

Administratorhandbuch für NSX-T Data Center

Geändert am 24. Mai 2019
VMware NSX-T Data Center 2.3



vmware®

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

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

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie diese an:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

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

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

Inhalt

Grundlegende Informationen zur Verwaltung von VMware NSX-T Data Center 9

1 Logische Switches und Konfigurieren einer VM-Anfügung 10

Grundlegendes zu den BUM-Frame-Replizierungsmodi 11

Erstellen eines logischen Switches 13

Schicht 2-Bridging 14

Erstellen eines Bridge-Clusters 16

Erstellen eines Bridge-Profiles 17

Erstellen eines Bridge-gestützten logischen Schicht-2-Switches 17

Erstellen eines logischen VLAN-Switch für den NSX Edge-Uplink 19

Verbinden einer VM mit einem logischen Switch 21

Anfügen einer auf vCenter Server gehosteten VM an einen logischen NSX-T Data Center-Switch 21

Verknüpfen einer auf eigenständigem ESXi gehosteten VM mit einem logischen NSX-T Data Center-Switch 23

Anfügen einer auf KVM-Hosts gehosteten VM an einen logischen NSX-T Data Center-Switch 28

Testen der Schicht-2-Konnektivität 29

2 Logischer Switch Port 33

Erstellen eines logischen Switch-Ports 33

Überwachen der Aktivität eines Ports für einen logischen Switch 34

3 Switching-Profile für logische Switches und logische Ports 36

Grundlegendes zum QoS-Switching-Profil 37

Konfigurieren eines benutzerdefinierten QoS-Switching-Profiles 38

Grundlegendes zum Switching-Profil für die IP-Ermittlung 40

Konfigurieren eines Switching-Profiles für die IP-Ermittlung 41

Grundlegendes zu SpoofGuard 42

Konfigurieren von Port-Adressbindungen 43

Konfigurieren eines SpoofGuard-Switching-Profiles 44

Grundlegendes zum Switching-Profil für die Switch-Sicherheit 44

Konfigurieren eines benutzerdefinierten Switching-Profiles für die Switch-Sicherheit 45

Grundlegendes zum Switching-Profil für die MAC-Verwaltung 46

Konfigurieren des Switching-Profiles für die MAC-Verwaltung 47

Zuordnen eines benutzerdefinierten Profils zu einem logischen Switch 48

Zuordnen eines benutzerdefinierten Profils zu einem logischen Port 49

4 Logischer Tier-1-Router 51

Erstellen eines logischen Tier-1-Routers	52
Hinzufügen eines Downlink-Ports auf einem logischen Tier-1-Router	53
Hinzufügen eines VLAN-Ports auf einem logischen Tier-0- oder Tier-1-Router	54
Konfigurieren einer Routenankündigung auf einem logischen Tier-1-Router	55
Konfigurieren einer statischen Route auf einem logischen Tier-1-Router	57
Erstellen eines eigenständigen logischen Tier-1-Routers	59

5 Logischer Ebene-0-Router 61

Erstellen eines logischen Tier-0-Routers	63
Anfügen von Tier-0 und Tier-1	64
Überprüfen des Abrufs von Routen von einem Tier-1-Router für einen Tier-0-Router	66
Verbinden eines logischen Tier-0 Routers mit einem logischen VLAN-Switch für den NSX Edge-Uplink	67
Überprüfen des logischen Tier-0 Routers und der TOR-Verbindung	68
Hinzufügen eines Loopback-Router-Ports	70
Hinzufügen eines VLAN-Ports auf einem logischen Tier-0- oder Tier-1-Router	71
Konfigurieren einer statischen Route	72
Überprüfen der statischen Route	73
BGP-Konfigurationsoptionen	75
Konfigurieren von BGP auf einem logischen Tier-0-Router	77
Überprüfen von BGP-Verbindungen von einem Tier-0-Dienstrouter aus	79
Konfigurieren von BFD auf einem logischen Tier-0 Router	80
Aktivieren von Route Redistribution auf dem logischen Tier-0-Router	81
Überprüfen der Nord-Süd-Konnektivität und Route Redistribution	82
Grundlegendes zum ECMP-Routing	84
Hinzufügen eines Uplink-Ports für den zweiten Edge-Knoten	85
Hinzufügen eines zweiten BGP-Nachbarn und Aktivieren des ECMP-Routings	86
Überprüfen der ECMP-Routing-Konnektivität	87
Erstellen einer IP-Präfix-Liste	88
Erstellen einer Community-Liste	90
Erstellen einer Route Map	90
Konfigurieren des Timers für die Weiterleitung der Aktiv-Benachrichtigung	91

6 Netzwerkadressübersetzung (NAT) 93

Tier-1-NAT	94
Konfigurieren einer Quell-NAT auf einem Tier-1-Router	94
Konfigurieren der Ziel-NAT auf einem Tier-1-Router	96
Ankündigen von Tier-1-NAT-Routen für den Upstream-Tier-0-Router	98
Ankündigen von Tier-1-NAT-Routen für die physische Architektur	99
Überprüfen der Tier-1-NAT	100
Tier-0-NAT	101
Konfigurieren der Quell- und Ziel-NAT auf einem Tier-0-Router	101

Reflexive NAT 102

Konfigurieren einer reflexiven NAT auf einem logischen Tier-0- oder Tier-1-Router 104

7 Firewallabschnitte und Firewallregeln 106

Hinzufügen eines Firewallregelabschnitts 107

Löschen eines Firewallregelabschnitts 108

Aktivieren und Deaktivieren von Abschnittsregeln 108

Aktivieren und Deaktivieren von Abschnittsprotokollen 109

Informationen über Firewallregeln 109

Hinzufügen einer Firewallregel 111

Löschen einer Firewallregel 113

Bearbeiten der standardmäßigen Regel für die verteilte Firewall 114

Ändern der Reihenfolge von Firewallregeln 115

Filtern der Firewallregeln 115

Konfigurieren der Firewall für den Bridge-Port eines logischen Switches 116

Konfigurieren einer Firewall-Ausschlussliste 116

Aktivieren und Deaktivieren der Firewall 117

Hinzufügen oder Löschen einer Firewallregel zu bzw. von einem logischen Router 117

8 Virtual Private Networks 119

Konfigurieren eines IPSec-VPNs 120

Konfigurieren eines L2VPN 123

9 Verwalten von Objekten, Gruppen, Diensten und VMs 125

Erstellen eines IP Sets 125

Erstellen eines IP-Pools 126

Erstellen eines MAC Set 126

Erstellen einer NS-Gruppe 127

Konfigurieren von Diensten und Dienstgruppen 129

Erstellen eines NS-Dienstes 129

Verwalten von Tags für eine virtuelle Maschine 130

10 Logischer Load Balancer 131

Wichtige Load Balancer-Konzepte 132

Skalieren von Load Balancer-Ressourcen 132

Unterstützte Load Balancer-Funktionen 133

Load Balancer-Topologien 134

Konfigurieren von Load Balancer-Komponenten 136

Erstellen eines Load Balancers 136

Konfigurieren einer aktiven Systemzustandsüberwachung 137

Konfigurieren von passiven Systemzustandsüberwachungen 141

- [Hinzufügen eines Serverpools für den Lastausgleich](#) 142
- [Konfigurieren der Komponenten des virtuellen Servers](#) 146

11 DHCP 169

- [Erstellen eines DHCP-Serverprofils](#) 169
- [Erstellen eines DHCP-Servers](#) 170
- [Anfügen eines DHCP-Servers an einen logischen Switch](#) 171
- [Trennen eines DHCP-Servers von einem logischen Switch](#) 171
- [Erstellen eines DHCP-Relay-Profils](#) 171
- [Erstellen eines DHCP-Relay-Dienstes](#) 172
- [Hinzufügen eines DHCP-Dienstes zu einem Logical Router Port](#) 172

12 Metadaten-Proxyserver 174

- [Hinzufügen eines Metadaten-Proxyservers](#) 174
- [Anfügen eines Metadaten-Proxyserver an einen logischen Switch](#) 176
- [Trennen eines Metadaten-Proxy-Servers von einem logischen Switch](#) 176

13 IP-Adressverwaltung 178

- [Verwalten von IP-Blöcken](#) 178
- [Verwalten von Subnetzen für IP-Blöcke](#) 179

14 NSX-Richtlinie 180

- [Übersicht](#) 180
- [Hinzufügen eines Erzwingungspunkts](#) 181
- [Hinzufügen eines Diensts](#) 182
- [Hinzufügen einer Domäne](#) 183
- [Konfigurieren der Sicherung des NSX Policy Managers](#) 184
- [Sichern des NSX Policy Managers](#) 185
- [Wiederherstellen des NSX Policy Managers](#) 185
- [Verknüpfen eines vIDM-Hosts mit dem NSX Policy Manager](#) 186
- [Verwalten von Rollenzuweisungen](#) 187

15 Service Insertion 189

- [Übersicht](#) 189
- [Registrieren eines Diensts](#) 190
- [Bereitstellen einer Dienstinanz](#) 192
- [Konfigurieren der Umleitung des Datenverkehrs](#) 193
- [Überwachung der Umleitung des Datenverkehrs](#) 193

16 NSX Cloud 195

- [Der Cloud Service Manager](#) 195

Clouds	196
System	203
Verwalten der Quarantäne-Richtlinie	205
Quarantäne-Richtlinie aktivieren oder deaktivieren	206
Quarantäne-Richtlinie-Auswirkungen bei Deaktivierung	208
Quarantäne-Richtlinie-Auswirkungen bei Aktivierung	209
NSX Cloud-Sicherheitsgruppen für die Public Cloud	210
Überblick über Onboarding und Verwaltung von Workload-VMs	211
Unterstützte Betriebssysteme	211
Einbinden von Arbeitslast-VMs von Microsoft Azure	212
Onboarding von Arbeitslast-VMs von AWS	213
Onboarden von Workload-VMs	214
Taggen von virtuellen Maschinen in der Public Cloud	215
Installieren von NSX Agent	215
Automatische Installation von NSX Agent	221
Verwalten von Workload-VMs	222
Auf verwaltete Workload-VMs zugreifen	222
Gruppen-VMs mit NSX-T Data Center und Public-Cloud-Tags	223
Einrichten von Mikro-Segmentierung für Workload-VMs	226
Verwendung von NSX-T Data Center-Funktionen mit der Public Cloud	227
Verwenden von erweiterten NSX Cloud-Funktionen	230
Aktivieren von Syslog-Weiterleitung	230
Fehlerbehebung	231
Überprüfen von NSX Cloud-Komponenten	231
Fehlerbehebung – Häufig gestellte Fragen	232

17 Vorgänge und Verwaltung 234

Hinzufügen eines Lizenzschlüssels	235
Verwalten von Benutzerkonten und der rollenbasierten Zugriffssteuerung	235
Ändern des CLI-Benutzerkennworts	236
Authentifizierungsrichtlinien-Einstellungen	236
Abrufen des Zertifikatfingerabdrucks von einem vIDM-Host	237
Verknüpfen eines vIDM-Hosts mit NSX-T	238
Zeitsynchronisierung zwischen NSX Manager, vIDM und zugehörigen Komponenten	239
Rollenbasierte Zugriffssteuerung	240
Verwalten von Rollenzuweisungen	245
Anzeigen von Prinzipalidentitäten	246
Einrichten von Zertifikaten	247
Erstellen einer Datei für die Zertifikatsignieranforderung	247
Importieren eines CA-Zertifikats	248
Importieren eines Zertifikats	249

Erstellen eines selbstsignierten Zertifikats	250
Ersetzen eines Zertifikats	251
Importieren einer Zertifikatswiderrufsliste	251
Importieren eines Zertifikats für eine CSR	252
Konfigurieren von Appliances	253
Hinzufügen eines Berechnungsmanagers	254
Tags verwalten	255
Suchen nach Objekten	256
Suchen nach dem SSH-Fingerabdruck eines Remote-Servers	257
Sichern und Wiederherstellen von NSX Manager	258
Sichern der NSX Manager-Konfiguration	259
Wiederherstellen der NSX Manager-Konfiguration	261
Wiederherstellen eines NSX Controller-Clusters	265
Verwalten von Appliances und Appliance-Clustern	267
Verwalten von NSX Manager	267
Verwalten von NSX Controller-Clustern	268
Verwalten von NSX Edge-Clustern	275
Protokollmeldungen	280
Konfigurieren der Remoteprotokollierung	281
Protokollmeldungs-IDs	283
Konfigurieren von IPFIX	284
Konfigurieren von Switch-IPFIX-Profilen	285
Konfigurieren von Firewall-IPFIX-Collectors	286
ESXi-IPFIX-Vorlagen	287
IPFIX-Vorlagen für KVM	292
Nachverfolgen des Pfads eines Pakets mit Traceflow	452
Anzeigen der Portverbindungsinformationen	454
Überwachen der Aktivität eines Ports für einen logischen Switch	455
Überwachen von Portspiegelungssitzungen	456
Überwachen von Fabric-Knoten	459
Anzeigen von Daten über Anwendungen, die auf virtuellen Maschinen ausgeführt werden	459
Erfassen von Support-Paketen	460
Programm zur Verbesserung der Benutzerfreundlichkeit	461
Bearbeiten der CEIP-Konfiguration (Einstellungen bzgl. der Teilnahme am „Programm zur Verbesserung der Benutzerfreundlichkeit“)	461

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 das Networking für logische Tier-Router einrichten. Außerdem wird dort die Konfiguration von NAT, Firewalls, SpoofGuard, Gruppierung und DHCP beschrieben.

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, die in der technischen Dokumentation von VMware verwendet werden, finden Sie unter <http://www.vmware.com/support/pubs>.

Logische Switches und Konfigurieren einer VM-Anfügung

1

Ein logischer NSX-T Data Center-Switch bildet die Switching-Funktionalität, Broadcast-, unbekannten Unicast- und Multicast (BUM)-Datenverkehr in einer virtuellen Umgebung ab, die vollständig von der zugrunde liegenden physischen Hardware entkoppelt ist.

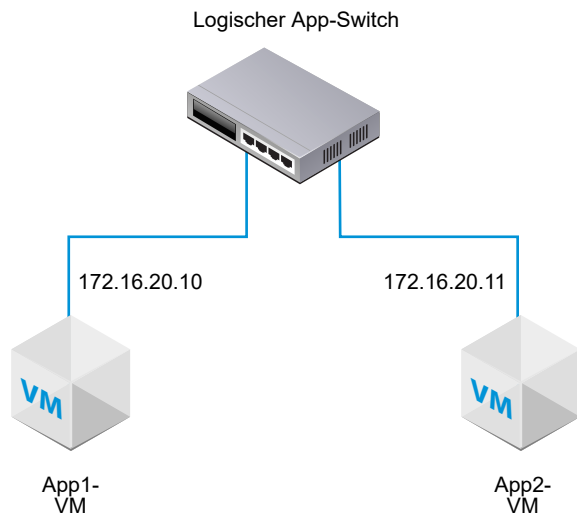
Hinweis zu NSX Cloud Wenn Sie NSX Cloud verwenden, finden Sie unter [Verwendung von NSX-T Data Center-Funktionen mit der Public Cloud](#) eine Liste der automatisch generierten logischen Elemente, unterstützten Funktionen und Konfigurationen, die für NSX Cloud erforderlich sind.

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 1-1. Topologie für einen logischen Switch



Beispielsweise enthält die Topologie 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.

Dieses Kapitel enthält die folgenden Themen:

- [Grundlegendes zu den BUM-Frame-Replizierungsmodi](#)
- [Erstellen eines logischen Switches](#)
- [Schicht 2-Bridging](#)
- [Erstellen eines logischen VLAN-Switch für den NSX Edge-Uplink](#)
- [Verbinden einer VM mit einem logischen Switch](#)
- [Testen der Schicht-2-Konnektivität](#)

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 1 Logische Switches und Konfigurieren einer VM-Anfügung](#) und [Grundlegendes zu den BUM-Frame-Replizierungsmodi](#).
- Stellen Sie sicher, dass Ihr NSX Controller-Cluster stabil ist.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie **Switching > Switches** aus.
- 3 Klicken Sie auf **Hinzufügen**.
- 4 Geben Sie für den logischen Switch einen Namen und optional eine Beschreibung ein.
- 5 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.
- 6 Geben Sie den Namen einer Uplink-Teaming-Richtlinie ein.
- 7 Legen Sie den **Administrativen Status** auf **Aktiv** oder **Inaktiv** fest.

- 8 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
Hierarchischer Zwei-Tier-Modus	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.
HEAD	Hosts erstellen eine Kopie jedes BUM-Frames und senden diese an jeden bekannten Tunnel-Endpoint für jeden VNI.

- 9 (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.

- 10 (Optional) Klicken Sie auf die Registerkarte **Switching-Profile** und wählen Sie Switching-Profile aus.

- 11 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](#).

Schicht 2-Bridging

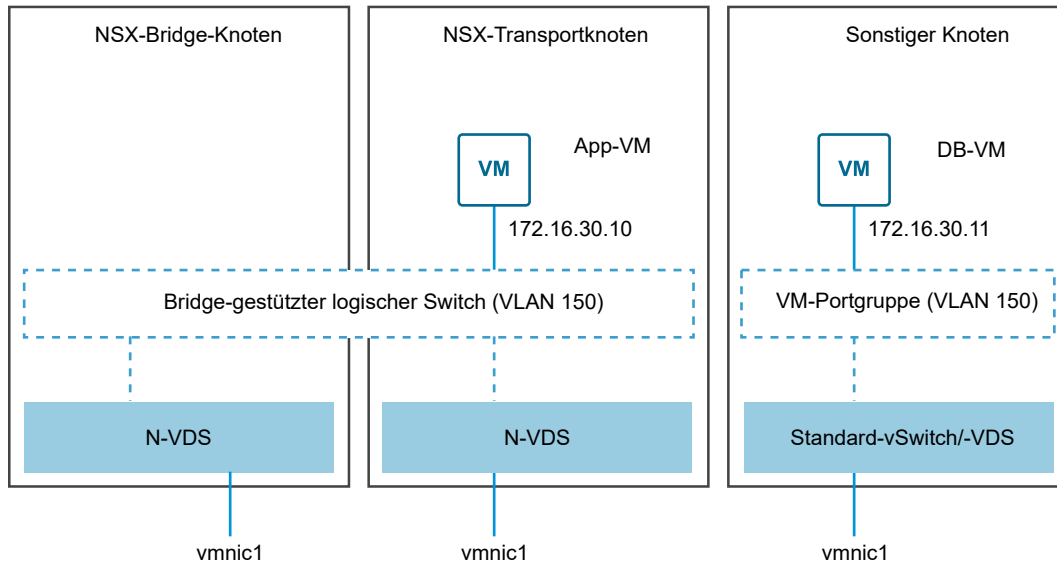
Wenn ein logischer NSX-T Data Center-Switch eine Schicht-2-Verbindung mit einer VLAN-gestützten Portgruppe benötigt oder ein anderes Gerät, z. B. ein Gateway, erreichen muss, das sich außerhalb einer NSX-T Data Center-Bereitstellung befindet, können Sie dafür eine NSX-T Data Center-Schicht-2-Bridge verwenden. Dies ist speziell in einem Migrationsszenario hilfreich, wenn Sie ein Subnetz auf physische und virtuelle Arbeitslasten aufteilen müssen.

Zum NSX-T Data Center-Konzept für das Schicht-2-Bridging gehören Bridge-Cluster, Bridge-Endpoints und Bridge-Knoten. Ein Bridge-Cluster ist eine HA-Zusammenstellung (High Availability, Hochverfügbarkeit) von Bridge-Knoten. Ein Bridge-Knoten ist ein Transportknoten, der das Bridging durchführt. Jeder für das Bridging einer virtuellen und physischen Bereitstellung verwendete logische Switch verfügt über eine zugeordnete VLAN-ID. Ein Bridge-Endpoint ermittelt die physischen Attribute der Bridge wie etwa die Bridge-Cluster-ID und die zugeordnete VLAN-ID.

Sie können das Schicht-2-Bridging unter Verwendung von ESXi-Host-Transportknoten oder NSX Edge-Transportknoten konfigurieren. Um ESXi-Host-Transportknoten für das Bridging zu verwenden, erstellen Sie einen Bridge-Cluster. Um NSX Edge-Transportknoten für das Bridging zu verwenden, erstellen Sie ein Bridge-Profil.

Im folgenden Beispiel sind zwei NSX-T Data Center-Transportknoten Bestandteil derselben Overlay-Transportzone. Auf diese Weise können ihre virtuellen Distributed Switches, die über NSX verwaltet werden, (N-VDS, vormals Host-Switch) an denselben Bridge-gestützten logischen Switch angehängt werden.

Abbildung 1-2. Bridge-Topologie



Der Transportknoten links gehört zu einem Bridge-Cluster und stellt deshalb einen Bridge-Knoten dar.

Da der logische Switch an einen Bridge-Cluster angefügt wurde, wird er als „Bridge-gestützter logischer Switch“ bezeichnet. Für eine Bridge-Stützung muss sich ein logischer Switch in einer Overlay-Transportzone und nicht in einer VLAN-Transportzone befinden.

Der mittlere Transportknoten ist nicht Bestandteil des Bridge-Clusters. Es handelt sich um einen normalen Transportknoten. Dies kann ein KVM- oder ESXi-Host sein. In dem Diagramm wird eine VM auf diesem Knoten (namens „App-VM“) dem Bridge-gestützten logischen Switch hinzugefügt.

Der Knoten rechts ist nicht Bestandteil des NSX-T Data Center-Overlay. Es kann sich um einen beliebigen Hypervisor mit einer VM (wie in dem Diagramm dargestellt) oder um einen physischen Netzwerkknoten handeln. Wenn es sich bei dem Nicht-NSX-T Data Center-Knoten um einen ESXi-Host handelt, können Sie einen Standard-vSwitch oder einen vSphere Distributed Switch für die Portanfügung verwenden. Die der Portanfügung zugeordnete VLAN-ID muss dabei mit der VLAN-ID auf dem Bridge-gestützten logischen Switch übereinstimmen. Darüber hinaus müssen, da die Kommunikation über Schicht 2 durchgeführt wird, die beiden Endgeräte über IP-Adressen im selben Subnetz verfügen.

Wie erläutert, besteht die Funktion der Bridge in der Gewährleistung der Schicht-2-Kommunikation zwischen zwei VMs. Wenn der Datenverkehr zwischen zwei VMs übermittelt wird, durchläuft er den Bridge-Knoten.

Hinweis Wenn zur Bereitstellung von Schicht-2-Bridging Edge-VMs auf einem ESXi-Host verwendet werden, sollte die Portgruppe auf dem Standard- oder verteilten Switch, der Datenverkehr auf der VLAN-Seite sendet und empfängt, im promiskuitiven Modus arbeiten. Um in diesem Fall eine optimale Leistung zu erzielen, ist Folgendes zu beachten:

- 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 auf 7 Gbit/s sinken, da der VLAN-Datenverkehr im promiskuitiven Modus an beide VMs weitergeleitet werden muss.
-

Erstellen eines Bridge-Clusters

Ein Bridge-Cluster ist eine Sammlung von ESXi-Host-Transportknoten, die einem logischen Switch Bridging auf der Ebene von Schicht 2 ermöglichen.

Ein Bridge-Cluster kann maximal zwei ESXi-Host-Transportknoten als Bridge-Knoten umfassen. Ein Bridge-Cluster mit zwei Bridge-Knoten ermöglicht Hochverfügbarkeit im Active-Standby-Modus. Selbst wenn Sie für das Bridging nur einen Bridge-Knoten verwenden möchten, müssen Sie dennoch einen Bridge-Cluster erstellen. Nach dem Erstellen des Bridge-Clusters können Sie später einen weiteren Bridge-Knoten hinzufügen.

Voraussetzungen

- Erstellen Sie mindestens einen NSX-T Data Center-Transportknoten für die Verwendung als Bridge-Knoten.
- Der als Bridge-Knoten verwendete Transportknoten muss ein ESXi-Host sein. KVM-Hosts werden für Bridge-Knoten nicht unterstützt.
- Es wird empfohlen, auf Bridge-Knoten keine VMs zu hosten.
- Ein Transportknoten kann nur einem Bridge-Cluster hinzugefügt werden. Ein bestimmter Transportknoten lässt sich nicht zu mehreren Bridge-Clustern hinzufügen.

Verfahren

- 1 Wählen Sie im Navigationsbereich die Option **Fabric > Knoten** aus.
- 2 Klicken Sie auf die Registerkarte **ESXi-Bridge-Cluster**.
- 3 Klicken Sie auf **Hinzufügen**.
- 4 Geben Sie einen Namen und optional eine Beschreibung ein.
- 5 Wählen Sie eine Transportzone für den Bridge-Cluster aus.

- 6 Wählen Sie in der Spalte **Verfügbar** die Transportknoten aus und klicken Sie auf den Pfeil nach rechts, um diese in die Spalte **Ausgewählt** zu übertragen.
- 7 Klicken Sie auf die Schaltfläche **Hinzufügen**.

Nächste Schritte

Sie können jetzt den Bridge-Cluster einem logischen Switch zuordnen.

Erstellen eines Bridge-Profiles

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

Voraussetzungen

- Stellen Sie sicher, dass Sie über einen NSX Edge-Cluster mit zwei NSX Edge-Transportknoten verfügen.

Verfahren

- 1 Wählen Sie im Navigationsbereich **Fabric > Profile**.
- 2 Klicken Sie auf die Registerkarte **Edge-Bridge-Profile**.
- 3 Klicken Sie auf **Hinzufügen**.
- 4 Geben Sie einen Namen und optional eine Beschreibung ein.
- 5 Wählen Sie einen NSX Edge-Cluster aus.
- 6 Wählen Sie einen Primärknoten aus.
- 7 Wählen Sie einen Sicherungsknoten aus.
- 8 Wählen Sie einen Failover-Modus aus.
Die Optionen sind **Vorbeugend** und **Nicht vorbeugend**.
- 9 Klicken Sie auf die Schaltfläche **Hinzufügen**.

Nächste Schritte

Sie können jetzt das Bridge-Profil einem logischen Switch zuordnen.

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.

Eine Beispieltopologie finden Sie unter [Abbildung 1-2. Bridge-Topologie](#).

Voraussetzungen

- Stellen Sie sicher, dass Sie über einen Bridge-Cluster oder ein Bridge-Profil verfügen.

- Mindestens ein ESXi- oder KVM-Host als regulärer Transportknoten. Dieser Knoten verfügt über gehostete VMs, für die eine Konnektivität mit Geräten außerhalb einer NSX-T Data Center-Bereitstellung erforderlich ist.
- Eine VM oder ein anderes Endgerät außerhalb der NSX-T Data Center-Bereitstellung. Dieses Endgerät muss an einen VLAN-Port angefügt sein, der der VLAN-ID des Bridge-gestützter logischer Switch entspricht.
- Ein logischer Switch in einer Overlay-Transportzone als Bridge-gestützter logischer Switch.

Verfahren

- 1 Melden Sie sich in einem Browser bei NSX Manager unter `https://<nsx-mgr>` an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Switching**.
- 3 Klicken Sie auf den Namen eines Overlay-Switches (Datenverkehrstyp: Overlay).
- 4 Klicken Sie auf **Zugehörig > ESXi-Bridge-Cluster** oder auf **Zugehörig > Edge-Bridge-Profile**.
- 5 Klicken Sie auf **Anhängen**.
- 6 Um den Switch an einen Bridge-Cluster anzuhängen, verfahren Sie wie folgt:
 - a Wählen Sie einen Bridge-Cluster aus.
 - b Geben Sie eine VLAN-ID ein.
 - c Aktivieren oder deaktivieren Sie **HA auf VLAN**.
 - d Klicken Sie auf **Anhängen**.
- 7 Um den Switch an ein Bridge-Profil anzuhängen, verfahren Sie wie folgt:
 - a Wählen Sie ein Bridge-Profil aus.
 - b Wählen Sie eine Transportzone aus.
 - c Geben Sie eine VLAN-ID ein.
 - d Klicken Sie auf **Speichern**.

- 8 Verbinden Sie VMs mit dem logischen Switch, wenn diese noch nicht verbunden sind.

Die VMs müssen sich auf Transportknoten in derselben Transportzone wie der Bridge-Cluster bzw. das Bridge-Profil befinden.

Ergebnisse

Sie können das Funktionieren der Bridge durch Senden eines Ping-Befehls von der NSX-T Data Center-internen VM an einen für NSX-T Data Center externen Knoten überprüfen. Beispielsweise muss die Anwendungs-VM auf dem NSX-T Data Center-Transportknoten in [Abbildung 1-2. Bridge-Topologie](#) in der Lage sein, einen Ping-Befehl an die DB-VM auf dem externen Knoten zu senden und umgekehrt.

Sie können den Datenverkehr auf dem Bridge-gestützten Switch überwachen, indem Sie auf die Registerkarte **Überwachen** klicken.

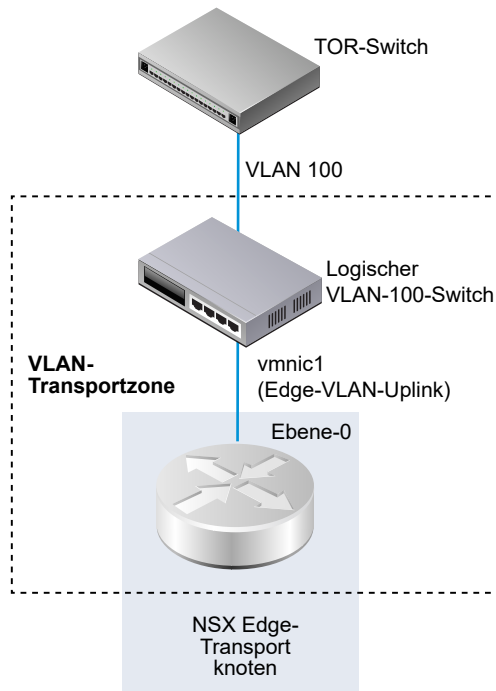
Der Bridge-Datenverkehr lässt sich auch mit dem API-Aufruf GET <https://192.168.110.31/api/v1/bridge-endpoints/<endpoint-id>/statistics> anzeigen:

```
{
  "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"
}
```

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 Ihr NSX Controller-Cluster stabil ist.
- 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 im Navigationsbereich **Netzwerk > Switching**.
- 3 Klicken Sie auf **Hinzufügen**.
- 4 Geben Sie für den logischen Switch einen Namen ein.
- 5 Wählen Sie eine Transportzone für den logischen Switch aus.
- 6 Wählen Sie eine Uplink-Teaming-Richtlinie.
- 7 Wählen Sie für den administrativen Status die Option **Aktiv** oder **Inaktiv**.
- 8 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.
- 9 (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.

Verbinden einer VM mit einem logischen Switch

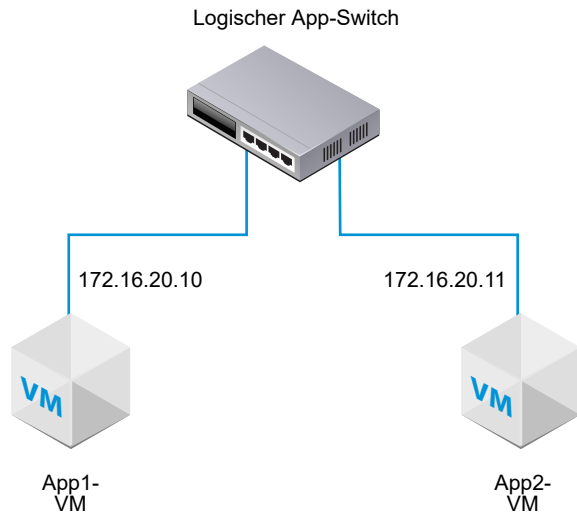
Die Konfiguration zum Verbinden einer VM mit einem logischen Switch ist vom jeweiligen Host abhängig.

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 (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 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 in NSX Manager Ports für logische Switches mit **Switching > Ports** anzeigen.

In der NSX-T Data Center-API haben Sie die Möglichkeit, NSX-T Data Center-angefügte VMs mit dem GET <https://<nsx-mgr>/api/v1/fabric/virtual-machines-API-Aufruf> einzusehen.

Die VIF-Anhang-ID unter **Switching > Ports** in der NSX-T Data Center Manager-Benutzeroberfläche entspricht der externen ID (ExternalID) im API-Aufruf. Suchen Sie nach der VIF-Anhang-ID, die der externen VM-ID (ExternalID) entspricht, und stellen Sie sicher, dass der Verwaltungsstatus sowie der Betriebsstatus aktiviert sind.

Wenn zwei VMs mit demselben logischen Switch verknüpft sind und in demselben Subnetz konfigurierte IP-Adressen aufweisen, sollten Sie sich gegenseitig Ping-Befehle senden können.

Nächste Schritte

Fügen Sie einen logischen Router hinzu.

Sie können die Aktivität am logischen Switch-Port überwachen, um Probleme zu beheben. Siehe „Überwachen der Aktivität eines Ports für einen logischen Switch“ im *Administratorhandbuch für NSX-T Data Center*.

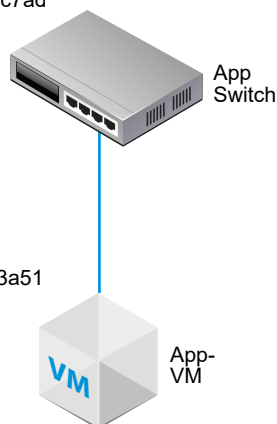
Verknüpfen einer auf eigenständigem ESXi gehosteten VM mit einem logischen NSX-T Data Center-Switch

Wenn Sie mit einem eigenständigen ESXi-Host arbeiten, können Sie nicht über den webbasierten vSphere Web Client auf die Host-VMs zugreifen. In diesem Fall haben Sie die Möglichkeit, mit diesem Vorgang VMs an logische NSX-T Data Center-Switches anzufügen.

Das in diesem Verfahren gezeigte Beispiel veranschaulicht das Verknüpfen einer VM namens app-vm mit einem logischen Switch namens app-switch.

Nicht transparente Switch-Netzwerk-ID:
22b22448-38bc-419b-bea8-b51126bec7ad

Externe VM-ID:
50066bae-0f8a-386b-e62e-b0b9c6013a51



Voraussetzungen

- Die VM muss auf Hypervisoren gehostet werden, die dem NSX-T Data Center-Fabric hinzugefügt wurden.
- Die Fabric-Knoten müssen über eine NSX-T Data Center-MPA (Verwaltungskomponenten)- und eine NSX-T Data Center-LCP (Steuerungskomponenten)-Konnektivität verfügen.
- Die Fabric-Knoten müssen einer Transportzone hinzugefügt werden.
- Ein logischer Switch muss erstellt werden.
- Sie müssen auf die NSX Manager-API zugreifen können.
- Sie benötigen Schreibzugriff für die VMX-Datei der VM.

Verfahren

- 1 Verwenden Sie die (installationsbasierte) vSphere Client-Anwendung oder ein anderes VM-Managementtool, um die VM zu bearbeiten und einen VMXNET 3-Ethernet-Adapter hinzuzufügen.

Wählen Sie ein beliebiges benanntes Netzwerk. Sie ändern die Netzwerkverbindung in einem späteren Schritt.

Hardware anpassen

Hardware der virtuellen Maschine konfigurieren

The screenshot shows the 'Hardware' configuration window in the vSphere Client. The 'Virtuelle Hardware' tab is active. The configuration list includes:

- CPU:** 1
- Arbeitsspeicher:** 4096 MB
- Neue Festplatte:** 40 GB
- Neuer SCSI-Controller:** LSI Logic SAS
- *Neues Netzwerk:** VM Network
 - Status: ☒ Beim Einschalten verbinden
 - Adaptertyp: VMXNET 3
 - DirectPath I/O: ☐ Aktivieren
 - MAC-Adresse: Automatisch
- Neues CD-/DVD-Laufwerk:** Clientgerät
- Neues Diskettenlaufwerk:** Clientgerät

At the bottom, there is a 'Neues Gerät' button and a 'Hinzufügen' button.

- 2 Geben Sie über die NSX-T Data Center-API den API-Aufruf GET <https://<nsx-mgr>/api/v1/fabric/virtual-machines/<VM-ID>> aus.

Suchen Sie die externalId der VM in den Ergebnissen.

Beispiel:

```
GET https://<nsx-mgr>/api/v1/fabric/virtual-machines/60a5a5d5-ea2b-407e-a806-4fdc8468f735

{
  "resource_type": "VirtualMachine",
  "id": "60a5a5d5-ea2b-407e-a806-4fdc8468f735",
  "display_name": "app-vm",
  "compute_ids": [
    "instanceUuid:50066bae-0f8a-386b-e62e-b0b9c6013a51",
    "moIdOnHost:5",
    "externalId:50066bae-0f8a-386b-e62e-b0b9c6013a51",
    "hostLocalId:5",
    "locationId:564dc020-1565-e3f4-f591-ee3953eef3ff",
    "biosUuid:4206f47d-fe7-08c5-5bf7-ea26a4c6b18d"
  ],
  "external_id": "50066bae-0f8a-386b-e62e-b0b9c6013a51",
  "type": "REGULAR",
  "host_id": "cb82b0fa-a8f1-11e5-92a9-6b7d1f8661fa",
  "local_id_on_host": "5"
}
```

- 3 Schalten Sie die VM aus und heben Sie ihre Registrierung beim Host auf.

Dazu können Sie das VM-Managementtool oder die ESXi-CLI verwenden, wie hier dargestellt.

```
[user@host:~] vim-cmd /vmsvc/getallvms
Vmid   Name      File           Guest OS      Version  Annotation
5      app-vm    [ds2] app-vm/app-vm.vmx  ubuntuGuest  vmx-08
8      web-vm    [ds2] web-vm/web-vm.vmx  ubuntu64Guest vmx-08

[user@host:~] vim-cmd /vmsvc/power.off 5
Powering off VM:

[user@host:~] vim-cmd /vmsvc/unregister 5
```

- 4 Rufen Sie über die NSX Manager-Benutzeroberfläche die ID des logischen Switches ab.

Beispiel:

app-switch	
Übersicht Überwachen Verwalten ▾ Zugehörig ▾	
<div> <div>▾ Übersicht</div> <div>BEARBEITEN</div> </div>	
Name	app-switch
ID	b68e7ac3-877a-420e-af47-53e974c17915
Speicherort	
Beschreibung	lswitch202 (created through automation)
Administrativer Status	● Aktiv
Replizierungsmodus	Head-Replikation
VLAN	Nicht verfügbar
VNI	71681
Logische Ports	1
Datenverkehrstyp	Overlay
Transportzone	transportzone1
Name der Uplink-Teamingricht...	[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 in der NSX Manager-Benutzeroberfläche unter **Switching > Ports** die VIF-Anhang-ID, die mit der externalId der VM übereinstimmt, und stellen Sie sicher, dass der Verwaltungsstatus und der Betriebsstatus beide „Hochgefahren“ lauten.

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

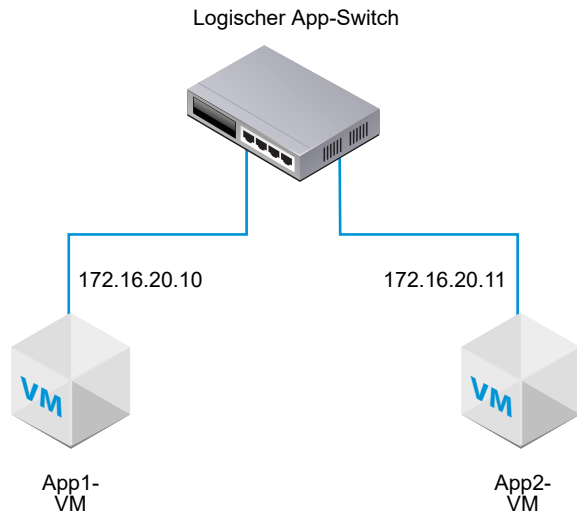
Fügen Sie einen logischen Router hinzu.

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 Port hinzu und verwenden Sie die Schnittstellen-ID der VM für die VIF-Anfügung.

Ergebnisse

Suchen Sie in der NSX Manager-Benutzeroberfläche unter **Switching > Ports** die VIF-Anhang-ID und stellen Sie sicher, dass der Verwaltungsstatus sowie der Betriebsstatus aktiviert sind.

Wenn zwei VMs mit demselben logischen Switch verknüpft sind und in demselben Subnetz konfigurierte IP-Adressen aufweisen, sollten Sie sich gegenseitig Ping-Befehle senden können.

Nächste Schritte

Fügen Sie einen logischen Router hinzu.

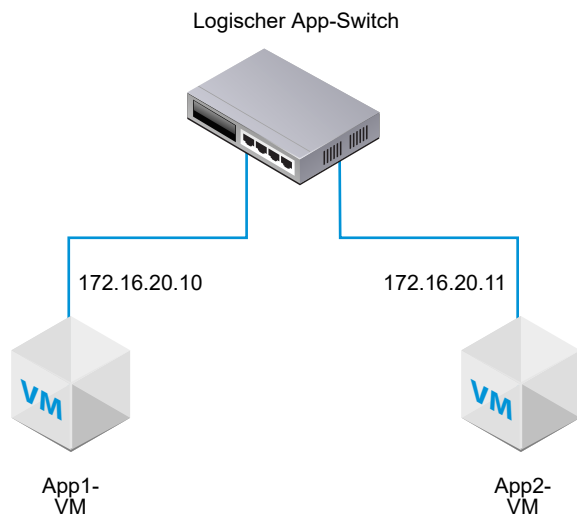
Sie können die Aktivität am logischen Switch-Port überwachen, um Probleme zu beheben. Siehe „Überwachen der Aktivität eines Ports für einen logischen Switch“ im *Administratorhandbuch für NSX-T Data Center*.

