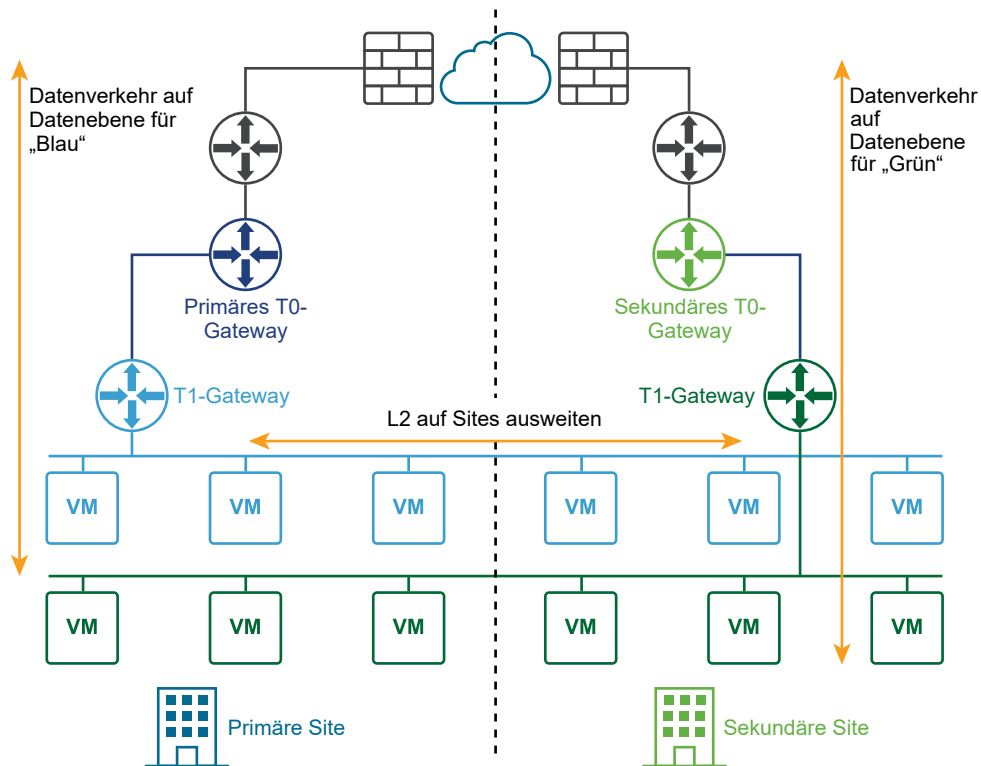
- Notfallwiederherstellung
- Aktiv-Aktiv

Das folgende Diagramm veranschaulicht eine Bereitstellung für die 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.



Sie können zwei Sites für die automatische oder manuelle/skriptbasierte Wiederherstellung der Management Plane und der Data Plane bereitstellen.

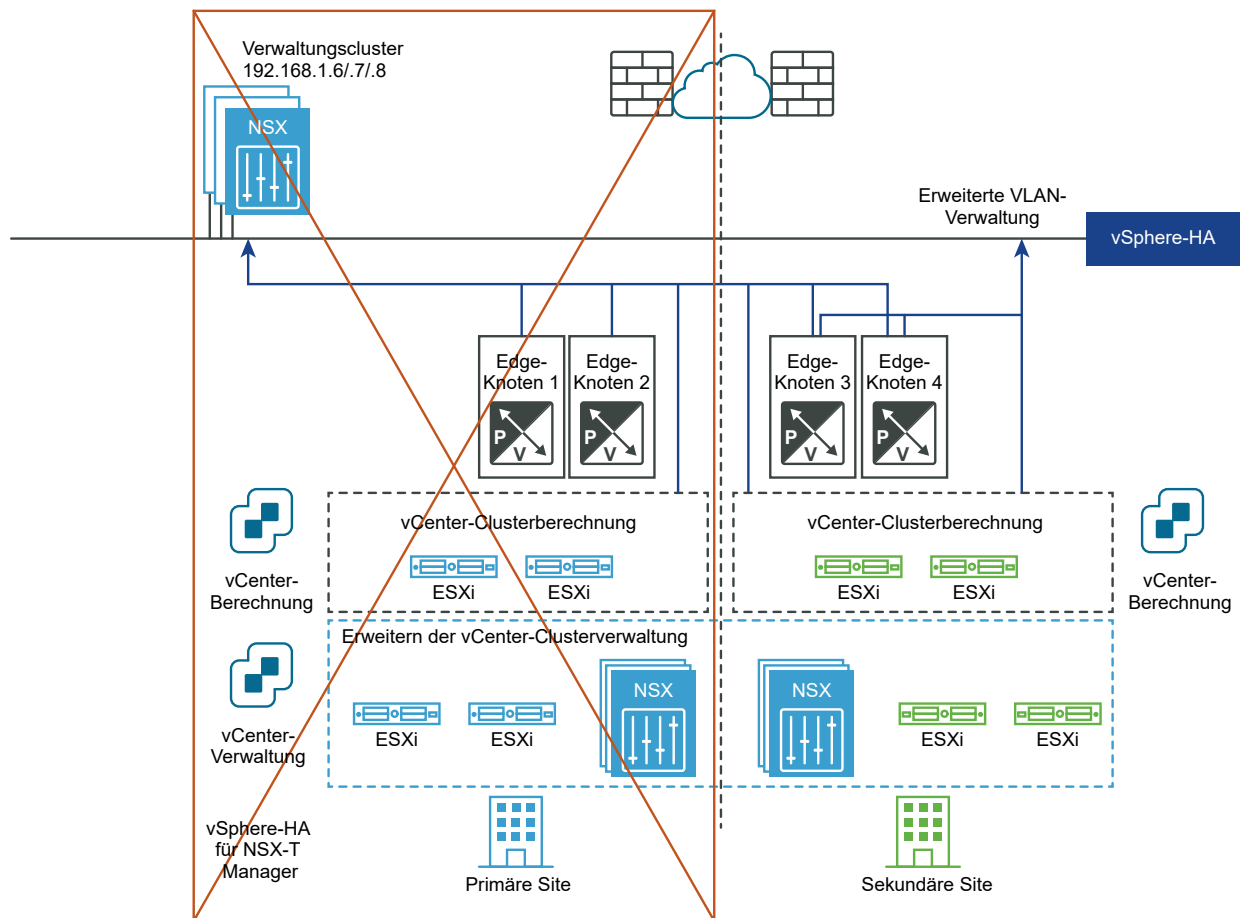
## Automatische Wiederherstellung der Management Plane

Anforderungen:

- Ein ausgeweiteter vCenter-Cluster mit Konfiguration siteübergreifende HA.
- Ein ausgeweitetes Management-VLAN.

Der NSX Manager-Cluster wird im Management-VLAN bereitgestellt und befindet sich physisch in der primären Site. Wenn eine primäre Site ausfällt, werden die NSX Manager auf der sekundären Site von vSphere HA neu gestartet. Alle Transportknoten werden automatisch erneut mit den neu gestarteten NSX Managern verbunden. Dieser Vorgang dauert ca. 10 Minuten. Während dieser Zeit ist die Management Plane nicht verfügbar, aber die Data Plane wird nicht beeinträchtigt.

Das folgende Diagramm veranschaulicht die automatische Wiederherstellung der Management Plane.



## Automatische Wiederherstellung der Data Plane

Anforderungen:

- Die maximale Latenz zwischen Edge-Knoten beträgt 10 ms.
- Der HA-Modus für das Tier-0-Gateway muss „Aktiv/Standby“ sein, und der Failover-Modus muss „Vorbeugend“ sein.

Hinweis: Der Failover-Modus des Ebene-1-Gateways kann präventiv oder nicht präventiv sein.

### Konfigurationsschritte:

- Erstellen Sie mithilfe der API Fehlerdomänen für die beiden Sites, z. B. `FD1A-Preferred_Site1` und `FD2A-Preferred_Site1`. Setzen Sie den Parameter `preferred_active_edge_services` auf `true` für die primäre Site und setzen Sie ihn auf `false` für die sekundäre Site.

```
POST /api/v1/failure-domains
{
  "display_name": "FD1A-Preferred_Sitel",
  "preferred_active_edge_services": "true"
}
```

```
POST /api/v1/failure-domains
{
  "display_name": "FD2A-Preferred_Site1",
  "preferred_active_edge_services": "false"
}
```

- Konfigurieren Sie mithilfe der API einen Edge-Cluster, der über die beiden Sites ausgedehnt ist. Beispielsweise verfügt der Cluster über die Edge-Knoten `EdgeNode1A` und `EdgeNode1B` auf der primären Site und die Edge-Knoten `EdgeNode2A` und `EdgeNode2B` auf der sekundären Site. Die aktiven Tier-0- und Tier-1-Gateways werden auf `EdgeNode1A` und `EdgeNode1B` ausgeführt. Die Tier-0- und Tier-1-Gateways im Standby werden auf `EdgeNode2A` und `EdgeNode2B` ausgeführt.
- Verknüpfen Sie mithilfe der API jeden Edge-Knoten mit der Fehlerdomäne für die Site. Rufen Sie zuerst die `GET /api/v1/transport-nodes/<transport-node-id>-API` auf, um die Daten über den Edge-Knoten abzurufen. Verwenden Sie das Ergebnis der GET-API als Eingabe für die `PUT /api/v1/transport-nodes/<transport-node-id>-API`, wobei die zusätzliche Eigenschaft `failure_domain_id` entsprechend festgelegt ist. Beispiel:

```
GET /api/v1/transport-nodes/<transport-node-id>
Response:
{
  "resource_type": "TransportNode",
  "description": "Updated NSX configured Test Transport Node",
  "id": "77816de2-39c3-436c-b891-54d31f580961",
  ...
}

PUT /api/v1/transport-nodes/<transport-node-id>
{
  "resource_type": "TransportNode",
  "description": "Updated NSX configured Test Transport Node",
  "id": "77816de2-39c3-436c-b891-54d31f580961",
  ...
  "failure_domain_id": "<UUID>",
}
```

- Konfigurieren Sie mithilfe der API den Edge-Cluster, um Knoten basierend auf der Fehlerdomäne zuzuteilen. Rufen Sie zuerst die `GET /api/v1/edge-clusters/<edge-cluster-id>-API` auf, um die Daten über den Edge-Cluster abzurufen. Verwenden Sie das Ergebnis der GET-API als Eingabe für die `PUT /api/v1/edge-clusters/<edge-cluster-id>-API`, wobei die zusätzliche Eigenschaft `allocation_rules` entsprechend festgelegt ist. Beispiel:

```
GET /api/v1/edge-clusters/<edge-cluster-id>
Response:
{
  "_revision": 0,
  "id": "bf8d4daf-93f6-4c23-af38-63f6d372e14e",
  "resource_type": "EdgeCluster",
  ...
}
```

```

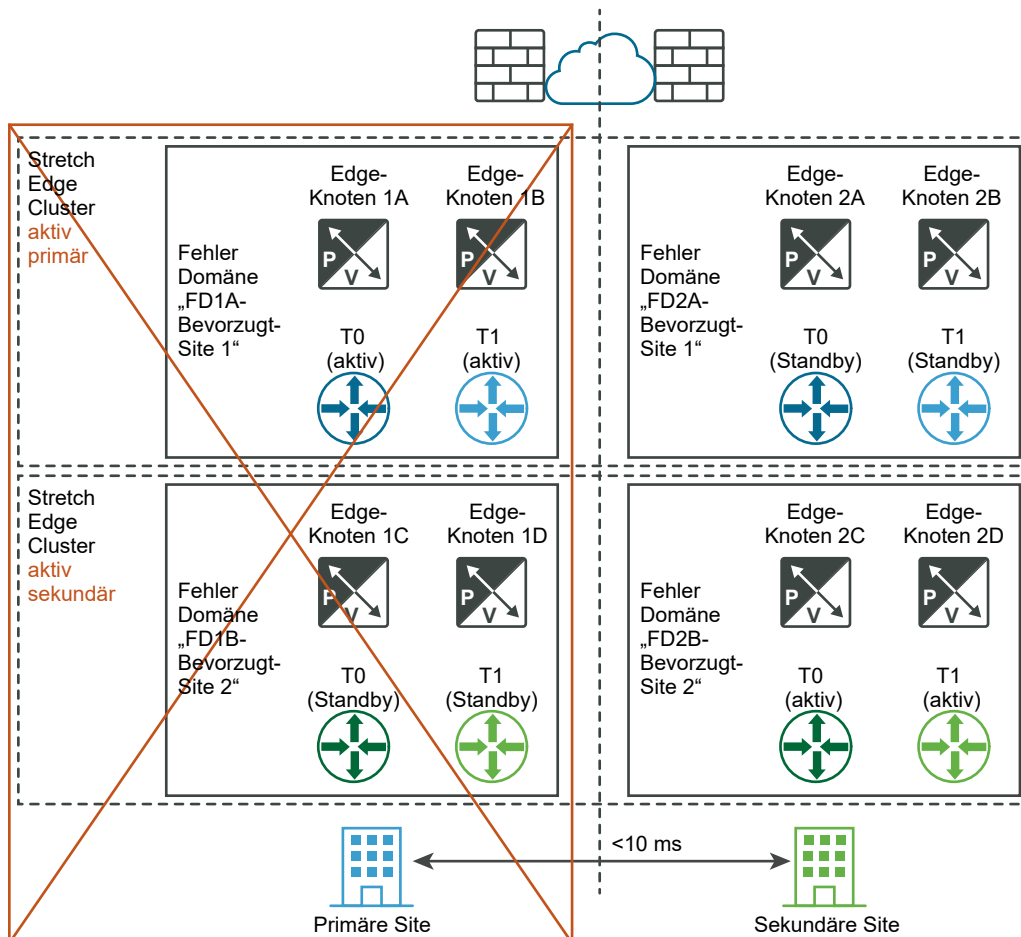
PUT /api/v1/edge-clusters/<edge-cluster-id>
{
  "_revision": 0,
  "id": "bf8d4daf-93f6-4c23-af38-63f6d372e14e",
  "resource_type": "EdgeCluster",
  ...
  "allocation_rules": [
    {
      "action": {
        "enabled": true,
        "action_type": "AllocationBasedOnFailureDomain"
      }
    }
  ],
}

```

- Erstellen Sie Tier-0- und Tier-1-Gateways mithilfe der API oder der NSX Manager-Benutzeroberfläche.

Wenn ein Edge-Knoten in der primären Site ausfällt, werden die auf diesem Knoten gehosteten Tier-0- und Tier-1-Gateways zu einem Edge-Knoten auf der sekundären Site migriert.

Das folgende Diagramm veranschaulicht die automatische Wiederherstellung der Data Plane.



## Manuelle/skriptbasierte Wiederherstellung der Management Plane

Anforderungen:

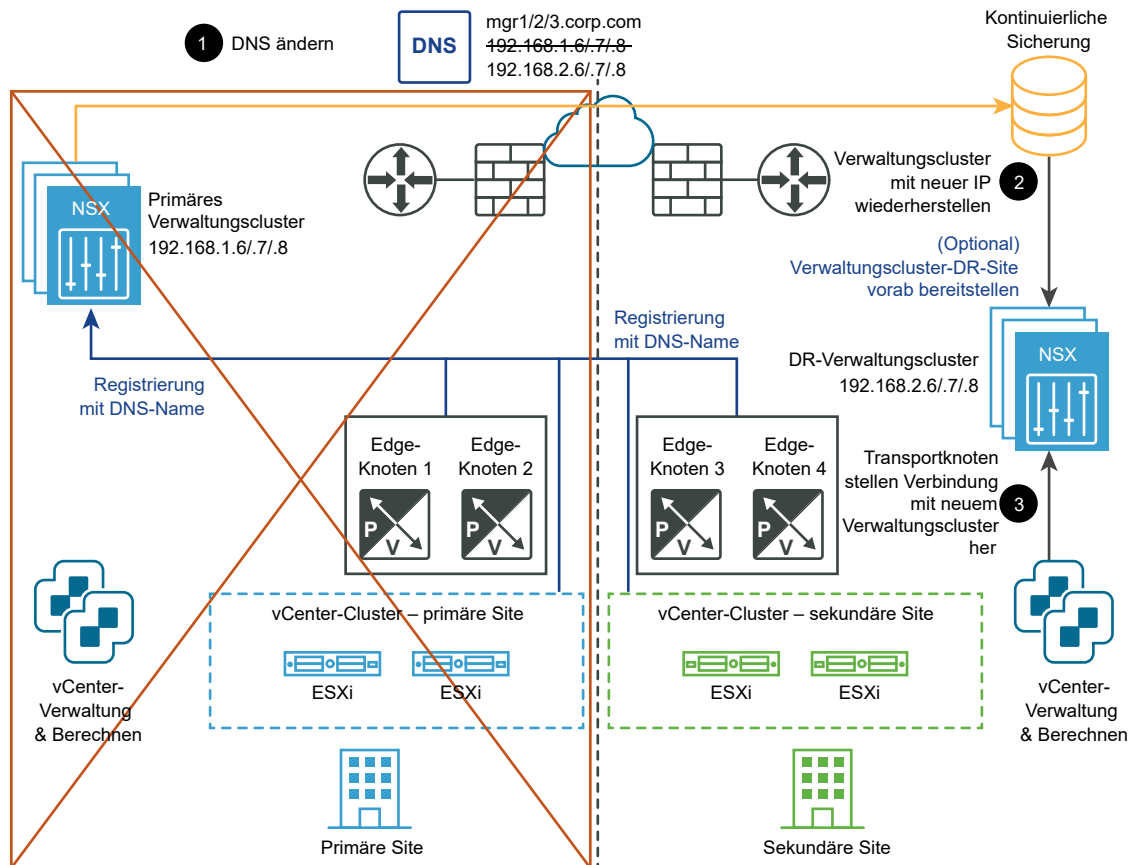
- DNS für NSX Manager mit einer kurzen TTL (z. B. 5 Minuten).
- Kontinuierliche Sicherung.

Weder vSphere HA noch ein ausgeweitetes Management-VLAN sind erforderlich. NSX-T-Manager müssen mit einem DNS-Namen mit einer kurzen TTL verknüpft sein. Alle Transportknoten (Edge-Knoten und Hypervisoren) müssen mit ihrem DNS-Namen eine Verbindung mit dem NSX Manager herstellen. Um Zeit zu sparen, können Sie optional einen NSX Manager-Cluster auf der sekundären Site vorab installieren.

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.

Das folgende Diagramm veranschaulicht die manuelle/skriptbasierte Wiederherstellung der Management Plane.



## Manuelle/skriptbasierte Wiederherstellung der Data Plane

Anforderung:

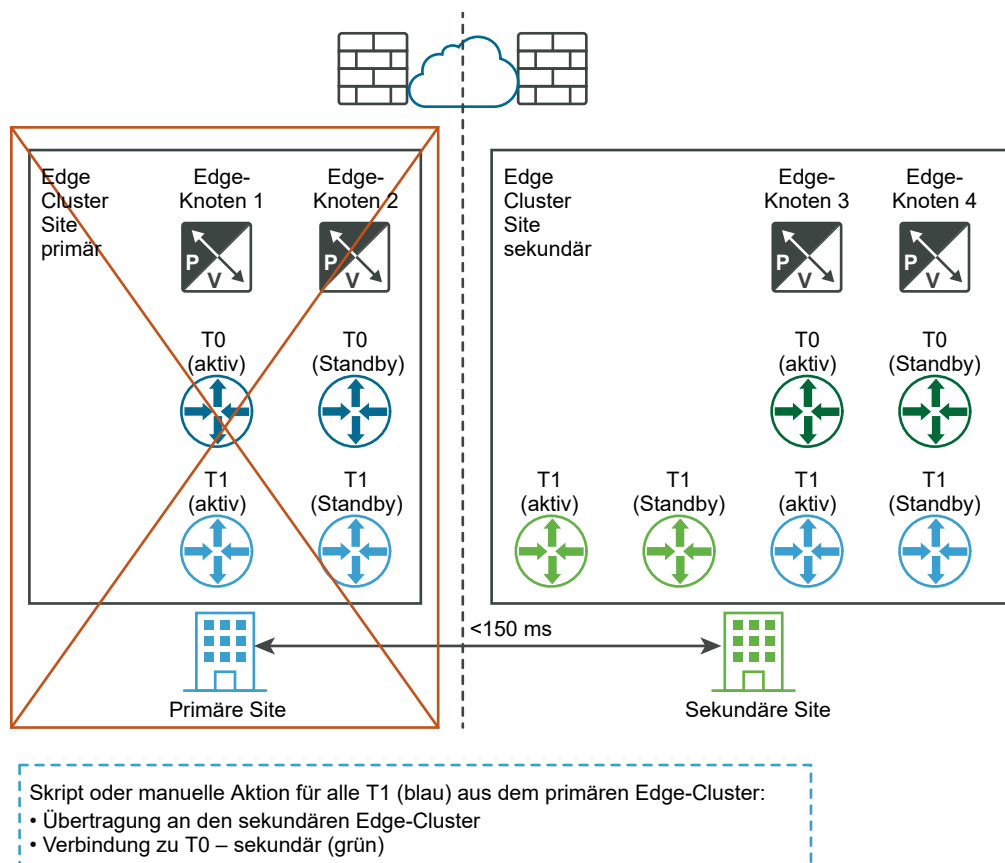
- Die maximale Latenz zwischen Edge-Knoten beträgt 150 ms.

Die Edge-Knoten können VMs oder Bare Metal sein. Das Tier-0-Gateway kann „Aktiv/Standby“ oder „Aktiv/Aktiv“ sein. Edge-Knoten-VMs können auf unterschiedlichen vCenter-Servern installiert werden. vSphere HA ist nicht erforderlich.

Die Wiederherstellung erfolgt mit den folgenden Schritten:

- Erstellen Sie ein Tier-0-Gateway in Standby auf einem vorhandenen Edge-Cluster in der Notfallwiederherstellungs-Site (DR-Site).
- Verschieben Sie mithilfe der API die Tier-1-Gateways, die mit einem Tier-0-Gateway verbunden sind, zum Tier-0-Gateway in der DR-Site.
- Verschieben Sie die eigenständigen Tier-1-Gateways mithilfe der API in die DR-Site.
- Verschieben Sie mithilfe der API die Schicht-2-Bridges auf die DR-Site.

Das folgende Diagramm veranschaulicht die manuelle/skriptbasierte Wiederherstellung der Data Plane.



## 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.
- Der HA-Modus für das Tier-0-Gateway muss „Aktiv/Standby“ sein, und der Failover-Modus muss „Vorbeugend“ sein.

### 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 Software für die Notfallwiederherstellungsberechnung muss NSX-T Data Center unterstützen, z. B. VMware SRM 8.1.2 oder höher.

## 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 21-7. Befehle und API-Anforderungen für die Systemkonfiguration.

Aufgabe	Befehlszeile (NSX Manager und NSX Edge)	API-Anforderung (nur NSX Manager)
Systemzeitzone festlegen	<code>set timezone &lt;timezone&gt;</code>	PUT <a href="https://&lt;nsx-mgr&gt;/api/v1/node">https://&lt;nsx-mgr&gt;/api/v1/node</a>
NTP-Server festlegen	<code>set ntp-server &lt;ntp-server&gt;</code>	PUT <a href="https://&lt;nsx-mgr&gt;/api/v1/node/services/ntp">https://&lt;nsx-mgr&gt;/api/v1/node/services/ntp</a>
DNS-Server festlegen	<code>set name-servers &lt;dns-server&gt;</code>	PUT <a href="https://&lt;nsx-mgr&gt;/api/v1/node/network/name-servers">https://&lt;nsx-mgr&gt;/api/v1/node/network/name-servers</a>
DNS-Suchdomäne festlegen	<code>set search-domains &lt;domain&gt;</code>	PUT <a href="https://&lt;nsx-mgr&gt;/api/v1/node/network/search-domains">https://&lt;nsx-mgr&gt;/api/v1/node/network/search-domains</a>

## 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:

- NSX Data Center Standard
- NSX Data Center Professional
- NSX Data Center Advanced
- NSX Data Center Enterprise Plus
- NSX Data Center Remote Office Branch Office (ROBO)
- NSX Advanced (verfügbar ab NSX-T Data Center 2.5.1)
- NSX Enterprise (verfügbar ab NSX-T Data Center 2.5.1)

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 können eine neue Evaluierungslizenz zuweisen, wenn die standardmäßige Evaluierungslizenz vorhanden ist. Die neue Evaluierungslizenz überschreibt die Standard-Evaluierungslizenz. Sie können auch die Zuweisung der nicht Standard-Evaluierungslizenz aufheben. In diesem Fall wird die Standard-Evaluierungslizenz wiederhergestellt.

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.

Wenn Ihre Lizenz innerhalb von 60 Tagen abläuft oder Sie abgelaufen ist, wird nach der Anmeldung bei NSX Manager ein Benachrichtigungsfenster angezeigt, in dem Sie über die Situation informiert werden. Sie können auch auf das Benachrichtigungssymbol in der oberen rechten Ecke des Fensters klicken, um die Benachrichtigung anzuzeigen.

### 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, vCPU und Kern für folgenden Funktionen auf:

- Switching und Routing
- NSX Edge-Load Balancer
- VPN
- DFW
- Kontextsensitive Mikrosegmentierung – Anwendungsidentifizierung
- Kontextsensitive Mikrosegmentierung – Identitäts-Firewall für Remotedesktop-Sitzungshost
- Service Insertion
- Identitätsbasierte Firewall
- Erweiterte Guest Introspection

---

**Hinweis** Die folgenden Funktionen sind für die Version mit Limited Export deaktiviert:

- IPSec-VPN
  - HTTPS-basierter Load Balancer
- 

## 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** aus.
- 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 Zertifikatsdatei 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.
<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** aus.
- 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.
<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.

Option	Beschreibung
<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** aus.

- 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** aus.
- 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.

### 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** aus.
- 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
```

Hinweis: die Zertifikatskette muss in der laut Branchenstandard typischen Reihenfolge 'certificate - intermediate - root' vorliegen.

Weitere Informationen zur API 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
```

Hinweis: die Zertifikatskette muss in der laut Branchenstandard typischen Reihenfolge 'certificate - intermediate - root' vorliegen.

Weitere Informationen zur API 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:

- widerrufene 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** aus.
- 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----- MIIBODCB4zANBgkqhkiG9w0BAQQFADBGMQswCQYDVQQGEwJBVTZEMMAoGA1 UECBMD UUxEMRkwFwYDVQQKEwBNaw5jb20gUHR5LiBMdGQuMQswCQYDVQQLEwJDUz EbMBkG A1UEAxMSU1NMZW51IGRlbW8gc2VydMVFw0wMTAxMTUxNjI2NTdaFw0wMT AyMTQx NjI2NTdaMFwEgIBARcNOTUxMDA5MjMzMjA1WjASAgEDFw05NTEyMDEwMT AwMDBa MBMCAhI0Fw0wMTAxMTUxNjE5NDdaMBMCAhI1Fw0wMTAxMTUxNjIzNDZaMA OGCSqG SIB3DQEBBAUAA0EAHPjQ3M93QOj8Ufi+jZM7Y78TfAzG4jJn/ E6MYBPFVQFY0/Gp UZexfjSVo5CIyySOtYscz8o07avwBxTiMpDEQg== -----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** aus.
- 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.

## Übereinstimmungsbasierte Konfiguration

NSX-T Data Center kann für die Verwendung von mit FIPS 140-2 validierten kryptografischen Modulen zur Ausführung im FIPS-kompatiblen Modus konfiguriert werden. Die Module werden nach FIPS 140-2-Standards vom NIST Cryptographic Module Validation Program (CMVP) validiert.

Alle Ausnahmen von der FIPS-Übereinstimmung können über den Übereinstimmungsbericht abgerufen werden. Weitere Informationen hierzu finden Sie unter [Anzeigen des Übereinstimmungsstatus](#).

Die folgenden validierten Module werden in NSX-T Data Center 2.5 verwendet:

- VMware OpenSSL FIPS Object Module Version 2.0.9: [Zertifikat #2839](#)
- VMware OpenSSL FIPS Object Module Version 2.0.20-vmw: [Zertifikat #3550](#)
- BC-FJA (Bouncy Castle FIPS Java API) Version 1.0.1: [Zertifikat #3152](#)
- VMware's IKE Crypto Module Version 1.1.0: [Zertifikat #3435](#)
- VMware VPN Crypto Module Version 1.0: [Zertifikat #3542](#)

Weitere Informationen zu den kryptografischen Modulen, die VMware anhand des FIPS 140-2-Standards validiert hat, finden Sie hier: <https://www.vmware.com/security/certifications/fips.html>.

Standardmäßig verwendet der Load Balancer Module, für die der FIPS-Modus deaktiviert ist. Sie können den FIPS-Modus für die vom Load Balancer verwendeten Module aktivieren. Weitere Informationen hierzu finden Sie unter [Konfigurieren des globalen FIPS-Übereinstimmungsmodus für den Load Balancer](#).

## Anzeigen des Übereinstimmungsstatus

Sie können einen Compliance-Bericht für NSX-T Data Center-Funktionen anzeigen. Mit dem Bericht können Sie Ihre NSX-T Data Center-Umgebung für die Einhaltung Ihrer IT-Richtlinien und Branchenstandards konfigurieren.

Der Compliance-Bericht enthält Informationen zu jeder nicht konformen Konfiguration.

**Tabelle 21-8. Informationen zum Compliance-Bericht**

Spalte im Compliance-Bericht	Beschreibung	Beispiel
<b>Code für Nichtübereinstimmung</b>	Code zur Identifizierung des Typs der Nichtkonformität.	72301
<b>Beschreibung</b>	Beschreibung des Typs der Nichtkonformität.	Zertifikat ist nicht von der Zertifizierungsstelle signiert.
<b>Ressourcenname</b>	Name oder ID der betroffenen Ressource.	nsx-manager-1
<b>Ressourcentyp</b>	Typ der betroffenen Ressource.	CertificateComplianceReporter
<b>Betroffene Ressourcen</b>	Anzahl der betroffenen Ressourcen. Die Anzahl kann 0 sein, wenn nicht konforme Konfigurationen vorhanden sind, aber die Funktion nicht verwendet wird.	1

Sie können den Bericht auch mit der API abrufen: `GET /policy/api/v1/compliance/status`.

## 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 der **Startseite** auf **Dashboardüberwachung > Compliance-Bericht**.

## Codes für Compliance-Statusberichte

Weitere Informationen zur Bedeutung des Compliance-Statusberichts finden Sie hier.