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 1-3. 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 **Switching > Switches** aus.

- e Klicken Sie auf den logischen Switch und notieren Sie die UUID- bzw. VNI-Informationen.
- f Führen Sie im NSX Controller die im Folgenden aufgeführten Befehle aus, um das Problem zu beheben.

Befehl	Beschreibung
get logical-switch <vni-oder-uuid> arp-table	<p>Zeigt die ARP-Tabelle für den angegebenen logischen Switch an.</p> <p>Beispielausgabe.</p> <pre> nsx-controller1> get logical-switch 41866 arp-table VNI IP MAC Connection-ID 41866 172.16.20.11 00:50:56:b1:70:5e 295422 </pre>
get logical-switch <vni-oder-uuid> connection-table	<p>Zeigt die Verbindungen für den angegebenen logischen Switch an.</p> <p>Beispielausgabe.</p> <pre> nsx-controller1> 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>
get logical-switch <vni-oder-uuid> mac-table	<p>Zeigt die MAC-Tabelle für den angegebenen logischen Switch an.</p> <p>Beispielausgabe.</p> <pre> nsx-controller1> 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>
get logical-switch <vni-oder-uuid> stats	<p>Zeigt statistische Informationen zum angegebenen logischen Switch an.</p> <p>Beispielausgabe.</p> <pre> nsx-controller1> 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>
get logical-switch <vni-oder-uuid> stats-sample	<p>Zeigt eine Übersicht aller im Zeitablauf erstellten Statistiken des logischen Switch an.</p> <p>Beispielausgabe.</p> <pre> nsx-controller1> 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>
get logical-switch <vni-oder-uuid> vtep	<p>Zeigt alle virtuellen Tunnel-Endpoints an, die zum angegebenen logischen Switch gehören.</p> <p>Beispielausgabe.</p> <pre>nsx-controller1> 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.

Logischer Switch Port

2

Ein Logischer Switch hat mehrere Switch-Ports. Elemente wie Router, VMs oder Container können über die logischen Switch-Ports mit einem logischen Switch verbunden werden.

Dieses Kapitel enthält die folgenden Themen:

- [Erstellen eines logischen Switch-Ports](#)
- [Überwachen der Aktivität eines Ports für einen logischen Switch](#)

Erstellen eines logischen Switch-Ports

Mithilfe eines logischen Switch-Ports können Sie eine andere Netzwerkkomponente, eine virtuelle Maschine oder einen Container mit einem logischen Switch verbinden.

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.

Voraussetzungen

Stellen Sie sicher, dass ein Port für den logischen Switch erstellt wurde. Siehe [Kapitel 1 Logische Switches und Konfigurieren einer VM-Anfügung](#).

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Switching**.
- 3 Klicken Sie auf die Registerkarte **Ports**.
- 4 Klicken Sie auf **Hinzufügen**.

- 5 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 in der Dropdown-Liste einen logischen Switch aus.
Verwaltungsstatus	Wählen Sie Aktiv oder Inaktiv aus.
Anhangstyp	Wählen Sie Keine oder VIF aus.
Anhangs-ID	Wenn der Anhangstyp VIF lautet, geben Sie die Anhangs-ID ein.

- 6 (Optional) Wählen Sie auf der Registerkarte **Switching-Profile** Switching-Profile aus.

- 7 Klicken Sie auf **Speichern**.

Überwachen der Aktivität eines Ports für einen logischen Switch

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 Port für den logischen Switch konfiguriert ist. Siehe [Verbinden einer VM mit einem logischen Switch](#).

Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Switching**.
- 3 Klicken Sie auf die Registerkarte **Ports**.
- 4 Klicken Sie auf den Namen eines Ports.
- 5 Klicken Sie auf die Registerkarte **Überwachen**.

Der Portstatus und Statistiken werden angezeigt.

- 6 Um eine CSV-Datei von den MAC-Adressen herunterzuladen, die vom Host abgerufen wurden, klicken Sie auf **MAC-Tabelle herunterladen**.
- 7 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 Port für den logischen Switch 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](#).

Switching-Profil für logische Switches und logische Ports

3

Switching-Profil umfassen Konfigurationsdetails für das Layer 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)
- IP-Ermittlung
- SpoofGuard
- Switch-Sicherheit
- MAC-Verwaltung

Hinweis Sie können die Standard-Switching-Profilen in NSX Manager nicht bearbeiten oder löschen. Stattdessen können Sie benutzerdefinierte Switching-Profilen erstellen.

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-Profiles 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-Profilen 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-Profile 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.

Dieses Kapitel enthält die folgenden Themen:

- [Grundlegendes zum QoS-Switching-Profil](#)
- [Grundlegendes zum Switching-Profil für die IP-Ermittlung](#)
- [Grundlegendes zu SpoofGuard](#)
- [Grundlegendes zum Switching-Profil für die Switch-Sicherheit](#)
- [Grundlegendes zum Switching-Profil für die MAC-Verwaltung](#)
- [Zuordnen eines benutzerdefinierten Profils zu einem logischen Switch](#)
- [Zuordnen eines benutzerdefinierten Profils zu einem logischen Port](#)

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 eingehenden und ausgehenden Datenverkehr konfigurieren und so den Grenzwert für die Übertragungsrate festzulegen. 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 Einstellungen für den eingehenden wie den ausgehenden Datenverkehr 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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Switching**.

- 3 Klicken Sie auf die Registerkarte **Switching-Profile**.
- 4 Klicken Sie auf **Hinzufügen**, und wählen Sie **QoS** aus.
- 5 Vervollständigen Sie die Details des QoS-Switching-Profiles.

Option	Beschreibung
Name und Beschreibung	<p>Weisen Sie dem QoS-Switching-Profil einen Namen zu.</p> <p>Optional können Sie für die im Profil geänderte Einstellung eine Beschreibung eingeben.</p>
Modus	<p>Wählen Sie die Option Vertrauenswürdig oder Nicht vertrauenswürdig 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>Hinweis 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>
Eingehend	<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 höchsten Bandbreitenrate wird der Burstdatenverkehr unterstützt. Die Burstdauer wird mit der Einstellung für die Burst-Größe festgelegt. Sie können die Bandbreite nicht dauerhaft gewährleisten. Allerdings haben Sie die Möglichkeit, mit dieser Einstellung die Netzwerkbandbreite zu beschränken. Der Standardwert beträgt 0 und deaktiviert den eingehenden Datenverkehr.</p> <p>Wenn Sie beispielsweise die durchschnittliche Bandbreite für den logischen Switch auf 30 Mbit/s festlegen, beschränkt die Richtlinie die Bandbreite. Sie können den Burstdatenverkehr auf 100 Mbit/s für eine Dauer von 20 Bytes begrenzen.</p>

Option	Beschreibung
Eingehender Broadcast	<p>Legen Sie benutzerdefinierte Werte für den eingehenden Netzwerkdatenverkehr von der VM zum logischen Netzwerk auf Broadcast-Basis fest.</p> <p>Der Standardwert beträgt 0 und deaktiviert den eingehenden Broadcast-Datenverkehr.</p> <p>Wenn Sie beispielsweise die durchschnittliche Bandbreite für einen logischen Switch auf 50 Kbit/s festlegen, beschränkt die Richtlinie die Bandbreite. Sie können den Burstdatenverkehr auf 400 Mbit/s für eine Dauer von 60 Bytes begrenzen.</p>
Ausgehend	<p>Legen Sie benutzerdefinierte Werte für den eingehenden Netzwerkdatenverkehr vom logischen Netzwerk zur VM fest.</p> <p>Der Standardwert beträgt 0 und deaktiviert den ausgehenden Datenverkehr.</p>

Wenn die Optionen für den eingehenden Datenverkehr, den eingehenden Broadcast-Datenverkehr und den ausgehenden Datenverkehr nicht konfiguriert sind, werden die Standardwerte als Protokollpuffer verwendet.

6 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 die IP-Ermittlung

Die IP-Ermittlung verwendet das DHCP-Snooping, ARP-Snooping oder VM Tools, um die MAC- und IP-Adressen der VM abzurufen. Nach dem Abrufen der MAC- und IP-Adressen werden die Einträge für den NSX Controller freigegeben, um die ARP-Unterdrückung zu ermöglichen. Die ARP-Unterdrückung minimiert die ARP-Datenverkehrsüberflutung zwischen den VMs, die mit demselben logischen Switch verbunden sind.

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

Das ARP-Snooping überprüft die ausgehenden ARPs und GARPs 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-Adressen, bereitstellen kann. Diese IP-Erkennungsmethode ist nur für VMs verfügbar, die auf ESXi-Hosts ausgeführt werden.

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

Konfigurieren eines Switching-Profiles für die IP-Ermittlung

Sie haben die Möglichkeit, das ARP- oder DHCP-Snooping oder VM Tools für das Erstellen eines benutzerdefinierten Switching-Profiles für die IP-Ermittlung zu aktivieren, das die IP- und MAC-Adressen lernt, um die IP-Integrität eines logischen Switch sicherzustellen. Die IP-Ermittlungsmethode für VM-Tools steht nur für ESXi-gehostete virtuellen Maschinen zur Verfügung.

Voraussetzungen

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

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Switching**.
- 3 Klicken Sie auf die Registerkarte **Switching-Profile**.
- 4 Klicken Sie auf **Hinzufügen**, und wählen Sie **IP-Ermittlung** aus.
- 5 Vervollständigen Sie die Details des Switching-Profiles für die IP-Ermittlung.

Option	Beschreibung
Name und Beschreibung	Geben Sie einen Namen und optional eine Beschreibung ein.
ARP-Snooping	Schalten Sie die Schaltfläche ARP-Snooping zur Aktivierung der Funktion um. Das ARP-Snooping prüft die ausgehenden ARP- und GARP-Verbindungen der VM, um die MAC- und IP-Adressen der VM abzurufen. Das ARP-Snooping kann verwendet werden, wenn die VM eine statische IP-Adresse anstelle von DHCP verwendet.
ARP-Bindungsgrenzwert	Geben Sie einen ARP-Bindungsgrenzwert von 1 bis 128 an.

Option	Beschreibung
DHCP-Snooping	Schalten Sie die Schaltfläche DHCP-Snooping zur Aktivierung der Funktion um. Das DHCP-Snooping prüft die DHCP-Pakete, die zwischen dem VM-DHCP-Client und dem DHCP-Server ausgetauscht werden, um die MAC- und IP-Adressen der VM abzurufen.
VM Tools	Schalten Sie die Schaltfläche VM Tools um, um die Funktion zu aktivieren. Diese Option ist nur für ESXi-gehostete virtuelle Maschinen verfügbar. VM Tools ist eine Software, die auf einer ESXi-gehosteten virtuellen Maschine ausgeführt wird und die MAC- und IP-Adresse der virtuellen Maschine bereitstellen kann.

6 Klicken Sie auf **Speichern**.

Ergebnisse

Ein benutzerdefiniertes Switching-Profil für die IP-Ermittlung wird als Link angezeigt.

Nächste Schritte

Fügen Sie dieses benutzerdefinierte Switching-Profil für die IP-Ermittlung an einen logischen Switch oder logischen Port an, damit die im Switching-Profil geänderten Parameter für den Netzwerkdatenverkehr angewendet werden. Siehe [Zuordnen eines benutzerdefinierten Profils zu einem logischen Switch](#) oder [Zuordnen eines benutzerdefinierten Profils zu einem logischen Port](#).

Grundlegendes zu SpoofGuard

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

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

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

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

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

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

Auf Switch-Ebene wird die Positivliste zulässiger MAC/VLAN/IP-Werte über die Adressbindungseigenschaft des Switch zur Verfügung gestellt. Dabei handelt es sich in der Regel um einen zulässigen IP-Bereich bzw. um ein zulässiges Subnetz für den Switch. SpoofGuard auf Switch-Ebene ist für die Authentifizierung des Datenverkehrs zuständig.

Der Datenverkehr muss durch SpoofGuard auf Port- UND auf Switch-Ebene gestattet werden, bevor er für den Switch zugelassen wird. Die Aktivierung/Deaktivierung von SpoofGuard auf Port- und Switch-Ebene kann mithilfe des SpoofGuard-Switch-Profiles gesteuert werden.

Konfigurieren von Port-Adressbindungen

Adressbindungen geben die IP- und MAC-Adresse eines logischen Ports an. Damit wird die Positivliste für Ports in SpoofGuard festgelegt.

Mit Port-Adressbindungen geben Sie die IP- und MAC-Adresse sowie das VLAN (sofern zutreffend) des logischen Ports an. Wenn SpoofGuard aktiviert ist, wird damit sichergestellt, dass die angegebenen Adressbindungen in den Datenpfad aufgenommen werden. Port-Adressbindungen werden nicht nur für SpoofGuard, sondern auch für DFW-Regelübersetzungen verwendet.

Verfahren

- 1 Navigieren Sie in NSX Manager zu **Netzwerk > Switching**.
- 2 Klicken Sie auf die Registerkarte **Ports**.
- 3 Klicken Sie auf den logischen Port, für den eine Adressbindung verwendet werden soll.

Die Übersicht für den logischen Port wird eingeblendet.

- 4 Erweitern Sie in der Registerkarte **Übersicht** die Option **Adressbindungen**.
- 5 Klicken Sie auf **Hinzufügen**.

Das Dialogfeld „Adressbindungen hinzufügen“ wird angezeigt.

- 6 Geben Sie die IP- und MAC-Adresse des logischen Ports an, für den eine Adressbindung angewendet werden soll. Sie können auch eine VLAN-ID angeben.

7 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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Switching**.
- 3 Klicken Sie auf die Registerkarte **Switching-Profile**.
- 4 Klicken Sie auf **Hinzufügen**, und wählen Sie die **SpoofGuard** aus.
- 5 Geben Sie einen Namen und optional eine Beschreibung ein.
- 6 Um SpoofGuard auf Portebene zu aktivieren, setzen Sie **Portbindungen** auf **Aktiviert**.
- 7 Klicken Sie auf **Hinzufügen**.

Ergebnisse

Es wurde ein neues Switching-Profil mit einem SpoofGuard-Profil erstellt.

Nächste Schritte

Ordnen Sie das SpoofGuard-Profil einem logischen Switch oder logischen Port zu. Siehe [Zuordnen eines benutzerdefinierten Profils zu einem logischen Switch](#) oder [Zuordnen eines benutzerdefinierten Profils zu einem logischen Port](#).

Grundlegendes zum Switching-Profil für die Switch-Sicherheit

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

Sie haben die Möglichkeit, Filter für die 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-Profils 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-Profils für die Switch-Sicherheit vertraut. Siehe [Grundlegendes zum Switching-Profil für die Switch-Sicherheit](#).

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Switching**.
- 3 Klicken Sie auf die Registerkarte **Switching-Profile**.
- 4 Klicken Sie auf **Hinzufügen**, und wählen Sie **Switch-Sicherheit** aus.
- 5 Vervollständigen Sie die Details des Switching-Profils für die Switch-Sicherheit.

Option	Beschreibung
Name und Beschreibung	Weisen Sie dem Switching-Profil für die Switch-Sicherheit einen Namen zu. Optional können Sie für die im Profil geänderte Einstellung eine Beschreibung eingeben.
BPDU-Filter	Schalten Sie die Schaltfläche BPDU-Filter zur Aktivierung der BPDU-Filterung um. 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.
Positivliste für den BPDU-Filter	Klicken Sie auf die Ziel-MAC-Adresse aus der Liste der BPDU-Ziel-MAC-Adressen, um den Datenverkehr zum zugelassenen Ziel zu ermöglichen.
DHCP-Filter	Schalten Sie die Schaltflächen Serverblock und Clientblock zur Aktivierung der DHCP-Filterung um. Die DHCP-Serverblockierung blockiert Datenverkehr von einem DHCP-Server an einen DHCP-Client. Dabei wird kein Datenverkehr von einem DHCP-Server an einen DHCP-Relay-Agent blockiert. Die DHCP-Clientblockierung verhindert, dass eine VM eine DHCP-IP-Adresse erhält, indem DHCP-Anforderungen blockiert werden.

Option	Beschreibung
Nicht-IP-Datenverkehr blockieren	<p>Schalten Sie die Schaltfläche Nicht-IP-Datenverkehr blockieren um, um nur IPv4-, IPv6-, ARP-, GARP- 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>
Ratenbegrenzungen	<p>Legen Sie einen Grenzwert für die Rate des eingehenden oder ausgehenden Broadcast- und Multicast-Datenverkehrs fest.</p> <p>Durch Konfiguration einer beschränkten Datenverkehrsrate können Sie den logischen Switch oder die VM schützen, z. B. vor exzessivem Broadcast-Datenverkehr.</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: den MAC-Lernvorgang und die 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.

Der MAC-Lernvorgang 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 den MAC-Lernvorgang 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-Lernvorgang 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.

Wenn Sie den MAC-Lernvorgang 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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Switching**.
- 3 Klicken Sie auf die Registerkarte **Switching-Profile**.
- 4 Klicken Sie auf **Hinzufügen**, und wählen Sie **MAC-Verwaltung** aus.
- 5 Vervollständigen Sie die Details zum MAC-Verwaltungsprofil.

Option	Beschreibung
Name und Beschreibung	Weisen Sie dem MAC-Verwaltungsprofil einen Namen zu. Optional können Sie für die im Profil geänderte Einstellung eine Beschreibung eingeben.
MAC-Änderung	Aktivieren oder deaktivieren Sie die Funktion zum Ändern der MAC-Adresse.
Status	Aktivieren oder deaktivieren Sie die MAC-Lernfunktion.

- 6 Klicken Sie auf **Hinzufügen**.

Ergebnisse

Ein MAC-Verwaltungsprofil 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](#).

Zuordnen eines benutzerdefinierten Profils zu einem logischen Switch

Sie können einem logischen Switch ein benutzerdefiniertes Switching-Profil zuordnen, sodass das Profil auf alle Ports auf dem Switch angewendet wird.

Wenn benutzerdefinierte Switching-Profile einem logischen Switch zugeordnet werden, setzen sie vorhandene Standard-Switching-Profile außer Kraft. Das benutzerdefinierte Switching-Profil wird von untergeordneten logischen Switch-Ports übernommen.

Hinweis Wenn Sie ein benutzerdefiniertes Switching-Profil einem logischen Switch zugeordnet haben, aber das Standard-Switching-Profil für einen der untergeordneten logischen Switch-Ports beibehalten möchten, müssen Sie eine Kopie des Standard-Switching-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 [Kapitel 3 Switching-Profile für logische Switches und logische Ports](#).

Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Switching**.
- 3 Klicken Sie auf die Registerkarte **Switches**.
- 4 Klicken Sie auf den logischen Switch, um das benutzerdefinierte Switching-Profil anzuwenden.
- 5 Klicken Sie auf die Registerkarte **Verwalten**.
- 6 Wählen Sie das benutzerdefinierte Switching-Profil im Dropdown-Menü aus.
 - **QoS**
 - **Portspiegelung**
 - **IP-Ermittlung**
 - **SpoofGuard**
 - **Switch-Sicherheit**
 - **MAC-Verwaltung**
- 7 Klicken Sie auf **Ändern**.
- 8 Wählen Sie das zuvor erstellte benutzerdefinierte Switching-Profil im Dropdown-Menü aus.
- 9 Klicken Sie auf **Speichern**.

Der logische Switch ist nun dem benutzerdefinierten Switching-Profil zugeordnet.

- 10 Stellen Sie sicher, dass das neue benutzerdefinierte Switching-Profil mit der geänderten Konfiguration auf der Registerkarte **Verwalten** angezeigt wird.
- 11 (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 [Kapitel 3 Switching-Profile für logische Switches und logische Ports](#).

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Switching**.
- 3 Klicken Sie auf die Registerkarte **Ports**.
- 4 Klicken Sie auf den logischen Port, um das benutzerdefinierte Switching-Profil anzuwenden.
- 5 Klicken Sie auf die Registerkarte **Verwalten**.
- 6 Wählen Sie das benutzerdefinierte Switching-Profil im Dropdown-Menü aus.
 - **QoS**
 - **Portspiegelung**
 - **IP-Ermittlung**
 - **SpoofGuard**

- **Switch-Sicherheit**
- **MAC-Verwaltung**

- 7 Klicken Sie auf **Ändern**.
- 8 Wählen Sie das zuvor erstellte benutzerdefinierte Switching-Profil im Dropdown-Menü aus.
- 9 Klicken Sie auf **Speichern**.
Der logische Port ist nun dem benutzerdefinierten Switching-Profil zugeordnet.
- 10 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*.

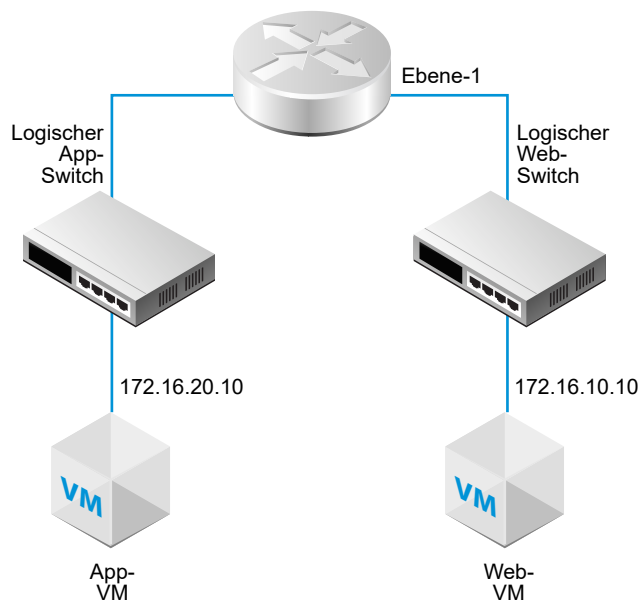
Logischer Tier-1-Router

4

Ein logischer NSX-T Data Center-Router bildet die Routing-Funktionalität in einer virtuellen Umgebung ab, die komplett von der zugrunde liegenden Hardware entkoppelt ist. Logische Tier-1-Router verfügen über Downlink-Ports, mit denen Sie eine Verbindung mit logischen NSX-T Data Center-Switches, und über Uplink-Ports, mit denen Sie eine Verbindung mit logischen NSX-T Data Center-Tier-0-Routern herstellen können.

Wenn Sie einen logischen Router hinzufügen, müssen Sie zuerst die Netzwerktopologie konzipieren, die aufgebaut werden soll.

Abbildung 4-1. 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.

Dieses Kapitel enthält die folgenden Themen:

- [Erstellen eines logischen Tier-1-Routers](#)
- [Hinzufügen eines Downlink-Ports auf einem logischen Tier-1-Router](#)
- [Hinzufügen eines VLAN-Ports auf einem logischen Tier-0- oder Tier-1-Router](#)
- [Konfigurieren einer Routenankündigung auf einem logischen Tier-1-Router](#)
- [Konfigurieren einer statischen Route auf einem logischen Tier-1-Router](#)
- [Erstellen eines eigenständigen logischen Tier-1-Routers](#)

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 [Kapitel 4 Logischer Tier-1-Router](#).

Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 3 Klicken Sie auf **Hinzufügen** und wählen Sie **Tier-1-Router**.
- 4 Geben Sie für den logischen Router einen Namen und optional eine Beschreibung ein.
- 5 (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.

- 6 (Optional) Wählen Sie einen NSX Edge-Cluster, der mit diesem logischen Tier-1-Router verbunden werden soll.

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.

- 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**.

Der neue logische Router wird in der Benutzeroberfläche von NSX Manager als anklickbarer Link angezeigt.

Ergebnisse

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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.

- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 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 einer Routenankündigung 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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 3 Klicken Sie auf den Namen eines Routers.
- 4 Klicken Sie auf die Registerkarte **Konfiguration** und wählen Sie **Router-Ports**.

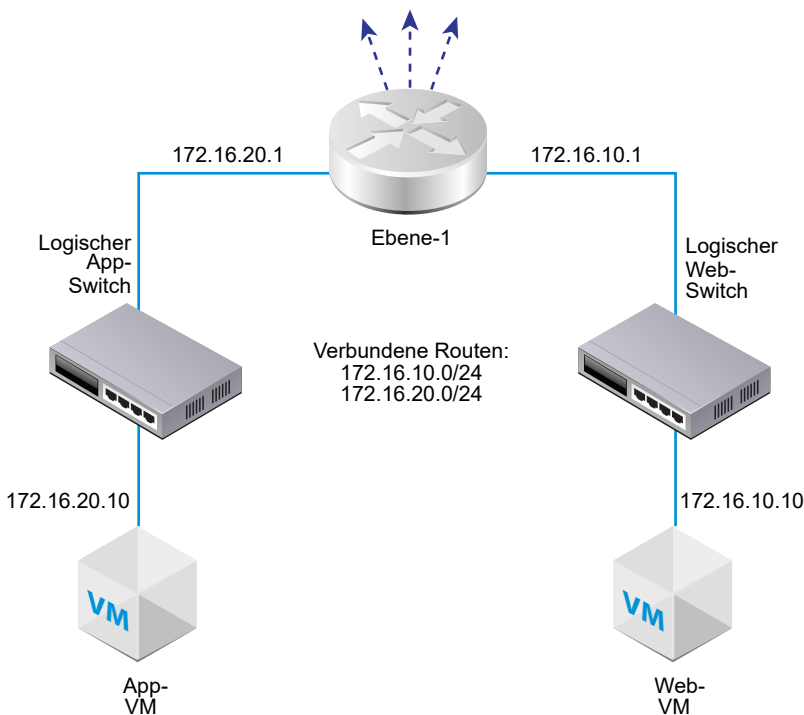
- 5 Klicken Sie auf **Hinzufügen**.
- 6 Geben Sie für den Router-Port einen Namen und optional eine Beschreibung ein.
- 7 Wählen Sie im Feld **Typ** die Option **Zentral** aus.
- 8 Wählen Sie als **URPF-Modus** entweder **Streng** oder **Keine** aus.
URPF (Unicast Reverse Path Forwarding) ist eine Sicherheitsfunktion.
- 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 Routenankündigung 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 die Tier-1-Routenankündigung 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 die Routenankündigung aktivieren.

Um beispielsweise eine Konnektivität zu und von VMs über andere Peer-Router bereitzustellen, muss für den logischen Tier-1-Router die Routenankündigung 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 1 Logische Switches und Konfigurieren einer VM-Anfügung](#).
- 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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 3 Klicken Sie auf den Namen eines Tier-1-Routers.
- 4 Wählen Sie im Dropdown-Menü **Routing** die Option **Routenankündigung** aus.
- 5 Klicken Sie auf **Bearbeiten**, um die Konfiguration der Routenankündigung 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**

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 Zulassen oder Verweigern an.
Routentypen abgleichen	Wählen Sie mindestens eine der folgenden Optionen aus: <ul style="list-style-type: none"> ■ Alle ■ NSX verbunden ■ Tier-1-LB-VIP ■ Statisch ■ Tier-1 NAT ■ Tier-1-LB-SNAT
Präfix-Operator	Wählen Sie GE oder EQ aus.

d Klicken Sie auf **Hinzufügen**.

Nächste Schritte

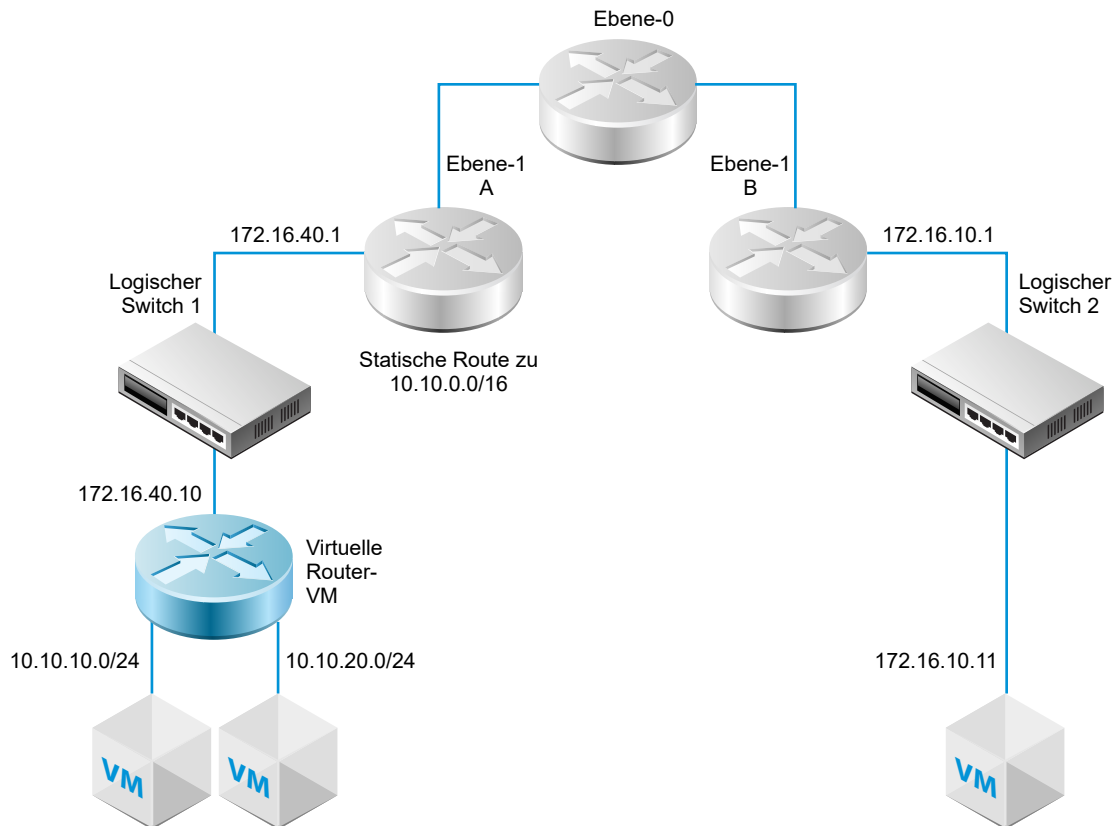
Machen Sie sich mit der Topologie des logischen Tier-0-Routers vertraut und erstellen Sie den logischen Tier-0-Router. Siehe [Kapitel 5 Logischer Ebene-0-Router](#).

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 Routenankündigung konfiguriert, um die statische Route zu Tier-1 B anzukündigen.

Abbildung 4-2. Topologie einer statischen Route auf einem logischen Tier-1-Router**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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 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.
Beispiel: 10.10.10.0/16

- 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 > Routenankündigung**.

- 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 lediglich den Lastausgleich und die NAT-Dienste.

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.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 3 Klicken Sie auf **Hinzufügen** und wählen Sie **Tier-1-Router**.
- 4 Geben Sie für den logischen Router einen Namen und optional eine Beschreibung ein.
- 5 (Erforderlich) Wählen Sie einen NSX Edge-Cluster, der mit diesem logischen Tier-1-Router verbunden werden soll.

6 (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.

7 Klicken Sie auf **Hinzufügen**.

8 Klicken Sie auf den Namen des Routers, den Sie gerade erstellt haben.

9 Klicken Sie auf die Registerkarte **Konfiguration** und wählen Sie **Router-Ports**.

10 Klicken Sie auf **Hinzufügen**.

11 Geben Sie für den Router-Port einen Namen und optional eine Beschreibung ein.

12 Wählen Sie im Feld **Typ** die Option **Zentral** aus.

13 Wählen Sie als **URPF-Modus** entweder **Streng** oder **Keine** aus.

URPF (Unicast Reverse Path Forwarding) ist eine Sicherheitsfunktion.

14 (Erforderlich) Wählen Sie einen logischen Switch aus.

15 Wählen Sie aus, ob diese Anfügung einen neuen Switch-Port erstellt oder einen vorhandenen Switch-Port aktualisiert.

16 Geben Sie die IP-Adresse des Routerports in CIDR-Notation ein.

17 Klicken Sie auf **Hinzufügen**.

Ergebnisse

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 nicht unterstützt. Daher dürfen Sie keine virtuelle IP-Serveradresse für den Lastausgleich oder für LB SNAT im CSP-Subnetz konfigurieren, es sei denn, Sie verwenden die CSP-IP-Adresse. Wenn beispielsweise die CSP-IP-Adresse 1.1.1.1/24 lautet, muss die virtuelle IP-Adresse entweder 1.1.1.1 lauten oder eine andere IP-Adresse im Subnetz sein. Es kann keine andere Adresse im Subnetz 1.1.1.1/24 lauten.
- 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.

Logischer Ebene-0-Router

5

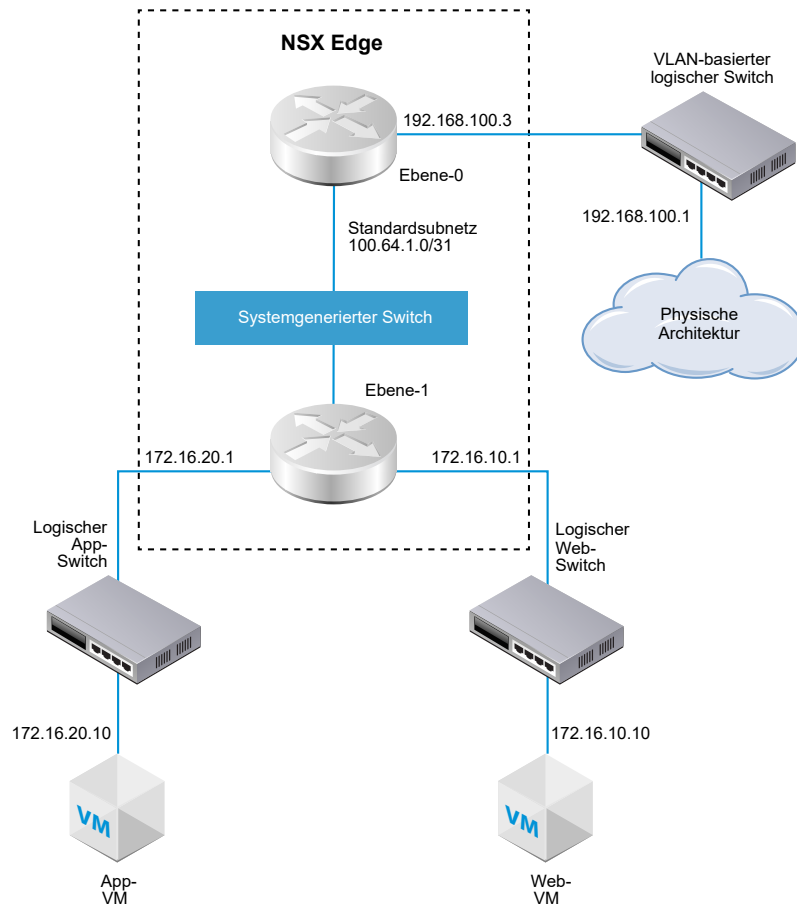
Ein logischer NSX-T Data Center-Router bildet die Routing-Funktionalität in einer virtuellen Umgebung ab, die komplett von der zugrunde liegenden Hardware entkoppelt ist. Der logische Tier-0-Router bietet einen aktivierbaren Gateway-Dienst zwischen dem logischen und dem physischen Netzwerk.

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

Ein NSX Edge-Cluster kann mehrere logische Tier-0-Router unterstützen. Tier-0-Router unterstützen das dynamische BGP-Routing-Protokoll und ECMP.

Wenn Sie einen logischen Tier-0-Router hinzufügen, müssen Sie zuerst die Netzwerktopologie entwickeln, die aufgebaut werden soll.

Abbildung 5-1. 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.

Dieses Kapitel enthält die folgenden Themen:

- Erstellen eines logischen Tier-0-Routers
- Anfügen von Tier-0 und Tier-1
- Verbinden eines logischen Tier-0 Routers mit einem logischen VLAN-Switch für den NSX Edge-Uplink
- Hinzufügen eines Loopback-Router-Ports
- Hinzufügen eines VLAN-Ports auf einem logischen Tier-0- oder Tier-1-Router

- [Konfigurieren einer statischen Route](#)
- [BGP-Konfigurationsoptionen](#)
- [Konfigurieren von BFD auf einem logischen Tier-0 Router](#)
- [Aktivieren von Route Redistribution auf dem logischen Tier-0-Router](#)
- [Grundlegendes zum ECMP-Routing](#)
- [Erstellen einer IP-Präfix-Liste](#)
- [Erstellen einer Community-Liste](#)
- [Erstellen einer Route Map](#)
- [Konfigurieren des Timers für die Weiterleitung der Aktiv-Benachrichtigung](#)

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 Ihr NSX Controller-Cluster stabil ist.
- 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 [Kapitel 5 Logischer Ebene-0-Router](#).

Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 3 Klicken Sie auf **Hinzufügen**, um einen logischen Tier-0-Router zu erstellen.
- 4 Wählen Sie **Tier-0-Router** im Dropdown-Menü aus.
- 5 Weisen Sie dem logischen Tier-0-Router einen Namen zu.
- 6 Wählen Sie im Dropdown-Menü einen vorhandenen NSX Edge-Cluster zur Unterstützung dieses logischen Tier-0-Routers aus.

- 7 (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.

- 8 (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.

- 9 (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, 100.64.0.0/10. Jede Tier-0-zu-Tier-1-Peer-Verbindung erhält ein /31-Subnetz innerhalb des 100.64.0.0/10-Adressraums.

- 10 Klicken Sie auf **Speichern**.

Der neue logische Tier-0-Router wird als Link angezeigt.

- 11 (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.

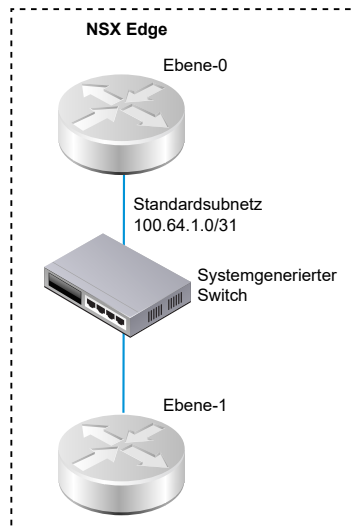
Konfigurieren Sie den logischen Tier-0-Router für dessen Verbindung mit einem logischen VLAN-Switch zum Erstellen eines Uplinks zu einem externen Netzwerk. Siehe [Verbinden eines logischen Tier-0 Routers mit einem logischen VLAN-Switch für den NSX Edge-Uplink](#).

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 100.64.0.0/10. Jede Tier-0-zu-Tier-1-Peer-Verbindung erhält ein /31-Subnetz innerhalb des 100.64.0.0/10-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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 3 Wählen Sie den logischen Tier-1-Router.
- 4 Klicken Sie auf der Registerkarte **Übersicht** auf **Bearbeiten**.
- 5 Wählen Sie im Dropdown-Menü den logischen Tier-0-Router aus.
- 6 (Optional) Wählen Sie einen NSX Edge-Cluster im Dropdown-Menü aus.

Der Tier-1-Router muss von einem Edge-Gerät unterstützt werden, wenn dieser für Dienste wie z. B. NAT (Network Address Translation) verwendet werden soll. Wenn Sie keinen NSX Edge-Cluster auswählen, kann der Tier-1-Router kein NAT ausführen.

- 7 Geben Sie Mitglieder und ein bevorzugtes Mitglied an.

Wenn Sie einen NSX Edge-Cluster auswählen und die Felder für die Mitglieder bzw. das bevorzugte Mitglied leer lassen, legt NSX-T Data Center das unterstützende Edge-Gerät vom angegebenen Cluster für Sie fest.

- 8 Klicken Sie auf **Speichern**.
- 9 Klicken Sie auf die Registerkarte **Konfiguration** des Tier-1-Routers, um zu prüfen, ob eine neue Punkt-zu-Punkt-IP-Adresse für den verknüpften Port erstellt wurde.

So kann die IP-Adresse des verknüpften Ports z. B. 100.64.1.1/31 lauten.

- 10 Wählen Sie aus dem Navigationsbereich den logischen Tier-0-Router aus.

- 11 Klicken Sie auf die Registerkarte **Konfiguration** des Tier-0-Routers, um zu prüfen, ob eine neue Punkt-zu-Punkt-IP-Adresse für den verknüpften Port erstellt wurde.

So kann die IP-Adresse des verknüpften Ports z. B. 100.64.1.1/31 lauten.

Nächste Schritte

Stellen Sie sicher, dass der Tier-0-Router Informationen über Routen abrufen, die von Tier-1-Routern angekündigt werden.

Überprüfen des Abrufs von Routen von einem Tier-1-Router für einen Tier-0-Router

Wenn ein logischer Tier-1 Router Routen für einen logischen Tier-0 Router ankündigt, werden die Routen in der Routing-Tabelle des Tier-0 Routers als statische NSX-T Data Center-Routen aufgeführt.

Verfahren

- 1 Führen Sie den Befehl `get logical-routers` auf NSX Edge aus, um die VRF-Nummer des Tier-0-Dienstrouters abzurufen.

```
nsx-edge-1> get logical-routers
Logical Router
UUID       : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf        : 0
type       : TUNNEL

Logical Router
UUID       : 421a2d0d-f423-46f1-93a1-2f9e366176c8
vrf : 5
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : f3ce9d7d-7123-47d6-aba6-45cf1388ca7b
vrf        : 6
type       : DISTRIBUTED_ROUTER

Logical Router
UUID       : c8e64eff-02b2-4462-94ff-89f3788f1a61
vrf        : 7
type       : SERVICE_ROUTER_TIER1

Logical Router
UUID       : fb6c3f1f-599f-4421-af8a-99692dff3dd4
vrf        : 8
type       : DISTRIBUTED_ROUTER
```

- 2 Führen Sie den Befehl `vrf <number>` aus, um den Kontext des Tier-0-Dienstrouters einzugeben.

```
nsx-edge-1> vrf 5
nsx-edge1(tier0_sr)>
```

- 3 Führen Sie auf dem Tier-0-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-0-Router abgerufen wurden, da der Tier-1-Router Routen ankündigt.

```
nsx-edge1(tier0_sr)> get route

Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

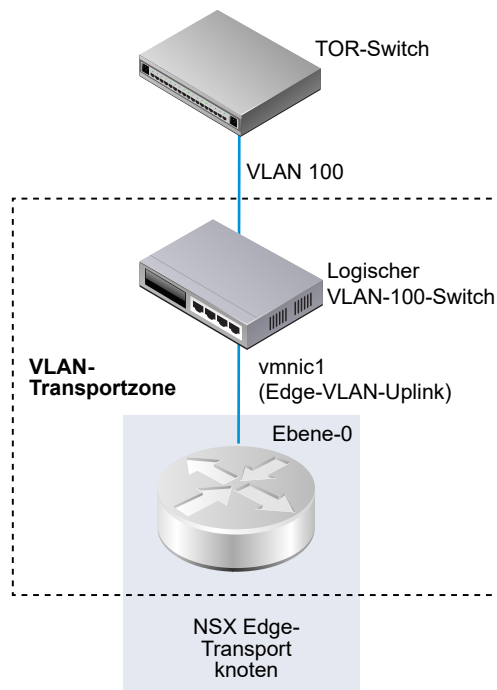
Total number of routes: 7

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

Verbinden eines logischen Tier-0 Routers mit einem logischen VLAN-Switch für den NSX Edge-Uplink

Um einen NSX Edge-Uplink zu erstellen, verbinden Sie einen Tier-0-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 über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 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-bbafb2786666
vrf        : 0
type       : TUNNEL

Logical Router
UUID       : 421a2d0d-f423-46f1-93a1-2f9e366176c8
vrf : 5
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : f3ce9d7d-7123-47d6-aba6-45cf1388ca7b
vrf        : 6
type       : DISTRIBUTED_ROUTER

Logical Router
UUID       : c8e64eff-02b2-4462-94ff-89f3788f1a61
vrf        : 7
type       : SERVICE_ROUTER_TIER1

Logical Router
UUID       : fb6c3f1f-599f-4421-af8a-99692dff3dd4
vrf        : 8
type       : DISTRIBUTED_ROUTER

```

- 3 Führen Sie den Befehl `vrf <number>` aus, um den Kontext des Tier-0-Dienstrouters einzugeben.

```

nsx-edge-1> vrf 5
nsx-edgel(tier0_sr)>

```

- 4 Führen Sie den Befehl `get route` auf dem Tier-0-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-edgel(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-0 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-0-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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 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

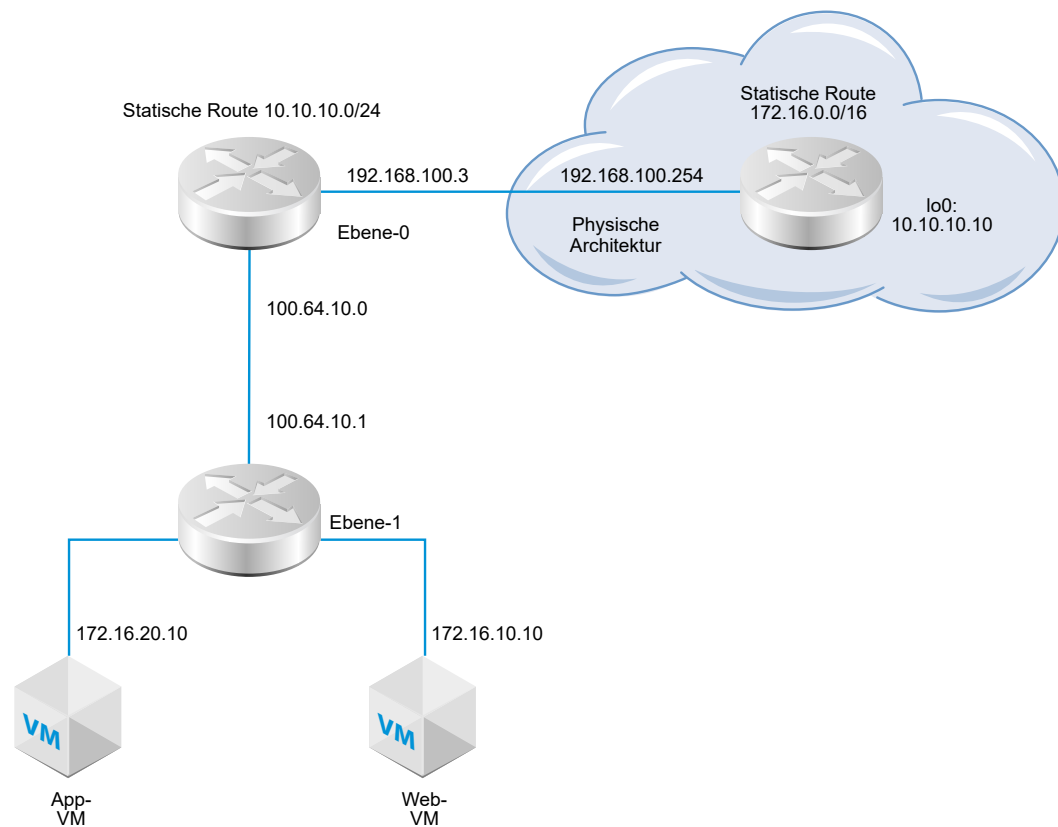
- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 3 Klicken Sie auf den Namen eines Routers.
- 4 Klicken Sie auf die Registerkarte **Konfiguration** und wählen 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 5-2. Topologie der statischen Route



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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.

- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 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 Port für den logischen Router 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 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.

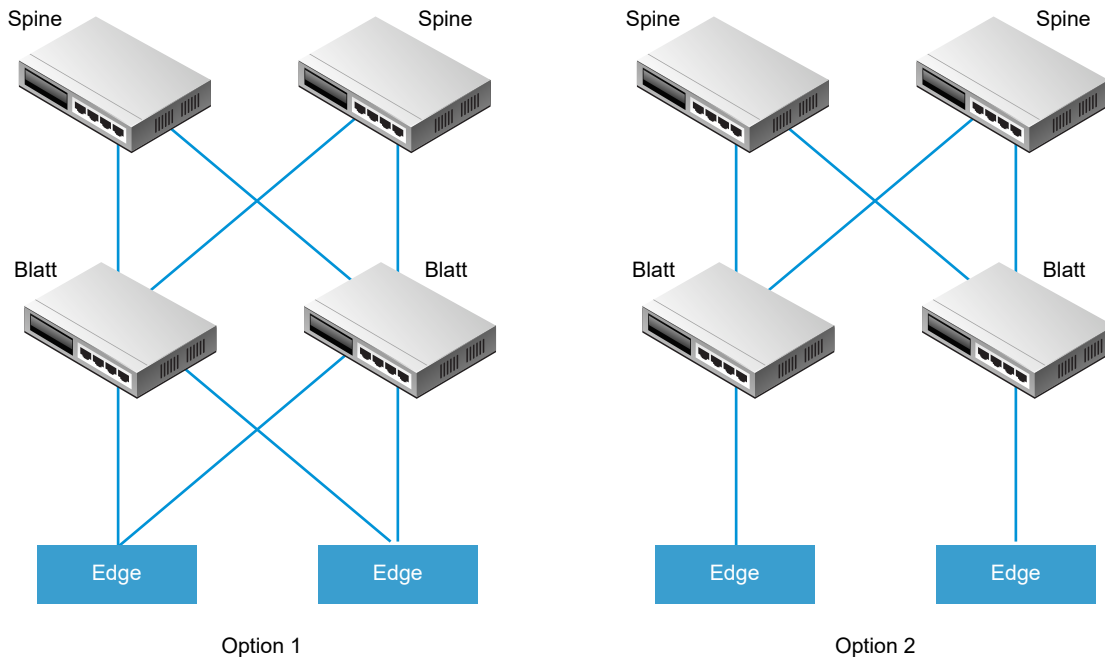
```
ping 10.10.10.10
```

```
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

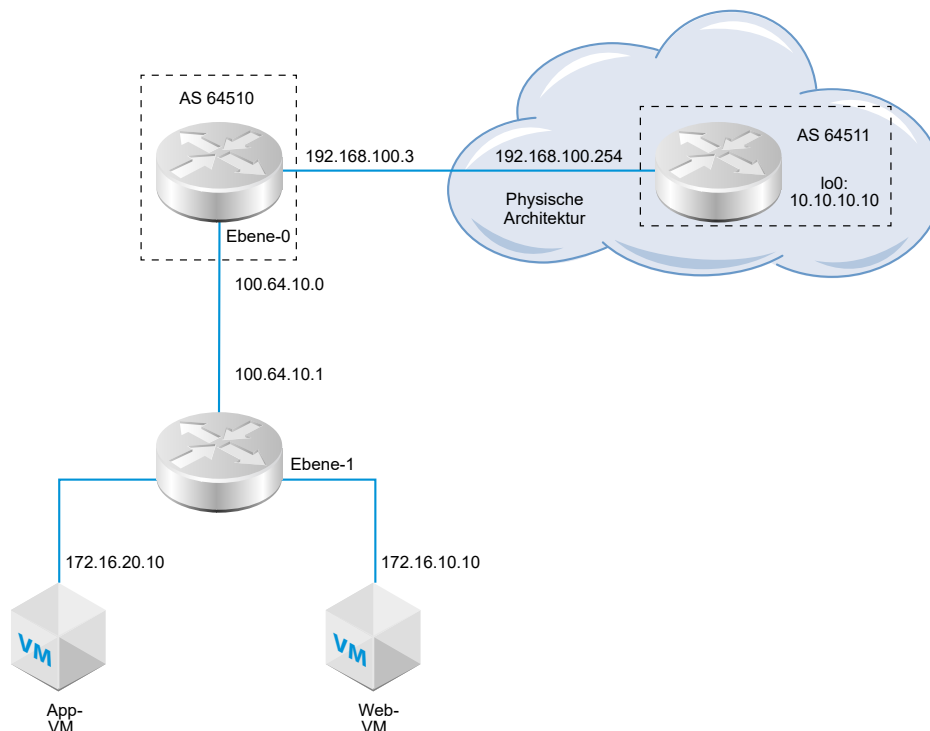
Um den Zugriff zwischen Ihren VMs und der Außenwelt zu ermöglichen, können Sie eine externe BGP-Verbindung (eBGP) zwischen einem logischen Tier-0-Router und einem Router in Ihrer physischen Infrastruktur konfigurieren.

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 des physischen Routers konfigurieren. In diesem Beispiel lautet die Remote-AS-Nummer 64511. Die Remote-Nachbar-IP-Adresse ist 192.168.100.254. Der Nachbar muss sich im selben IP-Subnetz wie der Uplink auf dem logischen Tier-0-Router befinden. BGP-Multihop wird unterstützt.

Für Testzwecke ist die Adresse 10.10.10.10/32 für die Loopback-Schnittstelle des externen Routers konfiguriert.

Hinweis Die für die Bildung von BGP-Sitzungen auf einem Edge-Knoten benötigte 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 5-3. BGP-Verbindungstopologie



Voraussetzungen

- Stellen Sie sicher, dass der Tier-1-Router für die Ankündigung verbundener Routen konfiguriert ist. Siehe [Konfigurieren einer Routenankündigung 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 über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 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 Konfigurieren Sie die lokale AS-Nummer.
Beispiel: 64510.
 - b Klicken Sie auf die Umschaltfläche **Status**, um BGP zu aktivieren.
Für die Statusschaltfläche muss „Aktiviert“ angezeigt werden.
 - c (Optional) Klicken Sie auf die Umschaltfläche **ECMP**, um ECMP zu aktivieren.
 - d (Optional) Klicken Sie auf die Umschaltfläche **Graceful Restart**, um Graceful Restart zu aktivieren.
 - e (Optional) Konfigurieren Sie die Routen-Zusammenfassung und aktivieren Sie Graceful Restart sowie ECMP.

Graceful Restart wird nur unterstützt, wenn der dem Tier-0-Router zugeordnete NSX Edge-Cluster nur über einen Edge-Knoten verfügt.
 - f 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 (Optional) Geben Sie das maximale Hop-Limit an.
Die Standardeinstellung ist 1.

- 9 Geben Sie die Remote-AS-Nummer ein.

Beispiel: 64511.

- 10 (Optional) Konfigurieren Sie die Timer (Keepalive-Timer und Hold-Down-Timer) und ein Kennwort.
- 11 (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.
- 12 (Optional) Klicken Sie auf die Registerkarte **Adressfamilien**, um eine Adressfamilie hinzuzufügen.
- 13 (Optional) 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-0-Dienstrouter aus](#).

Überprüfen von BGP-Verbindungen von einem Tier-0-Dienstrouter aus

Mit der Befehlszeilenschnittstelle (CLI) können Sie vom Tier-0-Dienstrouter aus überprüfen, ob eine BGP-Verbindung mit einem Nachbarn eingerichtet ist.

Voraussetzungen

Stellen Sie sicher, dass BGP konfiguriert ist. Siehe [Konfigurieren von BGP auf einem logischen Tier-0-Router](#).

Verfahren

- 1 Melden Sie sich bei der NSX Manager-Befehlszeilenschnittstelle (CLI) an.
- 2 Führen Sie den Befehl `get logical-routers` auf NSX Edge aus, um die VRF-Nummer des Tier-0-Dienstrouters abzurufen.

```
nsx-edge-1> get logical-routers
Logical Router
UUID       : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf        : 0
type       : TUNNEL

Logical Router
UUID       : 421a2d0d-f423-46f1-93a1-2f9e366176c8
vrf : 5
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : f3ce9d7d-7123-47d6-aba6-45cf1388ca7b
vrf        : 6
```

```

type      : DISTRIBUTED_ROUTER

Logical Router
UUID      : c8e64eff-02b2-4462-94ff-89f3788f1a61
vrf       : 7
type      : SERVICE_ROUTER_TIER1

Logical Router
UUID      : fb6c3f1f-599f-4421-af8a-99692dff3dd4
vrf       : 8
type      : DISTRIBUTED_ROUTER

```

- 3 Führen Sie den Befehl `vrf <number>` aus, um den Kontext des Tier-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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 3 Wählen Sie den logischen Tier-0-Router.
- 4 Klicken Sie auf die Registerkarte **Routing** und wählen Sie **Route Redistribution** im Dropdown-Menü aus.

- 5 Klicken Sie auf **Hinzufügen**, um die Route Redistribution-Kriterien auszufüllen.

Option	Beschreibung
Name und Beschreibung	Weisen Sie der Route Redistribution einen Namen zu. Sie können optional auch eine Beschreibung bereitstellen. Beispielname: advertise-to-bgp-neighbor
Quellen	Aktivieren Sie die Kontrollkästchen der Quellrouten, die Sie neu verteilen möchten. Statisch: Statische Tier-0-Routen. NSX – verbunden: verbundene Tier-1-Routen. NSX – statisch: statische Tier-1-Routen Diese statischen Routen werden automatisch erstellt. Tier-0-NAT: Routen, die generiert werden, wenn NAT auf dem logischen Tier-0-Router konfiguriert ist Tier-1-NAT: Routen, die generiert werden, wenn NAT auf dem logischen Tier-1-Router konfiguriert ist
Routenzuordnung	(Optional) Weisen Sie eine Routenzuordnung zu, um eine Reihe von IP-Adressen von der Route Redistribution herauszufiltern.

- 6 Klicken Sie auf **Speichern**.
- 7 Klicken Sie auf den Umschalter **Status**, um die Route Redistribution zu aktivieren.
- Die Schaltfläche „Status“ wird als „Aktiviert“ angezeigt.

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-0-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-0-Router](#).

Verfahren

- 1 Melden Sie sich bei der NSX Manager-Befehlszeilenschnittstelle (CLI) an.
- 2 Zeigen Sie die Routen an, die vom externen BGP-Nachbarn abgerufen wurden.

```
nsx-edge1(tier0_sr)> get route bgp

Flags: c – connected, s – static, b – BGP, ns – nsx_static
nc – nsx_connected, rl – router_link, t0n: Tier0-NAT, t1n: Tier1-NAT
```

```
b    10.10.10.0/24      [20/0]      via 192.168.100.254
```

- 3 Prüfen Sie über den externen Router, ob BGP-Routen abgerufen wurden und ob die VMs über das NSX-T Data Center-Overlay erreichbar sind.

- a Listen Sie die BGP-Routen auf.

```
user@router# run show ip route bgp
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

B>* 172.16.10.0/24 [20/0] via 192.168.100.2, eth2, 00:00:48
B>* 172.16.20.0/24 [20/0] via 192.168.100.2, eth2, 00:00:48
B>* 172.16.30.0/24 [20/0] via 192.168.100.2, eth2, 00:00:48
```

- b Pingen Sie die mit NSX-T Data Center verbundenen VMs über den externen Router an.

```
ping 172.16.10.10
```

```
PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
64 bytes from 172.16.10.10: icmp_req=1 ttl=62 time=127 ms
64 bytes from 172.16.10.10: icmp_req=2 ttl=62 time=1.96 ms
^C
--- 172.16.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.966/64.793/127.620/62.827 ms
```

- c Prüfen Sie den Pfad über das NSX-T Data Center-Overlay.

```
traceroute 172.16.10.10
```

```
traceroute to 172.16.10.10 (172.16.10.10), 30 hops max, 60 byte packets
 1 192.168.100.3 (192.168.100.3) 0.640 ms 0.575 ms 0.696 ms
 2 100.91.176.1 (100.91.176.1) 0.656 ms 0.604 ms 0.578 ms
 3 172.16.10.10 (172.16.10.10) 3.397 ms 3.703 ms 3.790 ms
```

- 4 Pingen Sie die externe IP-Adresse über die internen VMs an.

```
ping 10.10.10.10
```

```
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_req=1 ttl=62 time=119 ms
64 bytes from 10.10.10.10: icmp_req=2 ttl=62 time=1.93 ms
^C
--- 10.10.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.936/60.865/119.795/58.930 ms
```

Nächste Schritte

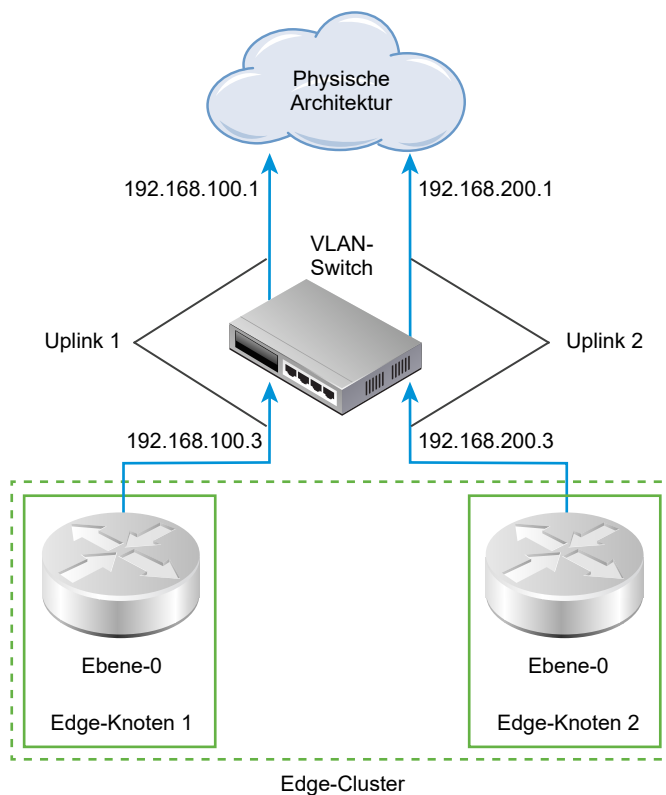
Konfigurieren Sie weitere Routing-Funktionen, wie ECMP.

Grundlegendes zum ECMP-Routing

Das ECMP-Routing-Protokoll (Equal Cost Multi-Path) erhöht die Bandbreite für die vertikale Kommunikation durch Hinzufügen eines Uplinks zum logischen Tier-0-Router und konfiguriert diesen für jeden Edge-Knoten in einem NSX Edge-Cluster. Die ECMP-Routing-Pfade werden für das Load Balancing des Datenverkehrs verwendet und bieten eine Fault Tolerance für fehlgeschlagene Pfade.

ECMP-Pfade werden automatisch aus den an logische Switches angefügten VMs für die Edge-Knoten erstellt, auf denen der logische Tier-0-Router instanziiert wurde. Es werden maximal acht ECMP-Pfade unterstützt.

Abbildung 5-4. ECMP-Routing-Topologie



In diesem Beispiel enthält die Topologie zwei logische Tier-0-Router in einem NSX Edge-Cluster. Jeder logische Tier-0-Router befindet sich in einem Edge-Knoten. Diese Knoten sind Bestandteil des Clusters. Die Uplink-Ports 192.168.100.3 und 198.168.200.3 definieren, wie der Transportknoten eine Verbindung mit dem logischen Switch herstellt, um auf das physische Netzwerk zugreifen zu können. Wenn die ECMP-Routing-Pfade aktiviert sind, verbinden diese die VMs, die an logische Switches angefügt wurden, und die beiden Edge-Knoten im NSX Edge-Cluster. Mehrere ECMP-Routing-Pfade erhöhen den Netzwerkdurchsatz und die Netzwerkausfallsicherheit.

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 über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 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
Name	Weisen Sie dem Router-Port einen Namen zu.
Beschreibung	Geben Sie eine zusätzliche Beschreibung ein, dass der Port der ECMP-Konfiguration dient.
Typ	Übernehmen Sie den Standardtyp Uplink .
Transportknoten	Weisen Sie den Hosttransportknoten im Dropdown-Menü zu.
Logischer Switch	Weisen Sie den logischen VLAN-Switch im Dropdown-Menü zu.
Port für den logischen Switch	Weisen Sie einen neuen Namen für den Switch-Port zu. Sie können auch einen vorhandenen Switch-Port verwenden.
IP-Adresse/-Maske	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-0-Router und dem logischen VLAN-Switch ein neuer Uplink-Port hinzugefügt. Der logische Tier-0-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 über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 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 **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-0-Router ein.

```
vrf 5
```

- 5 Stellen Sie sicher, dass der verteilte Tier-0-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 Öffnen Sie den aktiven Controller für den logischen Tier-0-Router.

- 8 Stellen Sie sicher, dass der verteilte Tier-0-Router auf dem Controller-Knoten verbunden ist.

```
get logical-router <UUID> route
```

Für den Routentyp der UUID sollte NSX_CONNECTED angezeigt werden.

- 9 Starten Sie eine SSH-Sitzung auf den beiden Edge-Knoten.

- 10 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>
```

- 11 Wechseln Sie zum Control Center und doppelklicken Sie auf die Skripts httpdata11.bat und httpdata12.bat.

Es wird eine große Anzahl an HTTP-Anforderungen an beide Web-VMs gesendet. Der Datenverkehr wird auf beide Pfade mithilfe der Edge-Knoten verteilt, d. h. ECMP funktioniert.

- 12 Beenden Sie die Erfassungssitzung.

```
del capture session 0
```

- 13 Entfernen Sie die BAT-Skripts.

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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 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 über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 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 EBGPeers.
- 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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 3 Wählen Sie den logischen Tier-0-Router.
- 4 Wählen Sie **Routing > Route Maps** aus.
- 5 Klicken Sie auf **Hinzufügen**.
- 6 Geben Sie einen Namen und eine optionale Beschreibung für die Route Map ein.
- 7 Klicken Sie auf **Hinzufügen**, um einen Eintrag in der Route Map hinzuzufügen.
- 8 Bearbeiten Sie die Spalte **IP-Präfix-Liste/Community-Liste abgleichen**, um entweder IP-Präfix-Listen oder Community-Listen auszuwählen, aber nicht beide.
- 9 (Optional) Legen Sie BGP-Attribute fest.

BGP-Attribut	Beschreibung
AS für Pfad voranstellen	Stellen Sie einem Pfad eine oder mehrere AS-Nummern des autonomen Systems voran, um den Pfad zu verlängern und damit in der Priorität herabzustufen.
MED	Der Multi-Exit Discriminator zeigt einem externen Peer einen bevorzugten Pfad für ein autonomes System an.
Gewicht	Legen Sie eine Gewichtung für die Pfadauswahl fest. Der Bereich liegt zwischen 0 und 65535.
Community	Geben Sie eine Community im Format „aa:nn“ an, z. B. 300:500. Sie können mithilfe des Dropdown-Menüs auch eine der folgenden Optionen auswählen: <ul style="list-style-type: none"> ■ NO_EXPORT_SUBCONFED – Keine Ankündigung für EBG-Peers. ■ NO_ADVERTISE – Keine Ankündigung für alle Peers. ■ NO_EXPORT – Keine Ankündigung außerhalb der BGP-Konföderation.

- 10 Wählen Sie in der Spalte „Aktion“ die Option **Zulassen** oder **Verweigern** aus.
Sie können es zulassen oder verweigern, dass IP-Adressen der IP-Präfix-Liste angekündigt werden.
- 11 Klicken Sie auf **Speichern**.

Konfigurieren des Timers für die Weiterleitung der Aktiv-Benachrichtigung

Sie können für logische Tier-0 Router einen Timer für die Weiterleitung der Aktiv-Benachrichtigung konfigurieren.

Der Timer für die Weiterleitung der Aktiv-Benachrichtigung definiert die Zeit in Sekunden, die der Router warten muss, bevor die Aktiv-Benachrichtigung nach dem Herstellen der ersten BGP-Sitzung gesendet wird. Dieser Timer (zuvor als Weiterleitungsverzögerung bezeichnet) minimiert die Ausfallzeit bei einem Failover für Aktiv/Aktiv- oder Aktiv/Standby-Konfigurationen logischer Router auf NSX Edge, die dynamisches Routing (BGP) verwenden. Er sollte auf die Anzahl Sekunden festgelegt werden, die ein externer Router (TOR) benötigt, um nach der ersten BGP/BFD-Sitzung alle Routen auf diesem Router zu veröffentlichen. Der Timer-Wert sollte direkt proportional zur Anzahl dynamischer Northbound-Routen sein, die der Router lernen muss. Dieser Timer sollte bei Konfigurationen mit individuellem Edge-Knoten auf 0 festgelegt werden.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 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**.

Netzwerkadressübersetzung (NAT)

6

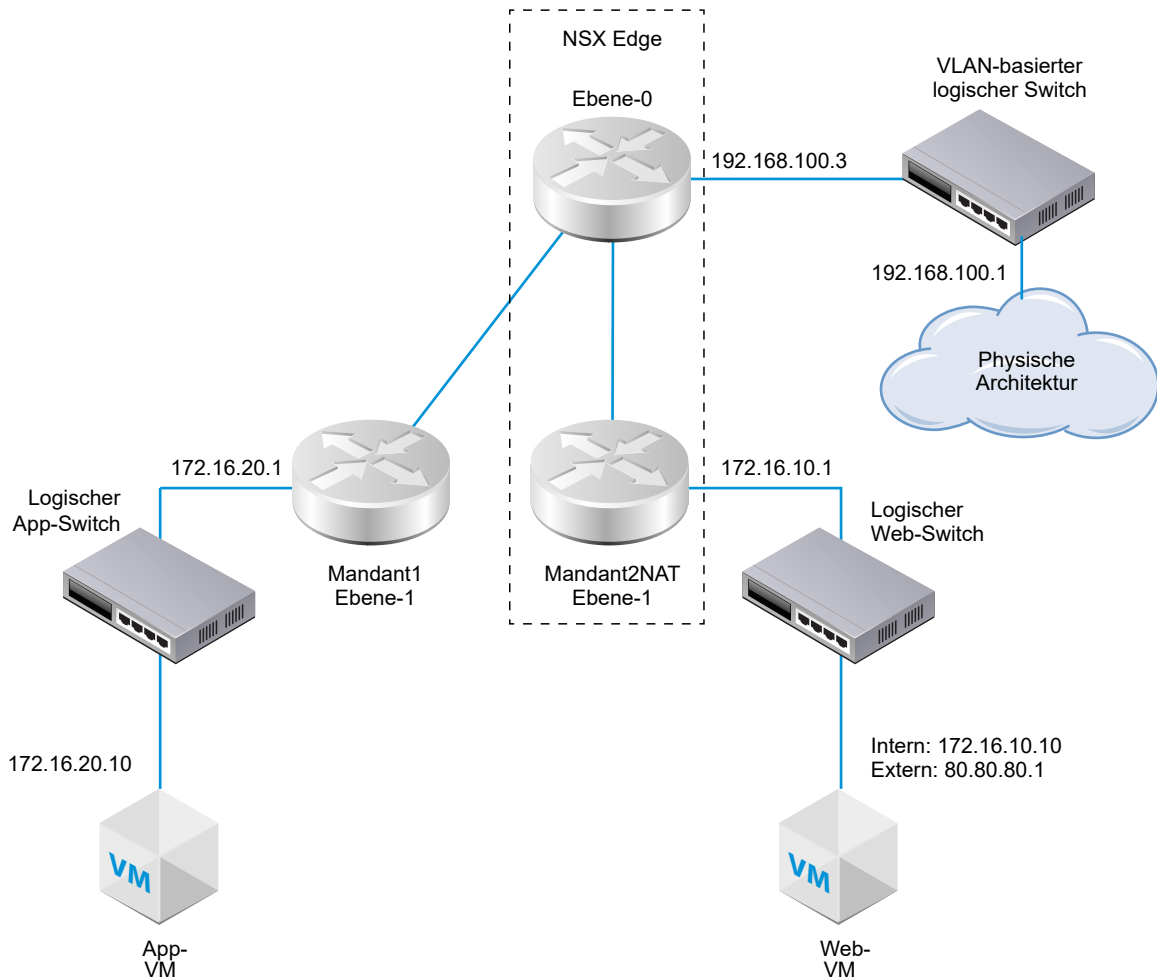
Die Netzwerkadressübersetzung (NAT, Network Address Translation) in NSX-T Data Center kann auf logischen Tier-0- und Tier-1-Routern konfiguriert werden.

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 6-1. NAT-Topologie



Dieses Kapitel enthält die folgenden Themen:

- Tier-1-NAT
- Tier-0-NAT
- Reflexive NAT

Tier-1-NAT

Logische Tier-1-Router unterstützen eine Quell-NAT und eine Ziel-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 einer Routenankündigung auf einem logischen Tier-1-Router](#).
- Die VMs müssen an die richtigen logischen Switches angefügt werden.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 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 eingeht, 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 einer Routenankündigung auf einem logischen Tier-1-Router](#).
- Die VMs müssen an die richtigen logischen Switches angefügt werden.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 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 über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 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 > Routenankündigung** aus.
- 5 Bearbeiten Sie die Regeln der Routenankündigung zur Aktivierung der NAT-Routenankündigung.

Ergebnisse

Tenant2NAT

Übersicht Konfiguration ▾ **Routing ▾** Dienste ▾

Routenankündigung | **BEARBEITEN**

Status ● Aktiviert

Alle NSX verbundene Routen ankündigen	● Ja
Alle NAT-Routen ankündigen	● Ja
Alle statischen Routen ankündigen	● Nein
Alle LB VIP-Routen ankündigen	● Nein
Alle LB SNAT-IP-Routen ankündigen	● Nein
Angekündigte Netzwerke	5 Netzwerke

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 über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager 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 Bearbeiten Sie die Regeln der Routenankündigung zur Aktivierung der Tier-1-NAT-Routenankündigung.

Ergebnisse

Redistribution-Kriterien bearbeiten - rule1 ? ×

Name *

Beschreibung

Quellen *

<input type="checkbox"/> Statisch	<input checked="" type="checkbox"/> Tier-1 NAT
<input checked="" type="checkbox"/> NSX verbunden	<input type="checkbox"/> Tier-1-LB-VIP
<input checked="" type="checkbox"/> NSX statisch	<input type="checkbox"/> Tier-1-LB-SNAT
<input type="checkbox"/> Tier-0 NAT	

Routenübersicht × ▼

ABBRECHEN

SPEICHERN

Nächste Schritte

Überprüfen Sie, ob NAT wie vorgesehen funktioniert.

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-O-NAT

Logische Tier-0-Router unterstützen Quell-NAT, Ziel-NAT und reflexive NAT.

Konfigurieren der Quell- und Ziel-NAT auf einem Tier-O-Router

Sie können eine Quell- und Ziel-NAT auf einem Tier-0-Router konfigurieren, der im Aktiv-Standby-Modus ausgeführt wird.

Sie können außerdem „Keine NAT“, „NO_SNAT“ oder „NO_DNAT“ konfigurieren, um NAT für eine IP-Adresse oder einen Adressbereich zu deaktivieren. Wenn für eine Adresse mehrere NAT-Regeln gelten, wird die Regel mit der höchsten Priorität angewendet.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 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**, **Keine NAT**, **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.

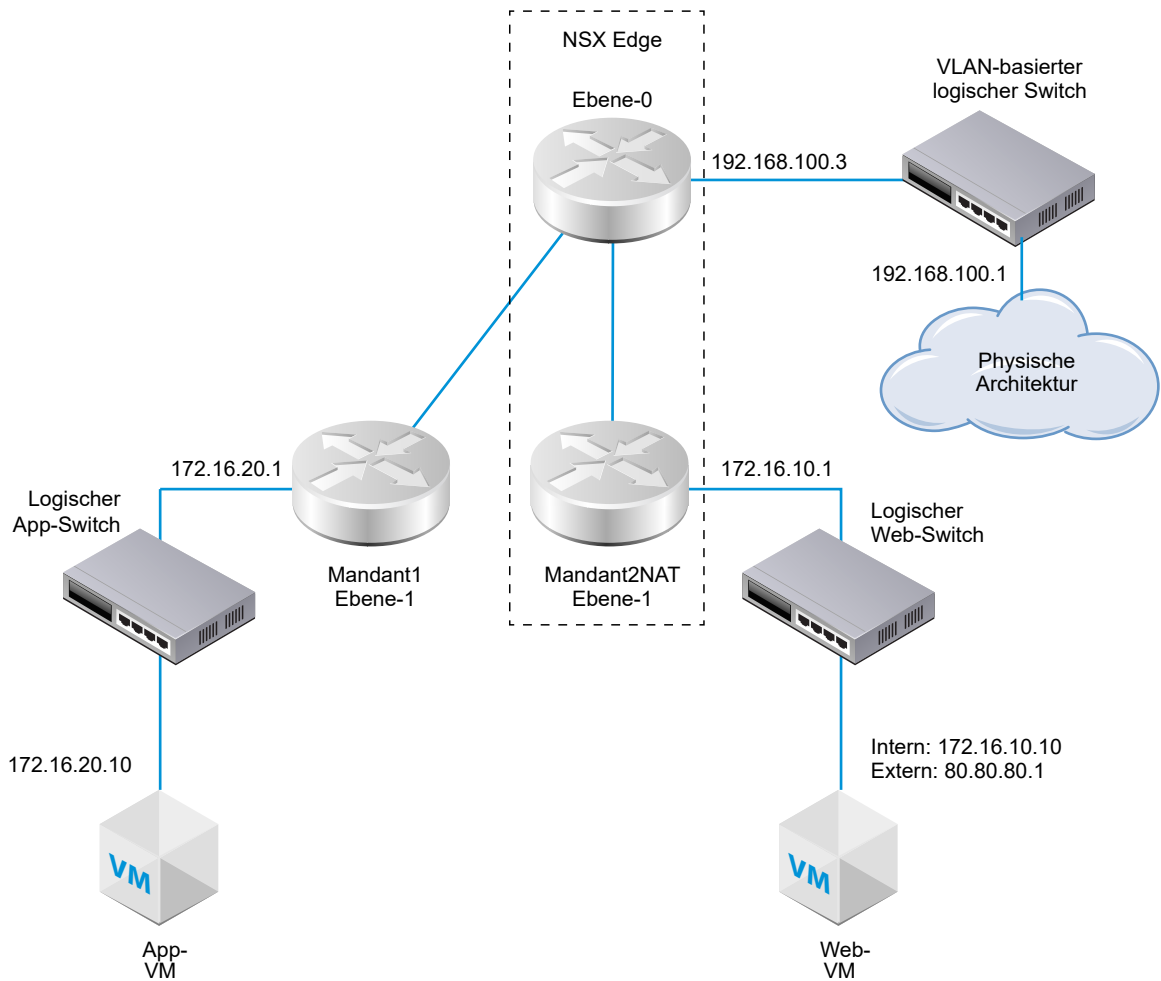
16 (Optional) Ändern Sie die Einstellung für die Firewall-Umgehung.

Diese Funktion ist standardmäßig aktiviert.

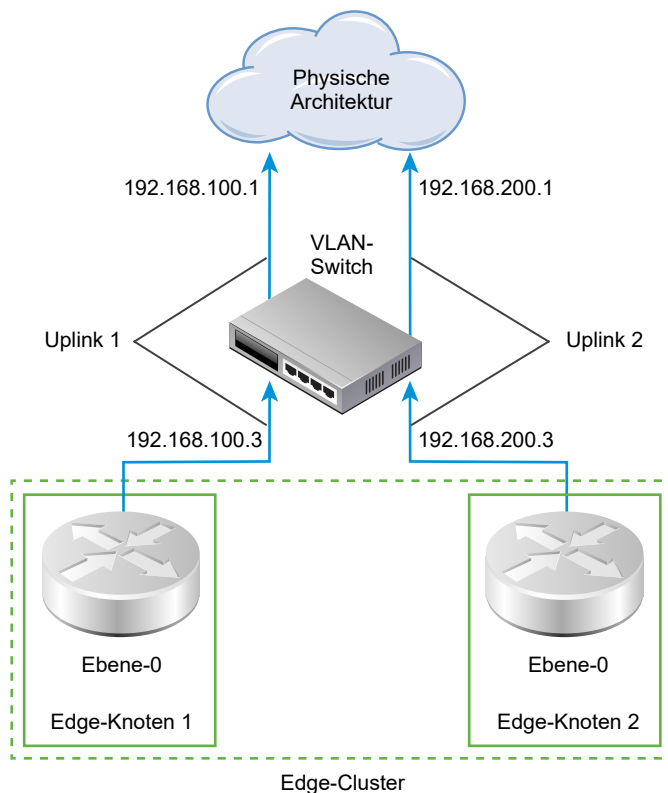
Reflexive NAT

Wenn ein logischer Tier-0- 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.

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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 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		

Firewallabschnitte und Firewallregeln

7

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 keinen 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.

Dieses Kapitel enthält die folgenden Themen:

- [Hinzufügen eines Firewallregelabschnitts](#)
- [Löschen eines Firewallregelabschnitts](#)
- [Aktivieren und Deaktivieren von Abschnittsregeln](#)

- [Aktivieren und Deaktivieren von Abschnittsprotokollen](#)
- [Informationen über Firewallregeln](#)
- [Hinzufügen einer Firewallregel](#)
- [Löschen einer Firewallregel](#)
- [Bearbeiten der standardmäßigen Regel für die verteilte Firewall](#)
- [Ändern der Reihenfolge von Firewallregeln](#)
- [Filtern der Firewallregeln](#)
- [Konfigurieren der Firewall für den Bridge-Port eines logischen Switches](#)
- [Konfigurieren einer Firewall-Ausschlussliste](#)
- [Aktivieren und Deaktivieren der Firewall](#)
- [Hinzufügen oder Löschen einer Firewallregel zu bzw. von einem logischen Router](#)

Hinzufügen eines Firewallregelabschnitts

Ein Firewallregelabschnitt lässt sich separat bearbeiten bzw. speichern und wird zur Anwendung eigener Firewallkonfigurationen für Mandanten verwendet.

Verfahren

- 1 Wählen Sie im Navigationsbereich **Sicherheit > Verteilte Firewall**.
- 2 Klicken Sie auf die Registerkarte **Allgemein** für Schicht-3-(L3-)Regeln oder auf die Registerkarte **Ethernet** für Schicht-2-(L2-)Regeln.
- 3 Klicken Sie auf einen vorhandenen Abschnitt oder eine vorhandene Regel.
- 4 Klicken Sie in der Menüleiste auf das Symbol „Abschnitt“ und wählen Sie **Abschnitt oben hinzufügen** oder **Abschnitt unten hinzufügen** aus.