Tabelle 21-9. Codes für Compliance-Berichte

Code	Beschreibung	Compliance-Statusquelle	Wartung
72001	Verschlüsselung ist deaktiviert.	Dieser Status wird gemeldet, wenn eine VPN-IPSec-Profilkonfiguration <code>NO_ENCRYPTION</code> , <code>NO_ENCRYPTION_AUTH_AES_GMAC_128</code> , <code>NO_ENCRYPTION_AUTH_AES_GMAC_192</code> oder <code>NO_ENCRYPTION_AUTH_AES_GMAC_256</code> <code>encryption_algorithms</code> enthält.  Dieser Status wirkt sich auf IPSec-VPN-Sitzungskonfigurationen aus, die die gemeldeten nicht kompatiblen Konfigurationen verwenden.	Um diesen Status zu standardisieren, fügen Sie ein VPN-IPSec-Profil hinzu, das kompatible Verschlüsselungsalgorithmen verwendet, und nutzen Sie das Profil in allen VPN-Konfigurationen. Siehe <a href="#">Hinzufügen von IPSec-Profilen</a> .
72011	BGP-Meldungen mit Nachbarn umgehen die Integritätsprüfung. Keine Nachrichtenauthentifizierung definiert.	Dieser Status wird gemeldet, wenn für BGP-Nachbarn kein Kennwort konfiguriert ist.  Dieser Status wirkt sich auf die BGP-Nachbarkonfiguration aus.	Um diesen Status zu standardisieren, konfigurieren Sie ein Kennwort für den BGP-Nachbarn und aktualisieren Sie die Tier-0-Gateway-Konfiguration für Verwendung des Kennworts. Siehe <a href="#">Konfigurieren des BGP-Protokolls</a> .
72012	Die Kommunikation mit dem BGP-Nachbarn verwendet eine schwache Integritätsprüfung. MD5 wird für die Nachrichtenauthentifizierung verwendet.	Dieser Status wird gemeldet, wenn die MD5-Authentifizierung für das BGP-Nachbarkennwort verwendet wird.  Dieser Status wirkt sich auf die BGP-Nachbarkonfiguration aus.	Keine Wartung verfügbar, da NSX-T Data Center nur die MD5-Authentifizierung für BGP unterstützt.

Tabelle 21-9. Codes für Compliance-Berichte (Fortsetzung)

Code	Beschreibung	Compliance-Statusquelle	Wartung
72021	SSL-Version 3 wird für die Herstellung einer sicheren Socket-Verbindung verwendet. Es wird empfohlen, TLSv 1.1 oder höher auszuführen und SSLv3 mit Protokollschwächen vollständig zu deaktivieren.	<p>Dieser Status wird gemeldet, wenn SSL-Version 3 im Client-SSL-Profil des Load Balancers im Server-SSL-Profil des Load Balancers oder im HTTPS-Monitor des Load Balancers konfiguriert ist.</p> <p>Dieser Status wirkt sich auf die folgenden Konfigurationen aus:</p> <ul style="list-style-type: none"> <li>■ Load Balancer-Pools, die mit HTTPS-Monitoren verknüpft sind.</li> <li>■ Virtuelle Load Balancer-Server, die mit Client-SSL-Profilen oder Server-SSL-Profilen von Lastausgleichsdiensten verknüpft sind.</li> </ul>	Um diesen Status zu standardisieren, konfigurieren Sie ein SSL-Profil für die Verwendung von TLS 1.1 oder höher und verwenden Sie dieses Profil in allen Load Balancer-Konfigurationen. Siehe <a href="#">Hinzufügen eines SSL-Profiles</a> .
72022	TLS-Version 1.0 wird für die Herstellung einer sicheren Socket-Verbindung verwendet. Es wird empfohlen, TLSv 1.1 oder höher auszuführen und TLSv1.0 mit Protokollschwächen vollständig zu deaktivieren.	<p>Dieser Status wird gemeldet, wenn TLSv1.0 im Client-SSL-Profil des Load Balancers im Server-SSL-Profil des Load Balancers oder im HTTPS-Monitor des Load Balancers konfiguriert ist.</p> <p>Dieser Status wirkt sich auf die folgenden Konfigurationen aus:</p> <ul style="list-style-type: none"> <li>■ Load Balancer-Pools, die mit HTTPS-Monitoren verknüpft sind.</li> <li>■ Virtuelle Load Balancer-Server, die mit Client-SSL-Profilen oder Server-SSL-Profilen von Lastausgleichsdiensten verknüpft sind.</li> </ul>	Um diesen Status zu standardisieren, konfigurieren Sie ein SSL-Profil für die Verwendung von TLS 1.1 oder höher und verwenden Sie dieses Profil in allen Load Balancer-Konfigurationen. Siehe <a href="#">Hinzufügen eines SSL-Profiles</a> .

Tabelle 21-9. Codes für Compliance-Berichte (Fortsetzung)

Code	Beschreibung	Compliance-Statusquelle	Wartung
72023	Es wird eine schwache Diffie-Hellman Group verwendet.	Dieser Fehler wird gemeldet, wenn ein VPN-IPSec-Profil oder eine VPN-IKE-Profilkonfiguration die folgenden Diffie-Hellman Groups enthält: 2, 5, 14, 15 oder 16. Die Gruppen 2 und 5 sind schwache Diffie-Hellman Groups. Die Gruppen 14, 15 und 16 sind keine schwachen Gruppen, aber nicht FIPS-kompatibel. Dieser Status wirkt sich auf IPSec-VPN-Sitzungskonfigurationen aus, die die gemeldeten nicht kompatiblen Konfigurationen verwenden.	Um diesen Status zu standardisieren, konfigurieren Sie die VPN-Profile für die Verwendung der Diffie-Hellman Group 19, 20 oder 21. Siehe <a href="#">Hinzufügen von Profilen</a> .
72024	Die globale FIPS-Einstellung für den Load Balancer ist deaktiviert.	Dieser Fehler wird gemeldet, wenn die globale FIPS-Einstellung für den Load Balancer deaktiviert ist. Dieser Status wirkt sich auf alle Load Balancer-Dienste aus.	Um diesen Status zu standardisieren, aktivieren Sie FIPS für den Load Balancer. Siehe <a href="#">Konfigurieren des globalen FIPS-Übereinstimmungsmodus für den Load Balancer</a> .
72200	Unzureichende wahre Entropie verfügbar.	Dieser Status wird gemeldet, wenn ein Pseudo-Zufallszahlen-Generator zum Generieren von Entropie verwendet wird, anstatt sich auf eine hardwaregenerierte Entropie zu verlassen. Hardwaregenerierte Entropie wird nicht verwendet, da der NSX Manager-Knoten nicht über die erforderliche Hardware-Beschleunigungsunterstützung verfügt, um eine ausreichende wahre Entropie zu erstellen.	Um diesen Status zu standardisieren, müssen Sie möglicherweise neuere Hardware verwenden, um den NSX Manager-Knoten auszuführen. Die neueste Hardware unterstützt diese Funktion.  <b>Hinweis</b> Wenn die zugrunde liegende Infrastruktur virtuell ist, erhalten Sie keine wahre Entropie.

Tabelle 21-9. Codes für Compliance-Berichte (Fortsetzung)

Code	Beschreibung	Compliance-Statusquelle	Wartung
72201	Entropiequelle unbekannt.	Dieser Status wird gemeldet, wenn für den angegebenen Knoten kein Entropiestatus verfügbar ist.	Um diesen Status zu standardisieren, stellen Sie sicher, dass der angegebene Knoten ordnungsgemäß funktioniert.
72301	Zertifikat ist nicht von der Zertifizierungsstelle signiert.	Dieser Status wird gemeldet, wenn eines der NSX Manager-Zertifikate nicht von der Zertifizierungsstelle signiert ist. NSX Manager verwendet die folgenden Zertifikate: <ul style="list-style-type: none"> <li>■ Syslog-Zertifikat.</li> <li>■ API-Zertifikate für die einzelnen NSX Manager-Knoten.</li> <li>■ Für NSX Manager VIP verwendetes Clusterzertifikat.</li> </ul>	Um diesen Status zu standardisieren, installieren Sie von der Zertifizierungsstelle signierte Zertifikate. Siehe <a href="#">Einrichten von Zertifikaten</a> .

## Konfigurieren des globalen FIPS-Übereinstimmungsmodus für den Load Balancer

Es gibt eine globale Einstellung für die FIPS-Übereinstimmung für Load Balancer. Standardmäßig ist die Einstellung deaktiviert, um die Leistung zu verbessern.

Eine Änderung der globalen Konfiguration für die FIPS-Übereinstimmung für Load Balancer wirkt sich auf neue Load Balancer-Instanzen aus, jedoch nicht auf vorhandene Load Balancer-Instanzen.

Wenn die globale Einstellung für FIPS für Load Balancer (`lb_fips_enabled`) auf `true` festgelegt ist, verwenden neue Load Balancer-Instanzen Module, die mit FIPS 140-2 konform sind.

Vorhandene Load Balancer-Instanzen verwenden möglicherweise nicht kompatible Module.

Damit die Änderung für vorhandene Load Balancer wirksam wird, müssen Sie den Load Balancer vom Tier-1-Gateway trennen und erneut anfügen.

Sie können den globalen FIPS-Übereinstimmungsstatus für den Load Balancer mithilfe von `GET /policy/api/v1/compliance/status` überprüfen.

```
...
{
  "non_compliance_code": 72024,
  "description": "Load balancer FIPS global setting is disabled.",
  "reported_by": {
    "target_id": "971ca477-df1a-4108-8187-7918c2f8c3ba",
    "target_display_name": "971ca477-df1a-4108-8187-7918c2f8c3ba",
    "target_type": "FipsGlobalConfig",
```

```

        "is_valid": true
    },
    "affected_resources": [
        {
            "path": "/infra/lb-services/LB_Service",
            "target_id": "/infra/lb-services/LB_Service",
            "target_display_name": "LB_1",
            "target_type": "LBService",
            "is_valid": true
        }
    ]
},
...

```

**Hinweis** Der Übereinstimmungsbericht zeigt die globale Einstellung für die FIPS-Übereinstimmung für den Load Balancer an. Jede angegebene Load Balancer-Instanz kann über einen FIPS-Übereinstimmungsstatus verfügen, der sich von der globalen Einstellung unterscheidet.

## Verfahren

- 1 Rufen Sie die globale FIPS-Einstellung für den Load Balancer ab.

```
GET https://nsx-mgr1/policy/api/v1/infra/global-config
```

Beispielantworttext:

```

{
  "fips": {
    "lb_fips_enabled": false
  },
  "resource_type": "GlobalConfig",
  "id": "global-config",
  "display_name": "global-config",
  "path": "/infra/global-config",
  "relative_path": "global-config",
  "marked_for_delete": false,
  "_create_user": "system",
  "_create_time": 1561225479619,
  "_last_modified_user": "admin",
  "_last_modified_time": 1561937915337,
  "_system_owned": true,
  "_protection": "NOT_PROTECTED",
  "_revision": 2
}

```

- 2 Ändern Sie die globale FIPS-Einstellung für den Load Balancer.

Die globale Einstellung wird verwendet, wenn Sie neue Load Balancer-Instanzen erstellen. Eine Änderung der Einstellung wirkt sich nicht auf vorhandene Load Balancer-Instanzen aus.

```
PUT https://nsx-mgr1/policy/api/v1/infra/global-config
```



Beispielanforderungstext:

```
{
  "fips": {
    "lb_fips_enabled": true
  },
  "resource_type": "GlobalConfig",
  "_revision": 2
}
```

Beispielantworttext:

```
{
  "fips": {
    "lb_fips_enabled": true
  },
  "resource_type": "GlobalConfig",
  "id": "global-config",
  "display_name": "global-config",
  "path": "/infra/global-config",
  "relative_path": "global-config",
  "marked_for_delete": false,
  "_create_user": "system",
  "_create_time": 1561225479619,
  "_last_modified_user": "admin",
  "_last_modified_time": 1561937960950,
  "_system_owned": true,
  "_protection": "NOT_PROTECTED",
  "_revision": 3
}
```

- 3 Wenn Sie möchten, dass vorhandene Load Balancer-Instanzen diese globale Einstellung verwenden, müssen Sie den Load Balancer vom Tier-1-Gateway trennen und erneut anfügen.

**Vorsicht** Das Trennen eines Load Balancer vom Tier-1-Gateway führt zu einer Unterbrechung des Datenverkehrs für die Load Balancer-Instanz.

- Navigieren Sie zu **Netzwerk > Load Balancing**.
- Klicken Sie für den Load Balancer, den Sie trennen möchten, auf das Menü mit den drei Punkten (⋮) und dann auf **Bearbeiten**.
- Klicken Sie auf (✕) und dann auf **Speichern**, um den Load Balancer vom Tier-1-Gateway zu trennen.

Name	Größe	Tier-1-Gateway
LB_1	Klein	TLR1_LR

- d Klicken Sie auf das Menü mit den drei Punkten (⋮) und anschließend auf **Bearbeiten**.
- e Wählen Sie das richtige Gateway aus dem Dropdown-Menü **Tier-1-Gateway** aus und klicken Sie dann auf **Speichern**, um den Load Balancer erneut an das Tier-1-Gateway anzufügen.

## 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 Kontrollkästchen, um die Pakete auf einen Remote-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 zum Senden des Pakets an einen Remote-Dateiserver nicht festgelegt wurde, klicken Sie auf **Herunterladen**, um das Paket herunterzuladen.

Die Paketerfassung schlägt für einen Manager-Knoten möglicherweise fehl, wenn nicht genügend Festplattenspeicher vorhanden ist. Wenn ein Fehler auftritt, überprüfen Sie, ob ältere Support-Pakete auf dem fehlgeschlagenen Knoten vorhanden sind. Melden Sie sich bei der NSX Manager-Benutzeroberfläche des fehlgeschlagenen Manager-Knotens mit seiner IP-Adresse an und initiieren Sie die Paketerfassung von diesem Knoten aus. Wenn Sie von NSX Manager dazu aufgefordert werden, laden Sie das ältere Paket herunter oder löschen Sie es.

# Protokollmeldungen und Fehlercodes

NSX-T Data Center-Komponenten schreiben in Protokolldateien des Verzeichnisses `/var/log`. Auf NSX-T-Appliances und KVM-Hosts sind NSX-Syslog-Meldungen mit RFC 5424 konform. Auf ESXi-Hosts sind die Syslog-Meldungen mit RFC 3164 konform.

## Anzeigen von Protokollen

Auf NSX-T-Appliances befinden sich die Syslog-Meldungen im Verzeichnis `/var/log/syslog`. Auf KVM-Hosts befinden sich die Syslog-Meldungen unter `/var/log/vmware/nsx-syslog`.

Auf NSX-T-Appliances können Sie den folgenden NSX-T-CLI-Befehl zum Anzeigen der Protokolle ausführen:

```
get log-file <auth.log | controller | controller-error | http.log | kern.log | manager.log |
node-mgmt.log | policy.log | syslog> [follow]
```

Die Protokolldateien lauten:

Name	Beschreibung
auth.log	Autorisierungsprotokoll
controller	Controller-Protokoll
controller-error	Controller-Fehlerprotokoll
http.log	HTTP-Dienstprotokoll
kern.log	Kernel-Protokoll
manager.log	Manager-Dienstprotokoll
node-mgmt.log	Knotenverwaltungsprotokoll
policy.log	Richtliniendienstprotokoll
syslog	Systemprotokoll

Auf Hypervisoren können Sie Linux-Befehle wie z. B. `tail`, `grep` oder `more` verwenden, um die Protokolle anzuzeigen.

Jede Syslog-Meldung enthält Komponentendetails (`comp`) und Unterkomponentendetails (`subcomp`), die es erleichtern, die Quelle der Meldung zu identifizieren.

NSX-T Data Center erzeugt Protokolle mit Facility `local6` mit einem numerischen Wert von 22.

Das Überwachungsprotokoll ist Teil eines Syslog. Eine Überwachungsprotokollmeldung kann durch die Zeichenfolge `audit="true"` im Feld `structured-data` identifiziert werden. Beispiel:

```
<182>1 2020-05-05T00:29:02.900Z nsx-manager1 NSX 14389 - [nsx@6876 audit="true"
comp="nsx-manager" level="INFO" reqId="fe75651d-c3e7-4680-8753-9ae9d92d7f0c" subcomp="policy"
username="admin"] UserName="admin", ModuleName="AAA", Operation="GetCurrentUserInfo",
Operation status="success"
```

Jeder-API-Aufruf erstellt eine Überwachungsprotokollmeldung. 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 und RFC 3164 definieren die folgenden Schweregrade:

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.

## Protokollmeldungsformate

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.
```

## Fehlercodes

Eine Liste der Fehlercodes finden Sie im Knowledgebase-Artikel 71077 [Fehlercodes für NSX-T Data Center 2.x](#).

## Konfigurieren der Remoteprotokollierung

Sie können NSX-T Data Center-Appliances und -Hypervisoren für das Senden von Meldungen zu einem Remote-Protokoll-Server 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

- Machen Sie sich mit dem CLI-Befehl `set logging-server` vertraut. Weitere Informationen finden Sie in der *Referenz zur NSX-T-CLI*.
- Wenn Sie die Protokolle TLS oder LI-TLS in der NSX CLI verwenden, um eine sichere Verbindung mit einem Protokoll-Server zu konfigurieren, müssen die Server- und Clientzertifikate auf jeder NSX-T Data Center-Appliance unter `/image/vmware/nsx/file-store` gespeichert werden. Beachten Sie, dass Zertifikate im Dateispeicher nur benötigt werden, wenn der Exporter über die NSX CLI konfiguriert wird. Wenn Sie die API verwenden, ist die Verwendung des Dateispeichers nicht erforderlich. Sobald Sie die Konfiguration des Syslog-Exporters abgeschlossen haben, müssen Sie alle Zertifikate und Schlüssel von diesem Speicherort löschen, um potenzielle Sicherheitsrisiken auszuschließen.

- Stellen Sie sicher, dass der Server mit einem von einer Zertifizierungsstelle signierten Zertifikat konfiguriert ist, um eine sichere Verbindung zu einem Protokoll-Server herzustellen. Wenn Sie beispielsweise über einen Log Insight-Server `vrli.prome.local` als Protokoll-Server verfügen, können Sie den folgenden Befehl von einem Client aus ausführen, um die Zertifikatskette auf dem Server zu sehen:

```
root@caserver:~# echo -n | openssl s_client -connect vrli.prome.local:443 | sed -ne '/
^Certificate chain/,/^---/p'
depth=2 C = US, L = California, O = GS, CN = Orange Root Certification Authority
verify error:num=19:self signed certificate in certificate chain
Certificate chain
 0 s:/C=US/ST=California/L=HTG/O=GSS/CN=vrli.prome.local
  i:/C=US/L=California/O=GS/CN=Green Intermediate Certification Authority
 1 s:/C=US/L=California/O=GS/CN=Green Intermediate Certification Authority
  i:/C=US/L=California/O=GS/CN=Orange Root Certification Authority
 2 s:/C=US/L=California/O=GS/CN=Orange Root Certification Authority
  i:/C=US/L=California/O=GS/CN=Orange Root Certification Authority
---
DONE
```

## Verfahren

- 1 Für die Konfiguration der Remote-Protokollierung auf einer NSX-T Data Center-Appliance 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>] [serverca <filename>] [clientca <filename>]
[certificate <filename>] [key <filename>] [structured-data <structured-data>]
```

Sie haben die Möglichkeit, den Befehl mehrmals zum Hinzufügen mehrerer Konfigurationen 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
```

Um nur Überwachungsprotokolle an den Remoteserver weiterzuleiten, geben Sie `audit="true"` im Parameter `structured-data` an. Beispiel:

```
set logging-server <server-ip> proto udp level info structured-data audit="true"
```

- 2 Zum Konfigurieren einer sicheren Remote-Protokollierung mithilfe des Protokolls „LI TLS“ geben Sie den Parameter `proto li-tls` an. Beispiel:

```
set logging-server vrli.prome.local proto li-tls level info messageid
SWITCHING,ROUTING,FABRIC,SYSTEM,POLICY,HEALTHCHECK,SHA,MONITORING serverca intermed-ca-
full-chain.crt
```

Wenn die Konfiguration erfolgreich ist, erhalten Sie eine Eingabeaufforderung ohne Text. Um den Inhalt der Serverzertifikatskette (intermediate gefolgt von root) zu sehen, melden Sie sich als `root` an und führen Sie den folgenden Befehl aus:

```
root@nsx1:~# keytool -printcert -file /image/vmware/nsx/file-store/intermed-ca-full-chain.crt
Certificate[1]:
Owner: CN=Green Intermediate Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd2
Valid from: Sun Mar 15 00:00:00 UTC 2020 until: Mon Mar 17 00:00:00 UTC 2025
Certificate fingerprints:
  MD5: 94:C8:9F:92:56:60:EB:DB:ED:4B:11:17:33:27:C0:C9
  SHA1: 42:9C:3C:51:E8:8E:AC:2E:5E:62:95:82:D7:22:E0:FB:08:B8:64:29
  SHA256:
58:B8:63:3D:0C:34:35:39:FC:3D:1E:BA:AA:E3:CE:A9:C0:F3:58:53:1F:AD:89:A5:01:0D:D3:89:9E:7B:C
5:69
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
Certificate[2]:
Owner: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd1
Valid from: Mon Mar 16 07:16:07 UTC 2020 until: Fri Mar 10 07:16:07 UTC 2045
Certificate fingerprints:
  MD5: ED:AC:F1:7F:88:05:83:2A:83:C0:09:03:D5:00:CA:7B
  SHA1: DC:B5:3F:37:DF:BD:E0:5C:A4:B7:F4:4C:96:12:75:7A:16:C7:61:37
  SHA256:
F2:5B:DE:8A:F2:31:9D:E6:EF:35:F1:30:6F:DA:05:FF:92:B4:15:96:AA:82:67:E3:3C:C1:69:A3:E5:27:B
9:A5
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
```

Die Protokolle sowohl für erfolgreiche als auch für Fehlerbedingungen befinden sich in `/var/log/loginsight-agent/liagent_2020-MM-DD-<file-num>.log`. Wenn die Konfiguration erfolgreich ist, können Sie die Log Insight-Konfiguration mit dem folgenden Befehl anzeigen:

```
root@nsx1:/image/vmware/nsx/file-store# cat /var/lib/loginsight-agent/liagent-effective.ini
; Dynamic file representing the effective configuration of VMware Log Insight Agent
(merged server-side and client-side configuration)
; DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
; Creation time: 2020-03-22T19:41:21.648800

[server]
hostname=vrli.prome.local
proto=cfapi
ssl=yes
ssl_ca_path=/config/vmware/nsx-node-api/syslog/bb466082-996f-4d77-b6e3-1fa93f4a20d4_ca.pem
ssl_accept_any_trusted=yes
port=9543
```

```
filter={filelog; nsx-syslog; pri_severity <= 6 and ( msgid == "SWITCHING" or msgid ==
"ROUTING" or msgid == "FABRIC" or msgid == "SYSTEM" or msgid == "POLICY" or msgid ==
"HEALTHCHECK" or msgid == "SHA" or msgid == "MONITORING" )}

[filelog|nsx-syslog]
directory=/var/log
include=syslog;syslog.*
parser=nsx-syslog_parser

[parser|nsx-syslog_parser]
base_parser=syslog
extract_sd=yes

[update]
auto_update=no
```

- 3 Zum Konfigurieren einer sicheren Remote-Protokollierung mithilfe des Protokolls „TLS“ geben Sie den Parameter `proto tls` an. Beispiel:

```
set logging-server vrli.prome.local proto tls level info serverca Orange-CA.crt.pem
clientca Orange-CA.crt.pem certificate gc-nsxt-mgr-full.crt.pem key gc-nsxt-mgr.key.pem
```

Beachten Sie Folgendes:

- Für den Parameter `serverCA` ist nur das Stammzertifikat erforderlich, nicht die vollständige Kette.
- Wenn `clientCA` sich von `serverCA` unterscheidet, ist nur das Root-Zertifikat erforderlich.
- Das Zertifikat sollte die vollständige Kette des NSX Manager enthalten (Sie sollte NDcPP-konform sein – ECU, BASIC und CDP (CDP – diese Prüfung kann ignoriert werden))

Sie können den Inhalt jedes Zertifikats überprüfen. Beispiel:

```
root@gc3:~# keytool -printcert -file /image/vmware/nsx/file-store/Orange-CA.crt.pem
Owner: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd1
Valid from: Mon Mar 16 07:16:07 UTC 2020 until: Fri Mar 10 07:16:07 UTC 2045
Certificate fingerprints:
    MD5: ED:AC:F1:7F:88:05:83:2A:83:C0:09:03:D5:00:CA:7B
    SHA1: DC:B5:3F:37:DF:BD:E0:5C:A4:B7:F4:4C:96:12:75:7A:16:C7:61:37
    SHA256:
F2:5B:DE:8A:F2:31:9D:E6:EF:35:F1:30:6F:DA:05:FF:92:B4:15:96:AA:82:67:E3:3C:C1:69:A3:E5:27:B
9:A5
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
root@gc3:~#

root@gc3:/image/vmware/nsx/file-store# keytool -printcert -file gc-nsxt-mgr-full.crt.pem
Certificate[1]:
Owner: CN=gc.prome.local, O=GS, L=HTG, ST=California, C=US
Issuer: CN=Green Intermediate Certification Authority, O=GS, L=California, C=US
Serial number: bdf43ab31340b87f323b438a2895a075
```



```

Valid from: Mon Mar 16 07:26:51 UTC 2020 until: Wed Mar 16 07:26:51 UTC 2022
Certificate fingerprints:
    MD5: 36:3C:1F:57:96:07:84:C0:6D:B7:33:9A:8D:25:4D:27
    SHA1: D1:4E:F9:45:2D:0D:34:79:D2:B4:FA:65:28:E0:5C:DC:74:50:CA:3B
    SHA256:
3C:FF:A9:5D:AA:68:44:44:DD:07:2F:DD:E2:BE:9C:32:19:7A:03:D5:26:8D:5F:AD:56:CA:D2:6C:91:96:2
7:6F
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
Certificate[2]:
Owner: CN=Green Intermediate Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd2
Valid from: Sun Mar 15 00:00:00 UTC 2020 until: Mon Mar 17 00:00:00 UTC 2025
Certificate fingerprints:
    MD5: 94:C8:9F:92:56:60:EB:DB:ED:4B:11:17:33:27:C0:C9
    SHA1: 42:9C:3C:51:E8:8E:AC:2E:5E:62:95:82:D7:22:E0:FB:08:B8:64:29
    SHA256:
58:B8:63:3D:0C:34:35:39:FC:3D:1E:BA:AA:E3:CE:A9:C0:F3:58:53:1F:AD:89:A5:01:0D:D3:89:9E:7B:C
5:69
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
Certificate[3]:
Owner: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd1
Valid from: Mon Mar 16 07:16:07 UTC 2020 until: Fri Mar 10 07:16:07 UTC 2045
Certificate fingerprints:
    MD5: ED:AC:F1:7F:88:05:83:2A:83:C0:09:03:D5:00:CA:7B
    SHA1: DC:B5:3F:37:DF:BD:E0:5C:A4:B7:F4:4C:96:12:75:7A:16:C7:61:37
    SHA256:
F2:5B:DE:8A:F2:31:9D:E6:EF:35:F1:30:6F:DA:05:FF:92:B4:15:96:AA:82:67:E3:3C:C1:69:A3:E5:27:B
9:A5
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3

```

Beispiele für eine erfolgreiche Protokollierung in /var/log/syslog:

```

<182>1 2020-03-22T21:54:34.501Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created CA PEM file /
config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_ca.pem for logging
server vrli.prome.local:6514
<182>1 2020-03-22T21:54:36.269Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created client CA PEM
file /config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_client_ca.pem
for logging server vrli.prome.local:6514
<182>1 2020-03-22T21:54:36.495Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert issuer = /C=US/L=California/O=GS/
CN=Green IntermediateCertification Authority
<182>1 2020-03-22T21:54:36.514Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert subject = /C=US/ST=California/L=HTG/
O=GS/CN=gc.promelocal

```

```
<182>1 2020-03-22T21:54:36.539Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] certificate trust check succeeded.
status: 200, result: {'status': 'OK'}
<182>1 2020-03-22T21:54:36.612Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] Certificate already exists, skip import
<182>1 2020-03-22T21:54:37.322Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created certificate PEM
file /config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_cert.pem for
logging server vrli.prome.local:6514
<182>1 2020-03-22T21:54:38.020Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created key PEM file /
config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_key.pem for logging
server vrli.prome.local:6514
```

Beispiele für eine fehlgeschlagene Protokollierung in /var/log/syslog:

```
<182>1 2020-03-22T21:33:30.424Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created client CA PEM
file /config/vmwarensx-node-api/syslog/76332782-1ec6-483a-95d4-2adeaf2ef112_client_ca.pem
for logging server vrli.prome.local:6514
<182>1 2020-03-22T21:33:30.779Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert issuer = /C=US/L=California/O=GS/
CN=Green IntermediateCertification Authority
<182>1 2020-03-22T21:33:30.803Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert subject = /C=US/ST=California/L=HTG/
O=GS/CN=gc.promelocal
<179>1 2020-03-22T21:33:30.823Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-
manager" subcomp="node-mgmt" username="root" level="ERROR" errorCode="NODE10"]
Certificate trust check failed. status:200, result: {'error_message': 'Certificate
CN=gc.prome.local,O=GS,L=HTG,ST=California,C=US was not verifiably signed by
CN=gc.prome.local,O=GS,L=HTG,ST=California,C=US: certificate does not verifywith supplied
key', 'status': 'ERROR'}
<179>1 2020-03-22T21:33:30.824Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-
manager" subcomp="node-mgmt" username="admin" level="ERROR" errorCode="NODE10"]
Failed to create certificate PEM file config/vmware/nsx-node-api/syslog/
76332782-1ec6-483a-95d4-2adeaf2ef112_cert.pem for logging server vrli.prome.local:6514
<182>1 2020-03-22T21:33:31.578Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully deleted CA PEM file /
config/vmwarensx-node-api/syslog/76332782-1ec6-483a-95d4-2adeaf2ef112_ca.pem
<182>1 2020-03-22T21:33:32.342Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully deleted client CA PEM
file /config/vmwarensx-node-api/syslog/76332782-1ec6-483a-95d4-2adeaf2ef112_ca.pem
<182>1 2020-03-22T21:33:32.346Z gc3.prome.local NSX 16698 - [nsx@6876 comp="nsx-cli"
subcomp="node-mgmt" username="admin" level="INFO" audit="true"] CMD: set logging-server
vrli.prome.local prototls level info serverca Orange-CA.crt.pem clientca Orange-CA.crt.pem
certifi
cate gc-nsxt-mgr.crt.pem key gc-nsxt-mgr.key.pem (duration: 6.365s), Operation status:
CMD_EXECUTED
```

Sie können überprüfen, ob das Zertifikat und der Privatschlüssel mit dem folgenden Befehl übereinstimmen. Wenn Sie übereinstimmen, wird die RSA-Schlüssel wird geschrieben ausgegeben. Eine andere Ausgabe bedeutet, dass Sie nicht übereinstimmen. Beispiel:

```
root@caserver:~/server-certs# diff <(openssl x509 -in certs/gc-nsxt-mgr.crt.pem -pubkey
-noout) <(openssl rsa -in private/gc-nsxt-mgr.key.pem -pubout)
writing RSA key
```

Beispiel für einen fehlerhaften Privatschlüssel:

```
root@caserver:~/server-certs# diff <(openssl x509 -in certs/gc-nsxt-mgr.crt.pem -pubkey
-noout) <(openssl rsa -in private/gc-nsxt-mgr-corrupt.key.pem -pubout)
unable to load Private Key
140404188370584:error:0D07209B:asn1 encoding routines:ASN1_get_object:too
long:asn1_lib.c:147:
140404188370584:error:0D068066:asn1 encoding routines:ASN1_CHECK_TLEN:bad object
header:tasn_dec.c:1205:
140404188370584:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1
error:tasn_dec.c:386:Type=RSA
140404188370584:error:04093004:rsa routines:OLD_RSA_PRIV_DECODE:RSA lib:rsa_ameth.c:119:
140404188370584:error:0D07209B:asn1 encoding routines:ASN1_get_object:too
long:asn1_lib.c:147:
140404188370584:error:0D068066:asn1 encoding routines:ASN1_CHECK_TLEN:bad object
header:tasn_dec.c:1205:
140404188370584:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1
error:tasn_dec.c:386:Type=PKCS8_PRIV_KEY_INFO
140404188370584:error:0907B00D:PEM routines:PEM_READ_BIO_PRIVATEKEY:ASN1
lib:pem_pkey.c:141:
1,14d0
< -----BEGIN PUBLIC KEY-----
< MIIICjANBgkqhkiG9w0BAQEFAAOCAg8AMIICGKCAgEAv3yH7pZidfkLrEP3zVa9
< EcOKXlFFjkThZRZMfguenlm8s6QHYVvuUX8IRB48Li3/DUfOj0bzaPWktpv+Q2P0
< N/j4LoX2RzjV/DPxYfLP6GMNMc21L3s9ruBeWUtthUP8khCwd2d2rZ09cUZVl0P9
< kIYBb5RMFC7Z1Outh3bkdepEf+sXz3DaKZ/WySzYq9x86QDaA3ABO3Q0i7txBscI
< FvXuMDOMQaC3pPp9FWO6IPRAWB57wahLJv6K5qGIfwubSBFG53grT4snf1lDZAHz
< 9hz5JgGr80GVyWyb7rgigpl9iUWAZx8U9De9XoxmvBN5iEGTIuKGaEgICL176crb
< RMkhjncQnHI+z6sQvpyJ7U0zZc72eBIWoHukcWWk3eU6Oy4OiyW6jYuXG7hZYlly
< nSkme3mZUWJKVcoX05+3zeCP623/HzE7X2sNyWFjzeF3XEvaUzrIbsJh/xp2ShDa
< uKKEY0gUGhLtCa3TpV9l8d6tFWVy8XjVjdjoVt4s7MfUo/airVmRykfsWrKyNUOQ
< qRZvSbqjt8pm+3bSvKdXX4ul7ptPG2GF20ETWHPwjK2JwQpGhR9zK8fsKzvm6hXi
< kq76zI4FefuVps3e1r39+0F+p6d6i2oUoo24sC1iSePTDhU74efVp6iv8HmnDgYX
< Ylm6Kusr0JT5TJFDfASmrj8CAwEAAQ==
< -----END PUBLIC KEY-----
```

Beispiel eines gültigen Schlüssels und Zertifikats, die jedoch nicht für die einzelnen Personen bereitgestellt wurden:

```
root@caserver:~/server-certs# diff <(openssl x509 -in certs/gc-nsxt-mgr.crt.pem -pubkey
-noout) <(openssl rsa -in private/vrli.key.pem -pubout)
writing RSA key
2,13c2,13
< MIIICjANBgkqhkiG9w0BAQEFAAOCAg8AMIICGKCAgEAv3yH7pZidfkLrEP3zVa9
< EcOKXlFFjkThZRZMfguenlm8s6QHYVvuUX8IRB48Li3/DUfOj0bzaPWktpv+Q2P0
```

```
< N/j4LoX2RzjV/DPxYfLP6GMNMc21L3s9ruBeWUthtUP8khCWd2d2rz09cUZVl0P9
< kIYBb5RMFC7Z10Uth3bKdepEf+sXz3DaKZ/WySzYq9x86QDaA3ABO3Q0i7txBscI
< FvXuMDOMQaC3pPp9FWO6IPRAWB57wahLJv6K5qGifwubSBFg53grT4snf11DZAhZ
< 9hz5JgGr80GVyWyb7rgigpl9iUWAZx8U9De9XoxmvBN5iEGTIuKGaEgICL176crb
< RMkhjnCqNHI+z6sQvpYJ7U0zZc72eBIWoHUKcWWk3eU60y40iyW6jYuXG7hZYlly
< nSkme3mZUWJKvcoX05+3zeCP623/HzE7X2sNyWFjzeF3XEvaUzrIbsJh/xp2ShDa
< uKKEY0gUGhLtCa3TpV9l8d6tFWVy8XjVjdjoVt4s7MfUo/airVmRykfsWrKyNUOQ
< qRZvSbqjt8pm+3bSvKdXX4ul7ptPG2GF20ETWHPwj2JwQpGhR9zK8fsKzvm6hXi
< kq76zI4FefuVps3e1r39+0F+p6d6i2oUoo24sC1iSePTDhU74efVp6iv8HmnDgYX
< Ylm6Kusr0JT5TJFDfASmrj8CAwEAAQ==
---
> MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICGKCAgEAqvsjay7+o7gCW7szT3ho
> bc34XX216u5J14/X/pUDI/YHmIf06bsZ1r/14bTL4Q7BM6+9MI6UYEE7DxUoINGO
> o4FEEQE32KWVFe3gw3homHU39q4pQjsJsxTcTE3oDM1IY0nWJ0PRUst3DdfyUH1L
> W0NUN9ydn+fa12Uf021iuDqVy9V8AH3ON6fu+QCA8nt71ZkzeTxSA0ldpl2NA17F
> rD8rm05wxnV7WtuV7V8PstISiClzhHgZRM1+B0r30OitnyAzEGLaRT3//PKfe0Oe
> HCdxGMLrUtMqxIIItJahEsqvMufyqNYecVscYXLHPelizKCsQfy8c08LnznG8VAdc
> YILSn3uYGZap6aF1SgVxsvZicwvlyNssmgE13Af0nScmfM96k9h5joHVEkWK6O8v
> oT5DGG1kVL2Qly97x0b6EnzUorzivv5zJMKvFcOektR8HdMHQit5uvmMRY3S5zow
> FtvfSDfWxxKyTy6GBRpp+8F+Jq9lyGy/qa9lhKBzT2lg+rJp7T8k7/Nm9Tjyx7jL
> EggEKZEL4chxpo8ucF98hvbXWRuaFHC2iDzGuUmuS1FfjVvHTuIbEMQfjapLZrHx
> 8jHfOP/PL+6kPbvNZ2rTpczuEoGTQFFW9vX48GzIEyMeR6QWpPR0F7r4xak68P5
> 2PJmMveinDhU35IqWEXHawcCAwEAAQ==
```

- 4 Führen Sie den Befehl `get logging-server` aus, um die Protokollkonfiguration anzuzeigen.  
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
```

- 5 Führen Sie den folgenden Befehl aus, um die Konfiguration der Remote-Protokollierung zu löschen:

```
nsx> clear logging-servers
```

- 6 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
```

## 7 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 21-10. Protokollmeldungs-IDs**

Meldungs-ID	Beispiele
FABRIC	Hostknoten Hostvorbereitung Edge-Knoten Transportzone Transportknoten Uplink-Profil Clusterprofil Edge-Cluster
SWITCHING	Logischer Switch Logischer Switch Port Switching-Profil Funktionen der Switch-Sicherheit
ROUTING	Logischer Router Logische Router Ports Statisches Routing Dynamisches Routing NAT
FIREWALL	Firewallregeln Firewallregelabschnitte
FIREWALL-PKTLOG	Protokolle der Firewallverbindung Protokolle des Firewallpakets

Tabelle 21-10. Protokollmeldungs-IDs (Fortsetzung)

Meldungs-ID	Beispiele
GROUPING	IP Sets MAC Sets NSGroups 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

## Fehlerbehebung für Probleme mit Syslog

Wenn der Remote-Protokollserver keine Protokolle empfängt, führen Sie die folgenden Schritte aus:

- Überprüfen Sie die IP-Adresse des Remote-Protokollservers.
- Überprüfen Sie, ob der `level`-Parameter korrekt konfiguriert ist.
- Überprüfen Sie, ob der `facility`-Parameter korrekt konfiguriert ist.
- Wenn das TLS-Protokoll verwendet wird, legen Sie stattdessen das UDP-Protokoll fest, um festzustellen, ob Zertifikate nicht übereinstimmen.
- Wenn das TLS-Protokoll verwendet wird, vergewissern Sie sich, dass Port 6514 an beiden Enden geöffnet ist.
- Entfernen Sie den Meldungs-ID-Filter und stellen Sie fest, ob der Server Protokolle empfängt.
- Starten Sie den rsyslog-Dienst mit dem Befehl `restart service rsyslogd` neu.

## Konfigurieren der seriellen Protokollierung auf einer Appliance-VM

Sie können die serielle Protokollierung auf einer Appliance-VM konfigurieren, um beim Absturz der VM Protokollmeldungen zu erfassen.

### Verfahren

- 1 Melden Sie sich bei der VM als `root` an.
- 2 Bearbeiten Sie `/etc/default/grub`.
- 3 Suchen Sie den Parameter `GRUB_CMDLINE_LINUX_DEFAULT` und fügen Sie `console=ttyS0 console=tty0` an.
- 4 Führen Sie den Befehl `update-grub2` aus.
- 5 Stellen Sie sicher, dass die Datei `/boot/grub/grub.cfg` die in Schritt 3 beschriebene Änderung enthält.
- 6 Schalten Sie die VM aus.
- 7 Bearbeiten Sie die Konfigurationsdatei der VM (`.vmx`) und fügen Sie folgende Zeilen hinzu:

```
serial0.present = "TRUE"
serial0.fileType = "file"
serial0.fileName = "serial.out"
serial0.yieldOnMsrRead = "TRUE"
answer.msg.serial.file.open = "Append"
```

- 8 Schalten Sie die VM ein.

### Ergebnisse

Wenn in der VM Kernel Panic auftritt, finden Sie die Datei `serial.out`, die Protokollmeldungen enthält, am selben Speicherort wie die `.vmx`-Datei.

## 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 [NSX-T Data Center-Funktionen mit Support in NSX Cloud](#) eine Liste der automatisch generierten logischen Einheiten, unterstützten Funktionen und Konfigurationen, die für NSX Cloud erforderlich sind.

---



Die meisten Objekte können maximal 30 Tags aufweisen. Für die folgenden Objekte ist der Maximalwert aufgrund von Tags, die intern erstellt und verwendet werden, niedriger.

**Tabelle 21-11. Maximale Anzahl Tags für Objekte, die mithilfe der Registerkarte „Netzwerk und Sicherheit – Erweitert“ erstellt wurden**

Objekt	Maximale Anzahl Tags
virtuelle Maschine	25
Logischer Port	29

**Tabelle 21-12. Maximale Anzahl Tags für Objekte, die mithilfe der Registerkarten „Netzwerk“, „Sicherheit“ oder „Bestand“ erstellt wurden**

Objekt	Maximale Anzahl Tags
Gruppe	29
Segment	27
Segment-Port	29
Logischer Routerport	30 – Anzahl Bezeichnungen
NAT-Regel	27
IPSec-VPN-Sitzung	29

**Tabelle 21-13. Maximale Anzahl Tags für Cloud Service Manager-Objekte**

Objekt	Maximale Anzahl Tags
BFD-Zustandsüberwachungsprofil, Transportzone, Uplink-Host-Switch-Profil, Transportknoten, Edge-Cluster	23

**Tabelle 21-14. Maximale Anzahl Tags für Public Cloud Manager-Objekte**

Objekt	Maximale Anzahl Tags
BFD-Zustandsüberwachungsprofil, Transportzone, logischer Switch, Knoten, Transportknoten, Edge-Cluster, logischer Router, Uplink-Port des logischen Routers, statische Route, DHCP-Profil, NSGroup, Firewall-Abschnittsregelliste	23
NAT-Regel	20
IP Set, NSGroup	22

## 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. 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 21-15. 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 **Netzwerk und Sicherheit – Erweitert > Bestandsliste > 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.

## Konfigurieren eines externen Load Balancer

Sie können einen externen Load Balancer konfigurieren, um den Datenverkehr an die NSX Manager in einem Manager-Cluster zu verteilen.

Ein NSX Manager-Cluster erfordert keinen externen Load Balancer. Die virtuelle NSX Manager-IP (VIP) sorgt beim Ausfall eines Manager-Knotens für Stabilität, hat aber die folgenden Einschränkungen:

- VIP führt keinen Load Balancing für die NSX Manager durch.
- VIP erfordert, dass sich alle NSX Manager im selben Subnetz befinden.
- Die Wiederherstellung der VIP dauert etwa 1–3 Minuten, falls ein Manager-Knoten ausfällt.

Ein externer Load Balancer kann die folgenden Vorteile bieten:

- Lastenausgleich zwischen den NSX Managern.
- Die NSX Manager können sich in unterschiedlichen Subnetzen befinden.
- Schnelle Wiederherstellungszeit beim Ausfall eines Manager-Knotens.

Beachten Sie, dass die NSX Manager-VIP nicht für einen externen Load Balancer verwendet werden kann. Konfigurieren Sie keine NSX Manager-VIP, wenn Sie einen externen Load Balancer verwenden.

Wenn Sie über einen externen Load Balancer mit einem Browser auf NSX Manager zugreifen, muss die Sitzungspersistenz auf dem Load Balancer aktiviert sein.

Wenn Sie über einen externen Load Balancer mit einem API-Client auf NSX Manager zugreifen, sind vier Authentifizierungsmethoden verfügbar (weitere Informationen finden Sie im *Handbuch zur NSX-T Data Center-API*):

- HTTP-Standardauthentifizierung: Sitzungspersistenz für Load Balancer ist nicht erforderlich.
- Clientzertifikatauthentifizierung: Sitzungspersistenz für Load Balancer ist nicht erforderlich.
- Authentifizierung bei vIDM: Sitzungspersistenz für Load Balancer ist nicht erforderlich.
- Sitzungsbasierte Authentifizierung: Sitzungspersistenz für Load Balancer ist erforderlich.

Empfehlung:

- Konfigurieren Sie für den Browser- und den API-Zugriff eine einzelne IP auf dem externen Load Balancer. Für den Load Balancer muss die Sitzungspersistenz aktiviert sein.

# 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:

- [Eine kurze Einführung in Cloud Service Manager](#)
- [Bedrohungserkennung mit der NSX Cloud-Quarantäne-Richtlinie](#)
- [NSX-erzwungener Modus](#)
- [Native Cloud-erzwungener Modus](#)
- [NSX-T Data Center-Funktionen mit Support in NSX Cloud](#)
- [Häufig gestellte Fragen](#)

## Eine kurze Einführung in 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="#">Bedrohungserkennung mit der NSX Cloud-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 VPCs/VNets pro Region anzeigen.
- Sie können die Anzahl Arbeitslast-VMs pro VPC/VNet 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 verfügt über VPCs/VNets und Instanzen. Wenn Sie PCGs bereitgestellt haben, werden diese hier als **Gateways** mit einem Indikator für den PCG-Zustand angezeigt.

## Clouds > {Ihre Public Cloud} > VPCs oder VNets

Im Abschnitt „VPCs“ bzw. „VNets“ wird Ihr Private Cloud-Bestand angezeigt.

Sie können die Bestandsliste nach Konto und Region filtern.

- Jede Karte steht für eine VPC/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):
      - Aktivieren oder deaktivieren Sie die Quarantäne-Richtlinie, wenn Sie sich im NSX-erzwungener Modus befinden.
      - Stellen Sie eine Fallback-Sicherheitsgruppe bereit, die erforderlich ist, wenn bei Verwendung des NSX-erzwungener Modus die Integration der VPC/des VNet in NSX Cloud aufgehoben wird. Siehe [Quarantäne-Richtlinie-Auswirkungen bei Deaktivierung](#).
      - 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.

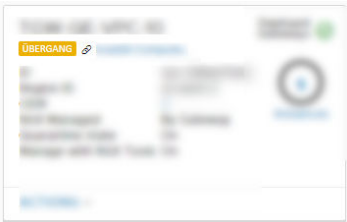
Sie können der CSM-Whitelist Instanzen hinzufügen oder Instanzen daraus entfernen. Einzelheiten dazu finden Sie unter [Verschieben von VMs in die Whitelist](#).

## Symbole von CSM

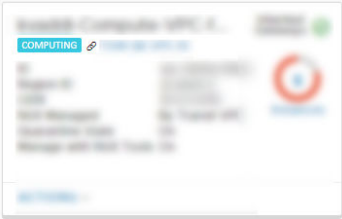
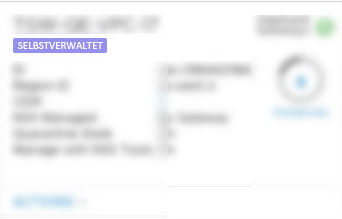
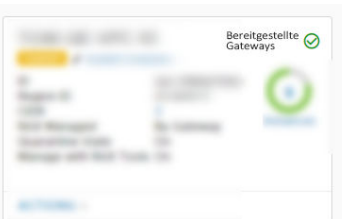
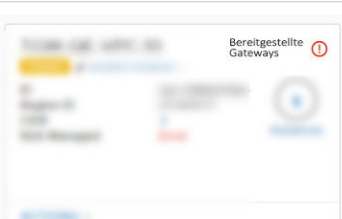
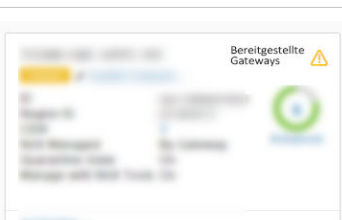
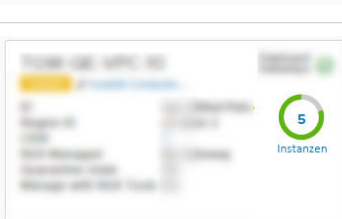
CSM zeigt den Zustand und die Integrität Ihrer Public Cloud-Konstrukte mithilfe von anschaulichen Symbolen an.

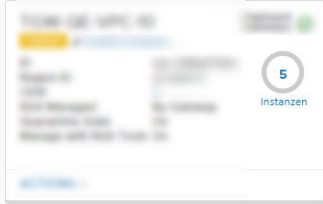
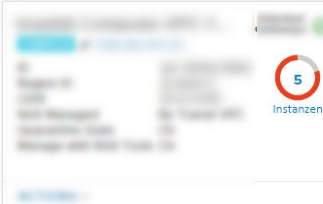
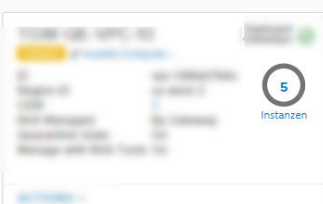
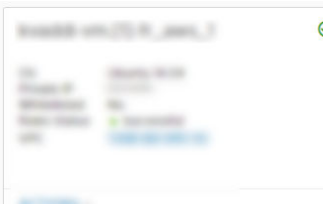
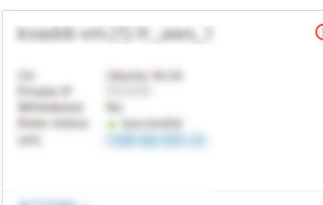
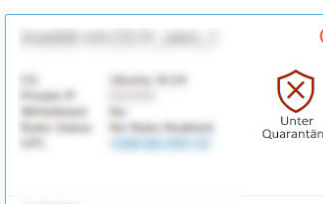
**Hinweis** Im Native Cloud-erzwungener Modus : Quarantäne-Richtlinie ist immer aktiviert und alle VMs sind immer NSX-verwaltet. Nur die Zustände, in denen die Quarantäne-Richtlinie für NSX-verwaltete VMs aktiviert ist, gelten in diesem Modus.

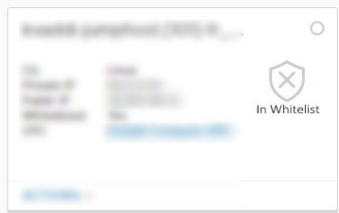
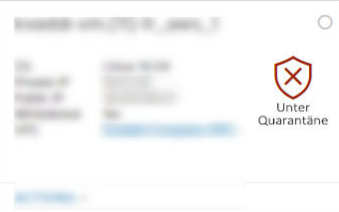
Im NSX-erzwungener Modus: Quarantäne-Richtlinie kann deaktiviert werden und es ist möglich, nicht verwaltete VMs in der VPC/im VNet zu verwenden. Alle relevanten Zustände gelten für diesen Modus.

CSM-Bereich und -Symbol	Beschreibung
VPCs/VNets	
	Transit-VPC/-VNet



CSM-Bereich und -Symbol	Beschreibung
	Computing-VPC/-VNet
	Selbstverwaltete VPC/selbstverwaltetes VNet
	VPC/VNet mit ordnungsgemäßen PCGs
	VPC/VNet mit PCGs im Fehlerzustand
	VPC/VNet mit jeweils einem PCG im fehlerhaften und ordnungsgemäßen Zustand.
	VPC/VNet mit NSX-verwalteten VMs.

CSM-Bereich und -Symbol	Beschreibung
	VPC/VNet mit nicht-NSX-verwalteten VMs.
	VPC/VNet mit VMs mit Fehlern.
	VPC/VNet mit ausgeschalteten VMs.
<b>Instanzen</b>	
	Von NSX verwaltete VMs ohne Fehler.
	Von NSX verwaltete VMs mit Fehlern und deaktivierter Quarantäne-Richtlinie.
	Von NSX verwaltete VMs mit Fehlern und aktivierter Quarantäne-Richtlinie.

CSM-Bereich und -Symbol	Beschreibung
	Nicht verwaltete VMs in der Whitelist.
	Nicht verwaltete VMs unter Quarantäne.

## 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](#).

## Bedrohungserkennung mit der NSX Cloud-Quarantäne-Richtlinie

Die Quarantäne-Richtlinienfunktion in NSX Cloud bietet einen Mechanismus zur Erkennung von Bedrohungen für Ihre NSX-verwalteten Arbeitslast-VMs.

Die Quarantäne-Richtlinie wird in den beiden VM-Verwaltungsmodi unterschiedlich implementiert.

**Tabelle 22-1. Quarantäne-Richtlinienimplementierung im NSX-erzwungener Modus und im Native Cloud-erzwungener Modus**

Konfigurationen im Zusammenhang mit der Quarantäne-Richtlinie	Im NSX-erzwungener Modus	Im Native Cloud-erzwungener Modus
Standardzustand	Bei der Bereitstellung von PCG mit NSX Tools deaktiviert. Sie können die Aktivierung im PCG-Bereitstellungsbildschirm oder später vornehmen. Siehe <a href="#">Quarantäne-Richtlinie aktivieren oder deaktivieren</a> .	Immer aktiviert. Kann nicht deaktiviert werden.
Automatisch erstellte Sicherheitsgruppen, die für jeden Modus eindeutig sind	Allen ordnungsgemäßen NSX-verwalteten VMs wird die <code>vm-underlay-sg</code> -Sicherheitsgruppe zugewiesen.	<code>nsx-&lt;NSX GUID&gt;</code> -Sicherheitsgruppen werden für NSX-verwaltete Arbeitslast-VMs erstellt und angewendet, die mit einer verteilten Firewall-Richtlinie in NSX Manager abgeglichen werden
Automatisch erstellte Public Cloud-Sicherheitsgruppen, die beide Modi gemeinsam haben:	<p>Die <b>gw</b>-Sicherheitsgruppen werden auf die entsprechenden PCG-Schnittstellen in AWS und Microsoft Azure angewendet.</p> <ul style="list-style-type: none"> <li>■ <code>gw-mgmt-sg</code></li> <li>■ <code>gw-uplink-sg</code></li> <li>■ <code>gw-vtep-sg</code></li> </ul> <p>Die <b>vm</b>-Sicherheitsgruppen werden auf von NSX verwaltete VMs angewendet. Dies ist von ihrem aktuellen Status und davon abhängig, ob die Quarantäne-Richtlinie aktiviert oder deaktiviert ist:</p> <ul style="list-style-type: none"> <li>■ <code>vm-quarantine-sg</code> in Microsoft Azure und <code>default</code> in AWS.</li> </ul> <p><b>Hinweis</b> In AWS ist die Sicherheitsgruppe <code>default</code> bereits vorhanden. Sie wird nicht von NSX Cloud erstellt.</p>	

## Allgemeine Empfehlung für NSX-erzwungener Modus:

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.

## Quarantäne-Richtlinie im NSX-erzwungener Modus

Die Aktivierung der Quarantäne-Richtlinie ist im NSX-erzwungener Modus optional.

### Quarantäne-Richtlinie aktivieren oder deaktivieren

Im NSX-erzwungener Modus können Sie die Quarantäne-Richtlinie auf zwei Arten aktivieren.

Die erste Möglichkeit zum Aktivieren der Quarantäne-Richtlinie besteht darin, dass Sie PCG für eine Transit-VPC/ein Transit-VNet bereitstellen oder eine Computing-VPC/ein Computing-VNet mit einer Übertragung verknüpfen. Ändern Sie den standardmäßigen Status **Deaktiviert** des Schiebereglers für **Quarantäne-Richtlinie für die zugeordnete VPC/das zugeordnete VNet** in **Aktiviert**. Siehe **Bereitstellen von PCG** im *Installationshandbuch für NSX-T Data Center*.

Sie können die Quarantäne-Richtlinie auch später im Anschluss an die hier beschriebenen Schritte aktivieren.

#### Voraussetzungen

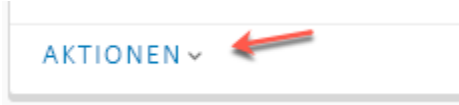
Wenn Sie die Quarantäne-Richtlinie nach dem Bereitstellen oder Verknüpfen mit einem PCG aktivieren, müssen sich eine bzw. ein oder mehrere Transit- oder Computing-VPCs/VNets im NSX-erzwungener Modus befinden, die Sie für die Verwendung von NSX Tools für die Verwaltung Ihrer Arbeitslast-VMs gewählt haben.

#### 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**

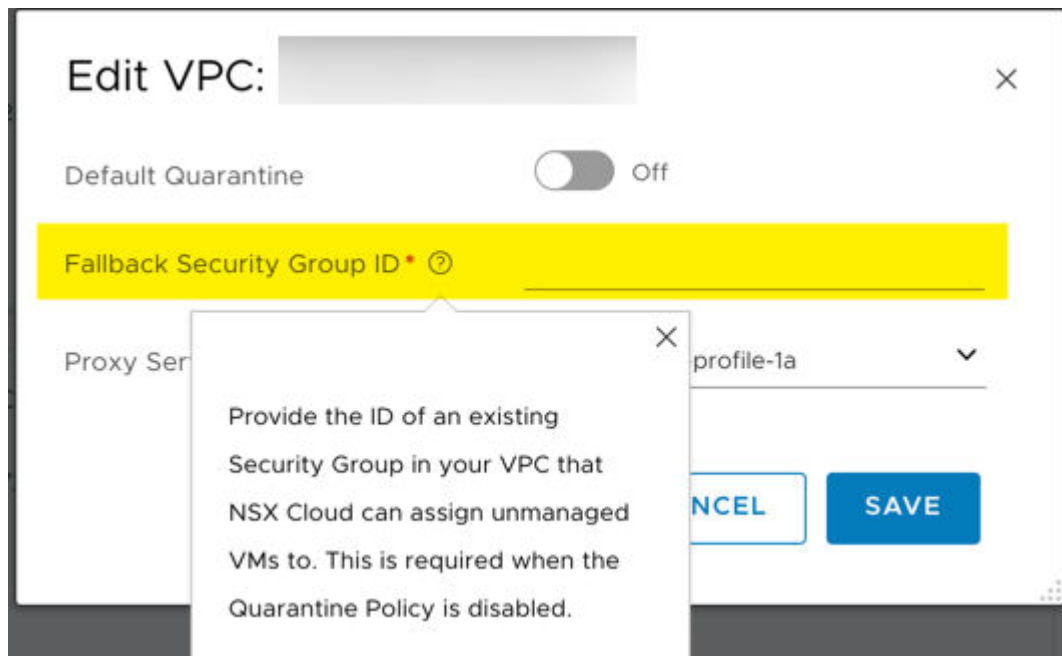


- ◆ Wenn Sie sich auf der VPC- oder VNet-Seite befinden, klicken Sie auf das Symbol „AKTIONEN“ und wählen Sie dann **Konfigurationen bearbeiten**.



- Schalten Sie **Standard-Quarantäne** ein oder aus, um sie zu aktivieren oder zu deaktivieren.
- 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.



- Allen nicht verwalteten 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

NSX Cloud verwaltet die Public Cloud-Sicherheitsgruppen von nicht markierten VMs nicht, wenn die Quarantäne-Richtlinie deaktiviert ist.

Für VMs, die mit `nsx.network=default` in der Public Cloud gekennzeichnet sind, weist NSX Cloud jedoch je nach Zustand der VM entsprechende Sicherheitsgruppen zu. Dieses Verhalten ähnelt dem, wenn die Quarantäne-Richtlinie aktiviert ist, aber die Regeln in den Quarantäne-Sicherheitsgruppen: `vm-quarantine-sg` in Microsoft Azure und `default` in AWS sind weniger restriktiv. Manuelle Änderungen an den Sicherheitsgruppen gekennzeichneteter VMs werden innerhalb von zwei Minuten auf die von NSX Cloud zugewiesene Sicherheitsgruppe zurückgesetzt.

---

**Hinweis** Wenn Sie nicht möchten, dass NSX Cloud Ihren NSX-verwalteten (gekennzeichneten) VMs Sicherheitsgruppen zuweist, können Sie sie in CSM in Whitelists verschieben. Siehe [Verschieben von VMs in die Whitelist](#).

---

Die folgende Tabelle zeigt, wie NSX Cloud die Public Cloud-Sicherheitsgruppen von Arbeitslast-VMs verwaltet, wenn die Quarantäne-Richtlinie deaktiviert ist.

**Tabelle 22-2. NSX Cloud-Zuweisung von Public Cloud-Sicherheitsgruppen, wenn die Quarantäne-Richtlinie deaktiviert ist**

Ist VM in der Public Cloud mit <i>nsx.network=default</i> gekennzeichnet?	Befindet sich die VM in der Whitelist?	Public Cloud-Sicherheitsgruppe der VM, wenn die Quarantäne-Richtlinie deaktiviert ist und Erläuterung
Gekennzeichnet	Nicht in der Whitelist	<ul style="list-style-type: none"> <li>■ Wenn die VM keine Bedrohungen aufweist: <i>vm-underlay-sg</i></li> <li>■ Wenn die VM potenzielle Bedrohungen aufweist (siehe Hinweis): <i>vm-quarantine-sg</i> in Microsoft Azure; <i>default</i> in AWS</li> </ul> <p><b>Hinweis</b> Die Zuweisung von Public Cloud-Sicherheitsgruppen wird innerhalb von 90 Sekunden nach der Anwendung des <i>nsx.network=default</i>-Tags auf Ihre Arbeitslast-VMs ausgelöst. Sie müssen NSX Tools dennoch installieren, damit die VMs von NSX verwaltet werden können. Bis zur Installation von NSX Tools werden die markierten Arbeitslast-VMs unter Quarantäne gestellt.</p>
Nicht gekennzeichnet	Nicht in der Whitelist	Behält die vorhandene Public Cloud-Sicherheitsgruppe bei, da NSX Cloud keine Aktionen für nicht gekennzeichnete VMs ausführt.
Gekennzeichnet	In Whitelist	Behält die vorhandene Public Cloud-Sicherheitsgruppe bei, da NSX Cloud keine Aktionen für VMs in der Whitelist ausführt.
Nicht gekennzeichnet		

Die folgende Tabelle zeigt, wie NSX Cloud die Public Cloud-Sicherheitsgruppen von VMs verwaltet, wenn die Quarantäne-Richtlinie zuvor aktiviert wurde und jetzt mit einer Fallback-Sicherheitsgruppe deaktiviert ist, die für die Verarbeitung von Sicherheitsgruppenzuweisungen für diese VPC/dieses VNet konfiguriert ist.

**Tabelle 22-3. NSX Cloud-Zuweisung von Public Cloud-Sicherheitsgruppen, wenn die Quarantäne-Richtlinie zunächst aktiviert war und dann deaktiviert ist**

Ist VM in der Public Cloud mit <i>nsx.network=default</i> gekennzeichnet?	Befindet sich die VM in der Whitelist?	Vorhandene Public Cloud-Sicherheitsgruppe der VM, wenn die Quarantäne-Richtlinie aktiviert ist	Die Public Cloud-Sicherheitsgruppe der VM nach der Quarantäne-Richtlinie ist deaktiviert und eine Fallback-Sicherheitsgruppe wird bereitgestellt
Nicht gekennzeichnet	Nicht in der Whitelist	vm-quarantine-sg (Microsoft Azure) oder default(AWS)	Dieser VM wird die Fallback-Sicherheitsgruppe zugewiesen, die Sie beim Deaktivieren der Quarantäne-Richtlinie angegeben haben, da sie nicht gekennzeichnet ist und nicht als NSX-verwaltet betrachtet wird. Deshalb stellt NSX Cloud die Sicherheitsgruppe wieder her, der diese VM zugewiesen wurde, wenn Sie die Quarantäne-Richtlinie deaktivieren.
Gekennzeichnet	Nicht in der Whitelist	vm-underlay-sg oder vm-quarantine-sg (Microsoft Azure) oder default(AWS)	Behält die von NSX Cloud zugewiesene Sicherheitsgruppe bei, da diese für gekennzeichnete VMs im Modus mit aktivierter oder deaktivierter Quarantäne konsistent ist.
Gekennzeichnet	In Whitelist	Beliebige vorhandene Public Cloud-Sicherheitsgruppe	Behält die vorhandene Public Cloud-Sicherheitsgruppe bei, da NSX Cloud keine Aktionen für VMs in der Whitelist ausführt.  <b>Hinweis</b> Wenn in den von NSX Cloud zugewiesenen Sicherheitsgruppen eine Whitelist-VM vorhanden ist, müssen Sie sie manuell in die vorgesehene Fallback-Sicherheitsgruppe verschieben.
Nicht gekennzeichnet			

## Quarantäne-Richtlinie-Auswirkungen bei Aktivierung

NSX Cloud verwaltet die Public Cloud-Sicherheitsgruppe aller Arbeitslast-VMs in dieser VPC/ diesem VNet, wenn die Quarantäne-Richtlinie aktiviert ist.

Manuelle Änderungen an den Sicherheitsgruppen werden innerhalb von zwei Minuten auf die von NSX Cloud zugewiesene Sicherheitsgruppe zurückgesetzt. Wenn Sie nicht möchten, dass NSX Cloud Ihren VMs Sicherheitsgruppen zuweist, können Sie sie in CSM in Whitelists verschieben. Siehe [Verschieben von VMs in die Whitelist](#).

**Hinweis** Das Entfernen der VM aus der Whitelist führt dazu, dass sie auf die von NSX Cloud zugewiesene Sicherheitsgruppe zurückgesetzt wird.

**Tabelle 22-4. NSX Cloud-Zuweisung von Public Cloud-Sicherheitsgruppen, wenn die Quarantäne-Richtlinie aktiviert ist**

Ist VM in der Public Cloud mit <i>nsx.network=default</i> gekennzeichnet?	Befindet sich die VM in der Whitelist?	Public Cloud-Sicherheitsgruppe der VM, wenn die Quarantäne-Richtlinie deaktiviert ist und Erläuterung
Gekennzeichnet	Nicht in der Whitelist	<ul style="list-style-type: none"> <li>■ Wenn die VM keine Bedrohungen aufweist: <i>vm-underlay-sg</i></li> <li>■ Wenn die VM potenzielle Bedrohungen aufweist (siehe Hinweis): <i>vm-quarantine-sg</i> in Microsoft Azure; <i>default</i> in AWS</li> </ul> <p><b>Hinweis</b> Die Zuweisung von Public Cloud-Sicherheitsgruppen wird innerhalb von 90 Sekunden nach der Anwendung des <i>nsx.network=default</i>-Tags auf Ihre Arbeitslast-VMs ausgelöst. Sie müssen NSX Tools dennoch installieren, damit die VMs von NSX verwaltet werden können. Bis zur Installation von NSX Tools werden die markierten Arbeitslast-VMs unter Quarantäne gestellt.</p>
Nicht gekennzeichnet	Nicht in der Whitelist	<i>vm-quarantine-sg</i> in Microsoft Azure; <i>default</i> in AWS. Nicht gekennzeichnete VMs werden als nicht verwaltet betrachtet und daher von NSX Cloud unter Quarantäne gestellt.
Gekennzeichnet	In Whitelist	Behält die vorhandene Public Cloud-Sicherheitsgruppe bei, da NSX Cloud keine Aktionen für VMs in der Whitelist ausführt.
Nicht gekennzeichnet		

In der folgenden Tabelle sind die Auswirkungen auf die Zuweisungen von Sicherheitsgruppen dargestellt, wenn die Quarantäne-Richtlinie zunächst deaktiviert war und Sie sie dann aktivieren:

**Tabelle 22-5. NSX Cloud-Zuweisung von Public Cloud-Sicherheitsgruppen, wenn die Quarantäne-Richtlinie zunächst deaktiviert war und dann aktiviert wird**

Ist VM in der Public Cloud mit <i>nsx.network=default</i> gekennzeichnet?	Befindet sich die VM in der Whitelist?	Vorhandene Public Cloud-Sicherheitsgruppe der VM, wenn die Quarantäne-Richtlinie deaktiviert ist	Public Cloud-Sicherheitsgruppe der VM, nachdem die Quarantäne-Richtlinie aktiviert wurde
Nicht gekennzeichnet	Nicht in der Whitelist	Beliebige vorhandene Public Cloud-Sicherheitsgruppe	vm-quarantine-sg (Microsoft Azure) oder default(AWS)
Gekennzeichnet	Nicht in der Whitelist	vm-underlay-sg oder vm-quarantine-sg (Microsoft Azure) oder default(AWS)	Behält die von NSX Cloud zugewiesene Sicherheitsgruppe bei, die für gekennzeichnete VMs im Modus mit aktivierter oder deaktivierter Quarantäne konsistent ist.
Gekennzeichnet	In Whitelist	Beliebige vorhandene Public Cloud-Sicherheitsgruppe.	Behält die vorhandene Public Cloud-Sicherheitsgruppe bei, da NSX Cloud keine Aktionen für VMs in der Whitelist ausführt.
Nicht gekennzeichnet			

## Quarantäne-Richtlinie im Native Cloud-erzwungener Modus

Die Quarantäne-Richtlinie ist im Native Cloud-erzwungener Modus immer aktiviert.

**Tabelle 22-6. Zuweisung von Public Cloud-Sicherheitsgruppen im Native Cloud-erzwungener Modus**

Ist die VM Teil einer gültigen NSX-T-Sicherheitsrichtlinie?	Befindet sich die VM in der Whitelist?	Public Cloud-Sicherheitsgruppe der VM und Erläuterung
Ja, VM wird mit einer gültigen NSX-T-Sicherheitsrichtlinie abgeglichen	Nicht in der Whitelist	Von NSX Cloud erstellte Public Cloud-Sicherheitsgruppe mit einem Namen wie <i>nsx-{NSX-GUID}</i> , die die entsprechende Public Cloud-Sicherheitsgruppe für die NSX-T-Sicherheitsrichtlinie ist.
Nein, VM verfügt über keine gültige NSX-T-Firewallrichtlinie	Nicht in der Whitelist	vm-quarantine-sg in Microsoft Azure oder default in AWS, da dies das Verhalten der Bedrohungserkennung von NSX Cloud ist. Im Native Cloud-erzwungener Modus imitieren die von NSX Cloud erstellten Sicherheitsgruppen vm-quarantine-sg in Microsoft Azure oder default in AWS die standardmäßige Public Cloud-Sicherheitsrichtlinie.  <b>Hinweis</b> In CSM zeigt die VM einen Fehlerzustand an.
Ja, VM verfügt über eine gültige NSX-T-Sicherheitsrichtlinie	In Whitelist	Behält die vorhandene Public Cloud-Sicherheitsgruppe bei, da NSX Cloud keine Aktionen für VMs in der Whitelist ausführt.
Nein, VM verfügt über keine gültige NSX-T-Sicherheitsrichtlinie		

## Verschieben von VMs in die Whitelist

Die Whitelist ist eine Option, die in CSM für alle Arbeitslast-VMs in Ihrem Public Cloud-Bestand verfügbar ist.

Die Whitelist funktioniert in beiden VM-Verwaltungsmodi: NSX-erzwungener Modus und Native Cloud-erzwungener Modus .

### Gründe für das Verschieben von VMs in die Whitelist

- Im NSX-erzwungener Modus: Wenn Sie die Quarantäne-Richtlinie aktiviert haben und bestimmte DFW-Richtlinien für vorhandene Anwendungen auf der VM überprüfen müssen, verschieben Sie eine derartige VM in die Whitelist, bevor Sie sie in NSX Cloud einbinden.
- Entweder im NSX-erzwungener Modus oder im Native Cloud-erzwungener Modus :
  - Wenn Sie über VMs mit Fehlern verfügen und Sie darauf zugreifen möchten, um Fehler zu beheben, verschieben Sie diese VMs in die Whitelist. Dadurch können Sie den Quarantänestatus für diese VMs aufheben und bei Bedarf Debugging-Tools verwenden.
  - Verschieben Sie VMs in Ihrem Public Cloud-Bestand in die Whitelist, die nicht von NSX-T verwaltet werden sollen, z. B. DNS-Weiterleitung, Proxy-Server usw.

### Vorgehensweise zum Hinzufügen von VMs zur Whitelist oder zum Entfernen aus der Whitelist

Befolgen Sie diese Anweisungen, um der Whitelist VMs hinzuzufügen oder um sie daraus zu entfernen.

#### Voraussetzungen

Sie müssen in CSM mindestens ein Public Cloud-Konto hinzugefügt haben.

#### Verfahren

- 1 Melden Sie sich mit einem Enterprise Admin-Konto bei CSM an und wechseln Sie zu Ihrem Public Cloud-Konto.
  - a Navigieren Sie bei Verwendung von AWS zu **Clouds > AWS > VPCs > Instanzen**.
  - b Navigieren Sie bei Verwendung von Microsoft Azure zu **Clouds > Azure > VNets > Instanzen**.
- 2 Wenn Sie sich im Kachelmodus befinden, wechseln Sie in den Rastermodus, indem Sie in der rechten Ecke der Instanzenansicht auf die Modusauswahl klicken.
- 3 Wählen Sie die VMs (Instanzen) aus, die Sie der Whitelist hinzufügen oder aus der Whitelist entfernen möchten.
- 4 Klicken Sie auf **Aktionen** und wählen Sie entweder **Zu Whitelist hinzufügen** oder **Aus Whitelist entfernen** aus.
- 5 Wechseln Sie zur Registerkarte „Konten“ zurück, wählen Sie die Kontokachel aus und klicken Sie auf **Aktionen > Konto neu synchronisieren**.

## Ergebnisse

Jede der Whitelist hinzugefügte VM verbleibt in der Sicherheitsgruppe, der sie vor dem Hinzufügen zur Whitelist zugewiesen wurde. Sie können jetzt jede andere Sicherheitsgruppe auf die VM anwenden, wenn dies erforderlich ist. NSX Cloud ignoriert Whitelist-VMs unabhängig vom Status der Quarantäne-Richtlinie.

Wenn Sie im Native Cloud-erzwungener Modus eine VM aus der Whitelist entfernen oder im NSX-erzwungener Modus eine von NSX verwaltete VM aus der Whitelist entfernen, beginnt NSX Cloud je nach Status mit der Zuweisung von Sicherheitsgruppen zu dieser VM.

## NSX-erzwungener Modus

Im NSX-erzwungener Modus, also unter Verwendung von NSX Tools, müssen Sie zuerst virtuelle Maschinen einbinden, indem Sie sie in der Public Cloud markieren und NSX Tools auf ihnen installieren, bevor Sie mit dem Verwalten dieser VMs mit NSX-T Data Center beginnen.

## Derzeit unterstützte Betriebssysteme für Arbeitslast-VMs

Dies ist die Liste der derzeit von NSX Cloud unterstützten Betriebssysteme für Ihre Arbeitslast-VMs im NSX-erzwungener Modus.

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. Für unterstützte Betriebssysteme wird davon ausgegangen, dass Sie die Standard-Linux-Kernel-Versionen verwenden. Public Cloud Marketplace-Images mit benutzerdefinierten Kernen, z. B. Upstream-Linux-Kernel mit geänderten Quellen, werden nicht unterstützt.

---

- Red Hat Enterprise Linux (RHEL) 7.2, 7.3, 7.4, 7.5, 7.6

- CentOS 7.2, 7.3, 7.4, 7.5, 7.6

---

**Hinweis** RHEL Extended Update Support (EUS)-Kernel in RHEL und CentOS werden nicht unterstützt.

---

**Hinweis** Nur die CentOS-Download-Center-Images, deren Verteilung mit ihren erwarteten Kernel-Unterversionen übereinstimmen, werden für NSX Cloud unterstützt. Beispiel: Die Verteilungsversionen und ihre entsprechenden Kernel-Versionen lauten erwartungsgemäß wie folgt:

RHEL-Version	Kernel-Version
RHEL 7.6	3.10.0-957
RHEL 7.5	3.10.0-862
RHEL 7.4	3.10.0-693
RHEL 7.3	3.10.0-514
RHEL 7.2	3.10.0-327

---

- Ubuntu 14.04, 16.04, 18.04
- Microsoft Windows Server 2016 – dienstbasierte Version, Desktop Experience (1709, 1803, 1809)
- Microsoft Windows Server 2019 Datacenter
- Microsoft Windows Server 2012 R2
- Microsoft Windows 10-Versionen 1809, 1803, 1709 (wird nur in Microsoft Azure in der aktuellen Version von NSX Cloud unterstützt)

## Einbinden von VMs im NSX-erzwungener Modus

In diesem Workflow finden Sie eine Übersicht über die Schritte zur Einbindung und Verwaltung von Arbeitslast-VMs von Ihrer Public Cloud im NSX-erzwungener Modus.



Tabelle 22-7. Tag-N-Workflow zum Onboarding Ihrer Arbeitslast-VMs in NSX Cloud

Aufgabe	Anweisungen
<input type="checkbox"/> Kennzeichnen Sie Arbeitslast-VMs mit dem Schlüsselwert <code>nsx.network=default</code> .	Befolgen Sie die Anleitung in Ihrer Public-Cloud-Dokumentation für das Taggen von Arbeitslast-VMs.
<input type="checkbox"/> Installieren Sie NSX Tools auf Ihren Windows- und Linux-Arbeitslast-VMs.	Siehe <a href="#">Installieren von NSX Tools</a> .
<b>Hinweis</b> Wenn die Funktion <b>Automatische Installation von NSX Tools</b> in CSM für Microsoft Azure-VNets aktiviert ist, werden NSX Tools automatisch installiert.	
<input type="checkbox"/> (Optional) Entfernen Sie in CSM alle VMs von der Whitelist, für die Sie die NSX-Verwaltung verwenden möchten.	Siehe <a href="#">Vorgehensweise zum Hinzufügen von VMs zur Whitelist</a> oder zum <a href="#">Entfernen aus der Whitelist</a> .
<b>Hinweis</b> Das Verschieben in die Whitelist ist ein manueller Schritt, der im day-0-Workflow empfohlen wird, sobald Sie Ihren Public Cloud-Bestand in CSM hinzufügen. Sie müssen die VMs nicht aus der Whitelist entfernen, wenn Sie ihr keine hinzugefügt haben.	

## Taggen von virtuellen Maschinen in der Public Cloud

Wenden Sie das Tag `nsx.network=default` auf die VMs an, die Sie mithilfe von NSX-T Data Center verwalten möchten.

### Verfahren

- 1 Melden Sie sich bei Ihrem Public Cloud-Konto an und wechseln Sie zu Ihrer VPC oder Ihrem VNet, in der bzw. dem die Arbeitslast-VMs von NSX-T Data Center verwaltet werden sollen.
- 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.