Hinweis Für jeden Datenverkehr, der die Firewall passieren soll, müssen die Paketinformationen den Regeln in der Reihenfolge genügen, wie Sie in der Regeltabelle angegeben werden. Die Überprüfung beginnt mit den Regeln an oberster Stelle und wird bis zu den Standardregeln unten fortgesetzt. In einigen Fällen kann die Rangfolge von zwei oder mehr Regeln für die Bestimmung der Disposition eines Pakets wichtig sein.

- 5 Geben Sie den Abschnittsnamen ein.
- 6 Um eine statusfreie Firewall zu erzwingen, wählen Sie die Option **Statusfreie Firewall aktivieren** aus. Diese Option steht nur für L3 zur Verfügung.

Zustandsfreie Firewalls überwachen den Netzwerkdatenverkehr und beschränken oder blockieren Pakete auf der Grundlage von Quell- und Zieladressen oder anderen statischen Werten.

Zustandsbehaftete Firewalls ermöglichen eine End-to-End-Überwachung von Datenverkehr-Streams.

Zustandsfreie Firewalls sind in der Regel schneller und bieten eine bessere Leistung bei hohem Datenverkehrsaufkommen. Mit zustandsbehafteten Firewalls lässt eine unberechtigte oder gefälschte Kommunikation besser ermitteln. Nach der Definition einer Firewall kann diese nicht von zustandsfrei auf zustandsbehaftet und umgekehrt geändert werden.

- 7 Wählen Sie ein oder mehrere Objekte zur Anwendung des Abschnitts aus.

Die Objekttypen sind logische Ports, logische Switches und NS-Gruppen. Wenn Sie eine NS-Gruppe auswählen, muss sie einen oder mehrere logische Switches oder logische Ports enthalten. Wenn die NS-Gruppe nur IP Sets oder MAC Sets enthält, wird sie ignoriert.

Hinweis Die Option **Angewendet auf** in einem Abschnitt hat Vorrang vor jeglichen Einstellungen für **Angewendet auf** in den Regeln dieses Abschnitts.

- 8 Klicken Sie auf **OK**.

Nächste Schritte

Fügen Sie dem Abschnitt Firewallregeln hinzu.

Löschen eines Firewallregelabschnitts

Der Abschnitt einer Firewallregel kann gelöscht werden, wenn er nicht mehr benötigt wird.

Wenn Sie den Abschnitt einer Firewallregel löschen, werden alle Regeln dieses Abschnitts gelöscht. Sie können einen Abschnitt löschen und zu einem anderen Ort in der Firewalltabelle hinzufügen. Dazu müssen Sie den Abschnitt löschen und die Konfiguration veröffentlichen. Fügen Sie anschließend den gelöschten Abschnitt zur Firewalltabelle hinzu und veröffentlichen Sie die Konfiguration erneut.

Verfahren

- 1 Wählen Sie im Navigationsbereich **Sicherheit > Verteilte Firewall**.
- 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 im Navigationsbereich **Sicherheit > Verteilte Firewall**.
- 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 vSphere ESXi- und KVM-Hosts gespeichert.

Verfahren

- 1 Wählen Sie im Navigationsbereich **Sicherheit > Verteilte Firewall**.
- 2 Klicken Sie auf die Registerkarte **Allgemein** für L3-Regeln oder auf die Registerkarte **Ethernet** für L2-Regeln.
- 3 Klicken Sie auf das Menüsymbol in der ersten Spalte des Abschnitts und wählen Sie **Protokolle aktivieren** oder **Protokolle deaktivieren** aus.
- 4 Klicken Sie auf **Veröffentlichen**.

Informationen über Firewallregeln

NSX-T Data Center legt mit Firewallregeln die Handhabung des Datenverkehrs zu und von einem Netzwerk fest.

Eine Firewall bietet mehrere Sets konfigurierbarer Regeln: Schicht-3-Regeln (Registerkarte „Allgemein“) und Schicht-2-Regeln (Registerkarte „Ethernet“). Schicht-2-Firewallregeln werden vor Schicht-3-Regeln verarbeitet. Sie können eine Ausschlussliste mit logischen Switches, logischen Ports oder Gruppen konfigurieren, die von den Firewallregeln ausgeschlossen werden sollen.

Firewallregeln werden wie folgt angewendet:

- Die Regeln werden von oben nach unten verarbeitet.
- Jedes Paket wird anhand der obersten Regel in der Regeltabelle überprüft, bevor zu den nächsten Regeln in der Tabelle nach unten übergegangen wird.
- Die erste Regel in der Tabelle, die den Datenverkehrsparametern entspricht, wird erzwungen.

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

Die am Ende der Regeltabelle platzierte Standardregel ist eine „Catchall“-Regel, die grundsätzlich gilt. Für Pakete, für die keinen anderen Regeln gelten, wird die Standardregel angewendet. Nach der Hostvorbereitung sind gemäß der Standardregel Aktionen möglich. Damit ist sichergestellt, dass die Kommunikation von VM zu VM während der Staging- oder Migrationsphase nicht unterbrochen wird. Als Best Practice sollte dann diese Standardregel geändert werden, um Aktionen zu blockieren und die Zugriffskontrolle über ein positives Kontrollmodell zu erzwingen. In einem solchen Modell ist nur Datenverkehr für das Netzwerk zulässig, der in der Firewallregel definiert ist.

Hinweis Für das TCP-Protokoll wird bei einer statusbehafteten Regel automatisch die strenge TCP-Überprüfung aktiviert. Dies bedeutet, dass ein Paket nur dann mit der TCP-Regel abgeglichen wird, wenn die Netzwerkverbindung mit einem SYN-Paket gestartet wurde.

Tabelle 7-1. 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. IPv6 wird für den Quell- und Zielbereich nicht 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. IPv6 wird für den Quell- und Zielbereich nicht 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 <code>/var/log/dfwptlogs.log</code> auf ESX- und KVM-Hosts gespeichert.
Aktion	Die Regel kann die Aktionen Zulassen , Verwerfen und Ablehnen anwenden. Die Standardeinstellung ist Zulassen .
IP-Protokoll	Die Optionen sind IPv4 , IPv6 und IPv4_IPv6 . Die Standardeinstellung ist IPv4_IPv6 . Um auf diese Eigenschaft zuzugreifen, klicken Sie auf das Symbol Erweiterte Einstellungen .
Richtung	Die Optionen sind Eingehend , Ausgehend und Ein/Aus . Die Standardeinstellung ist Ein/Aus . Dieses Feld 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 Ein/Aus bedeutet, dass Datenverkehr in beide Richtungen überprüft wird. Um auf diese Eigenschaft zuzugreifen, klicken Sie auf das Symbol Erweiterte Einstellungen .

Tabelle 7-1. Eigenschaften einer Firewallregel (Fortsetzung)

Eigenschaft	Beschreibung
Regel-Tags	Tags, die der Regel hinzugefügt wurden. Um auf diese Eigenschaft zuzugreifen, klicken Sie auf das Symbol Erweiterte Einstellungen .
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 bössartige virtuelle Maschine die Adresse einer anderen virtuellen Maschine beanspruchen kann. SpoofGuard (sofern aktiviert) überprüft jede erkannte Bindung, sodass nur zulässige Bindungen angezeigt werden.

Hinzufügen einer Firewallregel

Eine Firewall ist ein Netzwerksicherheitssystem, das den eingehenden und ausgehenden Datenverkehr des Netzwerks auf der Grundlage vordefinierter Firewallregeln überwacht und kontrolliert.

Firewallregeln werden dem NSX Manager-Bereich hinzugefügt. Wenn Sie das Feld „Angewendet auf“ verwenden, können Sie den Geltungsbereich einschränken, in dem Sie die Regel anwenden möchten. Sie können mehrere Objekte auf Quell- und Zielebene für jede Regel hinzufügen, um so die Gesamtzahl der zu erstellenden Firewallregeln zu verringern.

Hinweis Standardmäßig gilt eine Regel für den Standard jedes Quell-, Ziel- und Dienstregelements sowie für alle Schnittstellen und Datenverkehrsrichtungen. Wenn Sie die Gültigkeit der Regel auf bestimmte Schnittstellen sowie Datenverkehrsrichtungen beschränken möchten, müssen Sie dies in der Regel entsprechend festlegen.

Voraussetzungen

Um eine Gruppe von Adressen verwenden zu können, müssen Sie zuerst manuell die IP- und MAC-Adresse jeder VM ihrem logischen Switch zuordnen.

Verfahren

- 1 Wählen Sie im Navigationsbereich **Sicherheit > Verteilte Firewall**.
- 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-Adressen	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.
Containerobjekte	Die verfügbaren Objekte sind IP Set, Logischer Port, Logischer Switch und NS-Gruppe. Wählen Sie die Objekte aus und klicken Sie auf OK .

- 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-Adressen	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.
Containerobjekte	Die verfügbaren Objekte sind IP Set, Logischer Port, Logischer Switch und NS-Gruppe. Wählen Sie die Objekte aus und klicken Sie auf OK .

- 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"> ■ ALG ■ ICMP ■ IGMP ■ IP ■ L4-Port-Satz
Protokoll	Wählen Sie eines der verfügbaren Protokolle aus.

Option	Beschreibung
Quellports	Geben Sie den Quellport ein.
Zielports	Wählen Sie den Zielport aus.

11 Klicken Sie in der Spalte **Angewendet auf** auf das Symbol „Bearbeiten“ und wählen Sie Objekte aus.

12 Wählen Sie in der Spalte **Protokoll** die gewünschte Protokollierungsoption aus.

Die Protokolldaten werden in der Datei `/var/log/dfwpktlogs.log` auf ESXI- und KVM-Hosts gespeichert. Das Aktivieren der Protokollierung kann die Leistung beeinträchtigen.

13 Wählen Sie eine Aktion in der Spalte **Aktion** aus.

Option	Beschreibung
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.

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 im Navigationsbereich **Sicherheit > Verteilte Firewall**.

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 im Navigationsbereich **Sicherheit > Verteilte Firewall**.
- 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 im Navigationsbereich **Sicherheit > Verteilte Firewall**.
- 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 im Navigationsbereich **Sicherheit > Verteilte Firewall**.

- 2 Klicken Sie auf die Registerkarte **Allgemein** für L3-Regeln oder auf die Registerkarte **Ethernet** für L2-Regeln.
- 3 Klicken Sie in das Suchtextfeld auf der rechten Seite der Menüleiste, wählen Sie ein Objekt aus oder geben Sie die ersten Zeichen eines Objektnamens ein, um die Liste der auszuwählenden Objekte einzugrenzen.

Nachdem Sie ein Objekt ausgewählt haben, wird der Filter angewendet, und die Liste der Regeln wird aktualisiert. Daraufhin werden nur die Regeln angezeigt, die das Objekt in einer der folgenden Spalten enthalten:

- Quellen
- Ziele
- Angewendet auf
- Dienste

- 4 Um den Filter zu entfernen, löschen Sie den Objektnamen aus dem Textfeld.

Konfigurieren der Firewall für den Bridge-Port eines logischen Switches

Sie können Firewallabschnitte und -regeln für den Bridge-Port eines von einer Schicht--2-Bridge gestützten logischen Switches konfigurieren. Die Bridge muss unter Verwendung von NSX Edge-Knoten erstellt worden sein.

Voraussetzungen

Vergewissern Sie sich, dass der Switch an ein Bridge-Profil angehängt ist. Siehe [Erstellen eines Bridge-gestützten logischen Schicht-2-Switches](#).

Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Sicherheit > Bridge-Firewall**.
- 3 Wählen Sie einen logischen Switch aus.
Der Switch muss an ein Bridge-Profil angehängt sein.
- 4 Führen Sie anschließend die gleichen Schritte wie in den vorherigen Abschnitten für die Konfiguration der Schicht-2- oder Schicht-3-Firewall durch.

Konfigurieren einer Firewall-Ausschlussliste

Sie können einen logischen Port, einen logischen Switch oder eine NS-Gruppe von einer Firewallregel ausschließen.

Nachdem Sie einen Abschnitt mit Firewallregeln erstellt haben, können Sie einen NSX-T Data Center-Appliance-Port von den Firewallregeln ausschließen.

Verfahren

- 1 Wählen Sie im Navigationsbereich **Sicherheit > Verteilte Firewall**.
- 2 Klicken Sie auf die Registerkarte **Ausschlussliste**.
- 3 Klicken Sie auf **Hinzufügen**.
- 4 Wählen Sie einen Typ und ein Objekt aus.
Die verfügbaren Typen lauten **Logischer Port**, **Logischer Switch** und **NS-Gruppe**.
- 5 Klicken Sie auf **OK**.
- 6 Um ein Objekt aus der Ausschlussliste zu entfernen, wählen Sie das Objekt aus, und klicken Sie in der Menüleiste auf **Löschen**.

Aktivieren und Deaktivieren der Firewall

Sie können die Funktion für die verteilte Firewall aktivieren oder deaktivieren. Wenn sie deaktiviert ist, werden keine Regeln erzwungen.

Verfahren

- 1 Wählen Sie im Navigationsbereich **Sicherheit > Verteilte Firewall**.
- 2 Klicken Sie auf die Registerkarte **Einstellungen**.
- 3 Klicken Sie auf **Bearbeiten**.
- 4 Legen Sie im Dialogfeld den Firewall-Status auf Grün (aktiviert) oder Grau (deaktiviert) fest.
- 5 Klicken Sie auf **Speichern**.

Hinzufügen oder Löschen einer Firewallregel zu bzw. von einem logischen Router

Sie können einem logischen Tier-0- oder Tier-1-Router Firewallregeln hinzufügen, um die eingehende Router-Kommunikation zu steuern.

Voraussetzungen

Machen Sie sich mit den Parametern einer Firewallregel vertraut. Siehe [Hinzufügen einer Firewallregel](#).

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 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.

Virtual Private Networks

8

NSX-T Data Center unterstützt IPSec-VPNs und Schicht-2-VPNs (L2VPNs) auf dem NSX Edge.

Hinweis IPSec-VPNs und L2VPNs werden in der NSX-T Data Center-Version mit Exportbeschränkung nicht unterstützt.

IPSec-VPN

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

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 4500 festgelegt.

Hinweis IPSec-VPNs werden nur auf dem logischen Tier-0-Router unterstützt.

NSX Edge unterstützt zwei Arten von VPNs, richtlinienbasierte VPNs und routenbasierte VPNs.

Richtlinienbasierte VPNs erfordern die Anwendung einer Richtlinie auf Pakete, die an den IPSec-Dienst weitergeleitet werden. Diese Art von VPN wird als statisch angesehen, da bei Änderungen der lokalen Netzwerktopologie und -konfiguration auch die Richtlinieneinstellungen aktualisiert werden müssen, um den Änderungen Rechnung zu tragen.

Routenbasierte VPNs bieten Tunneling auf der Grundlage der dynamisch erlernten Routen über eine spezielle Schnittstelle, das so genannte Virtual Tunnel Interface (VTI), z. B. mit BGP als Protokoll. IPSec schützt den gesamten Datenverkehr, der über die virtuelle Tunnel-Schnittstelle (VTI) geleitet wird.

L2 VPN

L2VPN-Konnektivität ermöglicht die Erweiterung der Schicht-2-Netzwerke von einem lokalen Datencenter auf eine Cloud wie zum Beispiel VMware Cloud on Amazon (VMC). Diese Verbindung wird mit dem routenbasierten IPSec-Tunnel gesichert.

Das erweiterte Netzwerk besteht aus einem einzelnen Subnetz mit einer einzigen Broadcast-Domäne, sodass Sie VMs zwischen dem lokalen Datencenter und der Public Cloud migrieren können, ohne ihre IP-Adressen ändern zu müssen.

Außer für die Unterstützung der Migration von Datacentern eignet sich ein mit einem L2VPN erweitertes lokales Netzwerk auch für die Notfallwiederherstellung und die dynamische Einbindung von nicht-lokalen Computing-Ressourcen im Falle von Bedarfsspitzen mithilfe des so genannten Cloud-Bursting.

Jede L2VPN-Sitzung verfügt über genau einen GRE-Tunnel. Tunnelredundanz wird nicht unterstützt. Eine L2VPN-Sitzung kann bis zu 4.094 Schicht-2-Netzwerke erweitern.

Hinweis L2VPN wird zwischen NSX-T Data Center und einer NSX Edge unterstützt, die entweder nicht verwaltet oder in einem NSX Data Center for vSphere verwaltet wird.

Dieses Kapitel enthält die folgenden Themen:

- [Konfigurieren eines IPSec-VPNs](#)
- [Konfigurieren eines L2VPN](#)

Konfigurieren eines IPSec-VPNs

Sie können ein routenbasiertes VPN und eine richtlinienbasierte VPN-Sitzung mit nur der API erstellen.

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

Sie können NAT und IPSec-VPN nicht zusammen unter demselben Netzwerkprofil verwenden. Vergewissern Sie sich, dass Sie NAT und IPSec-VPN unter verschiedenen Netzwerkprofilen platzieren.

Voraussetzungen

Machen Sie sich mit dem IPSec-VPN-Konzept vertraut. Siehe [IPSec-VPN](#).

Verfahren

- 1 Konfigurieren Sie den IPSec-VPN-Dienst auf dem logischen Tier-0-Router.

Verwenden Sie den API-Aufruf `POST /api/v1/vpn/ipsec/services`.

```
POST /api/v1/vpn/ipsec/services
{
  "display_name": "IPSec VPN service",
  "logical_router_id": "f81f220f-3072-4a6e-9f53-ad3b8bb8af57"
}
```

- 2 Konfigurieren Sie das Dead-Peer-Detection-(DPD-)Profil.

Verwenden Sie den API-Aufruf `POST /api/v1/vpn/ipsec/dpd-profiles`.

Das Standard-Profil wird mit einem DPD-Prüfintervall von 60 Sekunden bereitgestellt.

```
POST /api/v1/vpn/ipsec/dpd-profiles
{
  "enabled": "true",
```



```
"dpd_probe_interval": 60,
"description": "DPD profile",
"display_name": "DPD profile"
}
```

3 Konfigurieren Sie die Parameter des IKE-Profiles.

Verwenden Sie den API-Aufruf `POST /api/v1/vpn/ipsec/ike-profiles`.

```
POST /api/v1/vpn/ipsec/ike-profiles
{
  "digest_algorithms": ["SHA2_256"],
  "description": "IKEProfile for site1",
  "display_name": "IKEProfile site1",
  "encryption_algorithms": ["AES_128"],
  "ike_version": "IKE_V2",
  "dh_groups": ["GROUP14"],
  "sa_life_time": 21600
}
```

4 Konfigurieren Sie ein Tunnelprofil für IPSec-VPN.

Verwenden Sie den API-Aufruf `POST /api/v1/vpn/ipsec/tunnel-profiles`.

```
POST /api/v1/vpn/ipsec/tunnel-profiles/
{
  "digest_algorithms": ["SHA1","SHA2_256"],
  "description": "Tunnel Profile for site 1",
  "display_name": "Tunnel Profile for site 1",
  "encapsulation_mode": "TUNNEL_MODE",
  "encryption_algorithms": ["AES_128","AES_256"],
  "enable_perfect_forward_secrecy": true,
  "dh_groups": ["GROUP14"],
  "transform_protocol": "ESP",
  "sa_life_time": 3600,
  "df_policy": "CLEAR"
}
```

5 Konfigurieren Sie einen Peer-Endpoint für die Kommunikation mit dem IPSec-VPN-Peer.

Verwenden Sie den API-Aufruf `POST /api/v1/vpn/ipsec/peer-endpoints`.

```
POST /api/v1/vpn/ipsec/peer-endpoints
{
  "display_name": "Peer endpoint for site 1",
  "connection_initiation_mode": "INITIATOR",
  "authentication_mode": "PSK",
  "ipsec_tunnel_profile_id": "640607f3-bb83-4e54-a153-57939965881c",
  "dpd_profile_id": "4808d04e-572d-480d-8182-61ddaa146461",
  "psk": "6721b9f1f5936956c0a8b4ed95286b452db04dae721edd0f264f0fcc6e94882b",
  "ike_profile_id": "a4db6863-b6f0-45bd-967e-a2e22c260329",
  "peer_address": "10.14.24.4",
  "peer_id": "10.14.24.4"
}
```

6 Konfigurieren Sie einen lokalen Endpoint für den VPN-Endpoint.

Verwenden Sie den API-Aufruf `POST /api/v1/vpn/ipsec/local-endpoints`.

```
POST /api/v1/vpn/ipsec/local-endpoints
{
  "local_address": "1.1.1.12",
  "local_id": "1.1.1.12",
  "display_name": "Local endpoint",
  "ipsec_vpn_service_id": {
    "target_id" : "81388ec0-b5e3-4a9e-b551-e372e700772c"
  }
}
```

7 Konfigurieren Sie eine routenbasierte VPN-Sitzung.

Verwenden Sie den API-Aufruf `POST /api/v1/vpn/ipsec/sessions`.

```
POST /api/v1/vpn/ipsec/sessions
{
  "resource_type": "RouteBasedIPSecVPNSession",
  "display_name": "RouteSession1",
  "ipsec_vpn_service_id": "657bcb55-48ce-4e0f-bfc7-a5a91b2990ae",
  "peer_endpoint_id": "cfc70ab5-16d1-4292-9391-fcee23ccea96",
  "local_endpoint_id": "9d4b44f1-0bfa-4705-ac67-09244a17d42e",
  "enabled": true,
  "tunnel_ports": [
    {
      "ip_subnets": [
        {
          "ip_addresses" : [
            "192.168.50.1"
          ],
          "prefix_length" : 24
        }
      ]
    }
  ]
}
```

8 Konfigurieren Sie eine richtlinienbasierte VPN-Sitzung.

Verwenden Sie den API-Aufruf `POST /api/v1/vpn/ipsec/sessions`.

```
POST /api/v1/vpn/ipsec/sessions
{
  "resource_type": "PolicyBasedIPSecVPNSession",
  "display_name": "PolicySession1",
  "ipsec_vpn_service_id": "ea071856-9e91-4826-a841-9ec7ee9ea534",
  "peer_endpoint_id": "0c2447d2-8890-4b55-bf02-8c6b1a94d1ce",
  "local_endpoint_id": "161acb63-c3f2-438d-9e5c-cb655e6a1099",
  "enabled": true,
  "policy_rules": [
    {
      "sources": [
```

```

    {
      "subnet": "2.2.2.0/24"
    }
  ],
  "logged": true,
  "destinations": [
    {
      "subnet": "3.3.3.0/24"
    }
  ],
  "action": "PROTECT",
  "enabled": true
}
]
}
```

Konfigurieren eines L2VPN

Sie können einen L2VPN-Dienst und eine L2VPN-Sitzung mit nur der API erstellen.

Hinweis L2VPNs werden in der NSX-T Data Center-Version mit Exportbeschränkung nicht unterstützt.

Voraussetzungen

- Machen Sie sich mit dem L2VPN-Konzept vertraut. Siehe [L2 VPN](#).
- Stellen Sie sicher, dass ein logischer Tier-0-Router mit Uplink-Profilen konfiguriert ist. Siehe *Installationshandbuch für NSX-T Data Center*.
- Stellen Sie sicher, dass ein logischer Switch konfiguriert ist. Siehe [Erstellen eines logischen Switches](#).
- Stellen Sie sicher, dass eine nicht verwaltete NSX Edge-Instanz in NSX Data Center for vSphere verfügbar ist.
- Stellen Sie sicher, dass ein IPSec-VPN konfiguriert ist. [Konfigurieren eines IPSec-VPNs](#)

Verfahren

- 1 Konfigurieren Sie einen L2VPN-Dienst.

Verwenden Sie den API-Aufruf `POST /api/v1/vpn/l2vpn/services`.

```

POST /api/v1/vpn/l2vpn/services
{
  "logical_router_id": "b6fe5455-619b-4030-b5f8-8575749f4404",
  "logical_tap_ip_pool" : [ "169.254.64.0/28" ],
  "enable_full_mesh" : true
}
```

2 Konfigurieren Sie eine L2VPN-Sitzung.

Verwenden Sie den API-Aufruf `POST /api/v1/vpn/l2vpn/sessions`.

```
POST /api/v1/vpn/l2vpn/sessions
{
  "l2vpn_service_id" : "421de3a2-c6ec-4c42-a891-5bde3b5feb68",
  "transport_tunnels" : [
    {
      "target_id" : "801e5140-6da8-4e78-ab44-f966de75f311"
    }
  ]
}
```

3 Konfigurieren Sie einen logischen Port mit Anhang.

Verwenden Sie den API-Aufruf `POST /api/v1/vpn/logical-ports`.

```
POST /api/v1/logical-ports/
{
  "resource_type": "LogicalPort",
  "display_name": "Extend logicalSwitch, port for service",
  "logical_switch_id": "f52abcee-27a7-426c-a128-037db2283582",
  "admin_state" : "UP",
  "attachment": {
    "attachment_type": "L2VPN_SESSION",
    "id": "6806c4ea-3b77-4b8a-8af2-ccc47b1ba8a9",
    "context" : {
      "resource_type" : "L2VpnAttachmentContext",
      "tunnel_id" : 10
    }
  }
}
```

4 Laden Sie die L2VPN-Peer-Code-Konfiguration herunter.

`GET /api/v1/vpn/l2vpn/sessions/<L2VPN-session-ID>/peer-codes`

5 Melden Sie sich bei der Befehlszeilenschnittstelle (CLI) der nicht verwalteten NSX Edge-Instanz des lokalen NSX Data Center for vSphere-Systems an.

6 Fügen Sie die L2VPN-Peer-Code-Konfiguration in der Befehlszeile ein.

7 (Optional) Überwachen Sie die L2VPN-Sitzung:

- Rufen Sie die L2VPN-Sitzungsübersicht ab mit `GET /api/v1/vpn/l2vpn/sessions/summary`.
- Rufen Sie die L2VPN-Sitzungsstatistik ab mit `GET /api/v1/vpn/l2vpn/sessions/<L2VPN-session-ID>/statistics`.

Verwalten von Objekten, Gruppen, Diensten und VMs

9

Sie können IP Sets, IP-Pools, MAC-Sätze, NS-Gruppen und NS-Dienste erstellen. Sie können auch die Tags für die virtuellen Maschinen verwalten.

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 Sie als Quellen und Ziele in Firewallregeln verwenden 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 NS-Gruppen sein.

Hinweis IPv6 wird für Quell- und Zielbereiche von Firewallregeln nicht unterstützt.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **Bestand > Gruppen** aus.
- 3 Wählen Sie **IP Sets** oben im Hauptfensterbereich aus.
- 4 Klicken Sie auf **Hinzufügen**.
- 5 Geben Sie einen Namen ein.

- 6 (Optional) Geben Sie eine Beschreibung ein.
- 7 Geben Sie einzelne Adressen oder einen Bereich von Adressen ein.
- 8 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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **Bestand > Gruppen** aus.
- 3 Wählen Sie **IP-Pools** oben im Hauptfensterbereich aus.
- 4 Klicken Sie auf **Hinzufügen**.
- 5 Geben Sie einen Namen ein.
- 6 (Optional) Geben Sie eine Beschreibung ein.
- 7 Klicken Sie auf **Hinzufügen**.
- 8 Geben Sie IP-Bereiche ein.

Setzen Sie den Mauszeiger oben rechts auf eine beliebige Zelle und klicken Sie auf das Bleistiftsymbol zur Bearbeitung.
- 9 (Optional) Geben Sie ein Gateway ein.
- 10 Geben Sie eine CIDR-IP-Adresse mit Suffix ein.
- 11 (Optional) Geben Sie DNS-Server ein.
- 12 (Optional) Geben Sie ein DNS-Suffix ein.
- 13 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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **Bestand > Gruppen** aus.
- 3 Wählen Sie **MAC Sets** oben im Hauptfensterbereich aus.
- 4 Klicken Sie auf **Hinzufügen**.

- 5 Geben Sie einen Namen ein.
- 6 (Optional) Geben Sie eine Beschreibung ein.
- 7 Geben Sie die MAC-Adressen ein.
- 8 Klicken Sie auf **Speichern**.

Erstellen einer NS-Gruppe

Sie können eine NS-Gruppe so konfigurieren, dass diese eine Kombination von IP-Sätzen, MAC Sets, logischen Ports, logischen Switches und anderen NS-Gruppen aufnimmt. NS-Gruppen lassen sich als Quellen und Ziele sowie im Feld **Applied To** in Firewallregeln angeben.

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

Eine NS-Gruppe verfügt über die folgenden Merkmale:

- Sie können direkte Mitglieder wie IP-Sätze, MAC Sets, logische Switches, logische Ports und NS-Gruppen festlegen.
- Sie können bis zu fünf Mitgliedschaftskriterien angeben, die auf logische Switches, logische Ports oder virtuellen Maschinen angewendet werden. Für ein Kriterium, das für logische Switches oder logische Ports gilt, können Sie ein Tag und optional einen Bereich angeben. Für ein Kriterium, das auf virtuelle Maschinen angewendet wird, können Sie einen Namen angeben, der mit einer bestimmten Zeichenfolge beginnt, damit identisch ist oder sie enthält.
- 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.
- Eine NS-Gruppe kann maximal 500 direkte Mitglieder enthalten.
- Der empfohlene Grenzwert für die Anzahl der effektiven Mitglieder in einer NS-Gruppe beträgt 5000. Wird diese Anzahl überschritten, beeinträchtigt dies nicht die Funktionalität, aber eventuell die Leistung. Wenn bei NSX Manager 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. Die Gesamtzahl von Mitgliedern in der NS-Gruppe beträgt ... in die Protokolldatei geschrieben. Wenn die Anzahl der Mitglieder dann größer als 5000 ist, enthält die Protokolldatei die Warnmeldung NS-Gruppe XYZ hat die maximale Anzahl an Mitgliedern erreicht. Die Gesamtzahl von

Mitgliedern in der NS-Gruppe = Wenn beim NSX Controller 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 im Container – IPs:..., MACs:..., VIFs:... in die Protokolldatei geschrieben. NSX Manager und NSX Controller überprüfen die NS-Gruppen zweimal täglich auf die Anzahl der Mitglieder, um 7:00 Uhr und um 19:00 Uhr.

- Die maximal unterstützte Anzahl VMs ist 10.000.

Für alle Objekte, die sich einer NS-Gruppe als Mitglieder hinzufügen lassen (d. h. logische Switches, logische Ports, IP-Sets, MAC-Sets, VMs und NS-Gruppen), können Sie zum Bildschirm des jeweiligen Objekts navigieren und die Option **Zugehörig > NS-Gruppen** auswählen, um alle NS-Gruppen anzuzeigen, die dieses Objekt direkt oder indirekt als Mitglied enthalten. Im obigen Beispiel würden dann nach der Auswahl von **Zugehörig > NS-Gruppen** im Bildschirm für LogischerSwitch-1 die Gruppen NS-Gruppe-1, NS-Gruppe-2 und NS-Gruppe-3 angezeigt werden, da alle drei Gruppen LogischerSwitch-1 direkt oder indirekt als Mitglied enthalten.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **Bestand > Gruppen** aus.
- 3 Klicken Sie auf die Registerkarte **Gruppen**, falls sie noch nicht ausgewählt ist.
- 4 Klicken Sie auf **Hinzufügen**.
- 5 Geben Sie einen Namen für die NS-Gruppe ein.
- 6 (Optional) Geben Sie eine Beschreibung ein.
- 7 (Optional) Klicken Sie auf **Mitgliedschaftskriterien**.

Ein Kriterium kann auf logische Switches, logische Ports oder virtuelle Maschinen angewendet werden. Für jedes Kriterium können Sie bis zu fünf Regeln angeben, die mit dem logischen Operator AND kombiniert werden. Für eine Regel, die für logische Switches oder logische Ports gilt, können Sie ein Tag und optional einen Bereich angeben. Für eine Regel, die auf virtuelle Maschinen angewendet wird, können Sie einen Namen angeben, der mit einer bestimmten Zeichenfolge beginnt, damit identisch ist oder sie enthält.

Sie können bis zu fünf Kriterien angeben, die mit dem logischen Operator OR kombiniert werden.

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

Es sind folgende Typen verfügbar: **IP Set**, **MAC Set**, **Logischer Switch**, **Logischer Port** und **NS-Gruppe**.

- 9 Klicken Sie auf **Speichern**.

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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **Bestand > Dienste** aus.
- 3 Klicken Sie auf **Hinzufügen**.
- 4 Geben Sie einen Namen ein.
- 5 (Optional) Geben Sie eine Beschreibung ein.
- 6 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.
- 7 Für einen einzelnen Dienst müssen Sie einen Typ und ein Protokoll auswählen.

Es sind folgende Typen verfügbar: **Ethernet**, **IP**, **IGMP**, **ICMP**, **ALG** und **L4-Port-Satz**.

- 8 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**.

- 9 Klicken Sie auf **Speichern**.

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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **Bestand > Virtuelle Maschinen** aus.

Die Liste der VMs weist 4 Spalten auf: Virtuelle Maschine, Externe ID, Quelle und Tag. Sie können auf das Filtersymbol in den ersten drei Spaltenüberschriften klicken, 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 eine VM aus.
- 4 Klicken Sie auf **TAGS VERWALTEN**.
- 5 Fügen Sie Tags hinzu bzw. löschen Sie Tags.

Option	Aktion
Tag hinzufügen	Klicken Sie auf HINZUFÜGEN , um ein Tag und optional einen Geltungsbereich anzugeben.
Tag löschen	Wählen Sie ein vorhandenes Tag aus und klicken Sie auf LÖSCHEN .

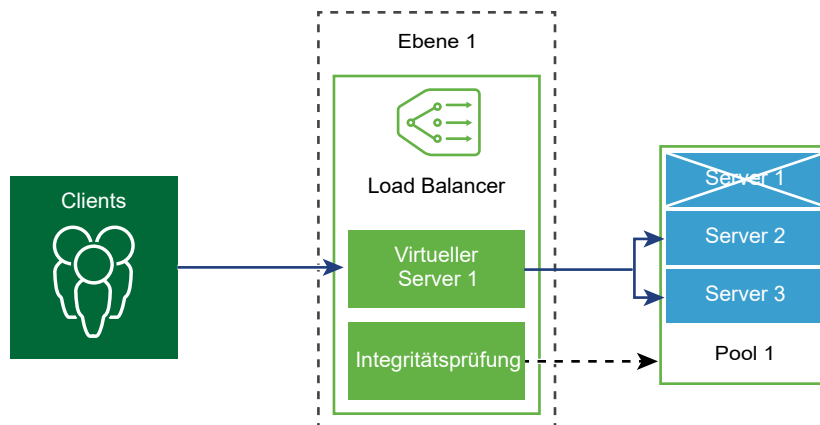
Eine virtuelle Maschine kann maximal 15 Tags aufweisen.

- 6 Klicken Sie auf **Speichern**.

Logischer Load Balancer

10

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



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

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

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

Hinweis Der logische Load Balancer wird nur 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:

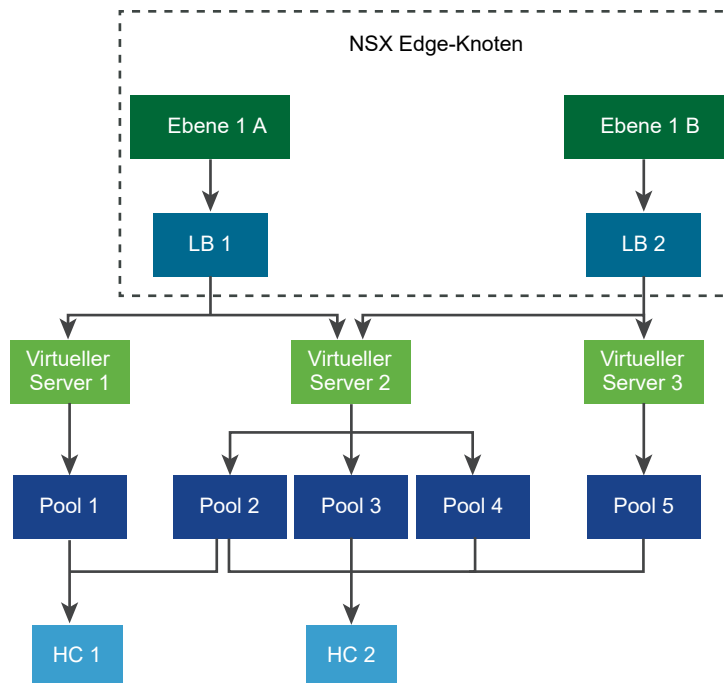
- [Wichtige Load Balancer-Konzepte](#)
- [Konfigurieren von Load Balancer-Komponenten](#)

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.



Skalieren von Load Balancer-Ressourcen

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

Ein Load Balancer ist an einen logischen Tier-1-Router angehängt. Dieser logische Tier-1-Router wird auf den NSX Edge-Knoten gehostet. NSX Edge hat den Formfaktor BareMetal sowie kleine, mittlere und große VM-Appliances. Je nach Formfaktor kann der NSX Edge-Knoten unterschiedliche viele Load Balancer hosten.

Tabelle 10-1. Load Balancer-Größe für den Load-Balancer-Dienst

Load Balancer-Dienst	Kleiner Load Balancer	Mittlerer Load Balancer	Großer Load Balancer
Anzahl der virtuellen Server pro Load Balancer	10	100	1000
Anzahl der Pools pro Load Balancer	20	200	2000
Anzahl der Poolmitglieder pro Load Balancer	200	2000	10.000

Tabelle 10-2. Load Balancer-Größe für NSX Edge-Knoten

Load Balancer pro NSX Edge-Knoten	Kleiner Load Balancer	Mittlerer Load Balancer	Großer Load Balancer	Maximale Anzahl Poolmitglieder
NSX Edge-VM – Klein	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar
NSX Edge VM - Mittel	1	Nicht verfügbar	Nicht verfügbar	200
NSX Edge-VM – Groß	40	4	Nicht verfügbar	5000
NSX Edge-VM – Bare Metal	750	75	7	20.000

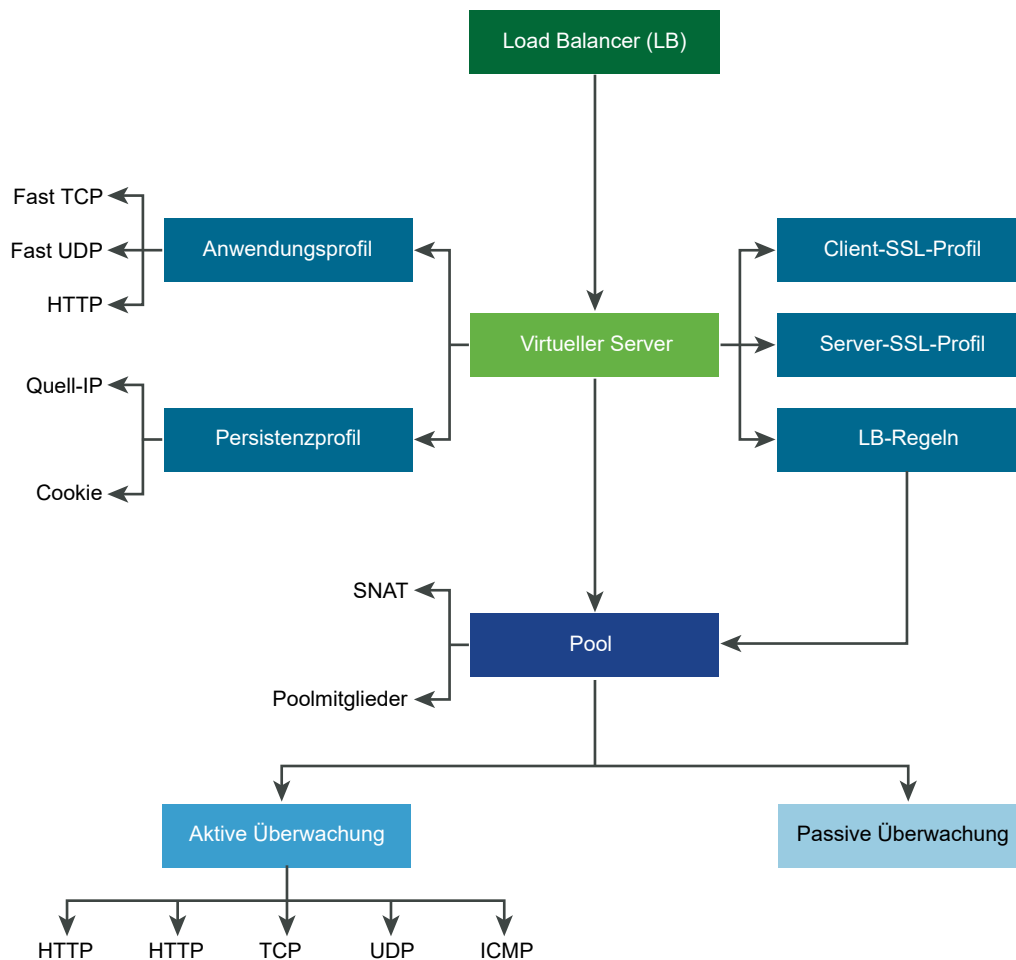
Unterstützte Load Balancer-Funktionen

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

- Schicht 4 – TCP und UDP
- Schicht 7 – HTTP und HTTPS mit Unterstützung von Load Balancer-Regeln
- Serverpools – Statisch und dynamisch mit NS-Gruppe
- 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 Version NSX-T Data Center 2.2 Limited Export nicht unterstützt.

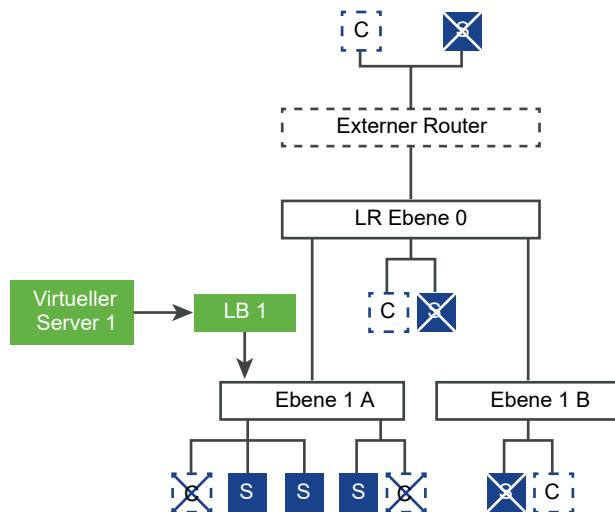


Load Balancer-Topologien

Load Balancer werden üblicherweise im Inline- oder One-Arm-Modus (einarmiger Modus) bereitgestellt.

Inline-Topologie

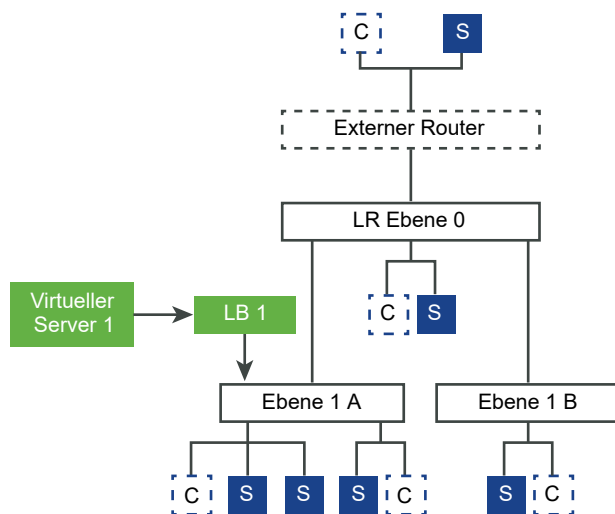
Im Inline-Modus befindet sich der Load Balancer im Datenverkehrspfad zwischen dem Client und dem Server. Clients und Server dürfen nicht mit demselben logischen Tier-1-Router verbunden sein. Diese Topologie erfordert keine SNAT des virtuellen Servers.



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.

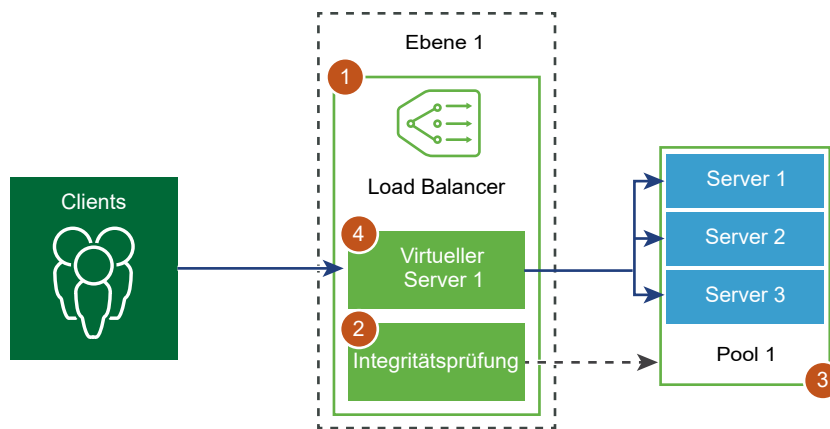
Wenn der Load Balancer den Clientdatenverkehr an die virtuelle IP-Adresse empfängt, wählt er ein Mitglied des Serverpools aus und leitet den Clientdatenverkehr an dieses Mitglied weiter. Im One-Arm-Modus ersetzt der Load Balancer die Client-IP-Adresse durch die IP-Adresse des Load Balancers, damit die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



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.

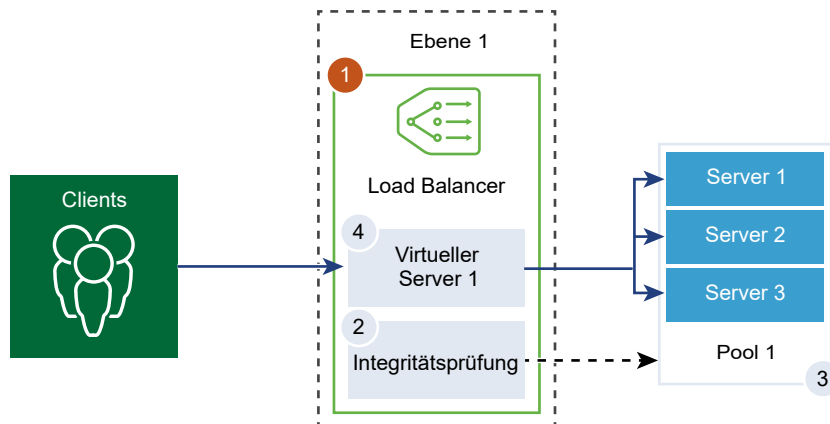


Erstellen eines Load Balancers

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 über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie **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.

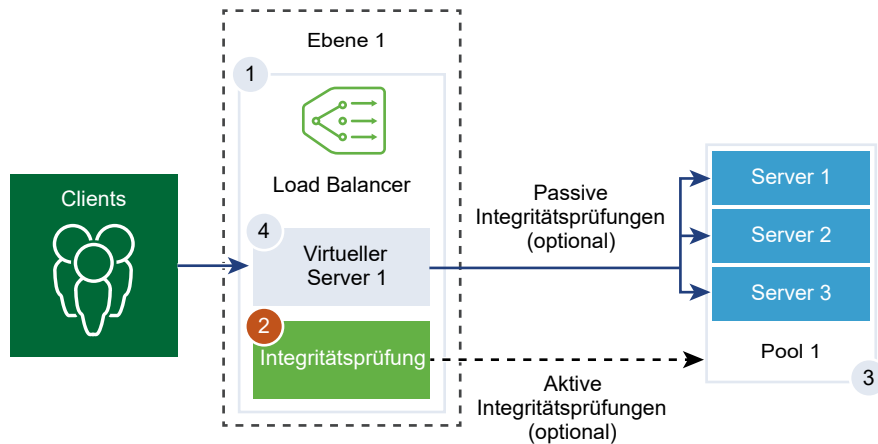
Konfigurieren einer aktiven Systemzustandsüberwachung

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 einen logischen Tier-1-Router 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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie **Load Balancer > Netzwerk > Überwachungen > Aktive Systemzustandsüberwachungen > 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, HTTP-Überwachung, HTTPS-Überwachung, ICMP-Überwachung, TCP-Überwachung und UDP-Überwachung im NSX Manager verwenden.

- 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
Überwachungsintervall	Geben Sie den Zeitraum in Sekunden an, nach dem von der Überwachung eine weitere Verbindungsanfrage an den Server gesendet wird.
Fehleranzahl	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.
Zeitüberschreitung	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
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_1 übernehmen.
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 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
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_1 übernehmen.
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.

- 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 den Lastausgleich](#).

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 über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie **Netzwerk > Load Balancer > Überwachungen > Passive Systemzustandsüberwachungen > 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
Fehleranzahl	Legen Sie einen Wert fest. Wenn die aufeinander folgenden Fehler diesen Wert erreichen, wird der Server als vorübergehend nicht verfügbar betrachtet.
Zeitüberschreitung	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 den Lastausgleich](#).

Hinzufügen eines Serverpools für den Lastausgleich

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.

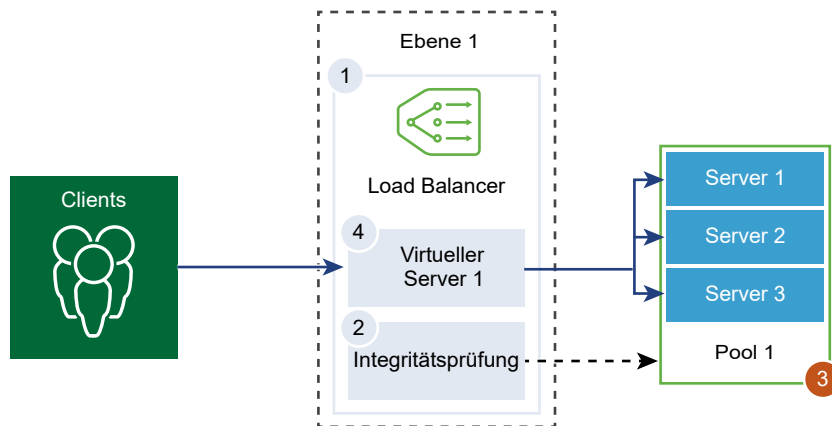
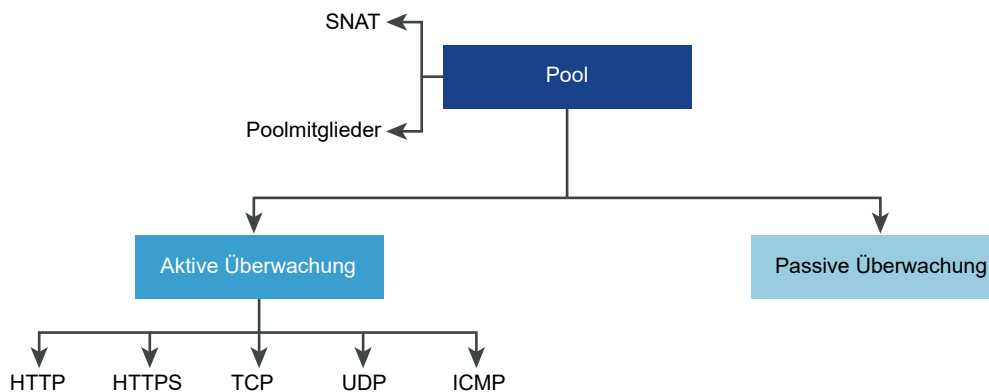


Abbildung 10-1. Konfiguration der Serverpool-Parameter



Voraussetzungen

- Wenn Sie dynamische Poolmitglieder verwenden, muss eine NS-Gruppe 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 über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie **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 Lastausgleichs-Algorithmus steuert, wie die eingehenden Verbindungen zwischen den Mitgliedern verteilt werden. Der Algorithmus kann direkt auf einem Serverpool oder einem Server verwendet werden.

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

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

Option	Beschreibung
ROUND_ROBIN	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.
WEIGHTED_ROUND_ROBIN	Jedem Server wird ein Gewichtungswert zugewiesen, der angibt, wie sich dieser Server im Vergleich zu anderen Servern im Pool verhält. Der Wert legt fest, wie viele Clientanforderungen im Vergleich zu anderen Servern im Pool an einen Server gesendet werden. Dieser Lastausgleichs-Algorithmus konzentriert sich auf eine gerechte Verteilung der Last auf die verfügbaren Serverressourcen.
LEAST_CONNECTION	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.
WEIGHTED_LEAST_CONNECTION	Jedem Server wird ein Gewichtungswert zugewiesen, der angibt, wie sich dieser Server im Vergleich zu anderen Servern im Pool verhält. Der Wert legt fest, wie viele Clientanforderungen im Vergleich zu anderen Servern im Pool an einen Server gesendet werden. Dieser Lastausgleichs-Algorithmus konzentriert sich auf eine angemessene 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.
IP-HASH	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 Lastausgleich 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
Transparent-Modus	Der Load Balancer verwendet die Client-IP-Adresse und Port-Spoofing, während er Verbindungen zu den Servern herstellt. SNAT ist nicht erforderlich.
Modus für die automatische Zuordnung	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.
IP-Listenmodus	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 Lastausgleichs-Algorithmus konfiguriert werden. Die Gewichtung gibt an, wie viel mehr oder weniger Last ein bestimmtes Poolmitglied im Vergleich zu anderen Mitgliedern im selben Pool verarbeiten kann.

Bei der Systemzustandsüberwachung kann ein Poolmitglied als Backup-Mitglied festgelegt werden, um einen aktiven/Standby-Zustand herbeizuführen. Datenverkehr-Failover tritt für Backup-Mitglieder ein, wenn die Systemdiagnose für aktive Mitglieder fehlschlägt.

Option	Beschreibung
Statisch	Klicken Sie auf Hinzufügen , um ein statisches Poolmitglied hinzuzufügen. Sie können auch ein vorhandenes statisches Poolmitglied klonen.
Dynamisch	Wählen Sie im Dropdown-Menü die NS-Gruppe 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.
- 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.

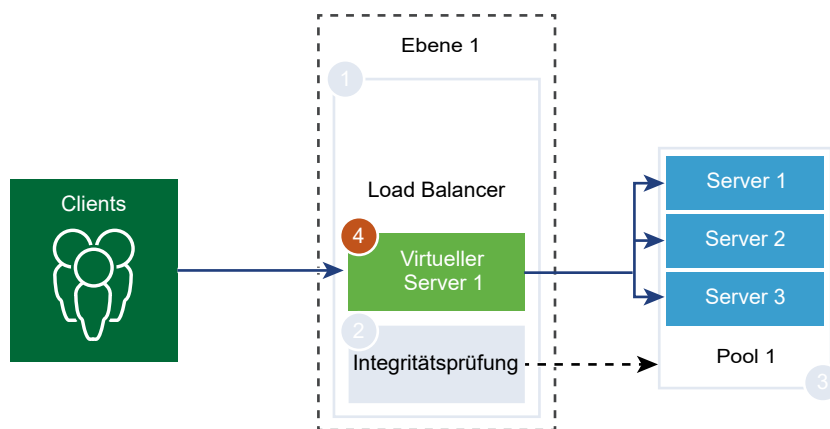
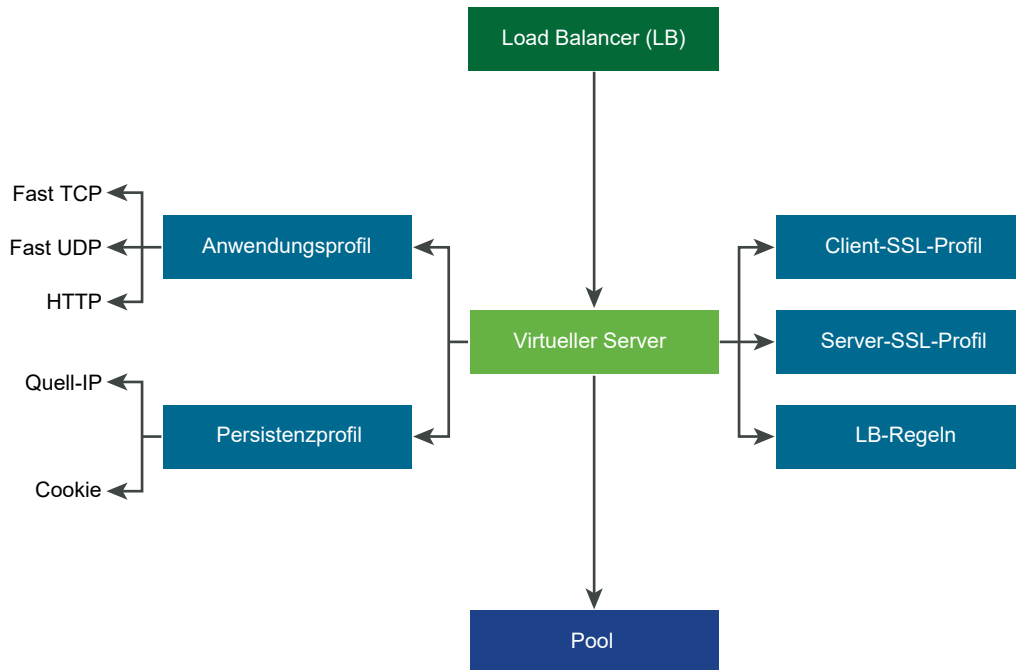


Abbildung 10-2. Komponenten des virtuellen Servers

Konfigurieren von Anwendungsprofilen

Anwendungsprofile sind mit virtuellen Servern verknüpft, um den Lastausgleich 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 keinen Lastausgleich auf Anwendungsebene benötigt, wie z. B. HTTP-URL-Lastausgleich. Diese Profile werden auch verwendet, wenn Sie nur Lastausgleich 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 Lastausgleich 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 10-3. TCP- und UDP-Anwendungsprofil der Schicht 4

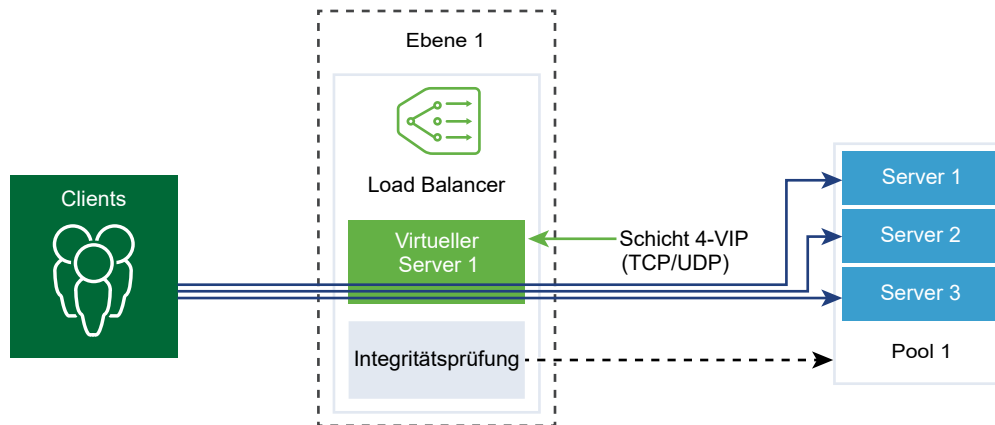
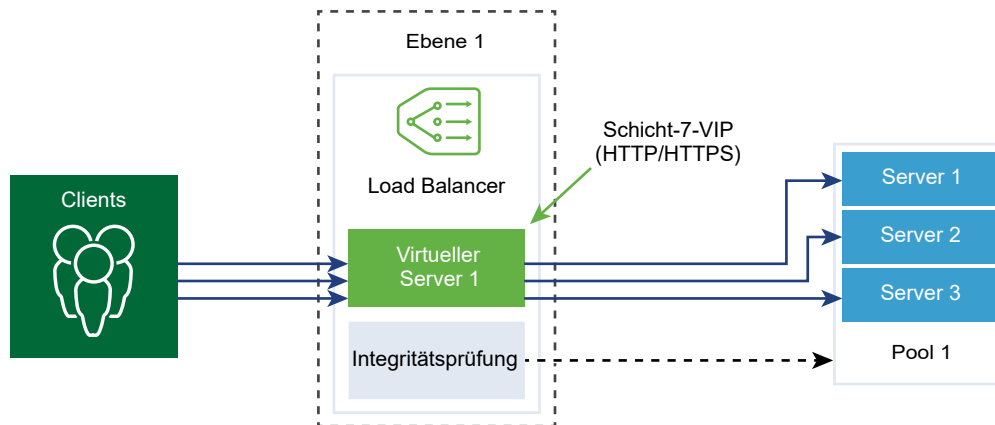


Abbildung 10-4. HTTPS-Anwendungsprofil der Schicht 7



Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie **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
Leerlaufzeitlimit für Verbindung	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.
Zeitlimit vor Schließen der Verbindung	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.
HA-Flow-Spiegelung	Schalten Sie die Schaltfläche um, um alle Flows zum zugehörigen virtuellen Server auf den HA-Standby-Knoten zu spiegeln.

- 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
Leerlaufzeitlimit	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 Lastausgleichszwecken 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.
HA-Flow-Spiegelung	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.

- a Wählen Sie im Dropdown-Menü die Option **Hinzufügen > Fast HTTP-Profil** aus.
- b 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"> ■ Keine – Wenn eine Website vorübergehend nicht verfügbar ist, erhält der Benutzer eine Meldung mit dem Hinweis, dass die Seite nicht gefunden werden konnte. ■ 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. <p>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.</p> <ul style="list-style-type: none"> ■ 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. <p>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.</p> <p>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 Lastausgleichsregeln verwendet werden.</p>
XFF (X-Forwarded-For)	<ul style="list-style-type: none"> ■ EINFÜGEN – 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. ■ ERSETZEN – Wenn der XFF-HTTP-Header bereits in der eingehenden Anfrage enthalten ist, kann der Load Balancer den Header ersetzen. <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>
Leerlaufzeitlimit für Verbindung	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.

Option	Beschreibung
Größe des Anforderungsheaders	Geben Sie die maximale Puffergröße in Byte an, die zum Speichern von HTTP-Anforderungsheadern verwendet wird.
NTLM-Authentifizierung	<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 den Lastausgleich 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**.

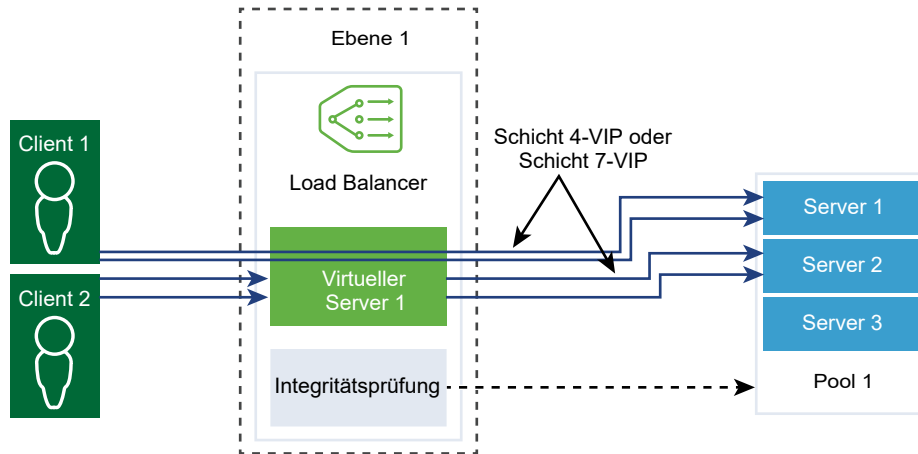
Konfigurieren von persistenten Profilen

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 Lastausgleichs-Algorithmus des Pools ein Mitglied des Serverpools auswählen. Das Quell-IP-Persistenzprofil wird von virtuellen Servern der Schichten 4 und 7 verwendet.

Das Cookie-Persistenzprofil fügt ein eindeutiges Cookie zur Identifizierung der Sitzung beim ersten Zugriff eines Clients auf die Site ein. Das HTTP-Cookie wird durch den Client in nachfolgenden Anforderungen weitergeleitet, und der Load Balancer verwendet diese Informationen zur Bereitstellung der Cookie-Persistenz. Das Cookie-Persistenzprofil kann nur von virtuellen Servern der Schicht 7 verwendet werden.



Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie **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
Persistenz freigeben	<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>
Zeitüberschreitung für Persistenzeintrag	<p>Geben Sie den Zeitraum für die Persistenz bis zum Ablauf in Sekunden ein. Die Persistenztabelle des Load Balancers enthält Einträge, die die Weiterleitung von Clientanforderungen an denselben Server aufzeichnen.</p> <ul style="list-style-type: none"> ■ Wenn von demselben Client keine neuen Verbindungsanforderungen innerhalb des festgelegten Zeitraums empfangen werden, verfällt der Persistenzeintrag und wird gelöscht. ■ Geht von demselben Client innerhalb des festgelegten Zeitraums eine neue Verbindungsanforderung ein, wird der Timer zurückgesetzt und die Clientanforderung an ein verfügbares Poolmitglied gesendet. <p>Nach Ablauf des festgelegten Zeitraums werden neue Verbindungsanforderungen an einen über den Lastausgleichs-Algorithmus bestimmten Server gesendet. Für den Fall einer TCP-Quell-IP-Persistenz mit dem L7-Load Balancer 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>
HA-Persistenzspiegelung	Schalten Sie die Schaltfläche um, um Persistenzeinträge mit dem HA-Peer zu synchronisieren.
Bei voller Tabelle Einträge löschen	<p>Die Einträge werden gelöscht, wenn die Persistenztabelle voll ist.</p> <p>Ein hoher Wert für die Zeitüberschreitung führt möglicherweise dazu, dass die Persistenztabelle sich schnell füllt, wenn der Datenverkehr hoch ist. Wenn die Persistenztabelle voll ist, wird für den aktuellen Eintrag der älteste Eintrag gelöscht.</p>

- 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.
- 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
Cookiemodus	Wählen Sie im Dropdown-Menü einen Modus aus. <ul style="list-style-type: none"> ■ EINFÜGEN – Fügt ein eindeutiges Cookie zur Identifizierung der Sitzung hinzu. ■ PRÄFIX – Wird an die vorhandenen HTTP-Cookie-Informationen angefügt. ■ UMSCHREIBEN – Schreibt die vorhandenen HTTP-Cookie-Informationen um.
Cookiename	Geben Sie den Cookienamen ein.
Cookie Domäne	Geben Sie den Domännennamen ein. Die HTTP-Cookie Domäne kann nur im Modus EINFÜGEN konfiguriert werden.
Cookiepfad	Geben Sie den URL-Pfad des Cookies ein. Der HTTP-Cookiepfad kann nur im Modus EINFÜGEN festgelegt werden.
Cookieverschlüsselung	Verschlüsseln Sie die Informationen zu IP-Adresse und Port des Cookieservers. Schalten Sie die Schaltfläche um, um die Verschlüsselung zu deaktivieren. Wenn die Verschlüsselung deaktiviert ist, liegen die Informationen zu IP-Adresse und Port des Cookieservers unverschlüsselt vor.
Cookie-Fallback	Wählen Sie einen neuen Server für die Verarbeitung einer Clientanforderung aus, wenn das Cookie auf einen Server verweist, der sich im Status DEAKTIVIERT oder INAKTIV befindet. Schalten Sie die Schaltfläche um, sodass die Clientanforderung abgelehnt wird, wenn ein Cookie auf einen Server verweist, der sich im Status DEAKTIVIERT oder INAKTIV befindet.

- f Geben Sie die Details zum Ablauf des Cookies an.

Option	Beschreibung
Cookiezeittyp	Wählen Sie im Dropdown-Menü einen Cookiezeittyp aus. Sowohl Sitzungscookies als auch Persistenzcookies laufen ab, wenn der Browser geschlossen wird.
Maximale Leerlaufzeit	Geben Sie die Zeit in Sekunden ein, die das Cookie im Leerlauf sein kann, bevor es abläuft.

- 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 10-5. SSL-Offloading

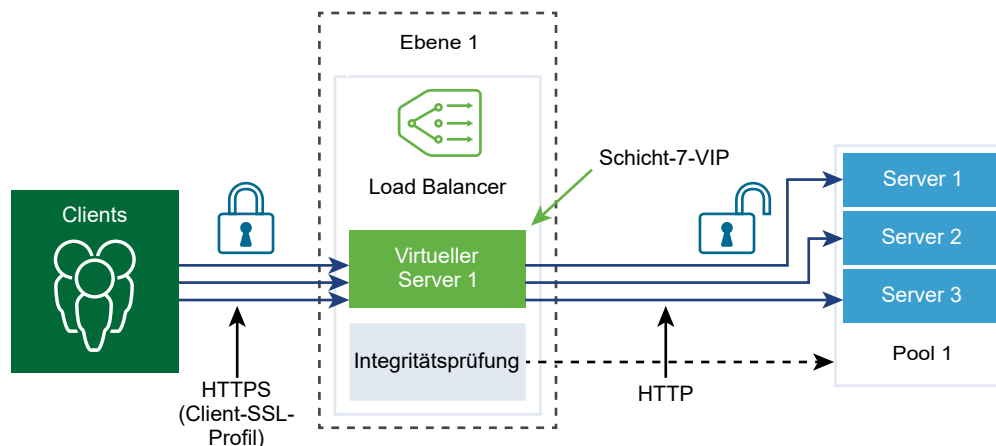
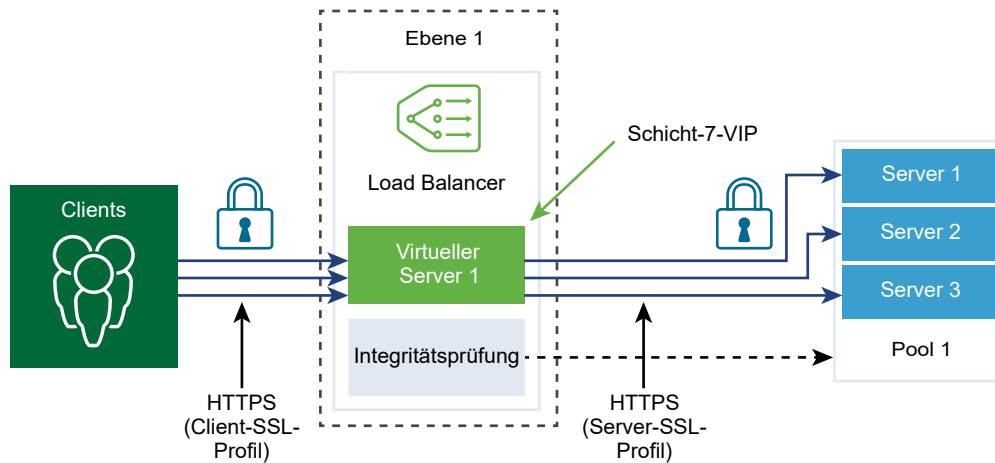


Abbildung 10-6. End-to-End-SSL



Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie **Netzwerk > Load Balancer > Profile > SSL-Profil**.
- 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
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.
Zeitüberschreitung für Cache-Eintrag der Sitzung	Geben Sie die Zeitüberschreitung für den Cache in Sekunden an, um festzulegen, wie lange die SSL-Sitzungsparameter beibehalten werden müssen und wiederverwendet werden können.
Serververschlüsselung bevorzugen	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 den Lastausgleich](#).

Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie **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
Maximale Anzahl gleichzeitiger Verbindungen	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.
Maximale Anzahl neuer Verbindungen	Legen Sie die maximale Anzahl neuer Verbindungen für ein Serverpoolmitglied fest, damit ein virtueller Server die Ressourcen nicht überlastet.
Standardport des Poolmitglieds	Geben Sie den Standardport eines Poolmitglieds ein, wenn der Port des Poolmitglieds für einen virtuellen Server nicht definiert ist. Wenn ein virtueller Server beispielsweise mit dem Portbereich 2000-2999 definiert ist und der Standardportbereich des Poolmitglieds auf 8000-8999 festgelegt ist, wird eine eingehende Clientverbindung für Port 2500 des virtuellen Servers an ein Poolmitglied mit einem auf 8500 gesetzten Zielpport gesendet.

9 Wählen Sie im Dropdown-Menü einen vorhandenen Serverpool aus.

Der Serverpool besteht aus einem oder mehreren auch als Poolmitglieder bezeichneten Servern mit ähnlicher Konfiguration, auf denen dieselbe Anwendung ausgeführt wird.

10 Wählen Sie im Dropdown-Menü einen vorhandenen Sorry-Serverpool aus.

Der Sorry-Serverpool stellt die Anforderung zu, wenn ein Load Balancer keinen Backend-Server auswählen kann, um die Anforderung aus dem Standardpool zuzustellen.

11 Klicken Sie auf **Weiter**.

12 Wählen Sie im Dropdown-Menü ein vorhandenes Persistenzprofil aus.

Das Persistenzprofil kann auf einem virtuellen Server aktiviert werden, damit verwandte Clientverbindungen an denselben Server gesendet werden können.

13 Klicken Sie auf **Fertigstellen**.

Konfigurieren von virtuellen Servern der Schicht 7

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

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

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

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

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

Voraussetzungen

- Stellen Sie sicher, dass Anwendungsprofile verfügbar sind. Siehe [Konfigurieren von Anwendungsprofilen](#).
- Stellen Sie sicher, dass persistente Profile verfügbar sind. Siehe [Konfigurieren von persistenten Profilen](#).
- Stellen Sie sicher, dass SSL-Profile für Client und Server verfügbar sind. Siehe [Konfigurieren von SSL-Profilen](#).
- Stellen Sie sicher, dass Serverpools verfügbar sind. Siehe [Hinzufügen eines Serverpools für den Lastausgleich](#).
- Stellen Sie sicher, dass Zertifizierungsstelle und Clientzertifikat verfügbar sind. Siehe [Erstellen einer Datei für die Zertifikatsignieranforderung](#).
- Stellen Sie sicher, dass eine Zertifikatssperrliste (CRL) verfügbar ist. Siehe [Importieren einer Zertifikatswiderrufsliste](#).
- [Konfigurieren des Pools und der Regeln eines virtuellen Servers der Schicht 7](#)
Auf virtuellen Servern der Schicht 7 können Sie optional Load Balancer-Regeln konfigurieren und das Lastausgleichsverhalten unter Verwendung von Übereinstimmungs- oder Aktionsregeln anpassen.
- [Konfigurieren von Load Balancer-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 über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie **Netzwerk > Load Balancer > Virtuelle Server > Hinzufügen**.
- 3 Geben Sie einen Namen und eine Beschreibung für den virtuellen Server der Schicht 7 ein.

- 4 Wählen Sie das Menüelement „Schicht 7“ aus.

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

Das vorhandene HTTP-Anwendungsprofil wird automatisch befüllt.

- 5 (Optional) Klicken Sie auf **Weiter**, um Serverpool- und Load Balancing-Profile zu konfigurieren.

- 6 Klicken Sie auf **Fertigstellen**.

Konfigurieren des Pools und der Regeln eines virtuellen Servers der Schicht 7

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

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

Bezüglich der Verwendung von Regex gelten folgende Einschränkungen:

- Vereinigungen und Schnittmengen von Zeichenklassen werden nicht unterstützt. Verwenden Sie beispielsweise nicht `[a-z[0-9]]` und `[a-z&&[aeiou]]`, sondern stattdessen `[a-z0-9]` bzw. `[aeiou]`.
- Es werden nur 9 Rückverweise unterstützt, und man kann sie mit Hilfe von `\1` bis `\9` referenzieren.
- Verwenden Sie zum Abgleichen von Oktalzeichen das `\0dd`-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 (?:s)ensitive“, sondern stattdessen „Case ((?: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
- \$_cookie_<name> – Wert des <name>-Cookies
- \$_host – in der folgenden Rangfolge: der Hostname aus der Anforderungszeile oder der Hostname im Anforderungsheader-Feld „Host“ oder der mit einer Anforderung übereinstimmende Servername
- \$_hostname – Hostname
- \$_http_<name> – beliebiges Feld des Anforderungsheaders; <name> ist der Name des Felds, konvertiert in Kleinbuchstaben, in dem Bindestriche durch Unterstriche ersetzt wurden.
- \$_https – „on“, wenn die Verbindung im SSL-Modus arbeitet, andernfalls „“
- \$_is_args – „?“ , wenn eine Anforderungszeile Argumente enthält, andernfalls „“
- \$_query_string – identisch mit „\$_args“
- \$_remote_addr – Client-Adresse
- \$_remote_port – Client-Port
- \$_request_uri – vollständiger ursprünglicher Anforderungs-URI (mit Argumenten)
- \$_scheme – Anforderungsschema, „http“ oder „https“
- \$_server_addr – Adresse des Servers, der eine Anforderung akzeptiert hat
- \$_server_name – Name des Servers, der eine Anforderung akzeptiert hat
- \$_server_port – Port des-Servers, der eine Anforderung akzeptiert hat
- \$_server_protocol – Anforderungsprotokoll, in der Regel „HTTP/1.0“ oder „HTTP/1.1“
- \$_ssl_client_cert – gibt für eine eingerichtete SSL-Verbindung das Client-Zertifikat im PEM-Format zurück, wobei jeder Zeile außer der ersten ein Tabulatorzeichen vorangestellt ist
- \$_ssl_server_name – gibt den über SNI angeforderten Servernamen zurück
- \$_uri – URI-Pfad in der Anforderung

Voraussetzungen

Stellen Sie sicher, dass ein virtueller 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
Maximale Anzahl gleichzeitiger Verbindungen	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.
Maximale Anzahl neuer Verbindungen	Legen Sie die maximale Anzahl neuer Verbindungen für ein Serverpoolmitglied fest, damit ein virtueller Server die Ressourcen nicht überlastet.
Standardport des Poolmitglieds	Geben Sie den Standardport eines Poolmitglieds ein, wenn der Port des Poolmitglieds für einen virtuellen Server nicht definiert ist. Wenn ein virtueller Server beispielsweise mit dem Portbereich 2000-2999 definiert ist und der Standardportbereich des Poolmitglieds auf 8000-8999 festgelegt ist, wird eine eingehende Clientverbindung für Port 2500 des virtuellen Servers an ein Poolmitglied mit einem auf 8500 gesetzten Zielpport gesendet.

- 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
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

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 Balancer-Profil zu konfigurieren.

- 10 Klicken Sie auf **Fertigstellen**.

Konfigurieren von Load Balancer-Profilen für virtuelle Server der Schicht 7

Mit virtuellen Servern der Schicht 7 können Sie optional Load Balancer-, Persistenz-, clientseitige und serverseitige SSL-Profil konfigurieren.

Hinweis SSL-Profil werden in der Version NSX-T Data Center 2.2 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 Balancer-Profil“.
- 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**.

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.

Dieses Kapitel enthält die folgenden Themen:

- [Erstellen eines DHCP-Serverprofils](#)
- [Erstellen eines DHCP-Servers](#)
- [Anfügen eines DHCP-Servers an einen logischen Switch](#)
- [Trennen eines DHCP-Servers von einem logischen Switch](#)
- [Erstellen eines DHCP-Relay-Profiles](#)
- [Erstellen eines DHCP-Relay-Dienstes](#)
- [Hinzufügen eines DHCP-Dienstes zu einem Logical Router Port](#)

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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > DHCP**.
- 3 Klicken Sie auf **Serverprofile** und dann auf **Hinzufügen**.
- 4 Geben Sie einen Namen und optional eine Beschreibung ein.
- 5 Wählen Sie einen NSX Edge-Cluster im Dropdown-Menü aus.
- 6 (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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > DHCP**.
- 3 Klicken Sie auf **Server** und dann auf **Hinzufügen**.
- 4 Geben Sie einen Namen und optional eine Beschreibung ein.
- 5 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.
- 6 (Erforderlich) Wählen Sie ein DHCP-Profil im Dropdown-Menü aus.
- 7 (Optional) Geben Sie gängige Optionen ein, wie Domänenname, Standard-Gateway, DNS-Server und Subnetzmaske.
- 8 (Optional) Geben Sie Optionen für klassenlose statische Routen ein.
- 9 (Optional) Geben Sie andere Optionen ein.
- 10 Klicken Sie auf **Speichern**.
- 11 Wählen Sie den neu erstellten DHCP-Server.
- 12 Blenden Sie den Abschnitt „IP-Pools“ ein.

- 13 Klicken Sie auf **Hinzufügen**, um IP-Bereiche, Standard-Gateway, Lease-Dauer, Warnungsschwellenwert, Fehlerschwellenwert, Option für klassenlose statische Route und weitere Optionen hinzuzufügen.
- 14 Blenden Sie den Abschnitt „Statische Bindungen“ ein.
- 15 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. DHCP-Server wird auf logischen VLAN-Switches nicht unterstützt.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Switching**.
- 3 Klicken Sie auf den logischen Switch, an den ein DHCP-Server angefügt werden soll.
- 4 Klicken Sie auf **Aktionen > DHCP-Server anfügen**.

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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Switching**.
- 3 Klicken Sie auf den logischen Switch, von dem ein DHCP-Server getrennt werden soll.
- 4 Klicken Sie auf **Aktionen > DHCP-Server trennen**.

Erstellen eines DHCP-Relay-Profiles

Ein DHCP-Relay-Profil legt einen oder mehrere externe DHCP-Server fest. Beim Erstellen eines DHCP-Relay-Dienstes müssen Sie ein DHCP-Relay-Profil angeben.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > DHCP**.
- 3 Klicken Sie auf **Relay-Profile** und dann auf **Hinzufügen**.
- 4 Geben Sie einen Namen und optional eine Beschreibung ein.
- 5 Geben Sie eine oder mehrere externe DHCP-Serveradressen ein.

Nächste Schritte

Erstellen Sie einen DHCP-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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > DHCP**.
- 3 Klicken Sie auf **Relay-Dienste** und dann auf **Hinzufügen**.
- 4 Geben Sie einen Namen und optional eine Beschreibung ein.
- 5 Wählen Sie ein DHCP-Relay-Profil im Dropdown-Menü aus.

Nächste Schritte

Fügen Sie einen DHCP-Dienst zu einem Port für einen logischen Router hinzu. Siehe [Hinzufügen eines DHCP-Dienstes zu einem Logical Router Port](#).

Hinzufügen eines DHCP-Dienstes zu einem Logical Router Port

Wenn Sie einen DHCP-Relay-Dienst zu einem Logical Router Port hinzufügen, können VMs des logischen Switch, der diesem Port angefügt ist, mit den DHCP-Servern kommunizieren, die in diesem Relay-Dienst konfiguriert wurden.