```
Key: nsx.network
Value: default
```

**Hinweis** Wenden Sie dieses Tag auf VM-Ebene an.

### Ergebnisse

Möglicherweise haben Sie die VPCs/VNets, bei denen Sie die `nsx.network=default`-Tags auf Arbeitslast-VMs angewendet haben, bereits integriert. Sie können diese VPCs/VNets auch nach der Anwendung des Tags einbinden. Das erfolgreiche Einbinden der VPC/des VNet führt dazu, dass die Arbeitslast-VMs als NSX-verwaltet betrachtet werden.

### Nächste Schritte

Installieren Sie NSX Tools auf diesen VMs. Siehe [Installieren von NSX Tools](#).

Wenn Sie Microsoft Azure verwenden, können Sie NSX Tools automatisch auf gekennzeichneten VMs installieren. Weitere Informationen finden Sie unter [Automatisches Installieren von NSX Tools](#).

## Installieren von NSX Tools

Installieren von NSX Tools auf Ihren Arbeitslast-VMs

Für die Installation von NSX Tools stehen mehrere Optionen zur Verfügung:

- Laden Sie NSX Tools herunter und installieren Sie sie auf einzelnen Arbeitslast-VMs. Zwischen Linux- und Windows-VMs gibt es einige Abweichungen.
- Verwenden Sie replizierbare Images mit darauf installierten NSX Tools. Nutzen Sie dabei die von Ihrer Public Cloud unterstützte Methode. Erstellen Sie beispielsweise ein AMI in AWS oder ein verwaltetes Image in Microsoft Azure.
- Nur AWS: Stellen Sie beim Starten von VMs den NSX Tools-Speicherort für Downloads und den Installationsbefehl unter **Benutzerdaten** bereit.
- Nur Microsoft Azure: Aktivieren Sie die automatische Installation von NSX Tools bei der Bereitstellung von PCG in einem Microsoft Azure-VNet oder beim Verknüpfen mit einem Transit-VNet oder durch Bearbeiten einer Transit/Computing-VNet-Konfiguration.

---

**Hinweis** Wenn Sie der Whitelist Arbeitslast-VMs hinzugefügt haben, auf den Sie NSX Tools installieren möchten, stellen Sie sicher, dass die folgenden Ports in den Sicherheitsgruppen geöffnet sind, die Sie diesen VMs zugewiesen haben:

- 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 von NSX Tools.
  - UDP 67, 68: für DHCP-Pakete.
  - UDP 53: für die DNS-Auflösung.
- 

### Installieren von NSX Tools auf Linux-VMs

Befolgen Sie diese Anweisungen, um NSX Tools auf Ihren Linux-Arbeitslast-VMs zu installieren.

Unter [Derzeit unterstützte Betriebssysteme für Arbeitslast-VMs](#) 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 Tools 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 PCG-Instanzen verwenden.

- 2 Notieren Sie sich im Bildschirmabschnitt **Herunterladen und Installieren von NSX Tools** den **Speicherort für Downloads** und den **Installationsbefehl** 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 **Speicherort für Downloads**, 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 NSX Tools zu installieren.

- 6 Nach dem Start der Installation von NSX Tools wird die Verbindung mit Ihrer Linux-VM getrennt. Meldungen wie die folgende werden auf dem Bildschirm angezeigt: `Installation completed!!! Starting NSX Agent service. SSH connection will now be lost..` Melden Sie sich erneut bei Ihrer VM an, um den Onboarding-Prozess abzuschließen.

## Ergebnisse

NSX Tools sind auf Ihrer Arbeitslast-VM installiert.

---

### Hinweis

- Nachdem NSX Tools erfolgreich installiert wurden, wird der Port 8888 auf der Arbeitslast-VM als offen angezeigt, ist aber für VMs im Underlay-Modus blockiert und darf nur verwendet werden, wenn er für die erweiterte Fehlerbehebung benötigt wird. Sie können mithilfe eines Jumphosts über Port 8888 auf Arbeitslast-VMs zugreifen, wenn sich der Jumphost in derselben VPC befindet wie die Arbeitslast-VMs, auf die Sie zugreifen möchten.
  - Das Skript verwendet `eth0` als die Standardschnittstelle.
- 

## Nächste Schritte

### Verwalten von VMs im NSX-erzwungener Modus

#### Installieren von NSX Tools auf Windows-VMs

Befolgen Sie diese Anweisungen, um NSX Tools auf Ihren Windows-Arbeitslast-VMs zu installieren.

Unter [Derzeit unterstützte Betriebssysteme für Arbeitslast-VMs](#) 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 **Herunterladen und Installieren von NSX Tools** den **Speicherort für Downloads** 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 **Speicherort für Downloads**, 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. Im Anschluss daran wird eine Meldung angezeigt, die angibt, ob die NSX Tools erfolgreich installiert wurden.

---

**Hinweis** Für das Skript ist die primäre Netzwerkschnittstelle die Standardeinstellung.

---

## Nächste Schritte

Verwalten von VMs im NSX-erzwungener Modus

## 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 Tools](#)
  - 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.

### Automatisches Installieren von NSX Tools

Wird derzeit nur für Microsoft Azure unterstützt.

Wenn in Microsoft Azure die folgenden Kriterien erfüllt sind, werden die NSX Tools automatisch installiert:

- Azure-VM-Erweiterungen werden auf den virtuellen Maschinen im VNet installiert, die in NSX Cloud hinzugefügt wurden. Weitere Informationen erhalten Sie in der [Microsoft Azure-Dokumentation zu VM-Erweiterungen](#).
- Die Sicherheitsgruppe, die auf VMs in Microsoft Azure angewendet wird, muss den Zugriff für die Installation der NSX Tools zulassen. Wenn die Quarantäne-Richtlinie aktiviert ist, können Sie die VMs in CSM vor der Installation in die Whitelist verschieben und sie nach der Installation aus der Whitelist entfernen.
- Mit dem Schlüssel `nsx.network` und dem Wert `default` gekennzeichnete VMs.

So aktivieren Sie diese Funktion:

- 1 Klicken Sie auf **Clouds > Azure > VNets**.
- 2 Wählen Sie das VNet aus, auf dessen VMs Sie CSM automatisch installieren möchten.
- 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 Registerkarte „VNet“ auf das Symbol „AKTIONEN“ und wählen Sie

dann **Konfigurationen bearbeiten** aus. 

- 4 Aktivieren Sie die Option **Automatische Installation von NSX Tools** mit dem Schieberegler.

---

**Hinweis** Wenn die Installation der NSX Tools fehlschlägt, führen Sie die folgenden Schritte aus:

- 1 Melden Sie sich beim Microsoft Azure-Portal an und navigieren Sie zu der VM, auf der die Installation der NSX Tools fehlgeschlagen ist.
- 2 Wechseln Sie zu den Erweiterungen der VM, und deinstallieren Sie die Erweiterung namens `VMwareNsxAgentInstallCustomScriptExtension`.
- 3 Entfernen Sie das Tag `nsx.network=default` von dieser VM.
- 4 Fügen Sie das Tag `nsx.network=default` auf dieser VM erneut hinzu.

Die NSX Tools werden innerhalb von drei Minuten auf dieser VM installiert.

---

### Installieren von NSX Tools mit Benutzerdaten in AWS

Wenn Sie eine neue Arbeitslast-VM in einer AWS-VPC starten, können Sie NSX Tools installieren, indem Sie die NSX Tools-Download- und -Installationsanweisungen im Feld „Benutzerdaten“ angeben.

Kopieren Sie die Download- und Installationsanweisungen für NSX Tools von CSM und fügen Sie sie beim Starten einer neuen Arbeitslast-VM unter „Benutzerdaten“ ein.

#### Verfahren

- 1 Melden Sie sich bei der AWS-Konsole an und starten Sie den Vorgang zum Starten einer neuen Arbeitslast-VM.
- 2 Melden Sie sich in einem anderen Browserfenster bei CSM an.

- a Navigieren Sie zu **Clouds > AWS > VPCs**

---

**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.

---

- b Klicken Sie auf eine Transit- oder Computing-VPC.
  - c Kopieren Sie im Bildschirmabschnitt **Herunterladen und Installieren von NSX Tools** den **Speicherort für Downloads** und den **Installationsbefehl** unter **Linux** oder **Windows**. Dies ist davon abhängig, welches Betriebssystem Sie für Ihre Arbeitslast-VM verwenden.
- 3 Fügen Sie in AWS in den Schritten zum Starten einer neuen Arbeitslast-VM-Instanz den Speicherort für Downloads und den Installationsbefehl als **Text** unter „Benutzerdaten“ im Abschnitt „Erweiterte Details“ ein.



## Ergebnisse

Die Arbeitslast-VM wird gestartet und NSX Tools werden automatisch darauf installiert.

## Deinstallieren von NSX Tools

Verwenden Sie diese betriebssystemspezifischen Befehle zum Deinstallieren von NSX Tools.

### Deinstallieren von NSX Tools 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 Tools 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
```

## Sicherheitsgruppen nach der Einbindung im NSX-erzwungener Modus

Die folgenden Sicherheitsgruppenkonfigurationen werden automatisch durchgeführt:

Wenn die Quarantäne-Richtlinie aktiviert ist:

- Ordnungsgemäße NSX-verwaltete VMs werden nach `vm-underlay-sg` in der Public Cloud verschoben.
- Nicht verwaltete VMs oder von NSX verwaltete VMs mit Fehlern werden in die `default`-Sicherheitsgruppe in AWS und in die `vm-quarantine-sg`-Netzwerksicherheitsgruppe in Microsoft Azure verschoben.
- VMs in der Whitelist sind nicht betroffen.

Wenn die Quarantäne-Richtlinie deaktiviert ist:

- Ordnungsgemäße NSX-verwaltete VMs werden nach `vm-underlay-sg` in der Public Cloud verschoben.
- Von NSX verwaltete VMs mit Fehlern werden in die `default`-Sicherheitsgruppe in AWS und in die `vm-quarantine-sg`-Netzwerksicherheitsgruppe in Microsoft Azure verschoben.
- Nicht verwaltete VMs und VMs in der Whitelist sind davon nicht betroffen.

## Verwalten von VMs im NSX-erzwungener Modus

Führen Sie die folgenden Schritte aus, um die Verwaltung erfolgreich integrierter VMs im NSX-erzwungener Modus zu starten.

**Tabelle 22-8. Mikrosegmentierungs-Workflow für Ihre NSX-verwalteten Workload-VMs im NSX-erzwungener Modus**

Aufgabe	Anweisungen
<input type="checkbox"/> Wenn Sie den eingehenden Zugriff auf Arbeitslast-VMs zulassen möchten, erstellen Sie nach Bedarf DFW-Regeln (verteilte Firewall).	Siehe <a href="#">Standard-Konnektivitätsstrategie für NSX-verwaltete Arbeitslast-VMs im NSX-erzwungener Modus</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.	Siehe <a href="#">Einrichten der Mikrosegmentierung für Arbeitslast-VMs im NSX-erzwungener Modus</a> . Siehe auch: <a href="#">Gruppen-VMs mit NSX-T Data Center und Public-Cloud-Tags</a>

### Standard-Konnektivitätsstrategie für NSX-verwaltete Arbeitslast-VMs im NSX-erzwungener Modus

Bei der PCG-Bereitstellung in Ihrem VPC/Ihrer VNet oder beim Verknüpfen einer Computing-VPC/einem Computing-VNet mit Transit erstellt NSX Cloud darin Standardsicherheitsrichtlinien und DFW-Regeln für NSX-verwaltete Arbeitslast-VMs.

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>cloud-stateful-cloud-&lt;VPC/VNet ID&gt;</code>	Eigenschaften
<code>cloud-&lt;VPC/VNet ID&gt;-managed</code>	Ermöglicht den Zugriff auf die VMs innerhalb derselben VPC oder desselben VNet.
<code>cloud-&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](#).

### Einrichten der Mikrosegmentierung für Arbeitslast-VMs im NSX-erzwungener Modus

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.

## Native Cloud-erzwungener Modus

Im Native Cloud-erzwungener Modus werden alle Arbeitslast-VMs automatisch von NSX verwaltet. Folgen Sie dem hier beschriebenen Workflow, um mit der Verwaltung dieser VMs mit NSX-T Data Center zu beginnen.