Voraussetzungen

- Stellen Sie sicher, dass Sie über einen konfigurierten DHCP-Relay-Dienst verfügen. Siehe [Erstellen eines DHCP-Relay-Dienstes](#).

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Routing**.
- 3 Wählen Sie den Router aus, der mit dem gewünschten logischen Switch verbunden ist, und klicken Sie auf die Registerkarte **Konfiguration**.
- 4 Wählen Sie den Router-Port aus, der mit dem gewünschten logischen Switch eine Verbindung herstellt, und klicken Sie auf **Bearbeiten**.
- 5 Wählen Sie einen DHCP-Relay-Dienst aus der Dropdown-Liste **DHCP-Dienst** aus und klicken Sie auf **Speichern**.

Der Logical Router Port zeigt den DHCP-Relay-Dienst in der Spalte **DHCP-Dienst** an.

Sie haben auch die Möglichkeit, einen DHCP-Relay-Dienst beim Hinzufügen eines neuen Logical Router Port auszuwählen.

Metadaten-Proxyserver

12

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.

Dieses Kapitel enthält die folgenden Themen:

- [Hinzufügen eines Metadaten-Proxyservers](#)
- [Anfügen eines Metadaten-Proxyserver an einen logischen Switch](#)
- [Trennen eines Metadaten-Proxy-Servers von einem logischen Switch](#)

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 über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > DHCP**.
- 3 Klicken Sie auf die Registerkarte **Metadaten-Proxys**.
- 4 Klicken Sie auf **Hinzufügen**.
- 5 Geben Sie einen Namen für den Metadaten-Proxyserver ein.
- 6 (Optional) Geben Sie eine Beschreibung ein.
- 7 Geben Sie die URL und den Port für den Nova-Server ein.
Der gültige Portbereich lautet 3000–9000.
- 8 Geben Sie einen Wert für **Geheimer Schlüssel** ein.
- 9 Wählen Sie einen NSX Edge-Cluster in der Dropdown-Liste aus.
- 10 (Optional) Wählen Sie die Mitglieder des NSX Edge-Clusters.

Beispiel

Beispiel:

New Metadata Proxy Server ? ×

Name *	<input type="text" value="metadata-proxy-1"/>
Description	<input type="text"/>
Nova Server URL *	<input type="text" value="https://123.1.1.1:8775"/>
Secret *	<input type="password" value="*****"/>
Edge Cluster *	<input type="text" value="edge_cluster_p1r1"/> ▼
Members	<input type="text" value="53524616-c67f-11e8-837f-020046520048"/> × ▼

CANCEL
ADD

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 über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > DHCP**.
- 3 Klicken Sie auf die Registerkarte **Metadaten-Proxys**.
- 4 Wählen Sie einen Metadaten-Proxyserver aus.
- 5 Wählen Sie die Menüoption **Aktionen > An logischen Switch anhängen** aus.
- 6 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 über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > DHCP**.
- 3 Klicken Sie auf die Registerkarte **Metadaten-Proxys**.
- 4 Wählen Sie einen Metadaten-Proxyserver aus.
- 5 Wählen Sie die Menüoption **Aktionen > Von logischem Switch trennen**.
- 6 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.

IP-Adressverwaltung

13

Mit der IP-Adressverwaltung (IPAM) können IP-Blöcke zur Unterstützung von NSX-T Container Plug-in (NCP) erstellen. Weitere Informationen über NCP finden Sie im *Installations- und Administratorhandbuch zum NSX-T Container Plug-in für Kubernetes*.

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-T Container Plug-in müssen Sie IP-Blöcke für die Container erstellen.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > IPAM**.
- 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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > IPAM**.
- 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**.

Eine Richtlinie ist eine Kombination aus Regeln und Diensten, wobei die Regeln die Kriterien für den Zugriff auf Ressourcen und deren Nutzung definieren. Mit NSX-Richtlinien können Sie den Zugriff auf Ressourcen und deren Nutzung verwalten, ohne sich um Einzelheiten kümmern zu müssen.

Dieses Kapitel enthält die folgenden Themen:

- [Übersicht](#)
- [Hinzufügen eines Erzwingungspunkts](#)
- [Hinzufügen eines Diensts](#)
- [Hinzufügen einer Domäne](#)
- [Konfigurieren der Sicherung des NSX Policy Managers](#)
- [Sichern des NSX Policy Managers](#)
- [Wiederherstellen des NSX Policy Managers](#)
- [Verknüpfen eines vIDM-Hosts mit dem NSX Policy Manager](#)
- [Verwalten von Rollenzuweisungen](#)

Übersicht

Mit NSX-Richtlinien können Sie Regeln für Objekte wie VMs, logische Ports, IP-Adressen und MAC-Adressen angeben, ohne sich um die Funktionsweise der Regeln kümmern zu müssen. Sie verwalten die Richtlinien nicht über den NSX Manager, sondern über den NSX Policy Manager.

Bevor Sie Richtlinien konfigurieren, müssen Sie den NSX Policy Manager installieren. Weitere Informationen finden Sie im *Installationshandbuch für NSX-T*. Im NSX Policy Manager müssen Sie auch einen oder mehrere Erzwingungspunkte hinzufügen, wobei Sie Informationen über den NSX Manager bereitstellen, der die Richtlinien anwenden wird.

Das folgende Beispiel veranschaulicht, wie Sie das Netzwerk für eine Anwendung mithilfe einer Richtlinie verwalten.

Die Anwendung weist drei Ebenen auf (Web, Anwendung und Datenbank). Die folgenden Regeln sollen auf die VMs der Anwendung angewendet werden:

- Datenverkehr zwischen der Web- und der Anwendungsebene zulassen

- Datenverkehr zwischen der Anwendungsebene und der Datenbankebene zulassen
- Datenverkehr zwischen einem System und der Webebene zulassen

Führen Sie die folgenden Schritte in NSX Manager aus:

- Legen Sie Web gefolgt von einer eindeutigen Zeichenfolge als den Arbeitslastnamen der Web-VMs fest.
- Legen Sie App gefolgt von einer eindeutigen Zeichenfolge als den Arbeitslastnamen der Anwendungs-VMs fest.
- Legen Sie DB gefolgt von einer eindeutigen Zeichenfolge als den Arbeitslastnamen der Datenbank-VMs fest.

Führen Sie die folgenden Schritte im NSX Policy Manager aus:

- Erstellen Sie eine Domäne und geben Sie Folgendes an:
 - Erstellen Sie eine Gruppe mit dem Namen WebGroup, die aus VMs besteht, deren Arbeitslastname mit Web beginnt.
 - Erstellen Sie eine Gruppe mit dem Namen AppGroup, die aus VMs besteht, deren Arbeitslastname mit App beginnt.
 - Erstellen Sie eine Gruppe mit dem Namen DBGroup, die aus VMs besteht, deren Arbeitslastname mit DB beginnt.
 - Geben Sie Sicherheitsrichtlinien an, die die Kommunikation zwischen den Gruppen steuern.
- Überprüfen Sie die Domänenkonfiguration, um sicherzustellen, dass keine Fehler vorhanden sind.
- Wählen Sie Erzwingungspunkte aus.

Nach der Auswahl der Erzwingungspunkte kommuniziert der NSX Policy Manager an den Erzwingungspunkten mit dem NSX Manager, der die Sicherheitsrichtlinien implementiert.

Rollenbasierte Zugriffssteuerung

NSX Policy Manager verfügt über die zwei integrierten Benutzer `admin` und `audit`. Sie können NSX Policy Manager in VMware Identity Manager (vIDM) integrieren und die rollenbasierte Zugriffssteuerung (RBAC) für die von vIDM verwalteten Benutzer konfigurieren.

Für diese Benutzer gilt die vom vIDM-Administrator konfigurierte Authentifizierungsrichtlinie und nicht die Authentifizierungsrichtlinie von NSX Policy Manager, die nur für die Benutzer `admin` und `audit` gilt.

Hinzufügen eines Erzwingungspunkts

Ein Erzwingungspunkt ist der Punkt, an dem die Regeln einer Richtlinie angewendet werden sollen. In dieser Version muss der Erzwingungspunkt eine NSX-T-Installation sein, und ein NSX Policy Manager unterstützt nur einen Erzwingungspunkt.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-policy-manager-IP-address> beim NSX Policy Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **System > Erzwingungspunkte** aus.
- 3 Klicken Sie auf **Hinzufügen**.
- 4 Geben Sie die folgenden Informationen an.

Parameter	Beschreibung
Name	Der Name des Erzwingungspunkts.
Anmeldedaten	Geben Sie den Benutzernamen und das Kennwort zur Anmeldung bei NSX Manager ein.
Erzwingungsadresse	Die IP-Adresse von NSX Manager.
Fingerabdruck	Der Zertifikatfingerabdruck von NSX Manager.

- 5 Klicken Sie auf **Speichern**.

Hinzufügen eines Diensts

Bei einem Dienst handelt es sich um ein Protokoll oder eine Softwarekomponente in Ihrer Umgebung. Eine Richtlinie enthält Regeln, die für Dienste gelten.

Beispiele für einen Dienst sind FTP, HTTP, Active Directory-Server, DHCP-Server, Oracle-Datenbank usw.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-policy-manager-IP-address> beim NSX Policy Manager an.
- 2 Wählen Sie im Navigationsbereich **Infra > Dienste** aus.
- 3 Klicken Sie auf **Neuen Dienst hinzufügen**.
- 4 Geben Sie einen Namen für den Dienst ein.
- 5 Klicken Sie auf **Diensteinträge festlegen**, um Diensteinträge hinzuzufügen.
 - a Klicken Sie auf **Neuen Diensteintrag hinzufügen**.
 - b Wählen Sie einen Diensttyp aus.
Die verfügbaren Typen sind **IP**, **IGMP**, **ICMP**, **ALG**, **TCP** und **UDP**.
 - c Klicken Sie auf die Dropdown-Liste **Weitere Eigenschaften**, um eine Eigenschaft auszuwählen. Sie können weitere Einträge hinzufügen oder vorhandene Einträge bearbeiten oder löschen.
- 6 Klicken Sie auf **Speichern**.

Hinzufügen einer Domäne

Eine Domäne ist eine logische Sammlung von Arbeitslasten, die einem gemeinsamen Geschäftsziel dienen und auf die Richtlinien angewendet werden müssen. Sie enthält eine Reihe von Gruppen und ihre entsprechenden Kommunikationsanforderungen.

Wenn Sie vorhaben, mehrere große Domänen (mit jeweils mehr als 200 resultierenden Regeln) zu erstellen, stellen Sie sie unbedingt nacheinander an den Erzwingungspunkten bereit und warten auf die Umsetzung jeder Domäne, bevor Sie mit der nächsten fortfahren. Wenn Sie diese Domänen mithilfe der API bereitstellen, wird empfohlen, die Kommunikationseinträge zu erstellen, bevor eine Domäne an einem Erzwingungspunkt bereitgestellt wird.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-policy-manager-IP-address> beim NSX Policy Manager an.
- 2 Wählen Sie im Navigationsbereich **Infra > Domänen** aus.
- 3 Klicken Sie auf **Domäne hinzufügen**, um eine Domäne hinzuzufügen.
- 4 Geben Sie einen Namen für die Domäne und optional eine Beschreibung ein.
- 5 Klicken Sie auf **Weiter**, um zum Schritt „Arbeitslastgruppen“ zu gelangen.
- 6 Klicken Sie auf **Gruppe hinzufügen**, um eine oder mehrere Arbeitslastgruppen hinzuzufügen. Führen Sie für jede Arbeitslastgruppe folgende Teilschritte durch:
 - a Geben Sie einen Namen an.
 - b Klicken Sie auf das Feld **Mitgliedertyp**, um den Typ der Gruppenmitglieder auszuwählen.
Die verfügbaren Optionen sind **Virtuelle Maschine**, **IP-Adresse** und **Mitgliedschaftskriterien**.
 - c Wenn Sie **Virtuelle Maschine** oder **IP-Adresse** auswählen, geben Sie einen entsprechenden Wert an.
 - d Wenn Sie **Mitgliedschaftskriterien** auswählen, klicken Sie auf **Mitgliedschaftskriterien festlegen**, um anzugeben, wie die Mitglieder ausgewählt werden.
- 7 Klicken Sie auf **Weiter**, um zum Schritt „Sicherheit“ zu gelangen.
- 8 Klicken Sie auf **Neuen Abschnitt hinzufügen**, um einen Firewallabschnitt hinzuzufügen, oder auf **Neue Regel hinzufügen**, um eine Firewallregel hinzuzufügen.
Sie können mehrere Abschnitte und Regeln hinzufügen.
- 9 Klicken Sie auf **Weiter**, um zum Schritt „Domänenkonfiguration überprüfen“ zu gelangen.
Eine grafische Darstellung der Domäne wird angezeigt.
- 10 Klicken Sie auf **Weiter**, um zum Schritt „Erzwingungspunkte auswählen“ zu gelangen.
- 11 Wählen Sie einen oder mehrere Erzwingungspunkte aus.
- 12 Klicken Sie auf **Fertigstellen**, um die Domäne bereitzustellen.

Konfigurieren der Sicherung des NSX Policy Managers

Sie können den NSX Policy Manager sichern, um die vom Policy Manager gespeicherten Daten zu schützen. Bevor Sie eine Sicherung durchführen können, müssen Sie die Sicherungseigenschaften konfigurieren.

Voraussetzungen

Stellen Sie sicher, dass Sie über den SSH-Fingerabdruck des Sicherungsdateiservers verfügen. Nur ein SHA256-gehashter ECDSA-Schlüssel wird als Fingerabdruck akzeptiert. Siehe [Suchen nach dem SSH-Fingerabdruck eines Remote-Servers](#).

Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://nsx-policy-manager-IP-address` beim NSX Policy Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **System > Dienstprogramme** aus.
- 3 Klicken Sie auf **Konfigurieren**.
- 4 Klicken Sie auf den Umschalter **Automatische Sicherung**, um automatische Sicherungen zu aktivieren oder zu deaktivieren.
- 5 Geben Sie die IP-Adresse oder den Hostnamen des Sicherungsdateiservers ein.
- 6 Bearbeiten Sie den Standardport, falls erforderlich.
- 7 Geben Sie den Benutzernamen und das Kennwort ein, die für die Anmeldung beim Sicherungsdateiserver erforderlich sind.
- 8 Geben Sie im Feld **Zielverzeichnis** den absoluten Verzeichnispfad ein, unter dem die Sicherungen gespeichert werden sollen.
Das Verzeichnis muss bereits vorhanden sein.
- 9 Geben Sie die Passphrase zur Entschlüsselung der Sicherungsdaten ein.
Diese Passphrase wird benötigt, um eine Sicherung wiederherzustellen. Wenn Sie die Sicherungspassphrase vergessen, können Sie keine Sicherungen wiederherstellen.
- 10 Geben Sie den SSH-Fingerabdruck des Servers ein, auf dem die Sicherungen gespeichert werden. Siehe [Suchen nach dem SSH-Fingerabdruck eines Remote-Servers](#).
- 11 Klicken Sie auf die Registerkarte **Zeitplan**.
- 12 Wählen Sie die Häufigkeit aus.
Wenn Sie **Wöchentlich** auswählen, geben Sie den Wochentag und die Uhrzeit an. Wenn Sie **Intervall** auswählen, geben Sie das Intervall an.
- 13 Klicken Sie auf **Speichern**.

Sichern des NSX Policy Managers

Sie können den NSX Policy Manager automatisch oder manuell sichern.

Wenn Sie automatische Sicherungen konfiguriert haben, werden diese automatisch angezeigt. Dieses Verfahren dient dem manuellen Initiieren einer Sicherung.

Voraussetzungen

Stellen Sie sicher, dass Sie die Sicherungseigenschaften konfiguriert haben. Siehe [Konfigurieren der Sicherung des NSX Policy Managers](#).

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-policy-manager-IP-address> beim NSX Policy Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **System > Dienstprogramme** aus.
- 3 Klicken Sie auf **Jetzt sichern**.

Wiederherstellen des NSX Policy Managers

Sie können den NSX Policy Manager aus einer Sicherung in einem früheren Zustand wiederherstellen.

Voraussetzungen

Stellen Sie sicher, dass Sie über den SSH-Fingerabdruck des Sicherungsdateiservers verfügen. Nur ein SHA256-gehashter ECDSA-Schlüssel wird als Fingerabdruck akzeptiert. Siehe [Suchen nach dem SSH-Fingerabdruck eines Remote-Servers](#).

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-policy-manager-IP-address> beim NSX Policy Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **System > Dienstprogramme** aus.
- 3 Klicken Sie auf **Jetzt wiederherstellen**.
- 4 Bestätigen Sie die Meldung über die Voraussetzungen und die Risiken und klicken Sie auf **Weiter**.
- 5 Geben Sie die IP-Adresse oder den Hostnamen des Sicherungsservers ein.
- 6 Ändern Sie die Portnummer, falls erforderlich.
Die Standardeinstellung ist 22.
- 7 Geben Sie den Benutzernamen und das Kennwort zur Anmeldung beim Server ein.
- 8 Geben Sie im Feld **Sicherungsverzeichnis** den absoluten Verzeichnispfad ein, in dem die Sicherung gespeichert wird.
- 9 Geben Sie die zur Verschlüsselung der Sicherungsdaten verwendete Passphrase ein.
- 10 Geben Sie den SSH-Fingerabdruck des Sicherungsservers ein.

11 Klicken Sie auf **Weiter**.

12 Wählen Sie eine Sicherung aus.

13 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.

Nachdem der Wiederherstellungsvorgang abgeschlossen ist, wird der Bildschirm „Wiederherstellung abgeschlossen“ angezeigt. Er zeigt das Ergebnis der Wiederherstellung, den Zeitstempel der Sicherungsdatei und die Start- und Endzeit des Wiederherstellungsvorgangs. Wenn die Wiederherstellung fehlschlägt, wird auf dem Bildschirm der Schritt angezeigt, in dem der Fehler aufgetreten ist. Um die Wiederherstellung erneut zu versuchen, müssen Sie eine neue Policy Manager-Appliance verwenden, und nicht die, bei der der Fehler aufgetreten ist.

Verknüpfen eines vIDM-Hosts mit dem NSX Policy Manager

Um die Integration des NSX Policy Managers in vIDM zu ermöglichen, müssen Sie Informationen über den vIDM-Host angeben.

Der vIDM-Server sollte über ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat verfügen. Andernfalls funktioniert die Anmeldung bei vIDM über NSX Policy Manager möglicherweise nicht mit bestimmten Browsern wie Microsoft Edge oder Internet Explorer 11. Informationen zum Installieren eines CA-signierten Zertifikats auf vIDM finden Sie unter <https://docs.vmware.com/de/VMware-Identity-Manager/3.1/vidm-install/GUID-B76761BF-4B12-4CD5-9366-B0A1A2BF2A8B.html>.

Wenn Sie NSX Policy Manager bei vIDM registrieren, geben Sie einen Umleitungs-URI an, der auf den Policy 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 Policy Manager anzumelden, müssen Sie den Hostnamen in der URL in derselben Weise angeben. Das heißt, wenn Sie den FQDN beim Registrieren des Manager bei vIDM verwenden, müssen Sie den FQDN in der URL verwenden. Verwenden Sie hingegen die IP-Adresse bei der Registrierung des Manager bei vIDM, müssen Sie die IP-Adresse auch in der URL verwenden. Die Anmeldung schlägt sonst fehl.

Voraussetzungen

- Stellen Sie sicher, dass Sie über den Fingerabdruck des Zertifikats vom vIDM-Host verfügen. Siehe [Abrufen des Zertifikatfingerabdrucks von einem vIDM-Host](#).
- Stellen Sie sicher, dass NSX Policy 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://www.vmware.com/support/pubs/identitymanager-pubs.html>.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-policy-manager-IP-address> beim NSX Policy Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **System > Benutzer** aus.
- 3 Klicken Sie auf die Registerkarte **Konfiguration**.
- 4 Klicken Sie auf **Bearbeiten**.
- 5 Klicken Sie auf die Umschaltfläche **VMware Identity Manager-Integration**, um die Option **Aktiviert** festzulegen.
- 6 Geben Sie die folgenden Informationen an.

Parameter	Beschreibung
VMware Identity Manager-Appliance	Der vollqualifizierte Domänenname (FQDN) des vIDM-Hosts.
OAuth-Client-ID	Die ID, die beim Registrieren des NSX Policy Managers für den vIDM-Host erstellt wird.
OAuth-Client-Secret	Der geheime Schlüssel, der beim Registrieren des NSX Policy Managers für den vIDM-Host erstellt wird.
SHA-256-Fingerabdruck	Der Fingerabdruck des Zertifikats für den vIDM-Host.
NSX-Richtlinien-Appliance	Die IP-Adresse oder der vollqualifizierte Domänenname (FQDN) des NSX Policy Managers. Wenn Sie einen FQDN angeben, müssen Sie über einen Browser mit dem FQDN des Managers in der URL auf den NSX Policy 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 Policy Manager-Client so konfigurieren, dass die Verbindung entweder über den FQDN oder über die IP-Adresse hergestellt werden kann.

- 7 Klicken Sie auf **Speichern**.

Verwalten von Rollenzuweisungen

Sie können Rollenzuweisungen für Benutzer oder Benutzergruppen hinzufügen, ändern und löschen, wenn VMware Identity Manager in NSX Policy Manager integriert ist.

Die folgenden Rollen sind vordefiniert. Sie können keine neuen Rollen hinzufügen.

- Enterprise-Administrator
- Auditor
- Site Reliability Engineer (SRE) (verfügbar in einer VMware Cloud-Bereitstellung)
- Cloud-Dienstadministrator (verfügbar in einer VMware Cloud-Bereitstellung)
- Cloud-Dienstauditor (verfügbar in einer VMware Cloud-Bereitstellung)

Voraussetzungen

- Stellen Sie sicher, dass der NSX Policy Manager mit einem vIDM-Host verknüpft ist. Weitere Informationen finden Sie unter [Verknüpfen eines vIDM-Hosts mit dem NSX Policy Manager](#).

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-policy-manager-IP-address> beim NSX Policy Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **System > Benutzer** aus.
- 3 Klicken Sie auf die Registerkarte **Rollenzuweisungen**, falls sie noch nicht ausgewählt ist.
- 4 Fügen Sie Rollenzuweisungen zu oder ändern oder löschen Sie sie.

Option	Aktionen
Hinzufügen von Rollenzuweisungen	Klicken Sie auf Hinzufügen , wählen Sie Benutzer oder Benutzergruppen aus, und wählen Sie Rollen aus.
Ändern von Rollenzuweisungen	Wählen Sie einen Benutzer oder eine Benutzergruppe aus und klicken Sie auf Bearbeiten .
Löschen von Rollenzuweisungen	Wählen Sie einen Benutzer oder eine Benutzergruppe aus und klicken Sie auf Löschen .

Mit Service Insertion können Sie Drittanbieter-Dienste sowohl auf Nord-Süd-Datenverkehr als auch auf Ost-West-Datenverkehr anwenden, der über einen Router übergeben wird. Die Dienste bieten in der Regel erweiterte Sicherheitsfunktionen, wie z. B. ein System zur Erkennung von Eindringversuchen (Intrusion Detection System, IDS) oder zum Schutz gegen Eindringversuche (Intrusion Prevention System, IPS).

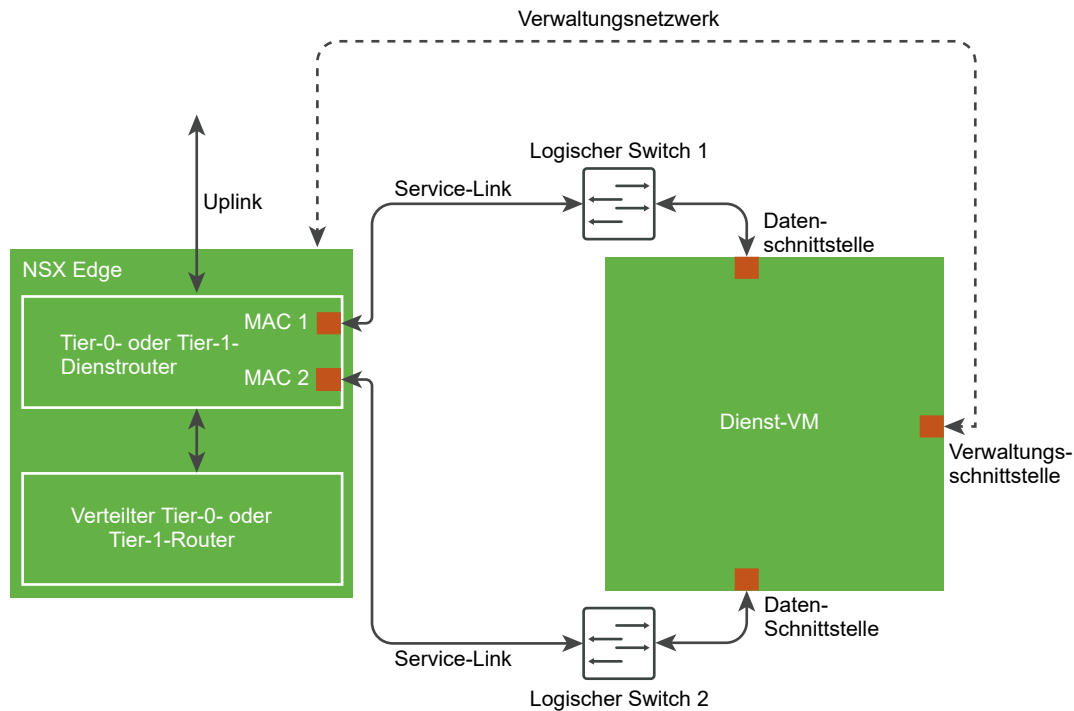
Dieses Kapitel enthält die folgenden Themen:

- [Übersicht](#)
- [Registrieren eines Diensts](#)
- [Bereitstellen einer Dienstinstanz](#)
- [Konfigurieren der Umleitung des Datenverkehrs](#)
- [Überwachung der Umleitung des Datenverkehrs](#)

Übersicht

Sie haben die Möglichkeit, Service Insertion einzurichten, um Nord-Süd-Datenverkehr bei einem Tier-0-Router oder Ost-West-Datenverkehr bei einem Tier-1-Router an eine VM umzuleiten. Ein Dienst, der auf der virtuellen Maschine ausgeführt wird, kann den Datenverkehr verarbeiten und entsprechende Aktionen ausführen.

Das folgende Architekturdiagramm zeigt den Datenfluss bei konfigurierter Service Insertion.



Service Insertion unterstützt Hochverfügbarkeit (High Availability, HA) im Aktiv-Standby-Modus mit zwei Edge-Knoten und zwei Dienst-VMs. Im Aktiv-Aktiv-Modus wird HA nicht unterstützt. Ein Router kann jeweils nur einen Dienst unterstützen.

Gehen Sie zum Einrichten von Service Insertion wie folgt vor:

- Registrieren Sie einen Dienst.
- Stellen Sie eine Dienstinstanz bereit.
- Konfigurieren Sie die Umleitung des Datenverkehrs.

Registrieren eines Diensts

Zum Registrieren eines Diensts ist ein API-Aufruf erforderlich. Nachdem ein Dienst registriert wurde, können Sie ihn in der NSX Manager-Benutzeroberfläche anzeigen.

Details zum API-Aufruf und zu den Eingabeparametern finden Sie in der *Referenz zur NSX-T Data Center-API*.

Verfahren

- 1 Führen Sie den folgenden API-Aufruf aus, um einen Dienst zu registrieren:

```
POST /api/v1/serviceinsertion/services
```

Beispiel:

```

POST https://<nsx-mgr>/api/v1/serviceinsertion/services
{
  "display_name": "NS Service for ABC partner",
  "description": "This service is inserted at T0 router and it provides advanced security",
  "attachment_point": [
    "TIER0_LR"
  ],
  "functionalities": [
    "NG_FW"
  ],
  "implementations": [
    "NORTH_SOUTH"
  ],
  "transports": [
    "L2_BRIDGE"
  ],
  "vendor_id": "ABC_Partner",
  "on_failure_policy": "ALLOW",
  "service_deployment_spec": {
    "deployment_specs": [{
      "ovf_url": "http://server.com/dir1/ABC-Company-HA-OVF/ABC-VM-ESX-2.0.ovf",
      "name": "NS_DepSpec",
      "host_type": "ESXI",
      "service_form_factor": "MEDIUM"
    }],
    "nic_metadata_list": [
      {
        "interface_label": "eth",
        "interface_index": 0,
        "interface_type": "MANAGEMENT"
      },
      {
        "interface_label": "eth",
        "interface_index": 1,
        "interface_type": "DATA1"
      },
      {
        "interface_label": "eth",
        "interface_index": 2,
        "interface_type": "DATA2"
      }
    ],
    "deployment_template": [{
      "name": "NS_DepTemp",
      "attributes": [{
        "attribute_type": "STRING",
        "display_name": "License",
        "key": "LicenseKey"
      }]
    }]
  }
}

```

- 2 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 3 Wählen Sie im Navigationsbereich die **Partnerdienste** aus.
- 4 Klicken Sie auf die Registerkarte **Katalog** und vergewissern Sie sich, dass der Dienst registriert ist.

Nächste Schritte

Stellen Sie eine Instanz des Diensts bereit. Siehe [Bereitstellen einer Dienstinstanz](#).

Bereitstellen einer Dienstinstanz

Nachdem Sie einen Dienst registriert haben, müssen Sie eine Instanz des Diensts bereitstellen, damit der Dienst mit der Verarbeitung des Netzwerkdatenverkehrs beginnen kann.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die **Partnerdienste** aus.
- 3 Klicken Sie auf **Bereitstellen**.
- 4 Geben Sie einen Namen und optional eine Beschreibung für die Instanz ein.
- 5 Klicken Sie auf das Feld **Partnerdienst** und wählen Sie einen Dienst aus.
- 6 Wählen Sie eine **Bereitstellungsspezifikation** aus.
- 7 Wählen Sie einen logischen Router aus.

Es werden nur Router angezeigt, auf denen Service Insertion nicht konfiguriert ist.

- 8 Klicken Sie auf **Weiter**.
- 9 Klicken Sie auf das Feld **Berechnungsmanager** und wählen Sie einen Berechnungsmanager aus.
- 10 Klicken Sie auf das Feld **Cluster** und wählen Sie einen Cluster aus.
- 11 (Optional) Klicken Sie auf das Feld **Ressourcenpool** und wählen Sie einen Ressourcenpool aus, wenn dieser in vCenter Serverkonfiguriert wurde.
- 12 Klicken Sie auf das Feld **Datenspeicher**, und wählen Sie einen Datenspeicher aus.
- 13 Wählen Sie einen **Bereitstellungsmodus** aus.
Mögliche Optionen sind **Eigenständig** oder **Hochverfügbarkeit**.
- 14 Wählen Sie eine **Fehlerrichtlinie** aus.
Mögliche Optionen sind **Zulassen** oder **Blockieren**.
- 15 Geben Sie die IP-Adresse der virtuellen Maschine ein.
- 16 Geben Sie das Standard-Gateway für die IP-Adresse der virtuellen Maschine ein.

- 17 Geben Sie die Subnetzmaske für die IP-Adresse der virtuellen Maschine ein.
- 18 Klicken Sie auf **Weiter**.
- 19 Wählen Sie eine **Bereitstellungsvorlage** aus.
- 20 Geben Sie eine Lizenz für den Partnerdienst ein.
- 21 Klicken Sie auf **Fertigstellen**.

Ergebnisse

Der Bereitstellungsvorgang kann je nach Implementierung des Anbieters einige Zeit in Anspruch nehmen. Sie können den Status in der Manager-Benutzeroberfläche anzeigen. Als Status wird Bereitstellung erfolgreich angezeigt, wenn die Bereitstellung gelungen ist.

Nächste Schritte

Konfigurieren Sie die Umleitung des Datenverkehrs für die Dienstinstanz. Siehe [Konfigurieren der Umleitung des Datenverkehrs](#).

Konfigurieren der Umleitung des Datenverkehrs

Nachdem Sie eine Dienstinstanz bereitgestellt haben, können Sie konfigurieren, 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 [Kapitel 7 Firewallabschnitte und Firewallregeln](#).

Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die **Partnerdienste** aus.
- 3 Klicken Sie auf den Namen einer Dienstinstanz.
- 4 Klicken Sie auf die Registerkarte **Umleitung des Datenverkehrs**.
- 5 Fügen Sie Abschnitte und Regeln hinzu oder entfernen Sie welche.

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 über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.

- 2 Wählen Sie im Navigationsbereich die **Partnerdienste** 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.

NSX Cloud ermöglicht es Ihnen, Ihre Public Cloud-Bestandsliste unter Verwendung von NSX-T Data Center zu verwalten und zu sichern.

Unter [Architektur und Komponenten von NSX Cloud](#) im *Installationshandbuch für NSX-T Data Center* finden Sie eine Liste und Beschreibungen der NSX Cloud-Komponenten.

Dieses Kapitel enthält die folgenden Themen:

- [Der Cloud Service Manager](#)
- [Verwalten der Quarantäne-Richtlinie](#)
- [Überblick über Onboarding und Verwaltung von Workload-VMs](#)
- [Onboarden von Workload-VMs](#)
- [Verwalten von Workload-VMs](#)
- [Verwenden von erweiterten NSX Cloud-Funktionen](#)
- [Fehlerbehebung](#)

Der Cloud Service Manager

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

Die CSM-Schnittstelle ist in folgende Kategorien unterteilt:

- **Suche:** Sie können das Textfeld „Suchen“ verwenden, um Public-Cloud-Konten oder zugehörige Konstrukte zu finden.
- **Clouds:** Ihr Public-Cloud-Bestand wird über die Abschnitte unter dieser Kategorie verwaltet.
- **System:** Über diese Kategorie können Sie auf **Einstellungen**, **Dienstprogramme** und **Benutzer** für Cloud Service Manager zugreifen.

Um Public Cloud-Vorgänge durchzuführen, wechseln Sie zum Unterabschnitt **Clouds** von CSM.

Navigieren Sie zum Unterabschnitt **System**, um systembasierte Operationen wie z. B. Sicherung, Wiederherstellung, Upgrade und Benutzerverwaltung durchzuführen.

Clouds

Dies sind die Abschnitte unter **Clouds**:

Clouds > (Übersicht)

Sie können auf Ihr Public Cloud-Konto zugreifen, indem Sie auf **Clouds** klicken.

Übersicht: Jede Kachel auf dieser Seite repräsentiert Ihr Public Cloud-Konto mit der Anzahl der Konten, Regionen, VPCs bzw. VNets und Instanzen (Arbeitslast-VMs), die es einschließt.

Sie können die folgenden Aufgaben durchführen:

Public Cloud-Konto oder -Abonnement hinzufügen	Sie können ein oder mehrere Public Cloud-Konten oder -Abonnements hinzufügen. Dies ermöglicht es Ihnen, Ihren Public Cloud-Bestand in CSM einzusehen, und gibt die Anzahl der VMs, die von NSX-T Data Center verwaltet werden, und ihren Zustand wieder. Detaillierte Anweisungen finden Sie unter Ihr Public Cloud-Konto hinzufügen 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 PCG bereitstellen oder Bereitstellung von PCG aufheben 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 Verwalten der Quarantäne-Richtlinie .
Zwischen Tabellen- und Kartenansicht umschalten	Die Karten zeigen eine Übersicht über Ihren Bestand an. Die Tabelle zeigt weitere Details. Klicken Sie auf die Symbole, um zwischen den Anzeigearten zu wechseln.

CSM bietet eine ganzheitliche Ansicht aller Ihrer Public Cloud-Konten, die Sie mit NSX Cloud verbunden haben, indem Ihr Public Cloud-Bestand auf unterschiedliche Weise dargestellt wird:

- Sie können die Anzahl der Regionen anzeigen, in denen Sie tätig sind.
- Sie können die Anzahl der privaten Netzwerke pro Region anzeigen.
- Sie können die Anzahl der Workload-VMs pro privatem Netzwerk anzeigen.

Unter **Clouds** gibt es vier Registerkarten.

Eine Beschreibung der UI-Elemente finden Sie unter [CSM-Diagramme und -Symbole](#).

Clouds > {Ihre Public Cloud} > Konten

Der Abschnitt „Konten“ von CSM enthält Informationen zu den Public Cloud-Konten, die Sie bereits hinzugefügt haben.

Jede Karte stellt ein Public Cloud-Konto des Cloud-Anbieters dar, den Sie unter „Clouds“ ausgewählt haben.

Von diesem Abschnitt aus können Sie die folgenden Aktionen ausführen:

- Konto hinzufügen

- Konto bearbeiten
- Konto löschen
- Konto neu synchronisieren

Clouds > {Ihre Public Cloud} > Regionen

Der Abschnitt „Regionen“ zeigt die Bestandsliste für eine ausgewählte Region an.

Sie können die Regionen nach Ihrem Public Cloud-Konto filtern. Jede Region hat VPCs bzw. VNet sowie Instanzen. Wenn Sie PCGs bereitgestellt haben, werden diese hier als Gateways mit einem Indikator für die PCG-Integrität angezeigt.

Clouds > {Ihre Public Cloud} > VPCs oder VNet

Der Abschnitt „VPCs“ bzw. „VNet“ zeigt Ihre Private-Cloud-Bestandsliste an.

Sie können die Bestandsliste nach Konto und Region filtern.

- Jede Karte steht für eine VPC oder ein VNet.
- In jeder VPC oder jedem VNet können ein oder (bei HA) zwei PCGs bereitgestellt werden.
- Sie können zu jeder VPC oder jedem VNet weitere Details anzeigen, indem Sie zur Rasteransicht wechseln.
- Durch Klicken auf **Aktionen** erhalten Sie Zugriff auf die folgenden Aktionen:
 - **Konfiguration bearbeiten:**
 - Quarantäne-Richtlinie aktivieren oder deaktivieren.
 - Proxy-Server-Auswahl ändern.
 - **NSX Cloud-Gateway bereitstellen:** Klicken Sie auf diese Option, um mit der Bereitstellung von PCG in dieser VPC oder diesem VNet zu beginnen. Wenn ein PCG oder ein PCG-Hochverfügbarkeits-Paar bereits bereitgestellt wird, ist diese Option nicht verfügbar. Detaillierte Anweisungen finden Sie unter **PCG bereitstellen** im *Installationshandbuch für NSX-T Data Center*.

Clouds > {Ihre Public Cloud} > Instanzen

Der Abschnitt „Instanzen“ zeigt Details zu den Instanzen in Ihrem VPC oder VNet an.

Sie können die Bestandsliste der Instanzen nach Konto, Region und VPC bzw. VNet filtern.

Jede Karte repräsentiert eine Instanz (Arbeitslast-VM) und zeigt eine Übersicht zu dieser an.

Ausführlichere Informationen zu einer Instanz erhalten Sie, indem Sie auf die Karte klicken oder zur Rasteransicht wechseln.

Hinweis CSM zeigt den Wert für die Betriebssystemversion für NSX-verwaltete VMs an, jedoch ist der angezeigte Betriebssystemtyp für VMs, die nicht von NSX verwaltet werden, im Detail minimal, da er von den Cloud-Anbieter-APIs übernommen wird.

CSM-Diagramme und -Symbole

CSM zeigt den Zustand und die Integrität Ihrer Public Cloud-Konstrukte mithilfe von anschaulichen und verständlichen Symbolen an.

Hinweis Die Quarantäne-Workflows werden nur angewendet, wenn die Einstellung **Quarantäne aktivieren** aktiviert ist. Die Einstellung ist standardmäßig deaktiviert.