---

**Hinweis** Alle Betriebssysteme werden für Ihre Arbeitslast-VMs im Native Cloud-erzwungener Modus unterstützt.

---

## Verwalten von VMs im Native Cloud-erzwungener Modus

Im Native Cloud-erzwungener Modus verwendet NSX Cloud NSX-T Data Center-Gruppen und Regeln für verteilte Firewalls, um entsprechende Anwendungssicherheitsgruppen und Netzwerksicherheitsgruppen in Microsoft Azure und Sicherheitsgruppen in AWS zu erstellen.

Alle Arbeitslast-VMs in Ihren VPCs/VNets, die in den Native Cloud-erzwungener Modus integriert sind, werden von NSX verwaltet.

Wenden Sie den folgenden Workflow an:

**Tabelle 22-9. Mikrosegmentierungs-Workflow für Ihre Arbeitslast-VMs im Native Cloud-erzwungener Modus**

Aufgabe	Anweisungen
<input type="checkbox"/> Erstellen Sie eine oder mehrere Gruppen in NSX Manager, um Arbeitslast-VMs aus Ihrer Public Cloud einzubeziehen.	Siehe <a href="#">Einrichten der Mikrosegmentierung für Arbeitslast-VMs im Native Cloud-erzwungener Modus</a> Siehe auch: <a href="#">Gruppen-VMs mit NSX-T Data Center und Public-Cloud-Tags</a>
<input type="checkbox"/> Erstellen Sie eine oder mehrere Sicherheitsrichtlinien in NSX Manager, die für die Gruppe(n) gelten, die Sie für Ihre Public Cloud-Arbeitslast-VMs erstellt haben.	
<input type="checkbox"/> Entfernen Sie Arbeitslast-VMs aus der Whitelist in CSM, wenn Sie von NSX-T-Sicherheitsrichtlinien verwaltet werden sollen.	
<input type="checkbox"/> Synchronisieren Sie Ihr Public Cloud-Konto in CSM neu.	
<input type="checkbox"/> Wechseln Sie in Ihrer VPC/Ihrem VNet zur Detailansicht in CSM, um eine Fehlerbehebung für die Sicherheitsrichtlinien durchzuführen, sofern Fehler vorhanden sind.	Siehe <a href="#">Aktuelle Einschränkungen und häufige Fehler</a>

## Einrichten der Mikrosegmentierung für Arbeitslast-VMs im Native Cloud-erzwungener Modus

In diesem Workflow finden Sie Informationen zur Konfiguration der Sicherheitsrichtlinie in NSX Manager für Arbeitslast-VMs im Native Cloud-erzwungener Modus . Das heißt, dass Sie NSX Tools nicht auf den Arbeitslast-VMs installieren.

### Voraussetzungen

Sie müssen über ein bzw. eine Transit- oder Computing-VPC/VNet im Native Cloud-erzwungener Modus verfügen.

## Verfahren

- 1 In NSX Manager können Sie Gruppen für Arbeitslast-VMs bearbeiten oder erstellen. VM-Namen, die mit web, app, db beginnen, könnten beispielsweise drei separaten Gruppen zugewiesen sein. Weitere Anweisungen finden Sie unter [Hinzufügen einer Gruppe](#). Informationen zur Verwendung von Public Cloud-Tags zum Erstellen von Gruppen für Ihre Arbeitslast-VMs finden Sie auch unter [Gruppen-VMs mit NSX-T Data Center und Public-Cloud-Tags](#).

Arbeitslast-VMs, die den Kriterien entsprechen, werden der Gruppe hinzugefügt. VMs, die nicht mit den Gruppierungskriterien übereinstimmen, werden in der `default`-Sicherheitsgruppe in AWS und in der `vm-quarantine-sg`-Netzwerksicherheitsgruppe in Microsoft Azure platziert.

---

**Hinweis** Sie können die von NSX Cloud automatisch erstellten Gruppen nicht verwenden.

---

**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 in NSX Manager Regeln für verteilte Firewalls für die Gruppen in den Feldern **Quelle**, **Ziel** oder **Angewendet auf**. Weitere Anweisungen finden Sie unter [Hinzufügen einer verteilten Firewall](#).

**Hinweis** Nur statusbehaftete Richtlinien werden für Public Cloud-Arbeitslast-VMs unterstützt. Statusfreie Richtlinien können in NSX Manager erstellt werden. Sie werden jedoch nicht mit Gruppen abgeglichen, die ihre Public Cloud-Arbeitslast-VMs enthalten.

---

- 3 Entfernen Sie in CSM die VMs aus der Whitelist, die in die NSX-Verwaltung einbezogen werden sollen. Weitere Anweisungen finden Sie unter [Vorgehensweise zum Hinzufügen von VMs zur Whitelist oder zum Entfernen aus der Whitelist](#).

**Hinweis** Das Verschieben in die Whitelist ist ein manueller Schritt, der im day-0-Workflow dringend empfohlen wird, sobald Sie Ihren Public Cloud-Bestand in CSM hinzufügen. Wenn Sie keine VMs in die Whitelist verschoben haben, müssen Sie sie nicht aus der Whitelist entfernen.

---

4 Für Gruppen und DFW-Regeln, die eine Übereinstimmung in der Public Cloud finden, erfolgt automatisch Folgendes:

- a In AWS erstellt NSX Cloud eine neue Sicherheitsgruppe mit einer Bezeichnung wie `nsx-<NSX_GUID>`.
- b In Microsoft Azure erstellt NSX Cloud eine Anwendungssicherheitsgruppe (ASG), die der in NSX Manager erstellten Gruppe entspricht, sowie eine Netzwerksicherheitsgruppe (NSG), die den DFW-Regeln entspricht, die mit gruppierten Arbeitslast-VMs abgeglichen werden.

---

**Hinweis** NSX Cloud synchronisiert NSX Manager und Public Cloud-Gruppen sowie DFW-Regeln alle 30 Sekunden.

---

5 Neusynchronisieren des Public Cloud-Kontos in CSM:

- a Melden Sie sich bei CSM an und wechseln Sie zu Ihrem Public Cloud-Konto:
- b Klicken Sie im Public Cloud-Konto auf **Aktionen > Neusynchronisierungskonto**. Warten Sie, bis das Upgrade abgeschlossen ist.
- c Navigieren Sie zum VPC/zur VNet und klicken Sie auf den roten Fehlerindikator. Dadurch gelangen Sie zur Ansicht „Instanzen“.
- d Wechseln Sie die Ansicht auf „Details“, wenn Sie das Raster anzeigen und klicken Sie in der Spalte „Regelumsetzung“ auf **Fehlgeschlagen**, um ggf. vorhandene Fehler anzuzeigen.

#### Nächste Schritte

Siehe [Aktuelle Einschränkungen und häufige Fehler](#).

### Aktuelle Einschränkungen und häufige Fehler

Weitere Informationen zur Fehlerbehebung bei der Verwaltung Ihrer Public Cloud-Arbeitslast-VMs im Native Cloud-erzwungener Modus erhalten Sie unter diesen bekannten Einschränkungen und allgemeinen Fehlern.

---

**Hinweis** Die folgenden Grenzwerte werden von Ihrer Public Cloud festgelegt:

- Die Anzahl Sicherheitsgruppen, die auf eine Arbeitslast-VM angewendet werden können.
- Die Anzahl Regeln, die für eine Arbeitslast-VM realisiert werden können.
- Die Anzahl Regeln, die pro Sicherheitsgruppe realisiert werden können.
- Der Geltungsbereich der Sicherheitsgruppenzuweisung, z. B. der Geltungsbereich der Netzwerksicherheitsgruppe (NSG) in Microsoft Azure, ist auf diese Region beschränkt, wohingegen der Geltungsbereich der Sicherheitsgruppe (SG) in AWS auf diese VPC beschränkt ist.

Weitere Informationen zu diesen Grenzwerten finden Sie in der Public Cloud-Dokumentation.

---

## Aktuelle Einschränkungen

Die aktuelle Version weist die folgenden Einschränkungen für DFW-Regeln für Arbeitslast-VMs auf:

- Geschachtelte Gruppen werden nicht unterstützt.
- Gruppen ohne VM und/oder IP-Adresse als Mitglied werden nicht unterstützt, z. B. auf Segment- oder logischen Ports basierte Kriterien werden nicht unterstützt.
- Sowohl Quelle als auch Ziel als IP-Adresse oder CIDR-basierte Gruppe wird nicht unterstützt.
- Sowohl Quelle als auch Ziel als „ANY“ werden nicht unterstützt.
- Die Gruppe **Applied\_To** kann nur eine Quell- oder Zielgruppe oder eine Quell- und Zielgruppe sein. Andere Optionen werden nicht unterstützt.
- Nur die lokale VPC/VNet-Regelerzwingung wird unterstützt. Sie können Gruppen in NSX Manager erstellen, die sich über VPC/VNets erstrecken. Die Umsetzung solcher Regeln funktioniert jedoch nur innerhalb der VPC/des VNet. VPC/VNet-übergreifende DFW-Regeln werden nicht realisiert.
- Nur TCP und UDP werden unterstützt.

---

### Hinweis Nur in AWS:

Ablehnungsregeln, die für Arbeitslast-VMs in Ihren AWS-VPCs erstellt wurden, werden in AWS nicht realisiert, da in AWS standardmäßig alles in die Blacklist verschoben wird. Dies führt zu den folgenden Ergebnissen in NSX-T Data Center:

- Wenn es eine Ablehnungsregel zwischen VM1 und VM2 gibt, ist der Datenverkehr zwischen VM1 und VM2 aufgrund des standardmäßigen AWS-Verhaltens und nicht aufgrund der Ablehnungsregel unzulässig. Die Ablehnungsregel wird in AWS nicht realisiert.
- Angenommen, die folgenden beiden Regeln werden in NSX Manager für dieselben VMs erstellt, wobei Regel 1 eine höhere Priorität hat als Regel 2:
  - a VM1 to VM2 DENY SSH
  - b VM1 to VM2 Allow SSH

Die Ablehnungsregel wird ignoriert, da sie in AWS nicht realisiert wird. Daher wird die Allow SSH-Regel umgesetzt. Dies widerspricht der Erwartung, ist aber eine Einschränkung aufgrund des standardmäßigen AWS-Verhaltens.

---

## Häufige Fehler und deren Auflösung

### Fehler: auf VM wird keine NSX-Richtlinie angewendet.

Wenn dieser Fehler angezeigt wird, wurden keine der DFW-Regeln auf die jeweilige VM angewendet. Bearbeiten Sie die Regel oder die Gruppe in NSX Manager, um diese VM einzubeziehen.

### Fehler: statusfreie NSX-Regel wird nicht unterstützt.

Wenn dieser Fehler angezeigt wird, bedeutet dies, dass Sie DFW-Regeln für Public Cloud-Arbeitslast-VMs in einer statusfreien Sicherheitsrichtlinie hinzugefügt haben. Dies wird nicht unterstützt. Erstellen Sie eine neue Sicherheitsrichtlinie oder verwenden Sie eine vorhandene Sicherheitsrichtlinie im statusbehafteten Modus.

## NSX-T Data Center-Funktionen mit Support in NSX Cloud

NSX Cloud erstellt eine Netzwerktopologie für Ihr Public Cloud-VPC oder -VNet durch Generierung logischer Netzwerkentitäten in NSX-T Data Center.

Verwenden Sie diese Liste als Referenz 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.

Tabelle 22-10.

NSX-T Data Center-Funktion	Details	NSX Cloud-Hinweis
Segmente oder logische Switches	Siehe <a href="#">Kapitel 4 Segmente</a> .	Für jedes Public Cloud-Subnetz wird ein Segment erstellt, an das eine verwaltete VM angeschlossen ist. Das ist ein Hybridsegment.
Gateways oder logische Router	Siehe <a href="#">Kapitel 2 Tier-0-Gateways</a> und <a href="#">Kapitel 3 Tier-1-Gateway</a> .	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.



Tabelle 22-10. (Fortsetzung)

NSX-T Data Center-Funktion	Details	NSX Cloud-Hinweis
IPFIX	Siehe <a href="#">Konfigurieren von IPFIX</a> .	<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>
Port-Mirroring	Siehe <a href="#">Überwachen von Port-Mirroring-Sitzungen</a> .	<p>Port-Mirroring wird in der aktuellen Version nur in AWS unterstützt.</p> <ul style="list-style-type: none"> <li>■ Für NSX Cloud konfigurieren Sie Port-Mirroring unter <b>Tools &gt; Port-Mirroring-Sitzungen</b>.</li> <li>■ Nur L3SPAN-Port-Mirroring wird unterstützt.</li> <li>■ Der Collector muss sich in derselben VPC bzw. demselben VNet befinden wie die Quell-Arbeitslast-VM.</li> </ul>
Gateway-Firewall	Siehe <a href="#">Konfigurieren einer Gateway-Firewall</a> .	Wird nur auf Tier-0-Gateways unterstützt.

## 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 22-11. Zusammenfassung der Tag-Typen und Einschränkungen

Tag-Typ	Tag-Geltungsbereich oder vorab festgelegtes Präfix	Einschränkungen	Enterprise-Administrator Berechtigungen	Auditor Berechtigungen
Systemdefiniert	Vollständige System-Tags: ■ azure:subscription_id ■ azure:region ■ azure:vm_rg ■ azure:vnet_name ■ azure:vnet_rg ■ aws:vpc ■ aws:availability zone	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 <hr/> <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. <hr/> Tags mit dem Präfix <b>nsx</b> werden ignoriert.	Nur Lesen	Nur Lesen
Benutzer	Benutzer-Tags können einen beliebigen Geltungsbereich (Schlüssel) und	Geltungsbereich (Schlüssel): 30 Zeichen Tag (Wert): 65 Zeichen Zulässiger Maximalwert: 25	Hinzufügen/Bearbeiten/Löschen	Nur Lesen

Tabelle 22-11. Zusammenfassung der Tag-Typen und Einschränkungen (Fortsetzung)

Tag-Typ	Tag-Geltungsbereich oder vorab festgelegtes Präfix	Einschränkungen	Enterprise-Administrator Berechtigungen	Auditor Berechtigungen
	Wert innerhalb der 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 22-12.

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=AbcdefghijklmnopqrstuvwxyzAb23690hgjgjuytreswqacvbcdefghijklmnopqrstuvwxyz	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 [Hinzufügen einer Gruppe](#).
- Siehe [Einrichten der Mikrosegmentierung für Arbeitslast-VMs im NSX-erzwungener Modus](#).

## Verwenden von Native Cloud-Diensten

Die folgenden Native-Cloud-Dienste werden für die Verwendung mit Ihren Public Cloud-Arbeitslast-VMs in NSX Manager unterstützt.

Wenn Sie PCG bereitstellen, wird eine Gruppe in NSX Manager für jeden unterstützten Native Cloud-Dienst erstellt.

Die folgenden Gruppen werden für die aktuell unterstützten Public Cloud-Dienste erstellt:

- aws-dynamo-db-service-endpoint
- aws-elb-service-endpoint
- aws-rds-service-endpoint
- aws-s3-service-endpoint
- azure-cosmos-db-service-endpoint
- azure-load-balancer-service-endpoint
- azure-sql-service-endpoint
- azure-storage-service-endpoint

Erstellen Sie zum Verwenden dieser Native Cloud-Dienste DFW-Richtlinien, die je nach Bedarf die Native Cloud-Dienstgruppe in den Quell- oder Zielfeldern der Regel enthalten.

DFW-Regeln werden auf VMs erzwungen, für die Native Cloud-Dienste.

---

**Hinweis** Im NSX-erzwungener Modus, das heißt, Verwalten Ihrer Arbeitslasten mit NSX Tools, gibt es momentan keine Unterstützung für die Native Cloud-Dienste von Microsoft Azure.

---

### Aktuelle Einschränkungen

ENDPOINT			DFW-Regel mit dem Dienst als ZIEL		DFW-Regel mit dem Dienst als QUELLE	
Public Cloud	Dienst	Geltungsbereich	Auf VM erzwungen?	Für Dienst erzwungen?	Für Dienst erzwungen?	Auf VM erzwungen?
Microsoft Azure	BLOB-Speicher	Global	Ja	Nein	Nein	Ja
	Cosmos-DB					
	SQL					
	Load Balancer					
AWS	S3	VPC lokal	Ja	Nein	Nein	Ja
	Dynamo DB					

ENDPOINT			DFW-Regel mit dem Dienst als ZIEL		DFW-Regel mit dem Dienst als QUELLE	
	RDS					
	ELB					

## 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 22-13. 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> .
	Erstellen eines IPSec-VPN-Tunnels zwischen der Dienst-Appliance und dem PCG.	Siehe <a href="#">Einrichten einer IPSec-VPN-Sitzung</a> .

**Tabelle 22-13. Überblick über die Konfigurationen, die für die Dienstefügung bei NSX-verwalteten Arbeitslast-VMs in der Public Cloud benötigt werden. (Fortsetzung)**

Häufigkeit	Aufgabe	Anweisungen
	Konfigurieren Sie BGP zwischen PCG und der Dienst-Appliance und kündigen Sie die VSIP in der Dienst-Appliance und die Standardroute (0.0.0.0/0) im PCG an.	Siehe <a href="#">Konfigurieren von BGP und Route Redistribution</a> .
	<b>Hinweis</b> In der aktuellen Version wird die Service Insertion nur für vertikalen Datenverkehr unterstützt.	
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
Name	Der Name dieses VPN-Diensts wird zum Einrichten des lokalen Endpoints und der IPSec-VPN-Sitzungen verwendet. Notieren Sie sich den Namen.
Diensttyp	Bestätigen Sie, dass dieser Wert auf IPSec festgelegt ist.
Tier-O-Gateway	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. <code>cloud-t0-vpc-6bcd2c13</code> .

- 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
Name	Der Name des lokalen Endpoints wird verwendet, um die IPSec-VPN-Sitzungen einzurichten. Notieren Sie sich den Namen.
VPN-Dienst	Wählen Sie den in Schritt 2 hinzugefügten VPN-Dienst aus.
IP-Adresse	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 <code>nsx:local_endpoint_ip</code> , 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
Typ	Bestätigen Sie, dass dieser Wert auf <b>Routenbasiert</b> festgelegt ist.
VPN-Dienst	Wählen Sie den in Schritt 2 hinzugefügten VPN-Dienst aus.
Lokaler Endpoint	Wählen Sie den in Schritt 3 erstellten lokalen Endpoint aus.
Remote-IP	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.

## 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
IP-Adresse	Verwenden Sie die IP-Adresse, die in der Tunnelschnittstelle der Dienst-Appliance für das VPN zwischen dem PCG und der Dienst-Appliance konfiguriert wurde.
Remote-AS-Nummer	Diese Zahl muss mit der AS-Nummer der Dienst-Appliance in Ihrer Public Cloud übereinstimmen.
Routenfilter	Richten Sie einen Filter für ausgehende Daten ein, um die Standardroute (0.0.0.0/0) vom PCG zur Dienst-Appliance anzukündigen.

#### 5 Aktivieren Sie auf dem Tier-0-Gateway im Abschnitt **Route Redistribution** statische Routen.

### Route Redistribution festlegen

Tier-0-Gateway cloud-t0-415... #Route Redistribution 1

ROUTE REDISTRIBUTION HINZUFÜGEN Suchen

Name	Route Redistribution	Route Map
Namen eingeben	Festlegen*	Routenzuordnung auswählen

#### Route Redistribution festlegen

Tier-0-Gateway cloud-t0-415... #Ausgewählte Quellen 1

Quellen unten auswählen

**Tier-0-Subnetze**

- ☒ Statische Routen
- ☐ Lokale IPSec-IP
- ☐ EVPN-TEP-IP
- ☐ Verbundene Schnittstellen und Segmente
  - ☐ Subnetz der Dienstschnittstelle
  - ☐ Subnetz der Loopback-Schnittstelle

- ☐ NAT-IP
- ☐ DNS-Weiterleitungs-IP
- ☐ Subnetz der externen Schnittstelle
- ☐ Verbundenes Segment

#### 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>Name:</b>	Geben Sie einen aussagekräftigen Namen für die Richtlinie an, z. B. <b>Vertikale Service Insertion für Azure-VMs</b> .
<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> .
<b>Anwenden auf:</b>	Wählen Sie das Tier-0-Gateway des PCGs aus.

- 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 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 22-14.

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.

## 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>
```

## Einrichten von VPN im erzwungenen NSX-Modus

Sie können VPN mithilfe von PCGs einrichten, die in der lokalen NSX-T Data Center-Bereitstellung als automatisch erstellte Tier-0-Gateways angezeigt werden. Diese Anweisungen gelten spezifisch für Arbeitslast-VMs, die im erzwungenen NSX-Modus ausgeführt werden.

Verwenden Sie PCGs auf dieselbe Weise wie Sie Tier-0-Gateways in NSX Manager verwenden, um VPN zu konfigurieren, indem Sie die folgenden Schritte ausführen. Sie können VPN-Tunnel zwischen PCGs erstellen, die in derselben Public Cloud oder unterschiedlichen Public Clouds oder mit einem lokalen Gateway oder Router bereitgestellt sind. Unter [Kapitel 5 Virtual Private Network \(VPN\)](#) finden Sie weitere Details zur VPN-Unterstützung in NSX-T Data Center.

### Voraussetzungen

- Prüfen Sie, ob ein PCG-Paar für Hochverfügbarkeit in einer VPC/einem VNet bereitgestellt wurde.
- Prüfen Sie, ob der Remote-Peer routenbasiertes VPN und BGP unterstützt.

### Verfahren

- 1 Suchen Sie in Ihrer Public Cloud den von NSX zugewiesenen lokalen Endpoint für das PCG und weisen Sie bei Bedarf eine öffentliche IP-Adresse zu:
  - a Wechseln Sie zu ihrer PCG-Instanz in der Public Cloud und navigieren Sie zu „Tags“.
  - b Notieren Sie sich die IP-Adresse im Wertfeld des Tags `nsx.local_endpoint_ip`.
  - c (Optional) Wenn Ihr VPN-Tunnel eine öffentliche IP erfordert, weil Sie z. B. ein VPN zu einer anderen Public Cloud oder zu einer lokalen NSX-T Data Center-Bereitstellung einrichten möchten:
    - 1 Navigieren Sie zur Uplink-Schnittstelle der PCG-Instanz.
    - 2 Hängen Sie eine öffentliche IP-Adresse an die `nsx.local_endpoint_ip`-IP-Adresse an, die Sie in Schritt **b**. notiert haben.
  - d (Optional) Wenn Sie ein Hochverfügbarkeitspaar aus PCG-Instanzen haben, wiederholen Sie die Schritte **a** und **b** und hängen Sie bei Bedarf eine öffentliche IP-Adresse an, wie in Schritt **c** beschrieben.



- 2 Aktivieren Sie in NSX Manager IPsec-VPN für das PCG, das als Tier-0-Gateway mit einem Namen wie z. B. `cloud-t0-vpc/vnet-<vpc/vnet-id>` angezeigt wird, und erstellen Sie routenbasierte IPsec-Sitzungen zwischen dem Endpoint dieses Tier-0-Gateways und der Remote-IP-Adresse des gewünschten VPN-Peers. Weitere Informationen finden Sie unter [Hinzufügen eines IPsec-VPN-Dienstes](#).

- a Wechseln Sie zu **Netzwerk > VPN > VPN-Dienste > Dienst hinzufügen > IPsec**. Geben Sie die folgenden Details an:

Option	Bezeichnung
Name	Geben Sie einen aussagekräftigen Namen für den VPN-Dienst ein, z. B. <code>&lt;VPC-ID&gt;-AWS_VPN</code> oder <code>&lt;VNet-ID&gt;-AZURE_VPN</code> .
Tier-0/Tier-1-Gateway	Wählen Sie das Tier-0-Gateway für das PCG in Ihrer Public Cloud aus.

- b Wechseln Sie zu **Netzwerk > VPN > Lokale Endpoints > Lokalen Endpoint hinzufügen**. Geben Sie die folgenden Informationen ein und lesen Sie [Hinzufügen von lokalen Endpoints](#) für weitere Details:

**Hinweis** Wenn Sie ein Hochverfügbarkeitspaar aus PCG-Instanzen haben, erstellen Sie für jede Instanz einen lokalen Endpoint, indem Sie die entsprechende lokale Endpoint-IP-Adresse verwenden, die diesem in der Public Cloud angehängt ist.

Option	Bezeichnung
Name	Geben Sie einen aussagekräftigen Namen für den lokalen Endpoint ein, z. B. <code>&lt;VPC-ID&gt;-PCG-preferred-LE</code> oder <code>&lt;VNET-ID&gt;-PCG-preferred-LE</code> .
VPN-Dienst	Wählen Sie den VPN-Dienst für das Tier-0-Gateway des PCG aus, das Sie in Schritt <b>2a</b> erstellt haben.
IP-Adresse	Geben Sie den Wert der lokalen Endpoint-IP-Adresse des PCGs ein, die Sie in Schritt <b>1b</b> notiert haben.

- c Wechseln Sie zu **Netzwerk > VPN > IPsec-Sitzungen > IPsec-Sitzung hinzufügen > Routenbasiert**. Geben Sie die folgenden Informationen ein und lesen Sie weitere Details unter [Hinzufügen einer routenbasierten IPsec-Sitzung](#):

**Hinweis** Wenn Sie zwischen in einer VPC bereitgestellten PCGs und in einem VNet bereitgestellten PCGs einen VPN-Tunnel erstellen, müssen Sie zwischen dem lokalen Endpoint jedes PCGs in der VPC und der Remote-IP-Adresse des PCG im VNet einen Tunnel erstellen und umgekehrt von den PCGs im VNet zu der Remote-IP-Adresse der PCGs in der VPC. Für aktive und Standby-PCGs müssen Sie separate Tunnel erstellen. Daraus ergibt sich ein vollständig vermaschtes Netz von IPsec-Sitzungen zwischen den beiden Public Clouds.

Option	Bezeichnung
Name	Geben Sie einen aussagekräftigen Namen für die IPsec-Sitzung ein, z. B. <code>&lt;VPC-ID&gt;-PCG1-to-remote_edge</code>
VPN-Dienst	Wählen Sie den in Schritt <b>2a</b> erstellten VPN-Dienst aus.
Lokaler Endpoint	Wählen Sie den in Schritt <b>2b</b> erstellten lokalen Endpoint aus.
Remote-IP	Geben Sie die öffentliche IP-Adresse des Remote-Peers ein, zu dem Sie den VPN-Tunnel erstellen.

**Schritt 2a.**

**VPN-DIENSTE** IPSEC-SITZUNGEN L2-VPN-SITZUNGEN LOKALE ENDPOINTS PROFILE

[DIENST HINZUFÜGEN](#) [ALLE REDUZIEREN](#) Nach Name, Pfad usw. filtern

Name	Diensttyp	Tier-0/Tier-1-Gateway	Sitzungen	Status
<VPC-ID>-AWS_VPN	IPSec	cloud-to-vpc-073617880a9622d93	1	Erfolgreich

**Beschreibung** VPN service on AWS Transit VPC ID vpc-073617880a9622d93

**Administrativer Status** Aktiviert

**IKE-Protokollebene** Info **Tags** 0

**Sitzungssynchronisierung** Aktiviert

**Globale Umgehungsregeln**

---

**Schritt 2b.**

**VPN-DIENSTE** IPSEC-SITZUNGEN L2-VPN-SITZUNGEN **LOKALE ENDPOINTS** PROFILE

[LOKALEN ENDPOINT HINZUFÜGEN](#) [ALLE REDUZIEREN](#) Nach Name, Pfad usw. filtern

Name	VPN-Dienst	IP-Adresse	Site-Zertifikate	Sitzungen	Status
<VPC-ID>-PCG-preferred-LE	<VPC-ID>-AWS_VPN	10.99.3.35	Nicht festgelegt	1	Erfolgreich

**Beschreibung** Nicht festgelegt

**Vertrauenswürdige CA-Zertifikate** Nicht festgelegt

**Lokale ID** 10.99.3.35

**Zertifikatswiderrufsliste** Nicht festgelegt

**Tags** 0

---

**Schritt 2c.**

**VPN-DIENSTE** **IPSEC-SITZUNGEN** L2-VPN-SITZUNGEN LOKALE ENDPOINTS PROFILE

[IPSEC-SITZUNG HINZUFÜGEN](#) [ALLE REDUZIEREN](#) admin

Name	Typ	VPN-Dienst	Lokaler Endpoint	Remote-IP	Status	Alarmer
<VPC-ID>-PCG-to-remote_edge	Routenbasiert	<VPC-ID>-AWS_VPN	<VPC-ID>-PCG-preferred-LE	3.213.92.220	Inaktiv	0

**Beschreibung** Nicht festgelegt

**Administrativer Status** Aktiviert

**Übereinstimmungs-Suite** Keine **Tunnelschnittstelle** 192.168.50.10/24

**Authentifizierungsmodus** PSK **Remote-ID** 172.0.3.145

**Vorinstallierter Schlüssel** .....

**Erweiterte Eigenschaften**

**IKE-Profil** nsx-default-l3vpn-ike **Initiierungsmodus der Verbindung** Initiator

[STATISTIK ANZEIGEN](#) [KONFIGURATION HERUNTERLADEN](#)

[AKTUALISIEREN](#) 1 - 1 von 1 IPsec-Sitzungen

- 3 Richten Sie an der IPsec-VPN-Tunnelschnittstelle, die Sie in Schritt 2 eingerichtet haben, BGP-Nachbarn ein. Weitere Informationen finden Sie unter [Konfigurieren des BGP-Protokolls](#).
  - a Navigieren Sie zu **Netzwerk > Tier-O-Gateways**
  - b Wählen Sie das automatisch erstellte Tier-O-Gateway aus, für das Sie die IPsec-Sitzung erstellt haben, und klicken Sie auf **Bearbeiten**.
  - c Klicken Sie auf die Zahl oder das Symbol neben **BGP-Nachbarn** unter dem Abschnitt **BGP** und geben Sie Folgendes ein:

Option	Bezeichnung
IP-Adresse	Verwenden Sie die IP-Adresse der Remote-VTI, die an der Tunnelschnittstelle in der IPsec-Sitzung für den VPN-Peer konfiguriert wurde.
Remote-AS-Nummer	Diese Nummer muss mit der AS-Nummer des Remote-Peers übereinstimmen.

Tier-O-Gateway

[GATEWAY HINZUFÜGEN](#) ALLE ERWEITERN Nach N

Name des Tier-O-Gateways	HA-Modus	Verknüpfte Tier-1-Gateways	Verknüpfte Segmente
<b>MULTICAST</b>			
<b>BGP</b>			
Lokale AS	1000	SR-übergreifendes iBGP	Ein
BGP	Ein	ECMP	Ein
Graceful Restart	Nur Helfer	Multipath Relax	Ein
Graceful Restart-Timer	180 Sekunden	Stale-Timer für Graceful Restart	600 Sekunden
Routenaggregation	0	BGP-Nachbarn	1

**Schritt 3.**

### BGP-Nachbarn

Tier-O-Gateway cloud-t0-415... [#Nachbarn](#)

	IP-Adresse	BFD	Remote-AS-Nummer
⋮	192.168.50.11	Deaktiviert	1000
	Quelladressen	Nicht festgelegt	
	Max. Hop-Grenzwert	1	

- 4 Kündigen Sie die Präfixe, die Sie für das für das VPN verwenden möchten, über das Neuverteilungsprofil an. Verbinden Sie im NSX-erzwungener Modus für Tier 1 aktivierte Routen im Neuverteilungsprofil.

**Tier-O-Gateway**

GATEWAY HINZUFÜGEN ALLE ERWEITERN Nach Name, Pfad us

	Name des Tier-O-Gateways	HA-Modus	Verknüpfte Tier-1-Gateways	Verknüpfte Segmente	Status <span>1</span>
>	BGP				
▼	ROUTE REDISTRIBUTION				
	Route Redistribution	2	Route Redistribution-Status	Ein	
⋮ >	VRF TOrvf	Aktiv-Aktiv	0	0	Erfolg

AKTUALISIEREN

**Schritt 4.**

Route Redistribution

Tier-O-Gateway cloud-to-vpc... #Ausgewählte Quellen 1

Tier-O-Subnetze

Angekündigte Tier-1-Subnetze

- Verbundene Schnittstellen und Segmente
- Subnetz der Dienstschnittstelle
- Verbundenes Segment

## Häufig gestellte Fragen

Hier finden Sie eine Auflistung einiger häufig gestellter Fragen.

### Wie kann ich prüfen, ob meine NSX Cloud-Komponenten installiert sind und ausgeführt werden?

- 1 Führen Sie folgende Schritte aus, um sicherzustellen, dass NSX Tools auf Ihrer Arbeitslast-VM mit PCG verbunden sind:
  - a Geben Sie den Befehl `nsxcli` ein, um die NSX-CLI zu öffnen.
  - b 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
```

- 2 Die Arbeitslast-VMs müssen über die korrekten Tags verfügen, um eine Verbindung zum PCG herstellen zu können:

- a Melden Sie sich bei der AWS-Konsole oder dem Microsoft Azure-Portal an.
- b Überprüfen Sie die Tags „eth0“ und „interface“ der VM.

Der Schlüssel `nsx.network` muss den Wert `default` aufweisen.

## Meine mit cloud-init gestarteten VMs werden unter Quarantäne gestellt und die Installation von Drittanbietertools ist nicht zulässig. Was soll ich tun?

Wenn die Quarantäne-Richtlinie aktiviert ist und Sie VMs mithilfe von cloud-init-Skripts mit den folgenden Spezifikationen starten, werden Ihre VMs beim Start unter Quarantäne gestellt und Sie können keine benutzerdefinierten Anwendungen oder Tools darauf installieren:

- gekennzeichnet mit `nsx.network=default`
- automatische Installation oder Bootstrap-Vorgang für benutzerdefinierte Dienste, wenn die VM eingeschaltet wird

### Lösung:

Aktualisieren Sie die Sicherheitsgruppe `default` (AWS) oder `default-vnet-<vnet-ID>-sg` (Microsoft Azure), um eingehende/ausgehende Ports hinzuzufügen, wie für die Installation von benutzerdefinierten oder Drittanbieteranwendungen erforderlich.

## Ich habe meine VM korrekt gekennzeichnet und NSX Tools 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.network` 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?

In Ihrer Public Cloud (AWS oder Microsoft Azure):

- 1 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 [Bedrohungserkennung mit der NSX Cloud-Quarantäne-Richtlinie](#).
  - NSX-T Data Center-DFW-Regeln Weitere Informationen finden Sie unter [Standard-Konnektivitätsstrategie für NSX-verwaltete Arbeitslast-VMs im NSX-erzwungener Modus](#).
  - Windows-Firewall oder IPTables unter Linux.
- 2 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.
  - 3 Sie können die gesperrte VM neu starten.
  - 4 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.

## Benötige ich PCG auch im Native Cloud-erzwungener Modus ?

Ja.

## Kann ich die Rolle „IAM“ für das PCG ändern, nachdem ich mein Public Cloud-Konto in CSM integriert habe?

Ja. Sie können das für Ihre Public Cloud anwendbare NSX Cloud-Skript erneut ausführen, um die PCG-Rolle erneut zu generieren. Bearbeiten Sie Ihr Public Cloud-Konto in CSM und geben Sie den neuen Rollennamen an, nachdem Sie die PCG-Rolle neu generiert haben. Alle neuen PCG-Instanzen, die in Ihrem Public Cloud-Konto bereitgestellt werden, verwenden diese neue Rolle.

Beachten Sie, dass vorhandene PCG-Instanzen weiterhin die alte PCG-Rolle verwenden. Wenn Sie die IAM-Rolle für eine vorhandene PCG-Instanz aktualisieren möchten, wechseln Sie zu Ihrer Public Cloud und ändern Sie die Rolle für diese PCG-Instanz manuell.

## Kann ich die lokalen NSX-T Data Center Lizenzen für NSX Cloud verwenden?

Ja das können Sie, wenn Ihr ELA eine entsprechende Klausel enthält.

VMware NSX® Intelligence™ bietet eine Visualisierung der Sicherheitsposition Ihrer lokalen NSX-T Data Center-Umgebung. Die Visualisierung basiert auf den Netzwerkdatenverkehrsflows, die innerhalb eines bestimmten Zeitraums aggregiert werden. NSX Intelligence unterstützt Sie auch bei der Planung der Mikrosegmentierung, indem auf Analysen basierende Empfehlungen mit einer Durchsetzung der Sicherheitsrichtlinien gegeben werden.

---

**Wichtig** Sie müssen über eine Enterprise-Administratorrolle verfügen, um die Berechtigung zum Installieren, Konfigurieren und Verwenden von NSX Intelligence zu erhalten.

---

Bevor Sie mit der Verwendung der NSX Intelligence-Funktionen beginnen können, müssen Sie die NSX Intelligence-Appliance zuerst installieren und konfigurieren. Weitere Informationen finden Sie unter „Installieren und Konfigurieren der NSX Intelligence-Appliance“ im *Installationshandbuch für NSX-T Data Center*.

Dieses Kapitel enthält die folgenden Themen:

- [Erste Schritte mit NSX Intelligence](#)
- [Grundlegendes zu NSX Intelligence-Ansichten und -Flows](#)
- [Arbeiten mit NSX Intelligence-Empfehlungen](#)
- [Sichern und Wiederherstellen von NSX Intelligence](#)
- [Fehlerbehebung bei NSX Intelligence-Problemen](#)

## Erste Schritte mit NSX Intelligence

Um mit den Funktionen von NSX Intelligence zu beginnen, machen Sie sich mit der grafischen Benutzeroberfläche von NSX Intelligence vertraut.

Nachdem die NSX Intelligence-Appliance installiert und konfiguriert wurde, sind die NSX Intelligence-Funktionen auf der Registerkarte **Planen und Fehler beheben** der NSX Manager-Benutzeroberfläche aktiviert. Verwenden Sie im Abschnitt **Erkennen und Planen** die Option **Ermitteln und Maßnahmen ergreifen**, um Ihre NSX-T-Datencenter-Entitäten zu visualisieren, und **Empfehlungen**, um Empfehlungen für die Planung der Mikro-Segmentierung zu erhalten.

## Tour der NSX Intelligence-Startseite

Sie greifen auf die NSX Intelligence-Startseite zu, indem Sie auf der NSX Manager-Benutzeroberfläche auf **Planen und Fehler beheben > Ermitteln und Maßnahmen ergreifen** klicken.

Wenn Sie NSX Intelligence zum ersten Mal installiert und konfiguriert haben und auf **Ermitteln und Maßnahmen ergreifen** klicken, kann folgende Meldung angezeigt werden: *Keine Daten gefunden*. Möglicherweise müssen Sie Ihre Filter oben ändern. Die Meldung wird angezeigt, weil NSX Intelligence noch keine Daten zum Netzwerkverkehr erhalten hat, die zum Erstellen einer Visualisierung verwendet werden können. Nachdem aus NSX Manager Daten zum Netzwerkverkehr empfangen wurden, kann NSX Intelligence damit beginnen, Visualisierungen zu rendern.

Standardmäßig wird beim Klicken auf **Ermitteln und Maßnahmen ergreifen** die Visualisierung des Sicherheitsstatus aller Gruppen in Ihrem lokalen NSX-T Data Center angezeigt, zwischen deren VM-Mitgliedern in den letzten 24 Stunden ungeschützter Datenverkehr aufgetreten ist. Ungeschützte Netzwerkdatenverkehrsflows sind Flows zwischen VMs, für die keine Mikro-Segmentierung implementiert ist. Wenn noch keine Gruppen definiert sind, werden keine Gruppen angezeigt. Wenn VMs vorhanden sind, aber keiner Gruppe angehören, wird das Symbol für die Gruppe „Nicht kategorisierte VMs“ angezeigt.



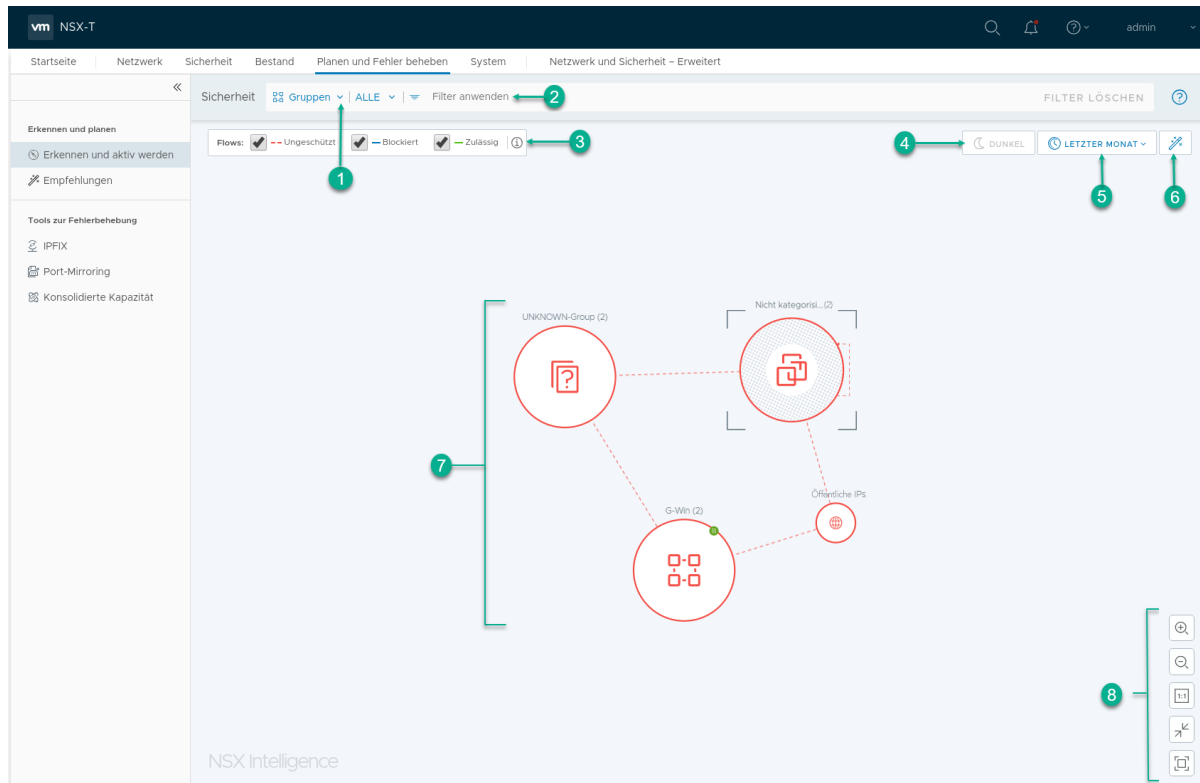
Wenn Sie bereits Gruppen definiert und Daten zum Netzwerkverkehr erfasst haben, kann eine Visualisierung ähnlich dem folgenden Screenshot angezeigt werden. In der folgenden Tabelle sind die nummerierten Abschnitte im Screenshot beschrieben.

---



**Hinweis** NSX Intelligence kategorisiert eine IP-Adresse, die als private IP-Adresse zu einer der folgenden CIDR-Notationen gehört: 192.168.0.0/16, 172.16.0.0/12 und 10.0.0.0/8. Jede IP-Adresse, die keiner dieser CIDR-Notationen angehört, wird als öffentliche IP-Adresse klassifiziert. Wenn die IP-Adresse Ihrer VM nicht in eine dieser CIDR-Notationen fällt, sollten Sie mithilfe der `PATCH /api/v1/intelligence/host-config-API` Ihre CIDR-Notation im *Handbuch für die NSX-T Data Center-API* hinzufügen.

---













Abschnitt	Beschreibung
1	<p>Der Auswahlbereich für die Sicherheitsansicht ist der Ort, an dem Sie den Typ der anzuzeigenden Sicherheitsvisualisierung auswählen. Es stehen zwei Typen von Sicherheitsansichten zur Verfügung: <b>Gruppen</b> und <b>VMs</b>. Wenn Sie auf <b>Ermitteln und Maßnahmen ergreifen</b> klicken, wird als Standardsicherheitsansicht die Ansicht „Gruppen“ mit den Gruppenobjekten in Ihrem NSX-T Data Center angezeigt, zwischen denen innerhalb der letzten 24 Stunden ungeschützter Datenverkehr aufgetreten ist.</p> <ul style="list-style-type: none"> <li>■ Um die Ansicht „VMs“ auszuwählen, klicken Sie neben <b>Gruppen</b> auf den Pfeil nach unten und wählen Sie <b>VMs</b> aus.</li> <li>■ Um die spezifischen Gruppen oder VMs auszuwählen, die in die Ansicht aufgenommen werden sollen, klicken Sie neben <b>ALLE</b> auf den Pfeil nach unten und wählen Sie aus der Liste aus.</li> <li>■ Um Ihre Auswahlfilter zu löschen, klicken Sie auf <b>FILTER LÖSCHEN</b> oben rechts auf dem Bildschirm. Wenn Sie auf <b>FILTER LÖSCHEN</b> klicken, während Sie sich in der Ansicht „VMs“ befinden, werden die Auswahlfilter gelöscht und die Ansicht „Gruppen“ wird angezeigt.</li> </ul> <p>Weitere Informationen zum Arbeiten mit den beiden Ansichtstypen finden Sie unter <a href="#">Arbeiten mit der Ansicht „Gruppen“</a> und <a href="#">Arbeiten mit der Ansicht „VMs“</a>.</p>
2	<p>Mit <b>Filter anwenden</b> können Sie die für die Visualisierung zu verwendenden Kriterien genauer festlegen. In der Dropdown-Liste können Sie die Kriterien auswählen, die für die Visualisierung verwendet werden sollen. Sie können VM-Mitglieder, Tags, Flow-Typen, Quell-IP, Ziel-IP, Regel-ID oder Name auswählen. Sie können mehrere Filter definieren, die angewendet werden sollen, indem Sie erneut auf <b>Filter anwenden</b> klicken.</p>



Abschnitt	Beschreibung
3	<p>Im Abschnitt <b>Flows</b> können Sie den Datenverkehrsflow-Typ auswählen, der während des ausgewählten Zeitraums in die Visualisierung einbezogen werden soll. Die Farben, die in der Visualisierung für die Flow-Typen verwendet werden, werden in diesem Abschnitt ebenfalls gezeigt.</p> <ul style="list-style-type: none"> <li>■ Rot gefärbte gestrichelte Linie für <b>ungeschützte</b> Flows</li> <li>■ Blau gefärbte durchgehende Linie für <b>blockierte</b> Flows</li> <li>■ Grün gefärbte durchgehende Linie für die <b>zulässigen</b> Flows</li> </ul> <p>Standardmäßig ist als Typ der <b>ungeschützte</b> Datenverkehrsflow für die aktuelle NSX Intelligence-Visualisierung ausgewählt. Weitere Informationen hierzu finden Sie unter <a href="#">Arbeiten mit Datenverkehrsflows</a>.</p>
4	<p>Im Abschnitt mit dem Anzeigemodus ist definiert, welches Design für die Visualisierung verwendet werden soll. Das helle Design ist der verwendete Standardmodus.</p> <ul style="list-style-type: none"> <li>■ Um das dunkle Design zu verwenden, klicken Sie auf das Symbol <b>DUNKEL</b>. Sie können das dunkle Design nur dann verwenden, wenn Sie die Visualisierung im Vollbildmodus anzeigen.</li> <li>■ Um in den Vollbildmodus zu wechseln, klicken Sie im Abschnitt „Anzeigesteuerung“ auf .</li> </ul>
5	<p>In diesem Abschnitt wählen Sie den Zeitraum aus, um zu bestimmen, welche Datenverkehrsflows zum Generieren der gewünschten Visualisierung und Empfehlung verwendet werden. Ihre Auswahl bestimmt die Verlaufsdaten, die in der Ansicht „Gruppen“ oder „VMs“ verwendet werden. Der Zeitraum ist relativ zum aktuellen Zeitpunkt und umfasst einen bestimmten Zeitraum in der Vergangenheit.</p> <p>„Letzte 24 Stunden“ ist der standardmäßig verwendete Zeitbereich. Um den ausgewählten Zeitraum zu ändern, klicken Sie auf den aktuell ausgewählten Zeitraum und wählen Sie <b>Letzte Std.</b>, <b>Letzte 12 Std.</b>, <b>Letzte 24 Std.</b>, <b>Letzte Woche</b> oder <b>Letzter Monat</b>.</p>
6	<p>Wenn Sie auf das Empfehlungssymbol  klicken, wird im Dialogfeld „Empfehlungen“ die Bestandsübersicht für die aktuelle Ansicht angezeigt. Wenn Sie sich in der Ansicht „VMs“ befinden, können Sie eine NSX Intelligence-Empfehlung generieren, indem Sie auf <b>Neue Empfehlung starten</b> klicken. Siehe <a href="#">Arbeiten mit NSX Intelligence-Empfehlungen</a>.</p>
7	<p>Dieser Abschnitt ist die Visualisierung des Sicherheitsstatus der Gruppen oder VMs in Ihrem lokalen NSX-T Data Center. Er enthält auch die Visualisierung der Netzwerkdatenverkehrsflows, die während des ausgewählten Zeitraums aufgetreten sind. In diesem Abschnitt können Sie auf einen spezifischen Knoten oder einen Flow-Pfeil zeigen, um Details zu dieser spezifischen Entität zu erhalten.</p> <p>Weitere Informationen hierzu finden Sie unter <a href="#">Kennenlernen von NSX Intelligence-Grafikelementen</a> und <a href="#">Grundlegendes zu NSX Intelligence-Ansichten und -Flows</a>.</p>
8	<p>Dieser Abschnitt enthält die Ansichtsteuerungen zum Vergrößern, Verkleinern, Anwenden des 1:1-Seitenverhältnisses, zur Größenanpassung der Ansicht und zum Wechseln in den Vollbildmodus. Sie können auch Tastenkombinationen verwenden, um Ihre Ansichtsteuerungen zu verwalten. Um das Hilfefenster für die Tastenkombinationen anzuzeigen, drücken Sie <b>Umschalt+ /</b>.</p> <p>Um zu einer zuvor angezeigten Visualisierung zu navigieren, verwenden Sie die Schaltfläche „Zurück“ Ihres Webbrowsers. Wenn Sie sich im Vollbildmodus befinden, klicken Sie auf <b>Zurück</b> (oben links auf dem Bildschirm), um dieselbe Schaltflächennavigation vorzunehmen.</p>

## Kennenlernen von NSX Intelligence-Grafikelementen

Die Benutzeroberfläche von NSX Intelligence bietet mehrere grafische Elemente, die bei der Visualisierung der Datacenter-Entitäten, der Datenverkehrsströme und bestimmter Aktivitäten in Ihrer NSX-T Data Center-Umgebung helfen.

Die folgende Tabelle enthält ein Glossar der NSX-T Data Center-Grafikelemente, die möglicherweise in einer NSX Intelligence-Visualisierung angezeigt werden.

Grafikelement	Beschreibung
	Dieses Symbol stellt eine Gruppe dar, d. h. eine Sammlung von VMs, auf die Sicherheitsrichtlinien, wie beispielsweise Firewallregeln für den Ost-West-Datenverkehr, angewendet werden können. Siehe <a href="#">Arbeiten mit der Ansicht „Gruppen“</a> .
	Dieses Symbol stellt eine virtuelle Maschine (VM) dar, die Teil Ihres NSX-T Data Center ist. Eine VM kann mehr als einer Gruppe angehören. Siehe <a href="#">Arbeiten mit der Ansicht „VMs“</a> .
	Dieses Symbol stellt die öffentlichen IPs im Internet dar. Wenn mindestens eine VM in Ihrer NSX-T Data Center-Umgebung während des ausgewählten Zeitraums mit einer öffentlichen IP-Adresse kommuniziert hat, ist dieser Datenverkehr in der aktuellen Visualisierung enthalten.
	Eine IP-Adresse, z. B. eine Unicast-, Broadcast- oder Multicast-IP-Adresse, die während des ausgewählten Zeitraums am Netzwerkdatenverkehr beteiligt war.
	Nicht kategorisi... (4) Dieses Symbol wird für VMs verwendet, die keiner Gruppe angehören.
	Ein Pfeil stellt einen Netzwerkdatenverkehr dar, der während eines ausgewählten Zeitraums zwischen zwei VMs aufgetreten ist. Es gibt drei verschiedene Arten von Pfeilen: ein gestrichelter rötlicher Pfeil für einen ungeschützten Flow, ein durchgezogener blauer Pfeil für einen blockierten Flow und ein durchgezogener grüner Pfeil für einen zulässigen Flow. Siehe <a href="#">Arbeiten mit Datenverkehrsflows</a> .
	Ein Knoten, der als aktueller Knoten im Fokus ausgewählt wurde, ist von einem gestrichelten Kreis umgeben. Es handelt sich um den angehefteten Knoten während des Auswahlmodus und die aktuell angezeigte Ansicht.
	Dieses Symbol wird auf dem Rand eines Gruppenknotens angezeigt, wenn die Gruppe während des ausgewählten Zeitraums der NSX-T Data Center-Bestandsliste hinzugefügt wurde. Wenn NSX-T Data Center während des ausgewählten Zeitraums eine VM erkannt hat, wird das Symbol auf dem Rand des VM-Knotens angezeigt.

Grafikelement	Beschreibung
	Dieses Symbol wird auf dem Rand des Gruppenknotens angezeigt, wenn die Gruppe während des ausgewählten Zeitraums gelöscht wurde, die VM-Mitglieder jedoch nicht. Auf dem Rand eines VM-Knotens zeigt dieses Symbol an, dass die VM während des ausgewählten Zeitraums gelöscht wurde. Auch wenn eine VM oder Gruppe gelöscht wurde, wird sie weiterhin in der aktuellen Visualisierung angezeigt, um in einer Verlaufsansicht nachvollziehen zu können, dass die VM oder Gruppe während des ausgewählten Zeitraums entfernt wurde.
	Dieses Symbol wird angezeigt, wenn Gruppen und VMs zusammen sichtbar sind, beispielsweise in einer Deep-Dive-Gruppenansicht oder bei verbundenen VMs einer Gruppe. Das Symbol wird in den folgenden Fällen auf dem Rand eines VM-Knotens angezeigt: <ul style="list-style-type: none"> <li>■ wenn die VM während des ausgewählten Zeitraums aus der aktuell angezeigten Gruppe verschoben wurde;</li> <li>■ wenn die VM irgendwann während des ausgewählten Zeitraums Teil der aktuell angezeigten Gruppe war, jetzt jedoch kein Mitglied dieser Gruppe mehr ist.</li> </ul>

## Grundlegendes zu NSX Intelligence-Ansichten und -Flows

Die NSX Intelligence-Visualisierung besteht aus den Gruppen oder VMs und den Netzwerk-Flows, die während des ausgewählten Zeitraums bei diesen Gruppen oder VMs aufgetreten sind.

**Wichtig** Die für einen bestimmten Zeitraum angezeigte Visualisierung stellt alle Netzwerk-Flows und Aktivitäten wie das Hinzufügen, Löschen oder Verschieben von VMs und Gruppen dar, die in Ihrem NSX-T-Datencenter während dieses Zeitraums aufgetreten sind. Es ist möglich, dass eine VM in der Visualisierung mehr als einmal angezeigt wird. Wenn eine VM beispielsweise mit einem ESXi-Host verbunden wird, der ursprünglich nicht verwaltet wurde, und der Host während des ausgewählten Zeitraums von einem VMware vCenter Server™ verwaltet wird, dann wird die VM in der Ansicht „VMs“ zweimal angezeigt. Wenn ein ESXi-Host von vCenter Server getrennt und während desselben ausgewählten Zeitraums wieder hinzugefügt wurde, werden die mit dem Host verbundenen VMs während des ausgewählten Zeitraums ebenso als gelöscht und neu angezeigt. Wenn in der Ansicht „Gruppen“ eine VM in der Gruppe „Nicht kategorisiert“ enthalten war und während desselben ausgewählten Zeitraums einer Gruppe hinzugefügt wurde, wird die VM sowohl in der Gruppe „Nicht kategorisiert“ als auch in der neuen Gruppe angezeigt.

NSX Intelligence unterstützt nur Gruppen mit VM-Mitgliedstypen. Wenn Sie über Gruppen mit anderen Mitgliedstypen verfügen, zeigt die Ansicht „Gruppen“ möglicherweise korrelierte Flows zwischen den Gruppen mit VM-Mitgliedstypen anstelle von tatsächlichen Gruppen in der Sicherheitsregel an.

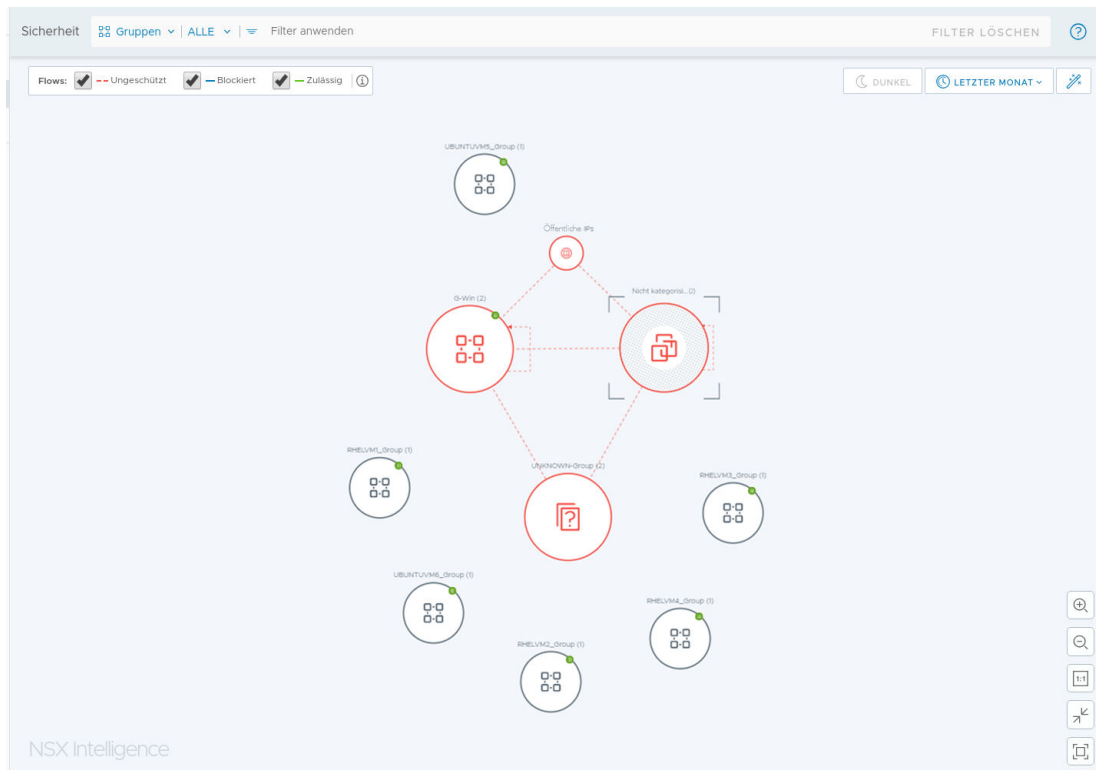
Verwenden Sie die Informationen in diesem Abschnitt, um mehr über das Arbeiten mit der Ansicht „Gruppen“, der Ansicht „VMs“ und den unterschiedlichen Datenverkehrsströmen zu erfahren.

## Arbeiten mit der Ansicht „Gruppen“





Die Standardansicht, die auf der NSX Intelligence-Startseite angezeigt wird, ist die Ansicht „Gruppen“. Diese Gruppenansicht wird gefiltert, um alle Gruppen anzuzeigen, die in den letzten 24 Stunden einen nicht gesicherten Datenverkehrsflow aufwiesen.

### Knoten und Pfeile in einer Ansicht „Gruppen“

Ein Knoten in der Ansicht „Gruppen“ stellt NSX-Objekte, wie VMs, IP Sets usw., in Ihrer NSX-T Data Center-Umgebung dar. Der folgende Screenshot zeigt ein Beispiel der Ansicht „Gruppen“.



In der folgenden Tabelle sind die Typen der Gruppenknoten aufgeführt, die in der Ansicht „Gruppen“ angezeigt werden.

Gruppenknotentyp	Symbol	Beschreibung
Reguläre Gruppe		Ein regulärer Gruppenknoten in NSX Intelligence stellt eine beliebige Sammlung von NSX-Objekten in ihrer NSX-T Data Center-Umgebung dar. Für diese Version sind diese NSX-Objekte nur VMs und daher unterstützt NSX Intelligence reguläre Gruppen nur mit VM-Mitgliedstypen. Ein NSX-Objekt kann mehr als einer Gruppe angehören, sodass das eine VM in mehr als einem Gruppenknoten angezeigt werden kann.
Gruppe „Nicht kategorisiert“		Ein Knoten der Gruppe „Nicht kategorisiert“ stellt eine Sammlung von VMs dar, die keiner Gruppe angehören.
Gruppe „Unbekannt“		Ein unbekannter Gruppenknoten stellt einen Satz von verschiedenen Objekten dar, die in Ihrer NSX-T Data Center-Bestandsliste nicht gefunden wurden. Diese Objekte kommunizieren jedoch mit mindestens einem NSX-Objekt in Ihrer NSX-T Data Center-Umgebung.
Gruppe „Öffentliche IPs“		Ein Knoten der Gruppe „Öffentliche IPs“ stellt eine Sammlung von öffentlichen IP-Adressen (IPv4 oder IPv6) dar, die mit NSX-Objekten in Ihrem NSX-T Data Center kommunizieren.