VNets

Abbildung 16-1. VNet mit von NSX Cloud verwalteten VMs, die sich in einem ordnungsgemäßen Systemzustand befinden

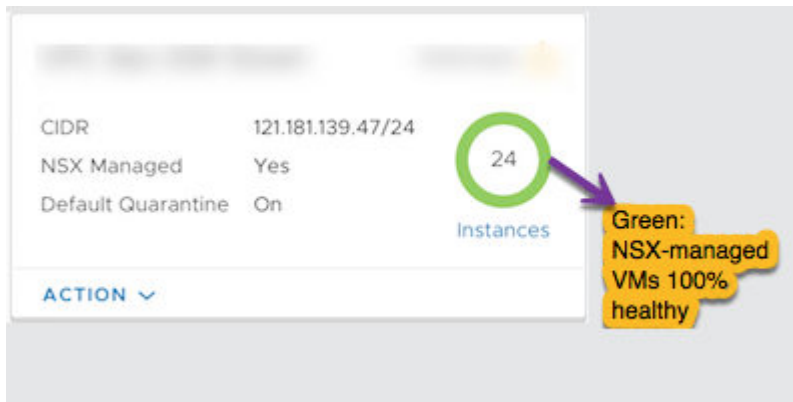


Abbildung 16-2. VNet mit von NSX Cloud verwalteten VMs, die Fehler aufweisen

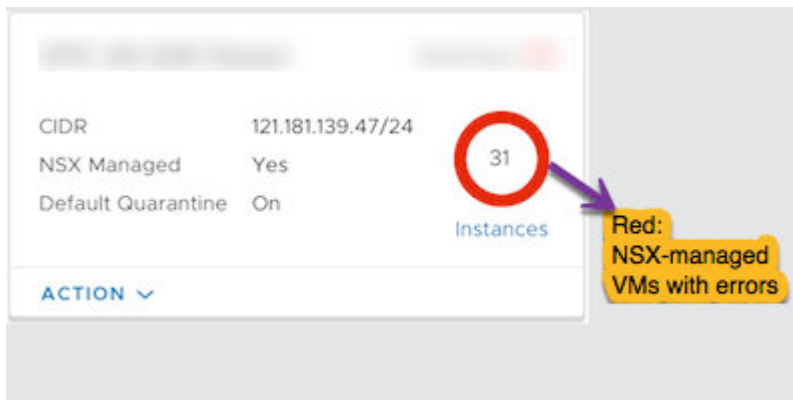


Abbildung 16-3. VNet mit ausgeschalteten VMs

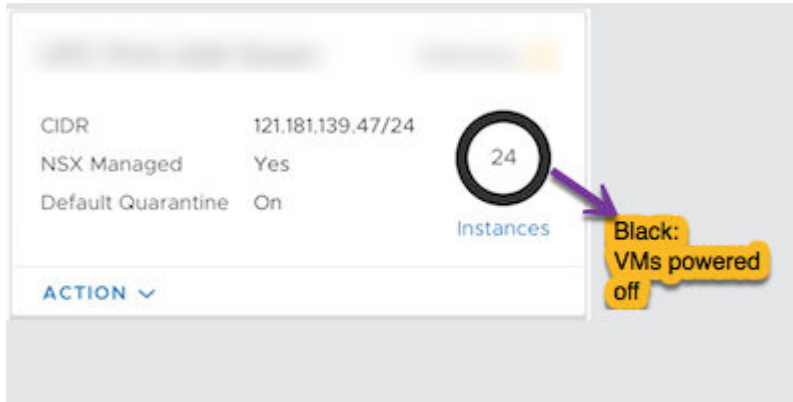


Abbildung 16-4. VNet mit Anzeige des standardmäßigen Quarantäne-Status

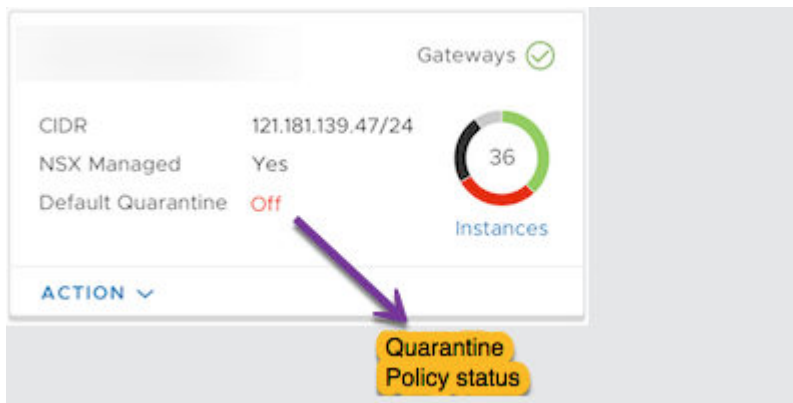
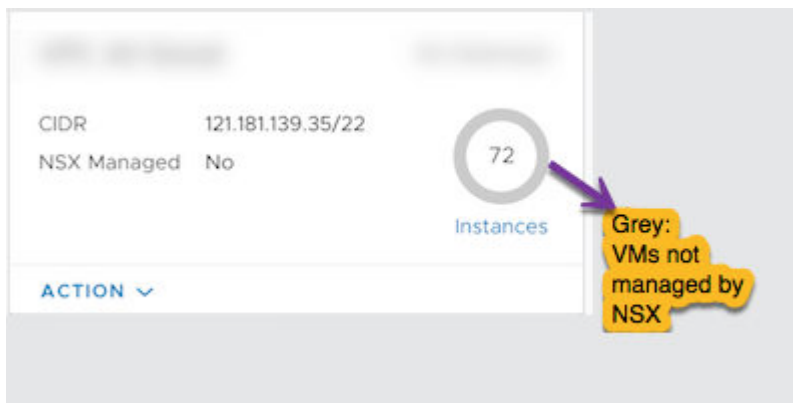


Abbildung 16-5. VNet mit VMs, die nicht von NSX Cloud verwaltet werden



Instanzen

Verwaltete Instanzen

Abbildung 16-6. Von NSX Cloud verwaltete Instanz, die sich in einem ordnungsgemäßen Systemzustand befindet

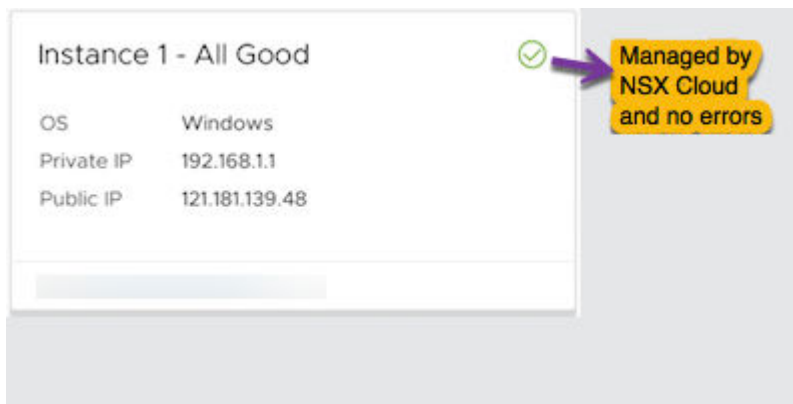


Abbildung 16-7. Von NSX Cloud verwaltete Instanz mit Fehlern

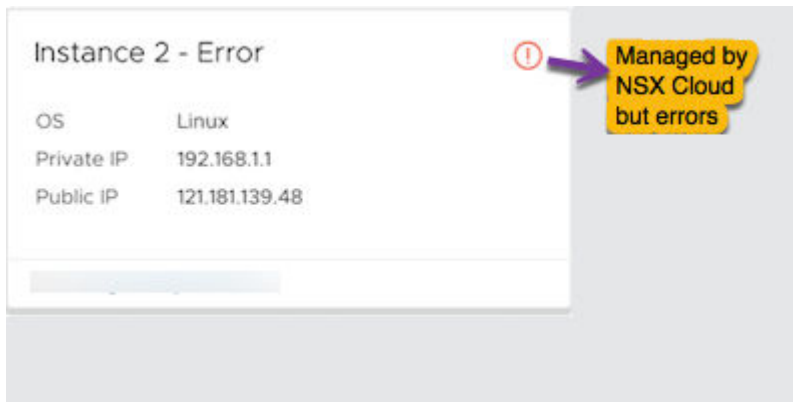


Abbildung 16-8. Von NSX Cloud verwaltete Instanz mit Fehlern und unter Quarantäne

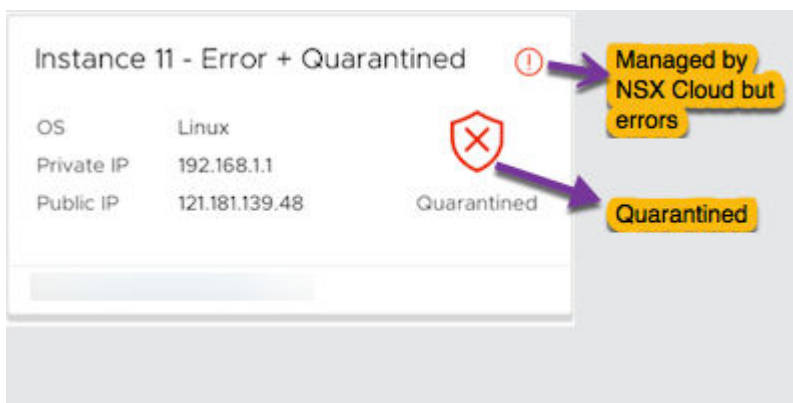


Abbildung 16-9. Von NSX Cloud verwaltete Instanz unter Quarantäne, die aber auf der Whitelist steht, solange die **vm-override-sg**-Netzwerksicherheitsgruppe zugewiesen ist

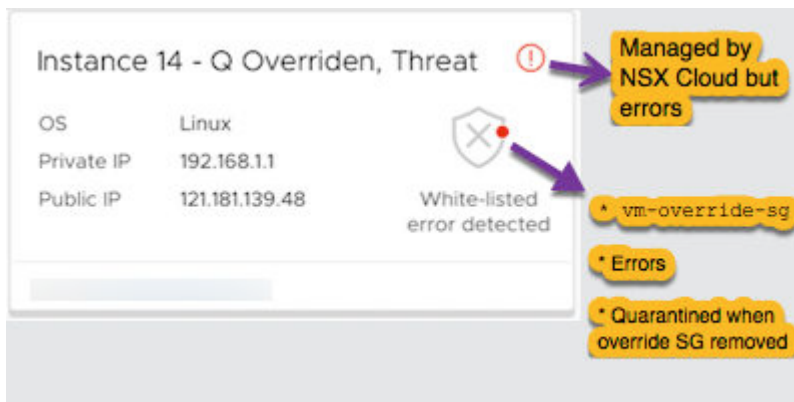
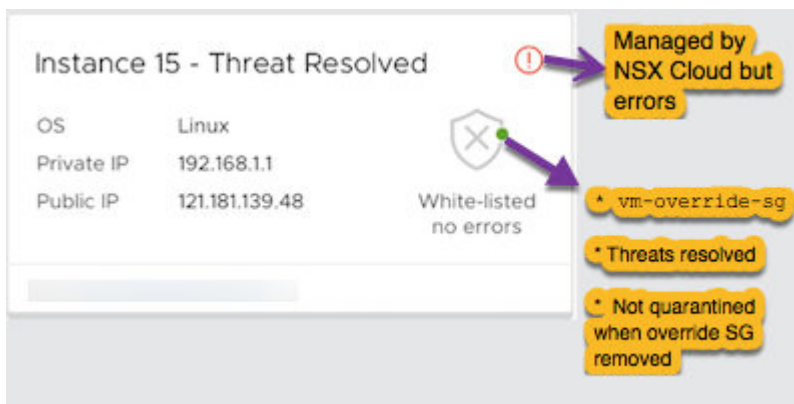


Abbildung 16-10. Von NSX Cloud verwaltete Instanz unter Quarantäne, die auf der Whitelist steht, mit behobenen Fehlern.



Nicht verwaltete Instanzen

Abbildung 16-11. VM, die nicht von NSX Cloud verwaltet wird und standardmäßig unter Quarantäne steht

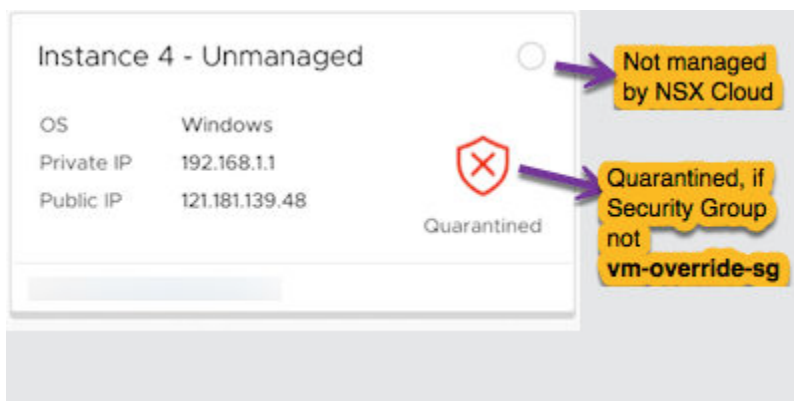
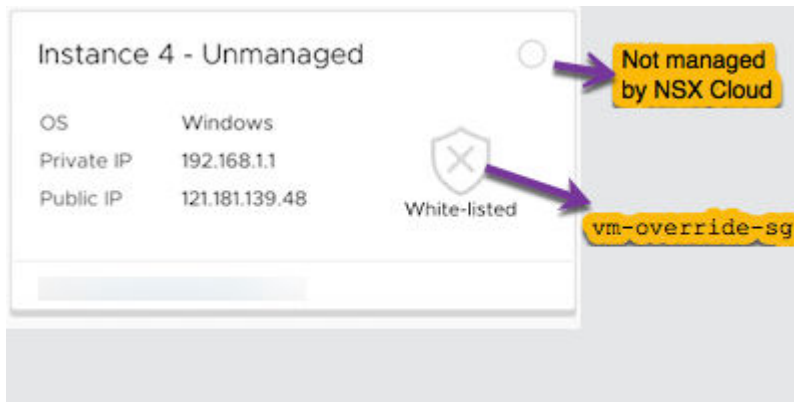


Abbildung 16-12. VM, die nicht von NSX Cloud verwaltet wird, aber auf der Whitelist steht, solange die **vm-override-sg** zugewiesen ist



Public Cloud Gateway (PCG)

Abbildung 16-13. VNet mit aktivem primärem und sekundärem PCG

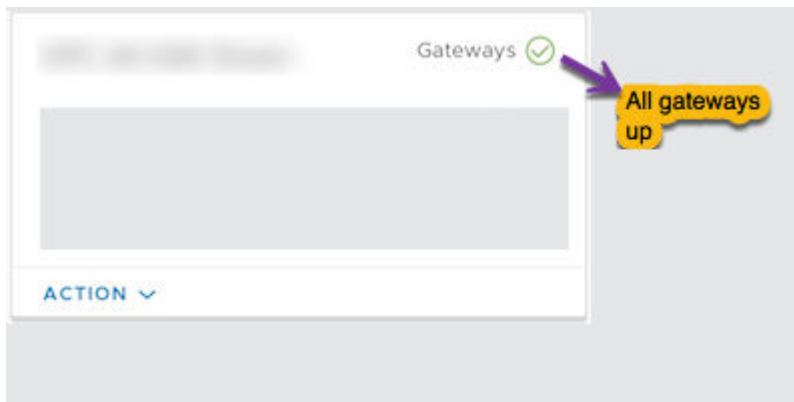


Abbildung 16-14. VNet mit inaktivem primärem oder sekundärem PCG

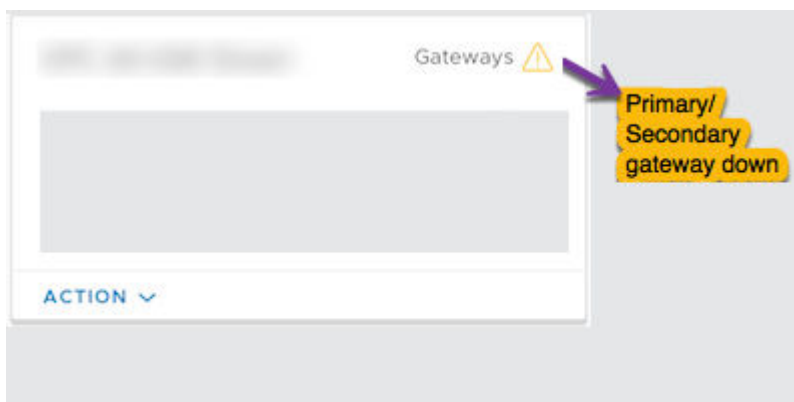
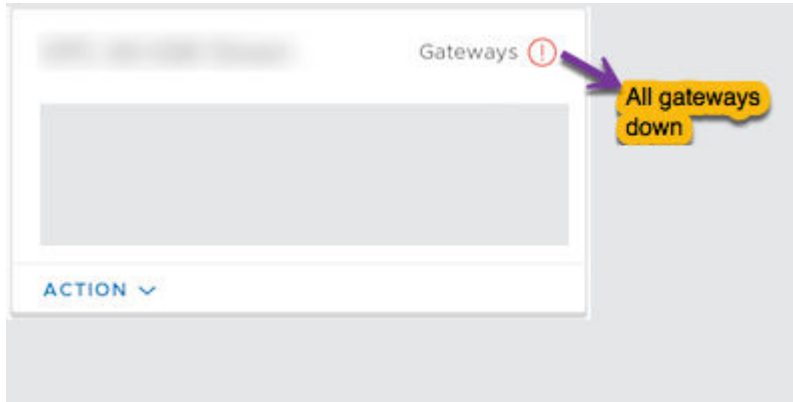


Abbildung 16-15. VNet mit inaktivem primärem und sekundärem PCG

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

Verfahren

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

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

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

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

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

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

- 5 Geben Sie Details zu NSX Manager ein.

Option	Beschreibung
NSX Manager-Hostname	Geben Sie den vollqualifizierten Domännennamen (FQDN) von NSX Manager ein, falls dieser verfügbar ist. Sie können auch die IP-Adresse von NSX Manager eingeben.
Administratoren-Anmeldedaten	Geben Sie einen Benutzernamen und ein Kennwort bei der Rolle „Enterprise-Administrator“ an.
Manager-Fingerabdruck	Geben Sie den Fingerabdruckwert von NSX Manager ein, den Sie in Schritt 2 abgerufen haben.

- 6 Klicken Sie auf **Verbinden**.

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

(Optional) Proxy-Server konfigurieren

Wenn Sie den gesamten internetgebundenen HTTP/HTTPS-Verkehr über einen zuverlässigen HTTP-Proxy routen und überwachen möchten, können Sie in CSM bis zu fünf Proxyserver konfigurieren.

Die gesamte Public Cloud-Kommunikation von PCG und CSM wird über den ausgewählten Proxyserver geleitet.

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 „Konfigurieren der Proxyserver“ die folgenden Details ein:

Option	Beschreibung
Standard	Verwenden Sie dieses Optionsfeld, um den Standard-Proxyserver anzugeben.
Profilname	Geben Sie einen Namen für das Proxyserverprofil an. Dies ist ein Pflichtfeld.
Proxyserver	Geben Sie die IP-Adresse des Proxyservers ein. Dies ist ein Pflichtfeld.
Port	Geben Sie den Port des Proxiservers ein. Dies ist ein Pflichtfeld.
Authentifizierung	Optional Wenn Sie eine zusätzliche Authentifizierung einrichten möchten, aktivieren Sie dieses Kontrollkästchen und geben Sie einen gültigen Benutzernamen und das Kennwort ein.
Benutzername	Dies ist erforderlich, wenn Sie das Kontrollkästchen „Authentifizierung“ aktivieren.
Kennwort	Dies ist erforderlich, wenn Sie das Kontrollkästchen „Authentifizierung“ aktivieren.
Zertifikat	Optional Wenn Sie ein Authentifizierungszertifikat für das Abfangen von HTTPS bereitstellen möchten, aktivieren Sie dieses Kontrollkästchen und fügen Sie das Zertifikat durch Kopieren/Einfügen in das angezeigte Textfeld ein.
Kein Proxy	Wählen Sie diese Option, wenn Sie keinen der konfigurierten Proxyserver verwenden möchten.

System > Dienstprogramme

Die folgenden Dienstprogramme stehen zur Verfügung.

Sichern und Wiederherstellen

Folgen Sie für das Sichern und Wiederherstellen von CSM den gleichen Anweisungen wie für NSX Manager. Weitere Informationen finden Sie unter [Sichern und Wiederherstellen von NSX Manager](#).

Support-Paket

Klicken Sie auf **Download**, um das Support-Paket für CSM abzurufen. Dies wird für die r-Fehlerbehebung verwendet. Weitere Informationen hierzu finden Sie im *Handbuch zur Fehlerbehebung von NSX-T Data Center*.

System > Benutzer

Benutzer werden mithilfe der rollenbasierten Zugriffssteuerung (RBAC) verwaltet.

Weitere Informationen finden Sie unter [Verwalten von Benutzerkonten und der rollenbasierten Zugriffssteuerung](#).

Verwalten der Quarantäne-Richtlinie

Informationen zum Aktivieren oder Deaktivieren von Quarantäne-Richtlinien und deren Auswirkungen auf Ihre Arbeitslast-VMs

NSX Cloud verwendet Public-Cloud-Sicherheitsgruppen zur Erkennung von Bedrohungen. Wenn beispielsweise bei aktivierter Quarantäne-Richtlinie der NSX-Agent auf einer verwalteten VM mit böswilliger Absicht gewaltsam gestoppt wird, wird die gefährdete VM mit der Sicherheitsgruppe quarantine (in Microsoft Azure) oder default (in AWS) unter Quarantäne gestellt.

Allgemeine Empfehlung:

Beginnen Sie für **Brownfield**-Bereitstellungen mit *deaktiviert* (disabled): Quarantäne-Richtlinie ist standardmäßig deaktiviert. Wenn Sie in Ihrer Public Cloud-Umgebung bereits VMs eingerichtet haben, verwenden Sie den Modus „deaktiviert“ (disabled) für die Quarantäne-Richtlinie, bis Sie Ihre Workload-VMs integrieren. Dadurch wird sichergestellt, dass Ihre vorhandenen VMs nicht automatisch in Quarantäne verschoben werden.

Beginnen Sie mit *aktiviert* (enabled) für **Greenfield**-Bereitstellungen: Für Greenfield-Bereitstellungen wird empfohlen, dass Sie die Quarantäne-Richtlinie aktivieren, damit die Bedrohungserkennung für Ihre VMs von NSX Cloud verwaltet werden kann.

Hinweis Wenn die Quarantäne-Richtlinie aktiviert ist, wenden Sie die `vm_override_sg` auf Arbeitslast-VMs an, um diese einbinden zu können, und entfernen Sie dann diese Sicherheitsgruppe, nachdem sie von NSX Cloud verwaltet werden. Entsprechende Sicherheitsgruppen werden innerhalb von zwei Minuten auf die VMs angewendet.

Quarantäne-Richtlinie aktivieren oder deaktivieren

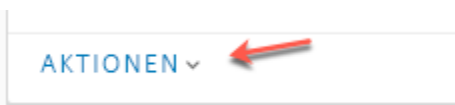
Bei der Bereitstellung von PCG haben Sie die Möglichkeit, die Quarantäne-Richtlinie zu aktivieren oder zu deaktivieren. Führen Sie diese Schritte aus, um die Quarantäne-Richtlinie anschließend zu aktivieren oder zu deaktivieren.

Voraussetzungen

Ein oder zwei PCGs müssen in Ihrer VPC oder Ihrem VNet bereitgestellt werden.

Verfahren

- 1 Melden Sie sich bei CSM an und gehen Sie zu Ihrer Public Cloud:
 - a Klicken Sie bei Verwendung von AWS auf **Clouds > AWS > VPCs**. Klicken Sie auf die VPC, auf der ein oder zwei PCGs bereitgestellt wurden und ausgeführt werden.
 - 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.
- 2 Aktivieren Sie die Option mit einer der folgenden Vorgehensweisen:
 - Klicken Sie in der Kachelansicht auf **AKTIONEN > Konfiguration bearbeiten**.



- Wenn Sie sich in der Rasteransicht befinden, aktivieren Sie das Kontrollkästchen neben der VPC oder dem VNet und klicken Sie dann auf **AKTIONEN > Konfiguration bearbeiten**.



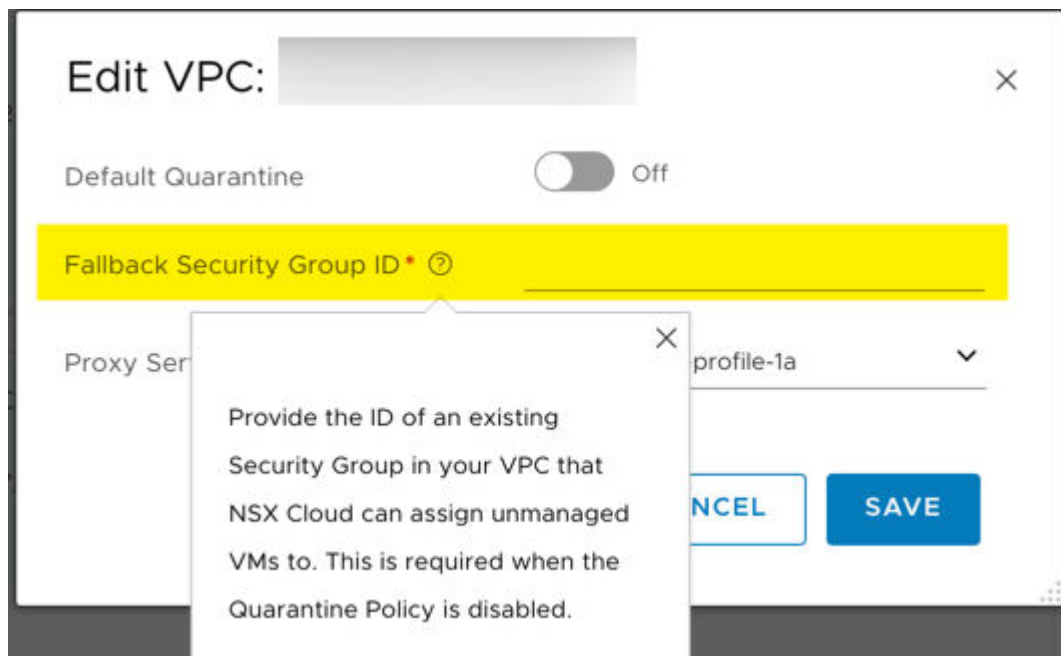
- ◆ Wenn Sie sich auf der VPC- oder VNet-Seite befinden, klicken Sie auf das Symbol „AKTIONEN“

und wählen Sie dann **Konfigurationen bearbeiten**.



- 3 Schalten Sie **Standard-Quarantäne** ein oder aus, um sie zu aktivieren oder zu deaktivieren.
- 4 Wenn Sie die Quarantäne-Richtlinie deaktivieren, müssen Sie eine Fallback-Sicherheitsgruppe einrichten.

Hinweis Die Fallback-Sicherheitsgruppe muss eine vorhandene benutzerdefinierte Sicherheitsgruppe in Ihrer Public Cloud sein. Sie können keine der NSX Cloud-Sicherheitsgruppen als Fallback-Sicherheitsgruppe verwenden. Eine Liste der NSX Cloud Sicherheitsgruppen finden Sie unter [NSX Cloud-Sicherheitsgruppen für die Public Cloud](#).



- Allen nicht verwalteten oder unter Quarantäne stehenden VMs in dieser VPC oder diesem VNet wird beim Deaktivieren der Quarantäne-Richtlinie die ihnen zugeordnete Fallback-Sicherheitsgruppe zugewiesen.
- Alle verwalteten VMs behalten die von NSX Cloud zugewiesene Sicherheitsgruppe. Wenn solche VMs nach dem Deaktivieren der Quarantäne-Richtlinie zum ersten Mal nicht mehr gekennzeichnet sind und nicht mehr verwaltet werden, erhalten auch sie die ihnen zugewiesene Fallback-Sicherheitsgruppe.

- 5 Klicken Sie auf **SPEICHERN**.

Quarantäne-Richtlinie-Auswirkungen bei Deaktivierung

Quarantäne-Richtlinie: deaktiviert

Wenn die Quarantäne-Richtlinie deaktiviert ist:

- NSX Cloud weist den in dieser VPC bzw. diesem VNet gestarteten virtuellen Maschinen keine Sicherheitsgruppen zu. Sie müssen den virtuellen Maschinen die richtigen NSX Cloud-Sicherheitsgruppen zuweisen, um die Bedrohungserkennung zu aktivieren.

Vom Microsoft Azure-Portal oder der AWS-Konsole aus:

- ■ Weisen Sie `vm-underlay-sg` VMs zu, für die Sie das von Microsoft Azure bzw. AWS bereitgestellte Underlay-Netzwerk verwenden möchten.

Quarantänerichtlinie: erst aktiviert, dann deaktiviert

In der folgenden Tabelle sind die Auswirkungen auf die Zuweisungen von Sicherheitsgruppen dargestellt, wenn die Quarantäne-Richtlinie aktiviert war und Sie sie dann deaktivieren.

Tabelle 16-1. Auswirkungen der Deaktivierung der Quarantäne-Richtlinie auf Sicherheitsgruppen

VM-ID	Verwaltet?	Sicherheitsgruppe	Sicherheitsgruppe für virtuelle Maschine, nachdem die Quarantäne-Richtlinie deaktiviert wurde
VM 1	Ja	<code>vm_underlay_sg</code>	<code>vm_underlay_sg</code> . Wenn Sie das Tag <code>nsx.network</code> von dieser VM entfernen, um sie aus der NSX-Verwaltung zu nehmen, wird dieser VM auch die ihr zugeordnete Fallback-Sicherheitsgruppe zugewiesen.
VM 2	Ja	<code>default</code> (AWS) oder <code>quarantine</code> (Microsoft Azure)	Die Fallback-Sicherheitsgruppe, die Sie beim Deaktivieren der Quarantäne-Richtlinie angeben. Weitere Informationen finden Sie unter Quarantäne-Richtlinie aktivieren oder deaktivieren .

Tabelle 16-1. Auswirkungen der Deaktivierung der Quarantäne-Richtlinie auf Sicherheitsgruppen (Fortsetzung)

VM-ID	Verwaltet?	Sicherheitsgruppe	Sicherheitsgruppe für virtuelle Maschine, nachdem die Quarantäne-Richtlinie deaktiviert wurde
VM 3	Nein	vm_override_sg	Die Fallback-Sicherheitsgruppe, die Sie beim Deaktivieren der Quarantäne-Richtlinie angeben.
VM 4	Nein	default (AWS) oder quarantine (Microsoft Azure)	Die Fallback-Sicherheitsgruppe, die Sie beim Deaktivieren der Quarantäne-Richtlinie angeben.

Hinweis Die Quarantäne-Richtlinie muss deaktiviert werden, bevor die Bereitstellung von PCG aufgehoben werden kann. Einzelheiten hierzu erhalten Sie unter **Aufhebung der Bereitstellung von PCGs** in der *Installationshandbuch für NSX-T Data Center*.

Quarantäne-Richtlinie-Auswirkungen bei Aktivierung

Quarantäne-Richtlinie: aktiviert

Wenn die Quarantäne-Richtlinie aktiviert ist:

- Die Zuweisung der Sicherheitsgruppe (SG bzw. der Netzwerk-Sicherheitsgruppe (NSG) für alle Schnittstellen für beliebige Workload-VMs, die zu dieser VPC bzw. diesem VNet gehören, wird von NSX Cloud wie folgt verwaltet:
 - Nicht verwaltete VMs werden in Microsoft Azure der NSG quarantine und in AWS der Sicherheitsgruppe default zugewiesen und in Quarantäne gestellt. Dies begrenzt den ausgehenden Datenverkehr und beendet allen eingehenden Datenverkehr zu solchen VMs.
 - Nicht verwaltete VMs können NSX-verwaltete VMs werden, wenn Sie NSX Agent auf der virtuellen Maschine installieren und Sie sie in der Public Cloud mit nsx.network taggen. Im Standardszenario weist NSX Cloud vm-underlay-sg zu, um entsprechenden eingehenden/ ausgehenden Datenverkehr zuzulassen.
 - Einer NSX-verwalteten VM kann nach wie vor die Sicherheitsgruppe quarantine oder default zugewiesen werden, und sie kann in Quarantäne gestellt werden, wenn eine Bedrohung auf der VM erkannt wird, z. B. wenn NSX Agent auf der VM angehalten wird.
 - Alle manuellen Änderungen an den Sicherheitsgruppen werden innerhalb von zwei Minuten zu der/den durch NSX festgelegten Sicherheitsgruppe(n) zurückgesetzt.

- Wenn Sie eine beliebige VM aus der Quarantäne verschieben möchten, weisen Sie `vm-override-sg` als einzige Sicherheitsgruppe für diese VM zu. NSX Cloud unterstützt keine automatische Änderung der Sicherheitsgruppe `vm-override-sg` und lässt den Zugriff auf die VM durch SSH und RDP zu. Das Entfernen von `vm-override-sg` bewirkt erneut, dass die VM-Sicherheitsgruppe(n) auf die durch NSX festgelegte Sicherheitsgruppe zurückgesetzt wird/werden.

Hinweis Wenn die Quarantäne-Richtlinie aktiviert ist, weisen Sie Ihren VMs `vm-override-sg` zu, bevor Sie NSX Agent darauf installieren. Nachdem Sie den Installationsprozess von NSX Agent abgeschlossen und die VM als „Underlay“ markiert haben, entfernen Sie die NSG `vm-override-sg` aus der VM. NSX Cloud weist den von NSX verwalteten VMs anschließend automatisch die richtige Sicherheitsgruppe zu. Dieser Schritt ist notwendig, weil er sicherstellt, dass der VM nicht die Sicherheitsgruppe `quarantine` oder `default` zugewiesen wird, während Sie sie für NSX Cloud vorbereiten.

Quarantäne-Richtlinie: erst deaktiviert, dann aktiviert

In der folgenden Tabelle sind die Auswirkungen auf die Zuweisungen von Sicherheitsgruppen dargestellt, wenn die Quarantäne-Richtlinie deaktiviert war und Sie sie dann aktivieren.

Tabelle 16-2. Auswirkungen der Aktivierung der Quarantäne-Richtlinie auf Sicherheitsgruppen

VM-ID	Verwalte t?	Bedrohung erkannt?	Sicherheitsgruppe nach der Aktivierung der Quarantäne-Richtlinie
VM 1	Ja	Nein	<code>vm_underlay_sg</code>
VM 2	Ja	Ja	<code>default</code> (AWS) oder <code>quarantine</code> (Microsoft Azure)
Hinweis Sie können <code>vm_override_sg</code> manuell verwalteten VMs zuweisen. Dadurch wird der Quarantäne-Modus für sie beendet und Sie können das Problem beheben, indem Sie über SSH oder RDP auf diese VMs zugreifen. Siehe Quarantäne-Richtlinie: aktiviert .			
VM 3	Nein	Nicht verfügbar	<code>default</code> (AWS) oder <code>quarantine</code> (Microsoft Azure)

NSX Cloud-Sicherheitsgruppen für die Public Cloud

Die folgenden Sicherheitsgruppen werden von NSX Cloud bei der Bereitstellung von PCG erstellt.

Die Sicherheitsgruppen **gw** werden auf die entsprechenden PCG-Schnittstellen angewendet.

Tabelle 16-3. Von NSX Cloud für PCG-Schnittstellen erstellte Public-Cloud-Sicherheitsgruppen

Name der Sicherheitsgruppe	Verfügbar in Microsoft Azure?	Verfügbar in AWS?	Vollständiger Name
gw-mgmt-sg	Ja	Ja	Gateway-Management-Sicherheitsgruppe
gw-uplink-sg	Ja	Ja	Gateway-Uplink-Sicherheitsgruppe
gw-vtep-sg	Ja	Ja	Gateway-Downlink-Sicherheitsgruppe

Tabelle 16-4. Von NSX Cloud für Workload-VMs erstellte Public Cloud-Sicherheitsgruppen

Name der Sicherheitsgruppe	Verfügbar in Microsoft Azure?	Verfügbar in AWS?	Beschreibung
quarantine	Ja	Nein	Quarantäne-Sicherheitsgruppe für Microsoft Azure
default	Nein	Ja	Quarantäne-Sicherheitsgruppe für AWS
vm-underlay-sg	Ja	Ja	Nicht-Overlay-VM-Sicherheitsgruppe
vm-override-sg	Ja	Ja	Überschreiben-VM-Sicherheitsgruppe
vm-overlay-sg	Ja	Ja	Overlay-VM-Sicherheitsgruppe (diese wird in der aktuellen Version nicht verwendet)
vm-outbound-bypass-sg	Ja	Ja	Ausgehende VM-Bypass-Sicherheitsgruppe (diese wird in der aktuellen Version nicht verwendet)
vm-inbound-bypass-sg	Ja	Ja	Eingehende VM-Bypass-Sicherheitsgruppe (diese wird in der aktuellen Version nicht verwendet)

Überblick über Onboarding und Verwaltung von Workload-VMs

Eine Übersicht des Onboarding-Workflow finden Sie in den Flussdiagrammen in Ihrer Public Cloud.

Unter [Installieren von NSX Cloud-Komponenten](#) im *Installationshandbuch für NSX-T Data Center* finden Sie Informationen zum Tag-0-Workflow.

Unterstützte Betriebssysteme

Dies ist die Liste der derzeit von NSX Cloudunterstützten Betriebssysteme für Ihre Workload-VM.

Derzeit werden die folgenden Betriebssysteme unterstützt:

Hinweis Im *Versionshinweise für NSX-T Data Center* erhalten Sie im Abschnitt „Bekannte Probleme bei NSX Cloud“ Informationen zu Ausnahmen.

- Red Hat Enterprise Linux (RHEL) 7.2, 7.3, 7.4, 7.5
- CentOS 7.2, 7.3, 7.4, 7.5
- Oracle Enterprise Linux 7.2, 7.3, 7.4 (Unbreakable Enterprise Kernel-Versionen nicht unterstützt)

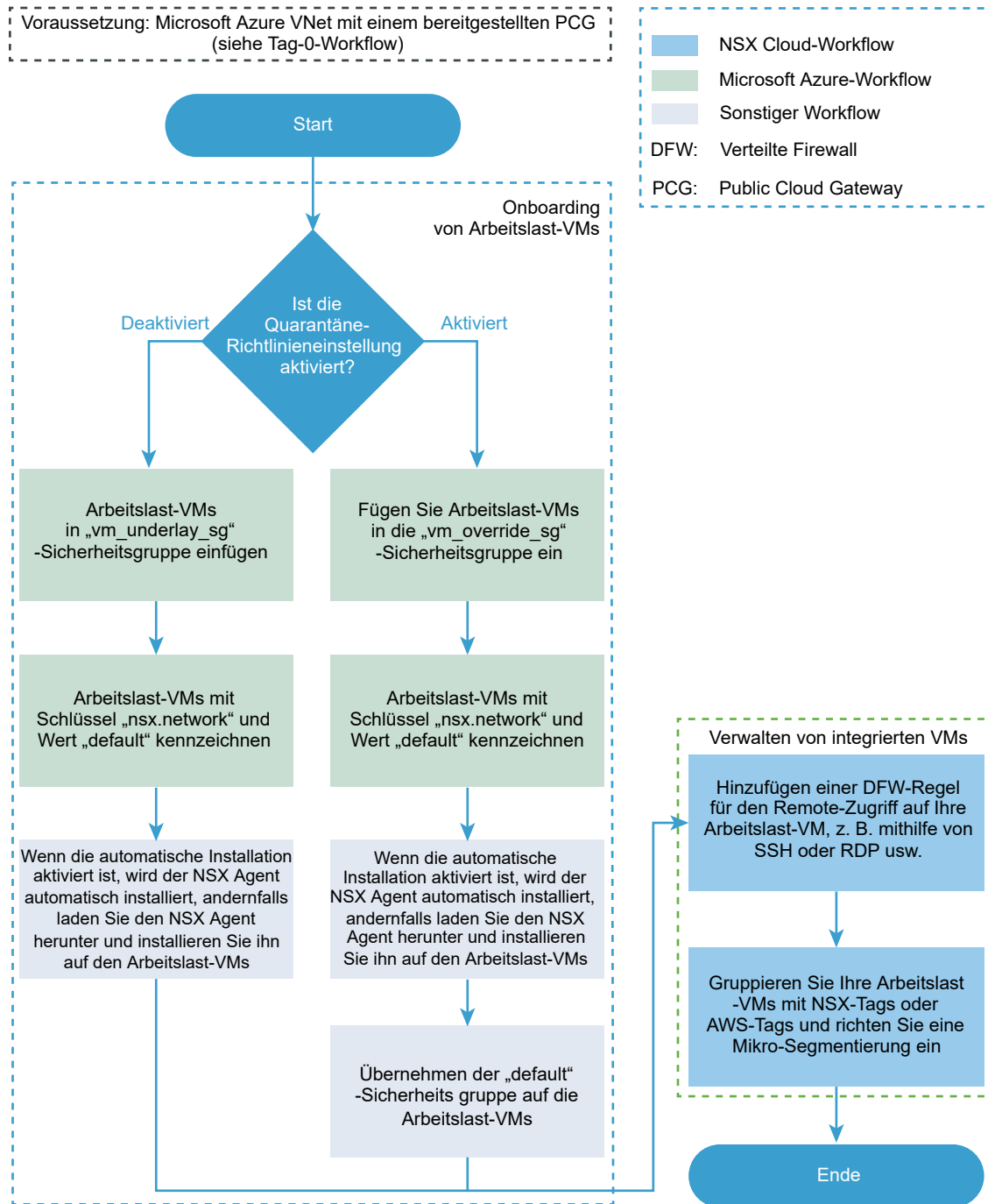
Hinweis SE Linux wird für Oracle Enterprise Linux, Red Hat Enterprise Linux und CentOS nicht unterstützt.

- Ubuntu 14.04, 16.04
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

Einbinden von Arbeitslast-VMs von Microsoft Azure

In diesem Flussdiagramm finden Sie eine Übersicht über die Schritte zum Onboarding von Arbeitslast-VMs von Microsoft Azure.