Die Größe eines Knotens in der Ansicht „Gruppen“ basiert auf der Anzahl der NSX-Objekte, wie beispielsweise VMs, die zu dieser Gruppe gehören. Je größer der Knoten der Gruppe, desto mehr Objekte, wie beispielsweise VMs, gehören zu dieser Gruppe. Der Name der Gruppe und die Gesamtzahl ihrer Mitglieder-VMs werden oberhalb des Knotens angezeigt.

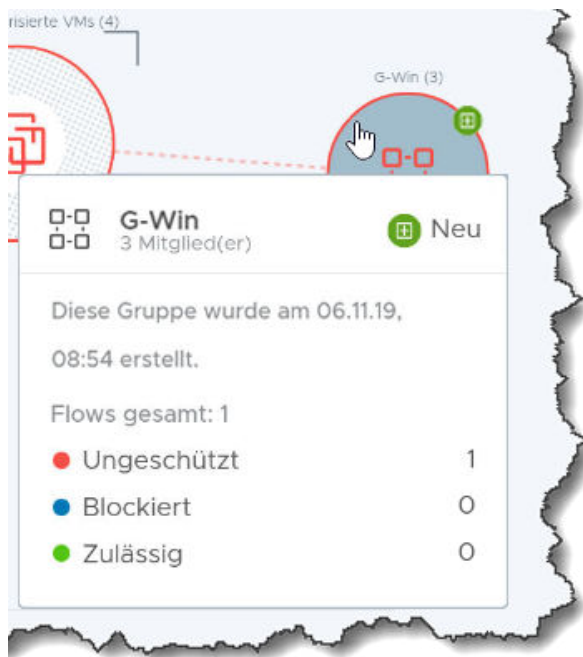
Die Pfeile zwischen den Gruppenknoten stellen die Datenverkehrsströme dar, die während des ausgewählten Zeitraums zwischen den VMs in diesen verbundenen Gruppenknoten aufgetreten sind. Ein selbstreferenzierender Pfeil auf einem Gruppenknoten gibt an, dass mindestens eine VM mit einer anderen VM innerhalb dieser Gruppe kommuniziert hat. Weitere Informationen hierzu finden Sie unter [Arbeiten mit Datenverkehrsflows](#).

Ein Knoten mit einem rötlichen Rand zeigt an, dass mindestens ein nicht gesicherter Flow für eine VM in der Gruppe erkannt wurde, unabhängig davon, wie viele blockierte oder zulässige Flows während des ausgewählten Zeitraums festgestellt wurden. Ein Knoten mit einem blauen Rand bedeutet, dass zwar keine ungeschützten Datenverkehrsflows erkannt wurden, aber mindestens ein blockierter Flow vorhanden ist, unabhängig davon, wie viele zulässige Flows während des ausgewählten Zeitraums erfasst wurden. Ein Knoten mit einem grünen Rand zeigt, dass während des ausgewählten Zeitraums keine ungeschützten oder blockierten Flows erkannt wurden und mindestens ein zulässiger Flow festgestellt wurde. Ein Knoten mit einem grauen Rand bedeutet, dass für die zu dieser Gruppe gehörenden VMs während des ausgewählten Zeitraums keine Datenverkehrsflows festgestellt wurden.

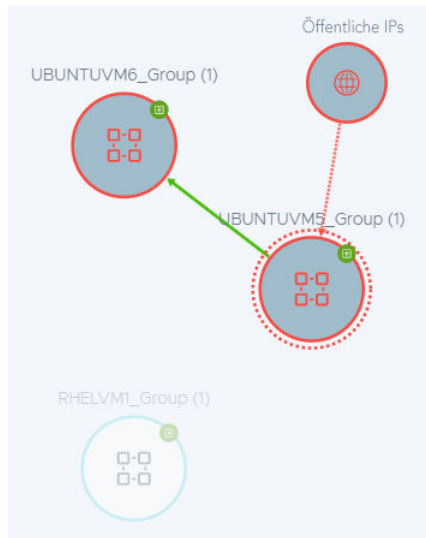
Wenn Sie die Ansicht „Gruppen“ nicht sehen, klicken Sie im Auswahlbereich für die Sicherheitsansicht neben **VMs** auf den Pfeil nach unten und wählen Sie **Gruppen** aus. In der Dropdown-Liste für die Auswahl können Sie **Alle Gruppen** oder bestimmte Gruppen aus der Liste auswählen und dann auf **Anwenden** klicken. Verwenden Sie das Textfeld **Suchen**, um die Auswahlliste zu filtern. Wenn Sie auf eine andere Stelle klicken, ohne eine Auswahl in der Dropdown-Liste vorzunehmen, oder wenn Sie **Alle Gruppen** in der Dropdown-Liste auswählen, wird die Option **Alle Gruppen** auf die Ansicht „Gruppen“ angewendet.

## Knotenauswahl in Ansicht „Gruppen“

Wenn Sie auf den Knoten einer Gruppe zeigen, werden Informationen zu dieser Gruppe angezeigt, wie im folgenden Beispiel für die Gruppe G-Win dargestellt. Die Anzahl und die Typen der während des ausgewählten Zeitraums erkannten Flows werden ebenfalls aufgeführt. Wenn die Gruppe während des ausgewählten Zeitraums hinzugefügt wurde, werden das Badge-Symbol „Neu“ und die Details zum Zeitpunkt der Erstellung der Gruppe ebenfalls angezeigt.



Wenn Sie auf den Knoten einer Gruppe klicken, wird die Auswahl durch einen gestrichelten Kreis als angehefteter Gruppenknoten markiert. Die anderen Gruppen, die mit dem ausgewählten Gruppenknoten verbunden sind, werden in der Ansicht auch stärker hervorgehoben. Alle anderen Knoten werden abgeblendet. Im folgenden Screenshot ist der Knoten UBUNTUVM5\_Group beispielsweise ausgewählt und andere Gruppen, die während des ausgewählten Zeitraums einen Datenverkehrsflow mit UBUNTUVM5\_Group gemeinsam genutzt haben, sind ebenfalls hervorgehoben. Alle anderen Gruppen, die nicht mit UBUNTUVM5\_Group kommuniziert haben, werden in der Ansicht abgeblendet.

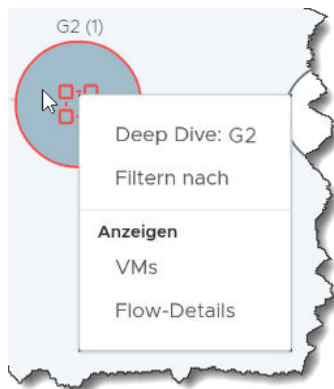


Um die angeheftete Auswahl zu löschen, klicken Sie in der Ansicht „Gruppen“ auf einen leeren Bereich.

Wenn Sie die Ansicht „Gruppen“ verkleinern und die Details zu den Knoten nicht mehr sichtbar sind, zeigen Sie auf einen beliebigen sichtbaren Teil eines Knotens, damit dessen Details angezeigt werden.

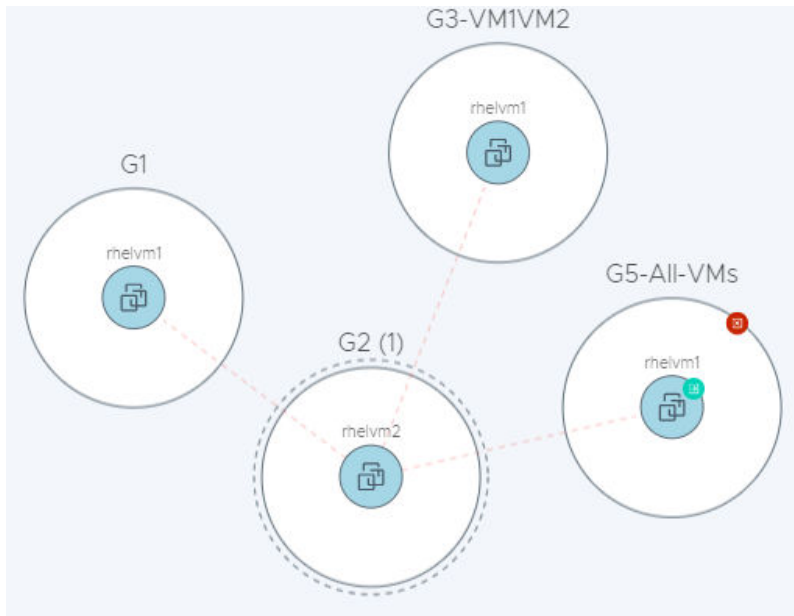
## Verfügbare Aktionen in der Ansicht „Gruppen“

Wenn Sie mit der rechten Maustaste auf den Knoten einer Gruppe klicken, wird ein Kontextmenü mit verfügbaren Aktionen angezeigt, wie in der folgenden Abbildung dargestellt.



- Durch Auswahl von **Deep Dive: Gruppennamen** wird der Knoten der ausgewählten Gruppe mit einem gestrichelten Kreis umrandet, um ihn als angehefteten Gruppenknoten oder als aktuelle Gruppe im Fokus zu markieren. Die VMs, die zur Gruppe gehören, werden innerhalb des Knotens der Gruppe angezeigt. Alle Gruppen, die während des ausgewählten Zeitraums einen Datenverkehrsflow mit den VMs in der angehefteten Gruppe gemeinsam genutzt haben, werden ebenfalls in der Ansicht „Gruppen“ platziert. Im folgenden Beispiel ist die Gruppe G2 die angeheftete Gruppe und die anderen Gruppen befinden sich in der Ansicht, da für ihre VM-Mitglieder während des ausgewählten Zeitraums Datenverkehrsflows mit rhelv2 in der Gruppe G2 aufgetreten sind.





- Wenn Sie **Filtern nach** auswählen, wird die aktuelle Gruppe dem Visualisierungsfiler hinzugefügt, der für die aktuelle Ansicht „Gruppen“ verwendet wird.
- Wenn Sie **VMs** auswählen, wird eine Tabelle mit allen VMs angezeigt, die während des ausgewählten Zeitraums zur aktuellen Gruppe gehörten. In der Tabelle „VMs anzeigen“ sehen Sie die Details zu den VMs, die zur ausgewählten Gruppe gehören, und zu den anderen Gruppen, zu denen die einzelnen VMs ebenfalls gehören. Um die VM dem aktuellen Visualisierungsfiler hinzuzufügen, klicken Sie auf das Filtersymbol.
- Wenn Sie **Flow-Details** auswählen, wird die Tabelle „Flow-Details“ für die aktuell ausgewählte Gruppe angezeigt, wie im folgenden Screenshot dargestellt. Sie zeigt die Details zu den Flows an, die in Verbindung mit den VMs der aktuellen Gruppe während des ausgewählten Zeitraums aufgetreten sind bzw. die aktuell aktiv sind. Zu den Details gehören der Flow-Typ, die Quell- und Zielgruppen des Flows, die Start- und Endzeit des Flows sowie die verwendeten Dienste. Sie können auf einige der Details klicken, um weitere Informationen zu erhalten. Weitere Informationen hierzu finden Sie unter [Arbeiten mit Datenverkehrsflows](#).

Flow-Details 🕒 Letzte 24 Std. ✕

Flow-Details für „Nicht kategorisierte VMs“ werden angezeigt

Abgeschlossene Flows Aktive Flows

Suchen

Quelle	Quellgruppe	Ziel	Zielgruppe	Dienste	Endzeit	Neuester Flow
ubuntu12.04.1-2G-LA...	G5	ubuntu12.04-pa...	UNCATEGORIZED	SSH... und 2 weitere	06.11.19, 08:05	🔴 Ungeschützt
ubuntu12.04.1-2G-LA...	G1	ubuntu12.04-pa...	UNCATEGORIZED	SSH... und 2 weitere	06.11.19, 08:05	🔴 Ungeschützt

🔄 Aktualisieren 1 - 2 of 2 Flow(s)

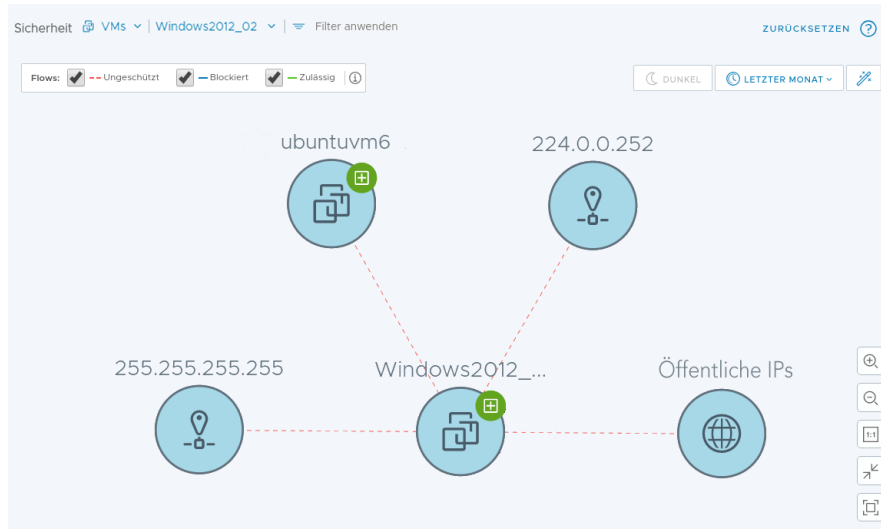
**SCHLIESSEN**

## Arbeiten mit der Ansicht „VMs“

Ein Knoten in der Ansicht „VMs“ stellt eine virtuelle Maschine (VM) in Ihrer lokalen NSX-T Data Center-Umgebung dar.

### Knoten und Pfeile in der Ansicht "VMs"

Wenn Sie sich in der Ansicht „VMs“ befinden, werden die Gruppengrenzen nicht angezeigt. Jeder Knoten, der mit einer der VMs in Ihrer NSX-T Data Center-Umgebung kommuniziert, aber nicht als Teil der NSX-T Data Center-Bestandsliste identifiziert wurde, wird auch in der Ansicht „VMs“ dargestellt. Im Folgenden ist eine einfache Ansicht „VMs“ dargestellt.



In der folgenden Tabelle sind die Typen der VM-Knoten aufgeführt, die unter „Ansichten“ angezeigt werden.

VM-Knotentyp	Symbol	Beschreibung
Reguläre VM		Ein regulärer VM-Knoten stellt eine virtuelle Maschine (VM) dar, die Teil Ihrer NSX-T Data Center-Umgebung ist. Eine VM kann mehr als einer Gruppe angehören.
Öffentliche IP-Adresse		Ein öffentlicher IP-Knoten stellt eine öffentliche IP-Adresse (entweder IPv4 oder IPv6) dar, die mit oder von ihrer NSX-T Data Center-Umgebung aus kommuniziert.
IP		Ein IP-Knoten stellt eine IP-Adresse dar, die während des ausgewählten Zeitraums am Netzwerkdatenverkehr beteiligt war. Eine IP-Adresse kann eine Unicast-, Broadcast- oder Multicast-IP-Adresse sein.

Wenn Sie die Ansicht „VMs“ nicht sehen, klicken Sie im Auswahlbereich für die Sicherheitsansicht neben **Gruppen** auf den Pfeil nach unten und wählen Sie **VMs** aus. In der Dropdown-Liste für die Auswahl können Sie **Alle VMs** oder bestimmte VMs aus der Liste auswählen und dann auf **Anwenden** klicken. Verwenden Sie das Textfeld **Suchen**, um die Auswahlliste zu filtern. Wenn Sie auf eine andere Stelle klicken, ohne eine Auswahl in der Dropdown-Liste vorzunehmen, oder wenn Sie **Alle VMs** in der Dropdown-Liste auswählen, wird die Option **Alle VMs** auf die Ansicht „VMs“ angewendet.

Die Pfeile zwischen den VM-Knoten stellen die Datenverkehrsflows dar, die während des ausgewählten Zeitraums zwischen den VMs aufgetreten sind. Weitere Informationen hierzu finden Sie unter [Arbeiten mit Datenverkehrsflows](#).

## Knotenauswahl in der Ansicht „VMs“

Wenn Sie auf einen VMs-Knoten zeigen, werden Informationen zum Knoten angezeigt, wie im folgenden Beispiel dargestellt. Die Anzahl und die Typen der während des ausgewählten Zeitraums erkannten Flows zur VM sind ebenfalls aufgeführt. Wenn die Gruppe während des ausgewählten Zeitraums hinzugefügt wurde, werden das Badge-Symbol „Neu“ und die Details zum Zeitpunkt, an dem die VM hinzugefügt wurde, ebenfalls angezeigt.



Wenn Sie auf den Knoten einer VM klicken, wird die Auswahl durch einen gestrichelten Kreis als angehefteter VM-Knoten markiert. Weitere VM-Knoten, die Datenverkehrsströme mit diesem angehefteten VM-Knoten gemeinsam genutzt haben, werden in der Ansicht „VMs“ ebenfalls stärker hervorgehoben. Alle anderen Knoten werden abgeblendet, um sie weniger sichtbar zu machen. Um die angeheftete Auswahl zu löschen, klicken Sie in der Ansicht „VMs“ auf einen leeren Bereich.

Wenn Sie die Ansicht „VMs“ verkleinern und die Details in den VM-Knoten nicht mehr sichtbar sind, können Sie auf einen beliebigen sichtbaren Teil eines VM-Knotens zeigen, um dessen Details zu sehen.

## Verfügbare Aktionen in der Ansicht „VMs“

Wenn Sie mit der rechten Maustaste auf den Knoten einer VM klicken, wird ein Kontextmenü mit verfügbaren Aktionen angezeigt, wie in der folgenden Abbildung dargestellt.






Auswahl	Beschreibung
<b>Filtern nach</b>	Die VM wird dem Visualisierungsfilter hinzugefügt, der für die aktuelle Ansicht „VMs“ verwendet wird.
<b>VM-Informationen</b>	Die Details der VM während des ausgewählten Zeitraums werden angezeigt.
<b>Verwandte Gruppen</b>	Die Tabelle „Gruppen“ mit Informationen zu Gruppen, zu denen die VM während des ausgewählten Zeitraums gehörte.
<b>Flow-Details</b>	<p>Zeigt die Details zu den Flows an, die für die VM während des ausgewählten Zeitraums aufgetreten sind bzw. derzeit aktiv sind. Mögliche Details:</p> <ul style="list-style-type: none"> <li>■ Flow-Typ</li> <li>■ Quell- und Zielgruppen des Flows</li> <li>■ Start- und Endzeit des Flows</li> <li>■ verwendete Dienste</li> </ul> <p>Sie können auf einige der Details klicken, um weitere Informationen zu erhalten. Weitere Informationen hierzu finden Sie unter <a href="#">Arbeiten mit Datenverkehrsflows</a>.</p>
<b>Empfehlung starten</b>	Zeigt den Assistenten „Neue Empfehlungen starten“ an. Weitere Informationen finden Sie unter <a href="#">Arbeiten mit NSX Intelligence-Empfehlungen</a> .

## Arbeiten mit Datenverkehrsflows

Die Pfeile zwischen den Gruppen- oder VM-Knoten stellen die Netzwerk-Datenverkehrsströme dar, die während des ausgewählten Zeitraums zwischen den VMs aufgetreten sind.

Der Netzwerkdatenverkehr basiert auf den vorhandenen L3-Regeln der verteilten Firewall (DFW) und den Datenverkehrsflows, die während des ausgewählten Zeitraums aufgetreten sind. Alle Datenverkehrsflows, die mit einer statusbehafteten L3-DFW-Regel unter Verwendung von IPv4 oder IPv6 und mit TCP-, UDP-, GRE-, ESP- und SCTP-Protokollen übereinstimmen, sind in den Visualisierungs- und Flow-Details enthalten. TCP- und UDP-Flows verfügen über Details auf IP- und Port-Ebene, für andere Flows sind nur Details auf IP-Ebene vorhanden.

Die Datenverkehrsflows werden in die folgenden Typen kategorisiert.

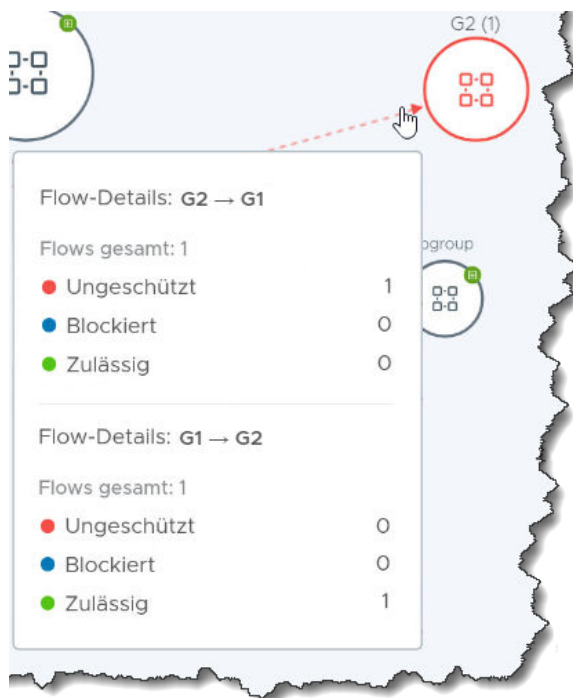
Flow-Typ	Grafik	Beschreibung
Ungeschützt		Ein gestrichelter rötlicher Pfeil weist darauf hin, dass das System erkannt hat, dass der Datenverkehrsflow eine Regel erreicht hat (Quelle: Beliebig   Ziel: Beliebig   Aktion: Zulassen oder Ablehnen oder Verwerfen) und dass präzisere Sicherheitsrichtlinien erforderlich sind. Diese Regel kann Ihre Standardregel sein oder sie kann sich an beliebiger Stelle der verteilten Firewall für den Ost-West-Datenverkehr befinden.
Blockiert		Ein durchgezogener blauer Pfeil zeigt, dass das System erkannt hat, dass der Datenverkehrsflow eine „Ablehnen“- oder „Verwerfen“-Regel erreicht hat, die präziser ist als die in der Flow-Definition „Ungeschützt“ angegebene Regel.
Zulässig		Ein durchgezogener grüner Pfeil zeigt, dass das System erkannt hat, dass der Datenverkehrsflow eine „Zulässig“-Regel erreicht hat, die präziser ist als die in der Flow-Definition „Ungeschützt“ angegebene Regel.

Um sich nur auf Objekte mit bestimmten Typ von Datenverkehrsflow zu konzentrieren, wählen Sie im Auswahlbereich für die Sicherheitsansicht den gewünschten Ansichtstyp aus und verwenden Sie das Filterattribut „Flow-Typ“, um die Auswahl einzugrenzen.

Wenn Sie die Auswahl eines Flow-Typs aufheben, werden die Flow-Linien für diesen Flow-Typ aus dem angezeigten Diagramm ausgeblendet. Sofern keine Filter angewendet werden, die bestimmte Objekte ausschließen, werden alle Gruppen- oder VM-Objekte unabhängig von den Datenverkehrstypen, die mit diesen Objekten während des ausgewählten Zeitraums aufgetreten sind, weiterhin angezeigt. Wenn Sie beispielsweise die Auswahl des Flow-Typs „Zulässig“ aufheben, werden alle Linien für zulässige Flows im Diagramm ausgeblendet. Allerdings werden immer noch alle Objekte angezeigt, selbst die Objekte, für die während des ausgewählten Zeitraums nur „zulässige“ Datenverkehrsflows vorhanden waren.

Die Richtung eines Flow-Pfeils gibt die Quelle und das Ziel des erkannten Datenverkehrsstroms an. Wenn Sie sich in der Ansicht „Gruppen“ befinden, zeigt ein selbstreferenzierender Pfeil auf einem Gruppenknoten an, dass mindestens eine VM mit einer anderen VM innerhalb dieser Gruppe kommuniziert hat. In der Ansicht „VMs“ gibt ein selbstreferenzierender Pfeil an, dass ein NSX-Objekt in der VM mit einem anderen NSX-Objekt in derselben VM kommuniziert hat.

Wenn Sie auf einen Flow-Pfeil zeigen, werden Informationen zu den Flows, die die Gruppe oder die virtuelle Maschine betreffen, angezeigt, wie im folgenden Beispiel für die Gruppe G2 dargestellt ist.



Wenn Sie auf einen Flow-Pfeil klicken, wird das Dialogfeld „Flow-Details“ angezeigt. Es zeigt die Details zu den abgeschlossenen und aktiven Flows an, die während des ausgewählten Zeitraums aufgetreten sind. Um detailliertere Informationen über die Quelle, das Ziel, den Dienstyp und den Typ des Flows zu erhalten, klicken Sie auf die Links in der Tabelle.

## Arbeiten mit NSX Intelligence-Empfehlungen

NSX Intelligence kann Mikrosegmentierungs-Empfehlungen bereitstellen, die auf den Mustern der Datenverkehrs-Flows basieren, die zwischen den VMs in Ihrer NSX-T Data Center-Umgebung während eines ausgewählten Zeitraums aufgetreten sind.

### Verstehen von NSX Intelligence-Empfehlungen

Zu den von NSX Intelligence generierten Empfehlungen zählen Sicherheitsrichtlinien, Richtlinien-Sicherheitsgruppen und Dienste für Anwendungen.

Die Empfehlungen basieren auf den Netzwerkdatenverkehr-Flow-Mustern zwischen VM-Arbeitslasten auf ESXi-Hosts, die von einem vCenter Server verwaltet werden. Sie können Sie beim Durchsetzen einer dynamischeren Sicherheitsrichtlinie unterstützen, indem sie die Datenverkehrsmuster der Kommunikation korrelieren, die in Ihrer NSX-T Data Center-Umgebung aufgetreten sind.

Die Sicherheitsrichtlinien-Empfehlungen entsprechen in ihrer Kategorie Ost-West-Sicherheitsrichtlinien für Anwendungen bei verteilten Firewalls. Die Sicherheitsgruppen-Empfehlungen bestehen aus einer Liste von VMs, die in den Datenverkehrs-Flows des Netzwerks angezeigt werden und für das angegebene Zeitintervall und die VM-Grenze analysiert wurden. Die Dienstempfehlungen sind Dienstobjekte, die in bestimmten Ports von Anwendungen in den von Ihnen angegebenen VMs verwendet wurden, aber die Dienste sind noch nicht in der NSX-T Data Center-Bestandsliste definiert.

Es gibt mehrere Möglichkeiten, die Empfehlung anzufordern, aber am einfachsten ist es, zu **Planen und Fehler beheben > Empfehlungen** zu navigieren und auf **Neue Empfehlungen starten** klicken. Sie stellen die virtuellen Maschinen (VMs) bereit, die die Anwendungsgrenzen und den Zeitraum umfassen, in dem der Netzwerkdatenverkehr für diese spezifischen VMs analysiert werden soll. Sobald die Empfehlungsanalyse abgeschlossen ist, können Sie die Details der Empfehlung anzeigen und bei Bedarf die Empfehlung ändern, bevor Sie veröffentlicht wird. Weitere Informationen hierzu finden Sie unter [Generieren einer neuen NSX Intelligence-Empfehlung](#).

## Generieren einer neuen NSX Intelligence-Empfehlung

Die Funktion für NSX Intelligence-Empfehlungen bietet Empfehlungen zur Unterstützung der Mikro-Segmentierung Ihrer Anwendungen.

Das Generieren einer NSX Intelligence-Empfehlung beinhaltet Empfehlungen für Sicherheitsrichtlinien, Richtlinien-Sicherheitsgruppen und Dienste für die Anwendung. Die Empfehlungen werden basierend auf dem Datenverkehrsmuster bei der Kommunikation zwischen VMs in Ihrem NSX-T Data Center erstellt. Es gibt mehrere Möglichkeiten, eine Empfehlung mithilfe der NSX Intelligence-Benutzeroberfläche zu generieren. In der folgenden Vorgehensweise werden die drei verfügbaren Methoden beschrieben.


### Voraussetzungen

Installieren Sie NSX Intelligence. Weitere Informationen finden Sie unter „Installieren und Konfigurieren von NSX Intelligence“ im *Installationshandbuch für NSX-T Data Center*.

### Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://<nsx-manager-ip-address>` mit Enterprise-Administratorrechten bei einem NSX Manager an.
- 2 Initiieren Sie das Generieren einer neuen Empfehlung.

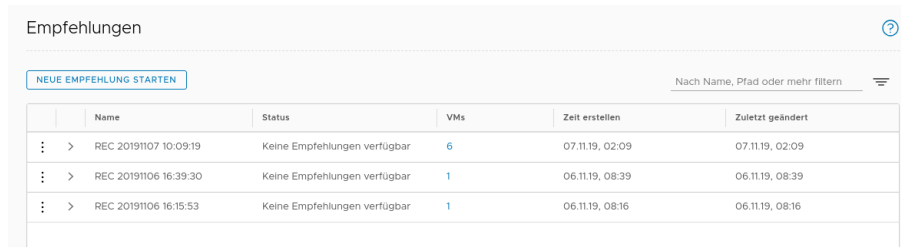
Verwenden Sie die folgende Tabelle, um zu entscheiden, welche der drei verfügbaren Methoden verwendet werden soll.

Methode	Schritte
Wählen Sie <b>Planen und Fehler beheben &gt; Empfehlungenaus.</b>	Klicken Sie auf <b>Neue Empfehlungen starten.</b>
Wählen Sie in der Ansicht „VMs“ eine VM aus und klicken Sie mit der rechten Maustaste.	Wählen Sie im Kontextmenü <b>Neue Empfehlungen starten</b> aus.
Wählen Sie <b>Planen und Fehler beheben &gt; Ermitteln und Maßnahmen ergreifen.</b>	<ol style="list-style-type: none"> <li>1 Klicken Sie im Filter „Sicherheitsposition“ auf den Pfeil nach unten und wählen Sie <b>VMs</b> aus.</li> <li>2 Wählen Sie die VMs aus, aus denen sich die Anwendungsgrenze zusammensetzt, und klicken Sie auf <b>Anwenden.</b></li> <li>3 Klicken Sie auf das Empfehlungssymbol .</li> <li>4 Klicken Sie im Dialogfeld „Empfehlungen“ auf <b>Neue Empfehlungen starten.</b></li> </ol>

- 3 Ändern Sie im Assistenten „Neue Empfehlungen starten“ optional den Standardwert für den **Empfehlungsnamen**.
- 4 Definieren oder ändern Sie die VMs, die als Begrenzung für die Sicherheitsrichtlinien-Empfehlung verwendet werden sollen.
  - a Klicken Sie auf **VMs auswählen** oder die Anzahl der VMs unter **Ausgewählte VMs**.
  - b Wählen Sie im Dialogfeld „VMs auswählen“ die VMs aus, die Sie als Begrenzung für die Analyse verwenden möchten, und deaktivieren Sie diejenigen, die Sie nicht hinzufügen möchten.  
  
Sie können bis zu 100 VMs für die Empfehlungsgrenze auswählen. Sie können auch den Namen in die Auswahlleiste eingeben, um die zur Auswahl stehenden VMs zu filtern.
  - c Klicken Sie auf **Speichern**.  
  
Die Anzahl der ausgewählten VMs wird im Dialogfeld „Neue Empfehlung erkennen“ angezeigt.
- 5 Erweitern Sie die Ansicht **Weitere Optionen**, um die für die Empfehlungsanalyse verwendeten Standardwerte für **Beschreibung** und **Zeitbereich** zu ändern. Der Standardwert für **Zeitbereich** ist „Letzter Monat“. Das bedeutet, dass bei der Empfehlungsanalyse der Netzwerkdatenverkehr verwendet wird, der im letzten Monat zwischen den ausgewählten VMs aufgetreten ist.
- 6 Klicken Sie auf **Ermittlung starten**.  
  
Die Empfehlungen werden seriell verarbeitet. Im Durchschnitt kann es zwischen 3 und 4 Minuten dauern, bis die Verarbeitung einer Empfehlung abgeschlossen ist, je nachdem, ob noch weitere Empfehlungen verarbeitet werden müssen. Wenn der zu analysierende Datenverkehr zwischen den VMs umfangreich ist, kann das Generieren einer



Empfehlung zwischen 10 und 15 Minuten dauern. Der Status kann über die Registerkarte **Empfehlungen** nachverfolgt werden. Es gibt folgende Status-Phasen: **Warten**, **Analyse** wird durchgeführt und schließlich **Bereit zum Veröffentlichen**. Der folgende Screenshot zeigt die drei unterschiedlichen Status der generierten Empfehlungen.



	Name	Status	VMs	Zeit erstellen	Zuletzt geändert
⋮ >	REC 20191107 10:09:19	Keine Empfehlungen verfügbar	6	07.11.19, 02:09	07.11.19, 02:09
⋮ >	REC 20191106 16:39:30	Keine Empfehlungen verfügbar	1	06.11.19, 08:39	06.11.19, 08:39
⋮ >	REC 20191106 16:15:53	Keine Empfehlungen verfügbar	1	06.11.19, 08:16	06.11.19, 08:16

Nachdem eine Empfehlung erfolgreich veröffentlicht wurde, wird der Status in „Veröffentlicht“ geändert.

### Nächste Schritte

Überprüfen Sie die generierte Empfehlung und entscheiden Sie, ob Sie veröffentlicht werden soll. Siehe [Überprüfen und Veröffentlichen einer generierten Empfehlung](#).

## Überprüfen und Veröffentlichen einer generierten Empfehlung

Wenn die generierte NSX Intelligence-Empfehlung den Status „Bereit zum Veröffentlichen“ aufweist, können Sie die Empfehlung überprüfen, sie bei Bedarf ändern und entscheiden, ob sie veröffentlicht werden soll.

### Voraussetzungen

Generieren Sie eine neue Empfehlung. Siehe [Generieren einer neuen NSX Intelligence-Empfehlung](#).

### Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://<nsx-manager-ip-address>> mit Unternehmensadministratorrechten bei einem NSX Manager an.
- 2 Klicken Sie auf **Planen und Fehler beheben > Empfehlungen**.
- 3 Um die Liste der angezeigten Empfehlungen einzugrenzen, klicken Sie oben rechts im Bildschirm auf **Nach Name, Pfad oder mehr filtern** und geben Sie die zu verwendenden Filterkriterien an.
- 4 Wenn Sie die Empfehlung nicht verwenden möchten, klicken Sie auf das Dreipunkt-Menüsymbol und wählen Sie **Löschen** aus.
- 5 Um die Übersicht über eine Empfehlung anzuzeigen, klicken Sie auf die Pfeilspitze neben dem Namen der Empfehlung, um die Zeile zu erweitern.

Sie sehen die Anzahl der generierten Regeln und die Anzahl der betroffenen Gruppen.

## 6 Überprüfen und verwalten Sie die Details der Empfehlung.

- a Klicken Sie auf den Namen der Empfehlung.

Der Assistent **Empfehlungen** wird ähnlich der folgenden Abbildung angezeigt.

The screenshot shows the 'Recommendations' assistant interface. On the left, a sidebar contains three steps: '1 Review Recommendations' (selected), '2 Place rules in FW context', and '3 Enforcement Summary'. The main area displays a recommendation for 'REC 20190719 15:59:02'. Below this, a summary bar shows 'Recommended FW Rules', 'Recommended Groups', and 'Recommended Services'. A table lists the recommended rules with columns for Name, Sources, Destinations, Services, Profiles, Applied To, and Action. The table shows six rules, all with 'Allow' actions and active status. At the bottom right, there are buttons for 'CANCEL', 'CONTINUE LATER', and 'NEXT'.

Name	Sources	Destinations	Services	Profiles	Applied To	Action
Policy-1 (REC 20190719 15:59:02)	(6)					
Rule-1 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	Win - RPC, DCOM, EP...	None	DFW	Allow
Rule-2 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	NBDS-Broadcast-V1	None	DFW	Allow
Rule-3 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	DHCP-Server	None	DFW	Allow
Rule-4 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	DHCPv6 Server	None	DFW	Allow
Rule-5 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	NBNS-Broadcast-V1	None	DFW	Allow
Rule-6 (REC 20190719 15:59:02)	Group-2 (REC 20190719 15:59:02)	Group-3 (REC 20190719 15:59:02)	SSH	None	Group-2 (REC 20190719 15:59:02)	Allow

- b Überprüfen Sie auf der Registerkarte **Empfohlene FW-Regeln** die Details zu den Firewall-Regeln. Um die Details zu ändern, klicken Sie in der entsprechenden Spalte auf den Wert und wählen Sie das Symbol für das Bearbeiten (Bleistift) aus.
- c Um zu definieren, wie die Pakete verarbeitet werden sollen, wählen Sie **Zulassen**, **Verwerfen** oder **Ablehnen** in der Spalte **Aktion** aus.
- d Verwenden Sie die Schaltfläche auf der rechten Seite, um die Regel zu aktivieren oder zu deaktivieren. Standardmäßig wird die generierte Regel so festgelegt, dass Sie bei der Veröffentlichung aktiviert wird, wie im vorherigen Schritt dargestellt.
- e Klicken Sie auf **Empfohlene Gruppen**.
- f Klicken Sie auf den Link in der Spalte **Mitglieder**, um die Details zu den VMs und IPs zu überprüfen, die für die Gruppen-Empfehlung festgelegt wurden.
- g Klicken Sie auf das Menüsymbol (drei Punkte) neben dem Namen der Gruppe und wählen Sie **Bearbeiten** aus, um Änderungen an der Gruppen-Empfehlung vorzunehmen.
- h Klicken Sie auf **Empfohlene Dienste** und überprüfen Sie die Details.
- i Klicken Sie auf das Menüsymbol (drei Punkte) neben dem Namen des Diensts und wählen Sie **Bearbeiten** aus, um Änderungen am Namen oder an der Beschreibung vorzunehmen. Bevor Sie einen Dienst löschen, stellen Sie sicher, dass der Dienst von keinen Regeln verwendet wird.
- j Klicken Sie auf **Weiter**.

- 7 Im Bereich **Regeln in FW-Kontext einfügen** können Sie die Reihenfolge ändern, in der die Regel-Empfehlung mit den vorhandenen Firewallregeln angewendet werden soll. Ziehen Sie den markierten Abschnitt, oder klicken Sie auf das Dreipunkt-Menüsymbol und wählen Sie **Über den ausgewählten Abschnitt verschieben** oder **Unter den ausgewählten Abschnitt verschieben** aus.
- 8 Klicken Sie auf **Veröffentlichen**.
- 9 Klicken Sie im Dialogfeld **Empfehlungen veröffentlichen** auf **Ja**.
- 10 Vergewissern Sie sich auf der Seite „Erzwingungsübersicht“, dass die Sicherheitsrichtlinien erfolgreich veröffentlicht wurden, und klicken Sie auf **Schließen**.

Der Wert in der Spalte „Status“ für die Empfehlung wird in der Tabelle der Empfehlungen zu „Veröffentlicht“ geändert.

### Ergebnisse

Sobald die Empfehlungen für die Sicherheitsrichtlinie erfolgreich veröffentlicht wurden, befinden Sie sich im schreibgeschützten Modus auf der Registerkarte **Planen und Fehler beheben > Empfehlungen**. Um die veröffentlichten Regel-Empfehlungen anzuzeigen und zu verwalten, wechseln Sie zu **Sicherheit > Verteilte Firewall**.

---

**Wichtig** Nachdem Sie die Regel-Empfehlungen veröffentlicht haben, zeigt die Visualisierung weiterhin die betroffenen Flows zwischen den VMs als orangefarbene Pfeile (ungeschützte Flows) an, bis neue Flows zwischen den betroffenen VMs generiert werden. Die Visualisierung meldet nur Datenverkehrsflows basierend auf der Zeit, in der sie auf dem Host aufgetreten sind, und spiegelt nicht den Regelsatz wider, der nach dem Auftreten dieser Datenverkehrsflows veröffentlicht wurde. Nachdem der Regelsatz veröffentlicht und neue Datenverkehrsflows generiert wurden, werden die neuen Flows als grüne Pfeile (zulässige Flows) angezeigt.

---

## Sichern und Wiederherstellen von NSX Intelligence

Wenn Ihre aktuelle NSX Intelligence-Konfiguration nicht mehr funktionsfähig ist oder wenn Sie Ihre Umgebung auf einen früheren Zustand zurücksetzen möchten, können Sie eine Wiederherstellung Ihrer Konfiguration anhand einer Sicherung durchführen. Der Sicherungs- und Wiederherstellungs-Workflow wird nur über das NSX Intelligence-CLI unterstützt.

Wenn Sie eine Sicherung durchführen, sichert NSX Intelligence nur die Konfigurationsdateien, die von allen Diensten verwendet werden, die die NSX Intelligence-Appliance umfassen. In der Sicherung sind keine Visualisierungsdaten enthalten.

Wenn Datenverlust oder -beschädigung in NSX Intelligence auftritt, gehen alle vorhandenen Daten für die korrelierten Flows und Empfehlungen ebenfalls verloren. Durch die Neuinstallation von NSX Intelligence wird die Erfassung von Netzwerkdatenverkehrsdaten neu gestartet, und die Visualisierung dieser erfassten Daten ist ab diesem Zeitpunkt verfügbar.

Nachdem Sie die Sicherungskonfiguration abgeschlossen haben, können Sie den Sicherungsbefehl jederzeit manuell über die NSX Intelligence-Appliance ausführen. Die Sicherung wird verschlüsselt, komprimiert und auf dem bei der Sicherungskonfiguration festgelegten Remoteserver gespeichert. Wenn Sie eine Sicherung erstellen, werden das Datum und die Uhrzeit der Sicherung an den Sicherungsdateinamen angehängt, sodass jede Sicherungsdatei eindeutig ist. Beispiel: `config-backup-2019-06-21T21_06_07UTC.tar.gz`.

Wenn Sie eine NSX Intelligence-Sicherung wiederherstellen, wird der Konfigurationsstatus beim Erstellen der Sicherung wiederhergestellt. Sie müssen die Sicherung auf einer NSX Intelligence-Appliance wiederherstellen, die dieselbe Version der NSX Intelligence-Appliance ausführt, über die die Sicherungsdatei erstellt wurde. Sie können eine vorhandene NSX Intelligence-Appliance wiederherstellen oder zu einer neu installierten NSX Intelligence-Appliance wechseln. Es ist jedoch wichtig, dass diese jeweils dieselbe Version wie die von Ihnen gesicherte NSX Intelligence-Appliance aufweisen.

## Konfigurieren von NSX Intelligence-Sicherungen

Sie müssen einen Sicherungsdateiserver konfigurieren, bevor Sie eine Sicherung Ihrer NSX Intelligence-Konfiguration durchführen können. Nachdem ein Sicherungsdateiserver konfiguriert wurde, können Sie jederzeit eine Sicherung für NSX Intelligence erstellen.

### Voraussetzungen

- Stellen Sie sicher, dass Sie über die CLI-Admin-Anmeldedaten für das NSX Intelligence-CLI verfügen.
- Stellen Sie sicher, dass Sie den Benutzernamen und das Kennwort für den Remoteserver kennen.
- Rufen Sie den Dateipfad ab, in dem die Sicherungsdateien auf dem Remoteserver gespeichert werden sollen.

### Verfahren

- 1 Melden Sie sich mithilfe einer Befehlszeilenaufforderung mit Administratorrechten beim NSX Intelligence-CLI-Host an.

```
$ ssh admin@cli-ip-address
admin@cli-ip-address's password:
```

- 2 Konfigurieren Sie den Sicherungsdateiserver.

Die Befehlssyntax lautet

```
set backup remote-host remote_host_address remote-path remote_folder_path remote-host-
username remote_host_username remote-host-password remote_host_password passphrase
pass_phrase
```

wobei *remote\_host\_address* die Remote-Host-IP- oder FQDN-Adresse des Sicherungsdateiservers ist. Das *remote\_host\_username*-Konto muss dabei die erforderlichen

Berechtigungen für das Erstellen der Sicherungsdateien unter *remote\_folder\_path* verfügen. Sie müssen für den *passphrase*-Parameter einen starken Wert angeben. Er muss mindestens acht Zeichen lang sein, mindestens einen Groß- und einen Kleinbuchstaben sowie ein Sonderzeichen enthalten. Beispiel:

```
set backup remote-host 10.11.22.33 remote-path /root remote-host-username root remote-host-
password MyRemotePassword passphrase MyPassPhra$e
```

### 3 Verifizieren Sie die Konfiguration.

```
get configuration
```

Überprüfen Sie in der Ausgabe, ob die Zeile mit `set backup` korrekt aussieht. Bei Verwendung des Beispiels im vorherigen Schritt muss die Ausgabe die folgende Zeile enthalten.

```
set backup remote-host 10.11.22.33 remote-path /root remote-host-username root
```

## Sichern von NSX Intelligence

Sie können Ihre NSX Intelligence-Appliance-Konfigurationsdateien mit dem CLI-Befehl sichern.

### Voraussetzungen

- Stellen Sie sicher, dass Sie über einen Administratorzugriff auf das NSX Intelligence-CLI verfügen.
- Konfigurieren Sie einen Sicherungsdateiserver. Siehe [Konfigurieren von NSX Intelligence-Sicherungen](#).

### Verfahren

- 1 Melden Sie sich mit Administratorrechten beim NSX Intelligence-CLI an.
- 2 Erstellen Sie die Sicherung.

```
backup intelligence configuration
```

Wenn die Sicherung erfolgreich war, wird eine Meldung ähnlich der folgenden angezeigt.

```
Backup Complete. Archived at: backup_file_server-IP_address:/root/backup_archives/
intelligence-config-backup-2019-07-18T07_00_26UTC.tar.gz
```

- 3 Sie können den Fortschritt der Sicherung über eine andere CLI-Sitzung anzeigen.
  - a Melden Sie sich bei einer anderen NSX Intelligence-CLI-Sitzung an.
  - b Geben Sie den folgenden Befehl ein.

```
get log-file node-mgmt.log follow
```

## NSX Intelligence-Sicherungen wiederherstellen

Wenn Sie eine Sicherung wiederherstellen, stellen Sie den Status der NSX Intelligence-Konfiguration zum Zeitpunkt der Sicherung wieder her. Sie können eine NSX Intelligence-Sicherung mit einem CLI-Befehl wiederherstellen.

Sie müssen eine Sicherung auf einer Installation der NSX Intelligence-Appliance wiederherstellen, die dieselbe Version wie die Sicherung ist, die Sie wiederherstellen. Standardmäßig ist die wiederhergestellte Sicherungsdatei die zuletzt generierte Sicherung. Wenn Sie eine Sicherung auf einer neu installierten NSX Intelligence-Appliance wiederherstellen, legen Sie den Archivnamen fest, bevor Sie die Sicherung wiederherstellen.

### Voraussetzungen

- Stellen Sie sicher, dass Sie über die Admin-Anmeldedaten und die Host-Informationen für den Sicherungsdateiserver verfügen.
- Stellen Sie sicher, dass Sie über einen Administratorzugriff auf das NSX Intelligence-CLI verfügen.

### Verfahren

- 1 Melden Sie sich mit Administratorrechten beim neuen NSX Intelligence-CLI-Server an.
- 2 Konfigurieren Sie den Remoteserver, auf dem sich die Sicherungen befinden.

Die Befehlssyntax lautet

```
set restore remote-host backup_server_IP_address remote-path remote_folder_path remote-  
host-username remote_host_username remote-host-password remote_host_password passphrase  
pass_phrase
```

wobei *backup\_server\_IP\_address* die Remote-Host-IP- oder FQDN-Adresse des Sicherungsdateiservers ist. Das *remote\_host\_username*-Konto muss über die erforderlichen Berechtigungen für den Zugriff auf die Sicherungsdateien unter *remote\_folder\_path* verfügen. Beispiel:

```
set restore remote-host 10.11.22.33 remote-path /root remote-host-username root remote-  
host-password MyRemotePassword passphrase MyPassPhra$e
```

- 3 Überprüfen Sie die Wiederherstellungskonfiguration.

```
get configuration
```

Überprüfen Sie in der Ausgabe, ob die Zeile mit `set restore` korrekt aussieht. Bei Verwendung des Beispiels im vorherigen Schritt muss die Ausgabe die folgende Zeile enthalten.

```
set restore remote-host 10.11.22.33 remote-path /root remote-host-username root
```

- 4 Stellen Sie die Sicherung über folgenden Befehl wieder her.

```
restore intelligence configuration
```

Wenn die Wiederherstellung erfolgreich war, wird eine Meldung ähnlich der folgenden angezeigt.

```
NSX Intelligence Restore Complete.
```

- 5 Sie können den Fortschritt der Sicherungswiederherstellung über eine andere CLI-Sitzung anzeigen.
  - a Melden Sie sich bei einer anderen NSX Intelligence-CLI-Sitzung an.
  - b Geben Sie den folgenden Befehl ein.

```
get log-file node-mgmt.log follow
```

## Fehlerbehebung bei NSX Intelligence-Problemen

Wenn die NSX Intelligence-Appliance nicht mehr reagiert oder Sie weitere Details zu einer Fehlermeldung benötigen, die Sie während der Verwendung der Appliance erhalten haben, können Sie bestimmte Befehle ausführen, um den Zustand der NSX Intelligence-Dienste abzurufen.

Sie können auch Support-Pakete zusammenstellen, die Sie und die VMware Support-Mitarbeiter beim Debugging von möglicherweise aufgetretenen Problemen unterstützen.

## Überprüfen des Status der NSX Intelligence-Appliance

Wenn die NSX Intelligence-Appliance nicht mehr reagiert, überprüfen Sie den Status der NSX Intelligence-Dienste.

### Problem

Die NSX Intelligence-Appliance reagiert nicht mehr oder Sie erhalten eine Fehlermeldung, die angibt, dass die Appliance nicht wie erwartet funktioniert.

### Ursache

Es ist möglich, dass einer oder mehrere der zugrunde liegenden NSX Intelligence-Dienste angehalten wurde oder sich nicht in einem fehlerfreien Zustand befindet.

### Lösung

- 1 Melden Sie sich unter Verwendung eines Kontos mit der Rolle „Enterprise-Administrator“ beim CLI-Host der NSX Intelligence-Appliance an.

## 2 Überprüfen Sie den Status der NSX Intelligence-Dienste mit dem Befehl `get services`.

Wenn alle NSX Intelligence-Dienste ordnungsgemäß funktionieren, wird eine Ausgabe ähnlich dem folgenden Beispiel angezeigt.

```
my_nsx-intel> get services
Service name:          druid
Service state:         running
Coordinator health:    good
Broker health:         good
Historical health:     good
Overlord health:       good
MiddleManager health:  good

Service name:          http
Service state:         running
Session timeout:       1800
Connection timeout:    30
Redirect host:         (not configured)
Client API rate limit: 100 requests/sec
Client API concurrency limit: 40
Global API concurrency limit: 199

Service name:          kafka
Service state:         running
Service health:        good

Service name:          liagent
Service state:         stopped

Service name:          mgmt-plane-bus
Service state:         stopped

Service name:          node-mgmt
Service state:         running

Service name:          nsx-config
Service state:         running

Service name:          nsx-message-bus
Service state:         stopped

Service name:          nsx-upgrade-agent
Service state:         running

Service name:          ntp
Service state:         running
Start on boot:         True

Service name:          pace-server
Service state:         running

Service name:          postgres
Service state:         running
Service health:        good
```



```

Service name:      processing
Service state:     running

Service name:      snmp
Service state:     stopped
Start on boot:     False

Service name:      spark
Service state:     running
Service health:    good

Service name:      spark-job-scheduler
Service state:     running

Service name:      ssh
Service state:     running
Start on boot:     True

Service name:      syslog
Service state:     running

Service name:      ui-service
Service state:     running

Service name:      zookeeper
Service state:     running
Service health:    good

my_nsx-intel>

```

Ein Dienst kann den Zustand `Wird ausgeführt` oder `Gestoppt` besitzen. Die Integrität eines Diensts kann gut oder herabgestuft sein.

- 3 Sie können auch die `syslog`-Datei anzeigen und nach der Ausgabe des Skripts `pace-monitor.sh` zur Integritätsprüfung suchen, das die Integrität der NSX Intelligence-Dienste in der `syslog`-Datei protokolliert.

Wenn alle Dienste wie erwartet funktionieren, wird nach Ausführen des Befehls `get log-file syslog | find pace-monitor` eine Ausgabe ähnlich wie im folgenden Beispiel angezeigt.

```

my_nsx-intel> get log-file syslog | find pace-monitor
<13>1 2019-08-30T03:19:20.409899+00:00 my_nsx-intel pace-monitor.sh - - -      "_self": {
<13>1 2019-08-30T03:19:20.410253+00:00 my_nsx-intel pace-monitor.sh - - -      "href": "/"
node/pace/appliance-health",
<13>1 2019-08-30T03:19:20.410623+00:00 my_nsx-intel pace-monitor.sh - - -      "rel":
"self"
<13>1 2019-08-30T03:19:20.410908+00:00 my_nsx-intel pace-monitor.sh - - -      },
<13>1 2019-08-30T03:19:20.411162+00:00 my_nsx-intel pace-monitor.sh - - -      "appliance-
health": {
<13>1 2019-08-30T03:19:20.411416+00:00 my_nsx-intel pace-monitor.sh - - -      "status":
"Following NSX Intelligence first boot services are either PENDING or FAILED - Token-
Registration",

```

```

<13>1 2019-08-30T03:19:20.411668+00:00 my_nsx-intel pace-monitor.sh - - - "sub-system-
status": {
<13>1 2019-08-30T03:19:20.411923+00:00 my_nsx-intel pace-monitor.sh - - - "app-
services": {
<13>1 2019-08-30T03:19:20.412280+00:00 my_nsx-intel pace-monitor.sh - - -
"services": [],
<13>1 2019-08-30T03:19:20.412528+00:00 my_nsx-intel pace-monitor.sh - - -
"status": ""
<13>1 2019-08-30T03:19:20.412807+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.413075+00:00 my_nsx-intel pace-monitor.sh - - - "base-
infra-services": {
<13>1 2019-08-30T03:19:20.413303+00:00 my_nsx-intel pace-monitor.sh - - -
"services": [
<13>1 2019-08-30T03:19:20.413613+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.413848+00:00 my_nsx-intel pace-monitor.sh - - -
"druid-health": {
<13>1 2019-08-30T03:19:20.414146+00:00 my_nsx-intel pace-monitor.sh - - -
"broker": "good",
<13>1 2019-08-30T03:19:20.414473+00:00 my_nsx-intel pace-monitor.sh - - -
"coordinator": "good",
<13>1 2019-08-30T03:19:20.414717+00:00 my_nsx-intel pace-monitor.sh - - -
"historical": "good",
<13>1 2019-08-30T03:19:20.414979+00:00 my_nsx-intel pace-monitor.sh - - -
"middlemanager": "good",
<13>1 2019-08-30T03:19:20.415295+00:00 my_nsx-intel pace-monitor.sh - - -
"overlord": "good"
<13>1 2019-08-30T03:19:20.415533+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.415762+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "druid"
<13>1 2019-08-30T03:19:20.415982+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.416269+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.416539+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.416772+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "kafka"
<13>1 2019-08-30T03:19:20.416991+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.417204+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.417510+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.417745+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "postgres"
<13>1 2019-08-30T03:19:20.418133+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.418389+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.418626+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.418855+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "spark"
<13>1 2019-08-30T03:19:20.419157+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.419435+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.419684+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.419928+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "zookeeper"
<13>1 2019-08-30T03:19:20.420165+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.420496+00:00 my_nsx-intel pace-monitor.sh - - - ],

```

```

<13>1 2019-08-30T03:19:20.420786+00:00 my_nsx-intel pace-monitor.sh - - -
"status": ""
<13>1 2019-08-30T03:19:20.421022+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.421255+00:00 my_nsx-intel pace-monitor.sh - - - "first-
boot-services": {
<13>1 2019-08-30T03:19:20.421539+00:00 my_nsx-intel pace-monitor.sh - - -
"services": [
<13>1 2019-08-30T03:19:20.421777+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.422010+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "degraded",
<13>1 2019-08-30T03:19:20.422277+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "token-registration"
<13>1 2019-08-30T03:19:20.422512+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.422770+00:00 my_nsx-intel pace-monitor.sh - - - ],
<13>1 2019-08-30T03:19:20.423012+00:00 my_nsx-intel pace-monitor.sh - - -
"status": "Following NSX Intelligence first boot, services are either PENDING or FAILED
- Token-Registration"
<13>1 2019-08-30T03:19:20.423354+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.423601+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.423882+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.424339+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.972629+00:00 my_nsx-intel pace-monitor.sh - - - NSX
Intelligence health OK.
<30>1 2019-08-30T03:19:20.973076+00:00 my_nsx-intel pace-monitor 20804 - - <13>Aug 30
03:19:19 pace-monitor.sh: NSX Intelligence health OK.
<182>1 2019-08-30T03:23:23.857Z my_nsx-intel NSX 21752 - [nsx@6876 comp="nsx-cli"
subcomp="node-mgmt" username="admin" level="INFO"] CMD: get log-file syslog | find pace-
monitor

```

Wenn ein Problem mit einem der Dienste vorliegt, wird nach dem Ausführen von `get log-file syslog | grep pace-monitor` möglicherweise die folgende Zeile angezeigt.

```
NSX Intelligence health DEGRADED. Return code not HTTP OK.
```

- 4 Wenn Sie eine der folgenden Ausgaben erhalten, starten Sie den Dienst mit dem Befehl `restart service Dienstname neu`.

- Nach dem Ausführen des Befehls `get services` wird für einen der Dienste Dienststatus: Gestoppt oder Dienstintegrität: herabgestuft angezeigt.
- Nach dem Ausführen des Befehls `get log-file syslog | grep pace-monitor` wird in der Ausgabe die folgende oder eine ähnliche Meldung angezeigt: PACE-Integrität HERABGESTUFT. Rückgabecode nicht HTTP OK..

Wenn z. B. der Zustand des postgres-Diensts gestoppt oder Wird ausgeführt lautet, die Dienstintegrität jedoch herabgestuft ist, führen Sie den folgenden Befehl aus.

```
restart service postgres
```

**Wichtig** Sie müssen den Befehl `restart service service-name` verwenden, um NSX Intelligence-Dienste neu zu starten. Wenn Sie sich stattdessen für die Verwendung der Befehle `stop service service-name` und `start service service-name` entscheiden, müssen Sie auch jeden der Dienste manuell neu starten, die von *service-name* abhängig sind. Die folgende Liste zeigt die Abhängigkeitsreihenfolge, in der die NSX Intelligence-Dienste neu gestartet werden müssen.

```
zookeeper > druid > kafka > spark > spark-job-scheduler > nsx-config > processing > pace-  
server
```

Wenn beispielsweise der `nsx-config`-Dienst angehalten und dann mit dem Befehl `stop | start service service-name` gestartet wird, müssen Sie auch den Befehl `restart service service-name` verwenden, um die `processing-pace-server`-Dienste neu zu starten.

Wenn Sie zudem den Befehl `restart service service-name` zum Neustarten der in der Liste der Abhängigkeitsreihenfolge angezeigten Dienste vor dem `spark-job-scheduler`-Dienst verwenden, müssen Sie auch den `spark-job-scheduler`-Dienst mithilfe des `restart service spark-job-scheduler`-Befehls manuell neu starten. Andernfalls wird der `spark-job-scheduler`-Dienst in einen fehlerhaften Zustand versetzt.

## Erfassen von NSX Intelligence-Support-Paketen

Sie können ein Support-Paket mithilfe der NSX Intelligence-CLI erfassen.

Der Inhalt der Support-Paketdatei enthält keine Daten. Es enthält Dateien in den folgenden Verzeichnissen.

- `/opt/vmware/`\*
- `/var/log/`\*
- `/etc/`\*
- Systemstatus mit `journalctl` und `systemctl`

### Voraussetzungen

Stellen Sie sicher, dass Sie über Enterprise-Administratorzugriff auf das NSX Intelligence-CLI verfügen.

### Verfahren

- 1 Melden Sie sich unter Verwendung eines Kontos mit der Rollenberechtigung „Enterprise-Administrator“ bei der NSX Intelligence-CLI an.

## 2 Generieren Sie das Support-Paket.

Die Befehlssyntax lautet wie folgt, wobei Sie den Wert für *support\_filename.tgz* angeben.

```
get support-bundle file support_filename.tgz
```

Beispiel:

```
get support-bundle file support_bundle123.tgz
```

Wenn die Paketdatei erfolgreich erstellt wurde, werden Meldungen angezeigt, die den folgenden ähneln.

```
„support_bundle123.tgz“ erstellt haben, verwenden Sie den folgenden Befehl, um die  
Datei zu übertragen: copy file support_bundle123.tgz url <url> Nach der Übertragung von  
„support_bundle123.tgz“ extrahieren Sie sie mit: tar xvf support_bundle123.tgz
```

## 3 Stellen Sie mithilfe des folgenden Befehls sicher, dass das Support-Paket vorhanden ist.

```
get files
```

Eine Meldung, die so oder ähnlich aussieht, wird angezeigt:

```
Directory of filestore:/  
-rw- 21377586 June 29 05:29:12 UTC support_bundle123.tgz
```