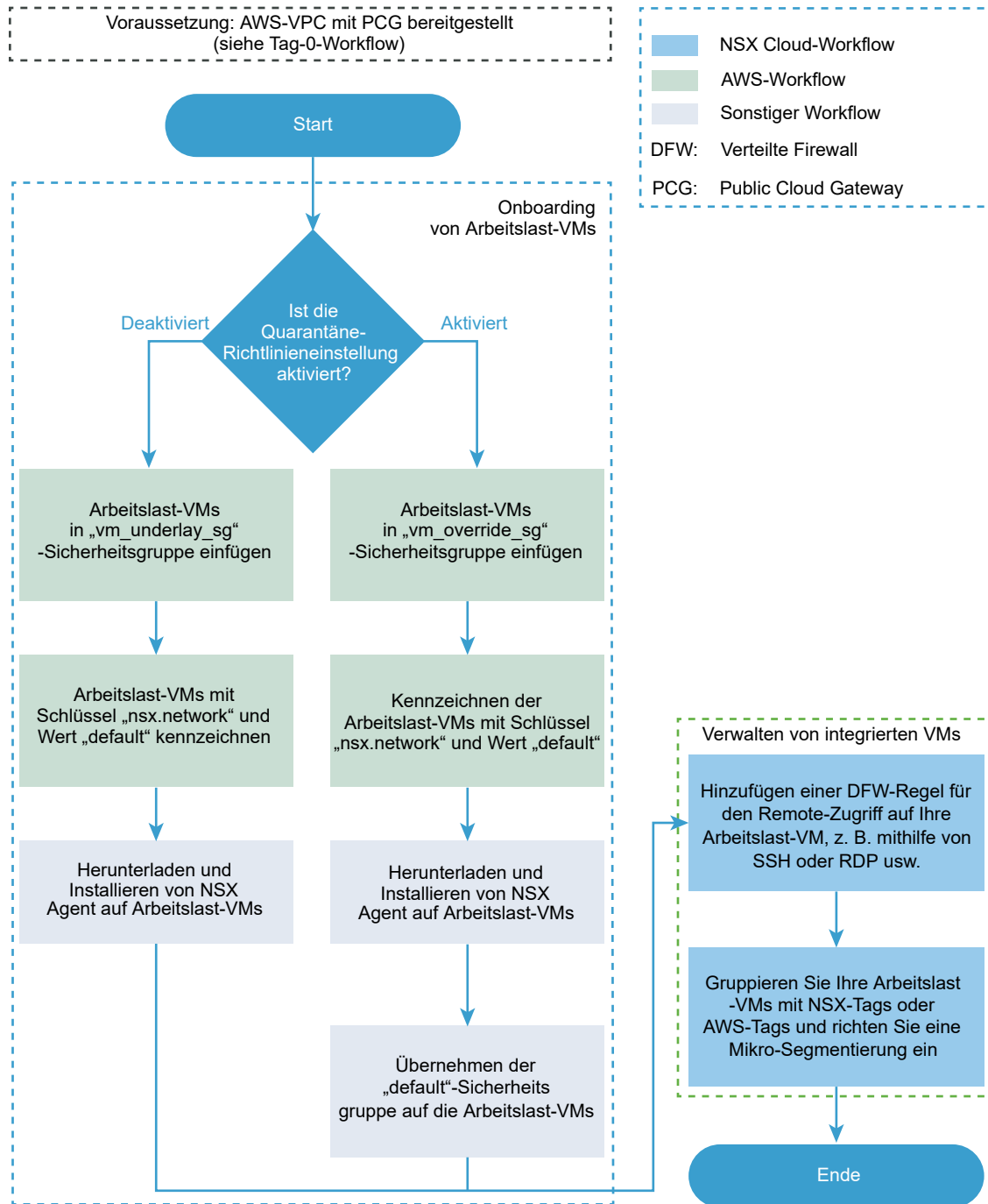
Abbildung 16-16. Tag-N-Onboarding-Workflow für Microsoft Azure



Onboarding von Arbeitslast-VMs von AWS

In diesem Flussdiagramm finden Sie eine Übersicht über die Schritte zum Onboarding von Arbeitslast-VMs von AWS.

Abbildung 16-17. Tag-N-Onboarding-Workflow für AWS



Onboarden von Workload-VMs

Integrieren Sie Ihre Arbeitslast-VMs, um sie mithilfe von NSX-T Data Center zu verwalten.

Taggen von virtuellen Maschinen in der Public Cloud

Wenden Sie das Tag **nsx.network** auf die VMs an, die Sie mithilfe von NSX-T Data Center verwalten möchten.

Voraussetzungen

Die VPC oder das VNet, in denen die Arbeitslast-VMs gehostet werden, muss mit NSX Cloud integriert sein. Weitere Informationen finden Sie unter **Hinzufügen Ihrer Public-Cloud-Bestandsliste** in *Installationshandbuch für NSX-T Data Center*.

Verfahren

- 1 Melden Sie sich bei Ihrem Public-Cloud-Konto an und navigieren Sie zu Ihrer VPC oder Ihrem VNet, die/das mit NSX Cloud integriert wurde.
- 2 Wählen Sie die VMs, die Sie mithilfe von NSX-T Data Center verwalten möchten.
- 3 Fügen Sie die folgenden Tag-Details für die VMs hinzu und speichern Sie Ihre Änderungen.

```
Name: nsx.network
Value: default
```

Hinweis Sie können dieses Tag entweder auf VM-Ebene oder auf der Ebene der Schnittstelle anwenden – beides hat denselben Effekt.

Beispiel

Nächste Schritte

Installieren Sie den NSX Agent auf diesen VMs. Siehe [Installieren von NSX Agent](#).

Wenn Sie Microsoft Azure verwenden, können Sie den NSX Agent automatisch auf gekennzeichneten VMs installieren. Weitere Informationen finden Sie unter [Automatische Installation von NSX Agent](#).

Installieren von NSX Agent

Installieren von NSX Agent auf Ihren Workload-VMs

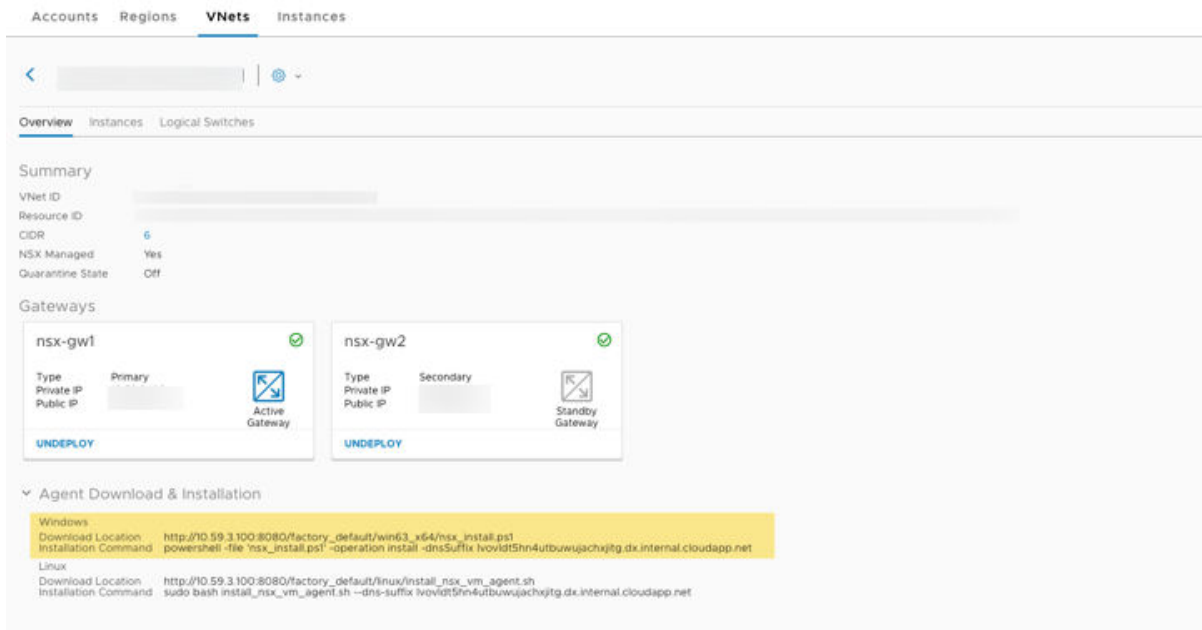
Installieren von NSX Agent auf virtuellen Windows-Maschinen

Folgen Sie diesen Anweisungen, um NSX Agent auf Ihrer Windows-Workload-VM zu installieren.

Unter [Unterstützte Betriebssysteme](#) finden Sie eine Liste der Microsoft Windows-Versionen, die gegenwärtig unterstützt werden.

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 VPC, auf der ein oder zwei PCGs bereitgestellt wurden und ausgeführt werden.
 - 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.
- 2 Notieren Sie sich im Bildschirmabschnitt **Agent Download & Installation** den **Downloadspeicherort** und den **Installationsbefehl** unter **Windows**.



Hinweis Das DNS-Suffix im **Installationsbefehl** wird passend zu den DNS-Einstellungen, die Sie beim Bereitstellen von PCG auswählen, dynamisch generiert.

- 3 Stellen Sie als Administrator eine Verbindung mit Ihrer Windows-Workload-VM her.
- 4 Laden Sie das Installationsskript von dem **Downloadspeicherort**, den Sie sich aus CSM notiert haben, auf Ihre virtuelle Windows-Maschine herunter. Sie können einen beliebigen Browser, beispielsweise Internet Explorer, verwenden, um das Skript herunterzuladen. Es wird in das Download-Standardverzeichnis Ihres Browsers, z. B. *C:\Downloads* heruntergeladen.
- 5 Öffnen Sie eine PowerShell-Eingabeaufforderung und wechseln Sie zu dem Verzeichnis, das das heruntergeladene Skript enthält.

- 6 Verwenden Sie zum Ausführen des heruntergeladenen Skripts den **Installationsbefehl**, den Sie aus CSM notiert haben.

Beispiel:

```
c:\> powershell -file 'nsx_install.ps1' -operation install -dnsSuffix <>
```

Hinweis Das Dateiarargument benötigt den vollständigen Pfad, sofern Sie sich nicht in demselben Verzeichnis befinden oder wenn sich das PowerShell-Skript bereits unter diesem Pfad befindet. Wenn Sie das Skript beispielsweise in *C:\Downloads* herunterladen und Sie sich momentan noch nicht in diesem Verzeichnis befinden, dann muss das Skript folgenden Speicherort enthalten:
powershell -file 'C:\Downloads\nsx_install.ps1'...

- 7 Das Skript wird ausgeführt, und wenn dies abgeschlossen ist, wird eine Meldung angezeigt, die angibt, ob NSX Agent erfolgreich installiert wurde.

Hinweis Für das Skript ist die primäre Netzwerkschnittstelle die Standardeinstellung.

Eine Liste aller Skriptoptionen und Anweisungen für die Deinstallation finden Sie unter [NSX Agent-Installationsskript-Optionen für Windows-VMs](#).

Nächste Schritte

[Verwalten von Workload-VMs](#)

Installieren von NSX Agent auf virtuellen Linux-Maschinen

Befolgen Sie diese Anweisungen, um NSX Agent auf Ihren Linux-Workload-VMs zu installieren.

Unter [Unterstützte Betriebssysteme](#) finden Sie eine Liste der aktuell unterstützten Linux-Distributionen.

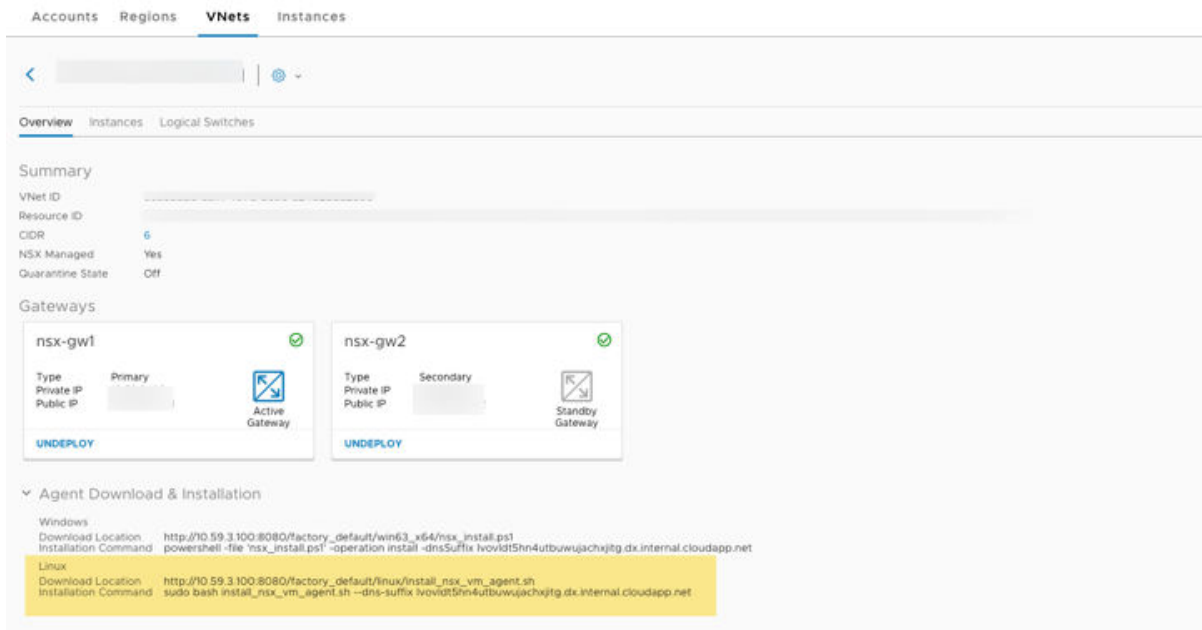
Voraussetzungen

Sie benötigen die Befehle **wget** und **nslookup**, um das Installationsskript für NSX Agent auszuführen.

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 VPC, auf der ein oder zwei PCGs bereitgestellt wurden und ausgeführt werden.
 - 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.

- Notieren Sie sich im Bildschirmabschnitt **Agent Download & Installation** den **Downloadspeicherort** und den **Befehl zur Installation** unter **Linux**.



Hinweis Das DNS-Suffix im Installationsbefehl wird in Übereinstimmung mit den DNS-Einstellungen, die Sie beim Bereitstellen von PCG auswählen, dynamisch generiert.

- Melden Sie sich bei der Linux-Workload-VM mit Superuser-Rechten an.
- Verwenden Sie `wget` oder einen vergleichbaren Befehl zum Herunterladen des Installationsskripts auf Ihre virtuelle Linux-Maschine von dem **Downloadspeicherort**, den Sie sich aus CSM notiert haben. Das Installationsskript wird in das Verzeichnis heruntergeladen, in dem Sie den Befehl `wget` ausführen.
- Ändern Sie gegebenenfalls Berechtigungen für das Installationsskript, um es ausführbar zu machen, und führen Sie es aus:

```
$ sudo chmod +x install_nsx_vm_agent.sh
$ sudo bash install_nsx_vm_agent.sh --dns-suffix <>
```

Hinweis: SELinux wird unter Red Hat Enterprise Linux und dessen Derivaten nicht unterstützt. Deaktivieren Sie SELinux, um den NSX-Agent zu installieren.

- Nach dem Start der Installation von NSX Agent geht die Verbindung mit Ihrer Linux-VM verloren. Meldungen wie die folgende werden auf dem Bildschirm angezeigt: `Installation completed!!! Starting NSX Agent service. SSH connection will now be lost..` Stellen Sie wieder eine Verbindung mit Ihrer VM her, um den Onboarding-Vorgang abzuschließen.

Ergebnisse

Der NSX Agent wird auf Ihren Workload-VMs installiert.

Hinweis

- Nachdem der NSX Agent erfolgreich installiert wurde, wird der Port 8888 auf der VM als offen angezeigt, ist aber für VMs im Underlay-Modus blockiert und sollte nur verwendet werden, wenn er für die erweiterte Fehlerbehebung benötigt wird.
- Das Skript verwendet eth0 als die Standardschnittstelle. Eine Liste der Skriptoptionen und Anweisungen für die Deinstallation finden Sie unter [Optionen für das NSX Agent-Installationsskript auf Linux-VMs](#).

Nächste Schritte

[Verwalten von Workload-VMs](#)

NSX Agent-Installationsskript-Optionen und -Deinstallation

Das NSX-Agent-Installationsskript bietet konfigurierbare Optionen. Diese Tabelle listet diese Optionen auf.

NSX Agent-Installationsskript-Optionen für Windows-VMs

Tabelle 16-5.

Option	Beschreibung
<code>--gateway <ip dns></code>	<p>IP-Adresse oder DNS-Name der NSX Public Cloud Gateway-Komponente</p> <p>Geben Sie diese Option an, wenn Sie eine IP-Adresse für das PCG verwenden möchten. Der Standard-DNS-Name des PCG wird verwendet, wenn dieser Parameter nicht angegeben ist.</p> <ul style="list-style-type: none"> ■ PCG DNS-Name in AWS: <code>nsx-gw.vmware.local</code> ■ PCG DNS-Name in Microsoft Azure: <code>nsx-gw</code> <p>Hinweis Geben Sie im HA-Modus von PCGs die Option „--gateway“ mit beiden PCG-Namen an. Bei einer virtuellen Microsoft Azure-Maschine würden Sie zum Beispiel Folgendes angeben: <code>--gateway "nsx-gw1;nsx-gw2"</code></p>
<code>--noStart true</code>	<p>Sie können eine VHD der VM erstellen, nachdem NSX Agent darauf installiert wurde. Führen Sie das Installationsskript mit dieser Option aus. Erstellen Sie anschließend aus dem Microsoft Azure-Portal eine VHD dieser VM.</p>
<code>--downloadPath <path></code>	<p>Dies ist der Pfad zu dem Verzeichnis, in das die Dateien heruntergeladen werden sollten. Wenn der Pfad Escape-Zeichen enthält, schließen Sie diese in einfache Anführungszeichen ein.</p> <p>Standard = <code>%temp%</code></p>
<code>--silentInstall <true/false></code>	<p>Wenn dies auf <code>true</code> eingestellt ist, führt das Skript eine Hintergrundinstallation aus.</p> <p>Der Standardwert lautet <code>false</code>.</p>

Tabelle 16-5. (Fortsetzung)

Option	Beschreibung
<code>-noSigCheck <true/false></code>	Dadurch können Sie angeben, ob die Signaturen für die Binärdateien überprüft werden sollen. Standard = <code>false</code>
<code>-logLevel <value></code>	Dadurch können Sie die Protokollebene für NSX-Komponenten angeben Standard = 1 Ausführlich = 3
<code>-operation <install/uninstall></code>	So können Sie den durchzuführenden Vorgang angeben: <code>install</code> oder <code>uninstall</code> Standard = <code>install</code>
<code>-bundlePath <path></code>	So können Sie den lokalen Pfad zum NSX-VM-Agent-Paket angeben Standardoption ist, das Paket von PCG herunterzuladen.

Deinstallieren von NSX Agent von einer Windows-VM

- 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
```

Optionen für das NSX Agent-Installationsskript auf Linux-VMs**Tabelle 16-6.**

Option	Beschreibung
<code>--gateway <ip dns></code>	IP-Adresse oder DNS-Name der NSX Public Cloud Gateway-Komponente Geben Sie diese Option an, wenn Sie eine IP-Adresse für das PCG verwenden möchten. Der Standard-DNS-Name des PCG wird verwendet, wenn dieser Parameter nicht angegeben ist. <ul style="list-style-type: none"> ■ PCG DNS-Name in AWS: <code>nsx-gw.vmware.local</code> ■ PCG DNS-Name in Microsoft Azure: <code>nsx-gw</code> Hinweis Geben Sie im HA-Modus von PCGs die Option „ <code>--gateway</code> “ mit beiden PCG-Namen an. Bei einer virtuellen Microsoft Azure-Maschine würden Sie zum Beispiel Folgendes angeben: <code>--gateway "nsx-gw1;nsx-gw2"</code>
<code>--no-start</code>	Sie können eine VHD der VM erstellen, nachdem NSX Agent darauf installiert wurde. Führen Sie das Installationsskript mit dieser Option aus. Erstellen Sie anschließend aus dem Microsoft Azure-Portal eine VHD dieser VM.
<code>--uninstall</code>	Führen Sie das Skript mit dieser Option aus, um NSX Agent zu deinstallieren.

Automatische Installation von NSX Agent

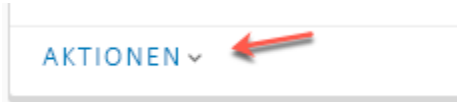
Wird derzeit nur für Microsoft Azure unterstützt.

Wenn die folgenden Kriterien erfüllt sind, wird der NSX-Agent in Microsoft Azure automatisch installiert:

- Azure-VM-Erweiterungen, die auf den virtuellen Maschinen im VNet installiert sind, werden NSX Cloud hinzugefügt. Weitere Informationen erhalten Sie in der [Microsoft Azure-Dokumentation zu VM-Erweiterungen](#).
- Mit `nsx.network` und dem Wert `default` getaggte VMs.

So aktivieren Sie diese Funktion:

- 1 Klicken Sie auf **Clouds > Azure > VNets**.
- 2 Wählen Sie das VNet aus, auf dessen virtuellen Maschinen NSX Agent automatisch installiert werden soll.
- 3 Aktivieren Sie die Option mit einer der folgenden Vorgehensweisen:
 - Klicken Sie in der Kachelansicht auf **AKTIONEN > Konfiguration bearbeiten**.



- In der Rasteransicht aktivieren Sie das Kontrollkästchen neben dem VNet. Klicken Sie dann auf

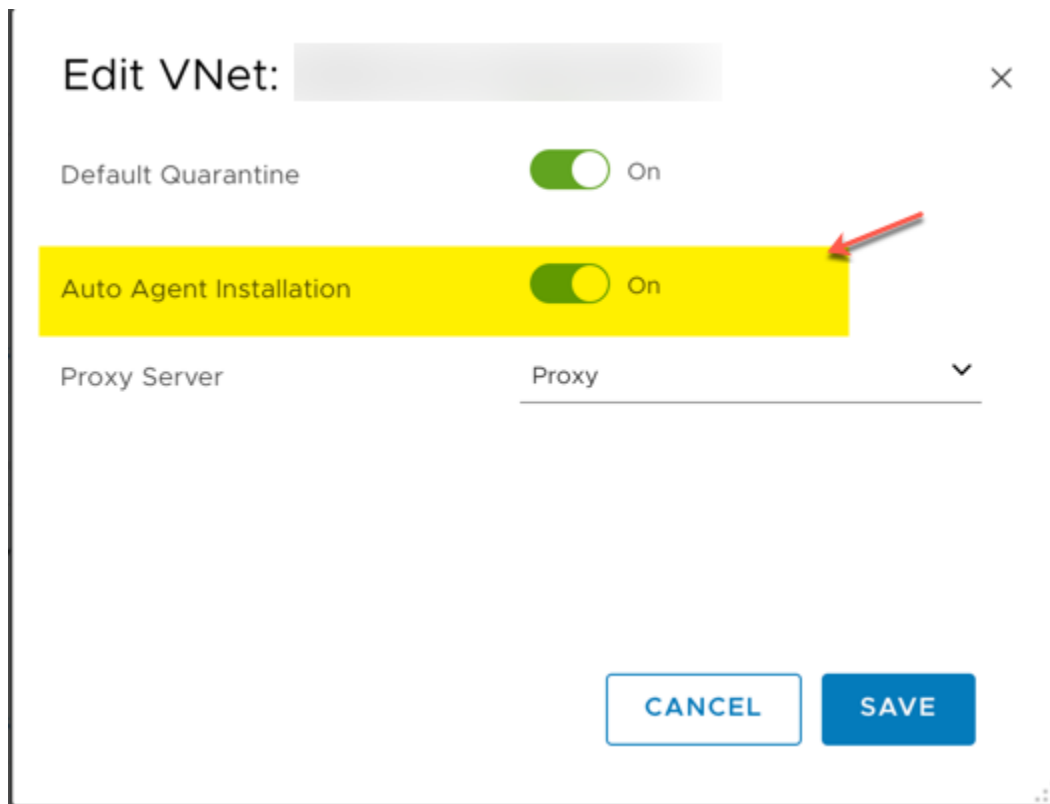
AKTIONEN > Konfiguration bearbeiten.



- Klicken Sie auf der Seite des VNet auf das Symbol „AKTIONEN“ und wählen Sie dann

Konfigurationen bearbeiten.





Verwalten von Workload-VMs

Nachdem Sie erfolgreich Workload-VMs integriert haben, können Sie NSX-T Data Center dazu verwenden, diese zu verwalten.

Auf verwaltete Workload-VMs zugreifen

Folgen Sie diesem Workflow, um auf verwaltete VMs im Underlay-Modus zuzugreifen.

Zum Zeitpunkt der Bereitstellung von PCG auf Ihrer VPC oder Ihrem VNet erstellt NSX Cloud standardmäßige Firewallregeln, um die Sicherheit Ihrer Workload-VMs zu verbessern.

Um auf verwaltete Workload-VMs im Underlay-Modus zuzugreifen, müssen Sie eine Regel für verteilte Firewalls (Distributed Firewall, DFW) hinzufügen, die Zugriff auf die virtuelle Maschine gewährleistet.

Gehen Sie wie folgt vor:

- 1 Öffnen Sie die NSX Manager-Konsole.
- 2 Wechseln Sie zu **Firewall > Allgemein > Regel hinzufügen**

- 3 Fügen Sie eine Regel mit den folgenden Konfigurationen hinzu. Detaillierte Anweisungen finden Sie unter [Hinzufügen einer Firewallregel](#).

Tabelle 16-7.

Option	Beschreibung
Name	Geben Sie einen Namen an, um den Zweck dieser Regel zu definieren, z. B. AllowRemoteAccessToUnderlay .
Quelle	Wählen Sie Beliebig aus.
Ziel	Wählen Sie den logischen Switch oder Port oder die NS-Gruppe (NSGroup), mit dem diese VM verbunden bzw. deren Mitglied sie ist.
Dienste	Wählen Sie Remote-Zugriff-Dienste für diese Workload-VM, z. B. SSH für Linux oder RDP für Windows.
Aktion	Wählen Sie Zulassen .

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 Workload-VMs angewendeten Public-Cloud-Tags unter der Voraussetzung, dass sie die vordefinierten Kriterien für Größe und reservierte Wörter erfüllen, in NSX Manager.

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
- aws:vpc
- aws:availabilityzone
- **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 Präfix **dis:azure:** versehen, um anzuzeigen, dass Microsoft Azure sie ermittelt hat.

Wenn Sie beliebige Änderungen an den Tags in der Public Cloud vornehmen, werden die Änderungen in NSX Manager innerhalb von zwei Minuten 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 16-8. Zusammenfassung der Tag-Typen und Einschränkungen

Tag-Typ	Tag-Geltungsbereich oder vorab festgelegtes Präfix	Einschränkungen	Enterprise-Administrator Berechtigungen	Auditor Berechtigungen
Systemdefiniert	Vollständige System-Tags: <ul style="list-style-type: none"> ■ azure:subscription_id ■ azure:region ■ azure:vm_rg ■ azure:vnet_name ■ azure:vnet_rg ■ aws:vpc ■ aws:availabilityzone 	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: dis:azure: Präfix für AWS-Tags, die von Ihrem VPC importiert werden: dis:aws:	Geltungsbereich (Schlüssel): 20 Zeichen Tag (Wert): 65 Zeichen Zulässiger Maximalwert: unbegrenzt <hr/> Hinweis Die Grenzwerte für Zeichen schließen das Präfix dis:<public cloud name> aus. Tags, die diese Grenzwerte überschreiten, werden in NSX Manager nicht wiedergegeben. <hr/> Tags mit dem Präfix nsx 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 16-8. 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"> das Scope- (Schlüssel-)Präfix dis:azure: oder dis:aws: derselbe Geltungsbereich (Schlüssel) wie System-Tags 			

Beispiele ermittelter Tags

Hinweis Tags liegen im Format **key=value** für die Public Cloud und **scope=tag** in NSX Manager vor.

Tabelle 16-9.

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=AbcdefghijklmnopqrstuvwxyzAb23690hgjguytreswqacvbcdefghijklmnopqrstuvwxyz	Nein (Wert überschreitet 65 Zeichen)	keine
nsx.name=Tester	Nein (Schlüssel hat das Präfix nsx)	keine

Wie Sie Tags in NSX Manager verwenden

- Siehe [Verwalten von Tags für eine virtuelle Maschine](#).
- Siehe [Suchen nach Objekten](#).
- Siehe [Einrichten von Mikro-Segmentierung für Workload-VMs](#).

Einrichten von Mikro-Segmentierung für Workload-VMs

Sie können die Mikro-Segmentierung für verwaltete Workload-VMs einrichten.

Führen Sie folgende Schritte aus, um Regeln für verteilte Firewalls auf integrierte Workload-VMs anzuwenden:

- 1 Erstellen Sie mithilfe des VM-Namens oder der Tags oder sonstiger Kriterien für die Mitgliedschaft NSGroups (NS-Gruppen), z. B. die Ebenen **web**, **app**, **DB**. Eine Anleitung dafür finden Sie unter [Erstellen einer NS-Gruppe](#).

Hinweis Sie können die folgenden Tags für die Kriterien für Mitgliedschaft verwenden. Weitere Informationen 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
-

- 2 Erstellen Sie einen Firewallregelabschnitt und wenden Sie diesen auf NS-Gruppen (NSGroups) an, sofern dies erforderlich ist. Siehe [Hinzufügen eines Firewallregelabschnitts](#).
- 3 Erstellen Sie Firewallregeln und verwenden Sie NS-Gruppen (NSGroups) für Quelle und Ziel gemäß den Anforderungen Ihrer Sicherheitsrichtlinie. Siehe [Hinzufügen einer Firewallregel](#).

Diese Mikro-Segmentierung wird wirksam, wenn der Bestand entweder manuell erneut über CSM synchronisiert wird oder innerhalb von etwa zwei Minuten, wenn die Änderungen von Ihrer Public Cloud in CSM übertragen werden.

Verwendung von NSX-T Data Center-Funktionen mit der Public Cloud

NSX Cloud erstellt eine Netzwerktopologie für Ihre Public Cloud und Sie dürfen die automatisch generierten logischen NSX-T Data Center-Entitäten nicht bearbeiten oder löschen.

Verwenden Sie diese Liste als Kurzreferenz für automatisch generierte Funktionen und die Verwendung von NSX-T Data Center-Funktionen, wie sie für die Public Cloud gelten.

NSX Manager-Konfigurationen

Die folgenden Entitäten werden automatisch im NSX Manager erstellt:

Wichtig Bearbeiten oder löschen Sie keine dieser automatisch erstellten Entitäten.

- Ein Edge-Knoten mit dem Namen **Public Cloud Gateway** (PCG) wird erstellt.
- Der PCG-Knoten wird dem Edge-Cluster hinzugefügt. Bei einer Hochverfügbarkeitsbereitstellung gibt es zwei PCG.
- Das PCG (oder PCGs) wird als Transportknoten mit zwei erstellten Transportzonen registriert.
- Zwei logische Standard-Switches werden erstellt.
- Ein logischer Ebene-0-Router wird erstellt.
- Ein IP-Ermittlungsprofil wird erstellt. Dies wird für logische Overlay-Switches verwendet.

- Ein DHCP-Profil wird erstellt. Dies wird für DHCP-Server verwendet.

Hinweis Obwohl das DHCP-Profil erstellt wird, wird es in der aktuellen Version nicht unterstützt, da es für Overlay-Netzwerke verwendet wird.

- Es wird eine standardmäßige NS-Gruppe mit dem Namen **PublicCloudSecurityGroup** erstellt, die die folgenden Mitglieder hat:
 - Der logische Standard-VLAN-Switch
 - Logische Ports, jeweils einer für die PCG-Uplink-Ports, wenn Sie HA aktiviert haben
 - IP-Adresse
- Es werden drei Regeln für verteilte Firewalls erstellt:
 - LogicalSwitchToLogicalSwitch
 - LogicalSwitchToAnywhere
 - AnywhereToLogicalSwitch

Hinweis Diese DFW-Regeln blockieren den gesamten Datenverkehr und müssen entsprechend Ihren spezifischen Anforderungen angepasst werden.

Verifizieren Sie diese Konfigurationen in NSX Manager:

- 1 Klicken Sie im Dashboard NSX Cloud auf **NSX Manager**.
- 2 Navigieren Sie zu **Fabric > Knoten > Edges**. Sie sollten **PCG -<Ihr-VPC-oder-VNet-Name>** als Edge-Knoten sehen.

Hinweis Verifizieren Sie, dass Bereitstellungsstatus, Manager-Verbindung und Controller-Verbindung verbunden sind (Status zeigt **Up** mit einem grünen Punkt).

- 3 Navigieren Sie zu **Fabric > Knoten > Edge-Cluster**, um zu überprüfen, ob die **PCG-Cluster -<Ihr-VPC-oder-VNet-Name>** hinzugefügt wird.
- 4 Navigieren Sie zu **Fabric > Knoten > Transportknoten** und stellen Sie sicher, dass PCG als Transportknoten registriert und mit zwei Transportzonen verbunden ist, die während der Bereitstellung von PCG automatisch erstellt wurden:
 - Datenverkehrstyp VLAN -- dies stellt eine Verbindung mit dem PCG-Uplink her
 - Datenverkehrstyp Overlay -- dies ist für die logische Overlay-Vernetzung

Hinweis Overlay wird in der aktuellen Version nicht unterstützt.

- 5 Verifizieren Sie, ob die logischen Switches und der logische Ebene-0-Router erstellt wurden und der logische Router dem Edge-Cluster hinzugefügt wurde.
 - Navigieren Sie zu **Netzwerk > Switching > Switches**. Sie sollten sehen, dass die **DefaultSwitch-Overlay-<Ihr-VPC-oder-VNet-Name>** und **DefaultSwitch-VLAN-<Ihr-VPC-oder-VNet-Name>**-Switches automatisch erstellt wurden.

- Navigieren Sie zu **Networking > Routing > Router**. Sie sollten sehen, dass die **PCG-Tier0-LR-
<Ihr-VPC-oder-VNet-Name>**-Router automatisch erstellt wurden.

Häufig gestellte Fragen zum logischen Switching

Tabelle 16-10.

Frage	Antwort
Erstellt NSX Cloud bei der Bereitstellung von PCG alle Standard-Switches?	Ja. NSX Cloud erstellt zwei Standard-Switches für jede VPC oder jedes VNet, in der bzw. dem Sie PCG bereitstellen. Die Switches werden wie folgt benannt: DefaultSwitch-Overlay- DefaultSwitch-VLAN-
Kann ich zusätzlich zum von NSX Cloud erstellten logischen Switch einen logischen VLAN-Switch erstellen?	Nein. Erstellen Sie keinen logischen VLAN-Switch.
Kann ich die von NSX Cloud erstellten logischen Standard-Switches bearbeiten oder löschen?	Über die Benutzeroberfläche können Sie die logischen Standardentitäten bearbeiten oder löschen. Automatisch von NSX Cloud erstellte Elemente dürfen Sie hingegen weder bearbeiten noch löschen.
Muss ich Ports erstellen?	Nein. Sie brauchen keine Ports zu erstellen. NSX Cloud erstellt Ports, wenn Sie VMs in AWS oder Microsoft Azure kennzeichnen. Bearbeiten und löschen Sie keine Ports, die von NSX Cloud automatisch erstellt wurden.
Muss ich Switching-Profil erstellen?	Nein. Sie brauchen keine Switching-Profil zu erstellen. Verwenden Sie das PublicCloud-Global-SpoofGuardProfile . Bearbeiten bzw. löschen Sie das Standard-Switching-Profil nicht.
Wo finde ich detaillierte Informationen über logische Switches?	Siehe Kapitel 1 Logische Switches und Konfigurieren einer VM-Anfügung .

Häufig gestellte Fragen zu logischen Routern

Tabelle 16-11.

Frage	Antwort
Erstellt NSX Cloud automatisch einen logischen Router, wenn ein PCG bereitgestellt wird?	Ja. Ein Logischer Ebene-0-Router wird von NSX Cloud automatisch erstellt, wenn PCG auf einer VPC oder in einem VNet bereitgestellt wird.
Wo finde ich weitere Informationen über logische Router?	Siehe Kapitel 5 Logischer Ebene-0-Router .

Häufig gestellte Fragen zu IPFIX

Tabelle 16-12.

Frage	Antwort
Sind für die Arbeit in der Public Cloud bestimmte Konfigurationen für IPFIX erforderlich?	Ja, <ul style="list-style-type: none"> ■ IPFIX wird in NSX Cloud nur auf UDP-Port 4739 unterstützt. ■ Der Collector muss sich in derselben VPC oder demselben VNet befinden wie die virtuelle Maschine, auf die das IPFIX-Profil angewendet wurde. ■ Switch und DFW IPFIX: 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.
Wo finde ich weitere Informationen über IPFIX?	Siehe Konfigurieren von IPFIX .

Häufig gestellte Fragen zur Portspiegelung

Tabelle 16-13.

Frage	Antwort
Sind für die Portspiegelung in der Public Cloud bestimmte Konfigurationen erforderlich?	Die Portspiegelung wird in der aktuellen Version nur in AWS unterstützt. <ul style="list-style-type: none"> ■ Für NSX Cloud konfigurieren Sie die Portspiegelung unter Tools > Portspiegelungssitzungen. ■ Nur die L3SPAN-Portspiegelung wird unterstützt. ■ Der Collector muss sich in derselben VPC bzw. demselben VNet befinden wie die Quell-Arbeitslast-VM.
Wo finde ich weitere Informationen über die Portspiegelung?	Siehe Überwachen von Portspiegelungssitzungen .

Sonstige FAQ

Tabelle 16-14.

Frage	Antwort
Sind die Tags, die ich auf meine Arbeitslast-VMs in der Public Cloud anwende, in NSX-T Data Center verfügbar?	Ja. Weitere Informationen finden Sie unter Gruppen-VMs mit NSX-T Data Center und Public-Cloud-Tags .
Wie richte ich eine Mikrosegmentierung für meine Arbeitslast-VMs ein, die von NSX-T Data Centerverwaltet werden?	Siehe Einrichten von Mikro-Segmentierung für Workload-VMs .

Verwenden von erweiterten NSX Cloud-Funktionen

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>
```

Fehlerbehebung

Hier erfahren Sie mehr über die Prüf- und Fehlerbehebungsoptionen von NSX Cloud.

Überprüfen von NSX Cloud-Komponenten

Es wird empfohlen sicherzustellen, dass alle Komponenten eingerichtet sind und ausgeführt werden, bevor diese in einer Produktionsumgebung bereitgestellt werden.

Überprüfen Sie, ob der NSX Agent mit PCG verbunden ist

Um sicherzustellen, dass der NSX Agent auf Ihrer Workload-VM mit PCG verbunden ist, führen Sie folgende Schritte aus:

- 1 Geben Sie den Befehl `nsxcli` ein, um die NSX-T Data Center-Befehlszeilenschnittstelle zu öffnen.
- 2 Geben Sie den folgenden Befehl zum Abrufen des Gateway-Verbindungsstatus ein, zum Beispiel:

```
get gateway connection status
Public Cloud Gateway : nsx-gw.vmware.com:5555 Connection Status : ESTABLISHED
```

Überprüfen des Schnittstellen-/Netzwerk-Modus der VM

Überprüfen Sie die Schnittstelle, auf der der NSX Agent installiert ist, wie folgt:

- 1 Geben Sie den Befehl `nsxcli` ein, um die NSX-T Data Center-Befehlszeilenschnittstelle zu öffnen.

- 2 Geben Sie den Befehl ein, um den Switch-Modus anzuzeigen, zum Beispiel:

```
get vm-network-mode
VM-Network-Mode : underlay Interface : eth0
```

Verifizieren Sie das VM-Schnittstellen-Tag in AWS oder Microsoft Azure

Die Arbeitslast-VMs müssen über die korrekten Tags verfügen, um eine Verbindung zum PCG herstellen zu können.

- 1 Melden Sie sich über die AWS-Konsole oder das Microsoft Azure-Portal an.
- 2 Überprüfen Sie die Tags „eth0“ und „interface“ der VM.

Der Schlüssel `nsx.network` muss den Wert `default` aufweisen.

Fehlerbehebung – Häufig gestellte Fragen

Hier finden Sie eine Auflistung einiger häufig gestellter Fragen.

Ich habe meine VM korrekt gekennzeichnet und den Agenten installiert, aber meine VM steht unter Quarantäne. Was soll ich tun?

Versuchen Sie Folgendes, wenn dieses Problem auftritt:

- Überprüfen Sie, ob das NSX Cloud-Tag: `nsx.managed` und dessen Wert: `default` korrekt eingegeben wurden. Beachten Sie dabei Groß- und Kleinschreibung.
- Synchronisieren Sie das AWS- oder Microsoft Azure-Konto erneut über CSM.
 - Melden Sie sich bei CSM an.
 - Navigieren Sie zu **Clouds > AWS/Azure > Konten**.
 - Klicken Sie in der Public-Cloud-Konto-Kachel auf **Aktionen** und klicken Sie auf **Account erneut synchronisieren**.

Was soll ich tun, wenn ich nicht auf meine Arbeitslast-VM zugreifen kann?

Unter bestimmten, selten auftretenden Bedingungen können Sie die Verbindung zu Ihren verwalteten Linux- oder Windows-basierten Arbeitslast-VMs verlieren. Führen Sie die folgenden Schritte aus:

Aus Ihrer Public Cloud (AWS oder Microsoft Azure)

- Stellen Sie sicher, dass alle Ports auf der VM, einschließlich der von NSX Cloud verwalteten Ports, der Betriebssystem-Firewall (Microsoft Windows oder IPTables) und NSX-T Data Center ordnungsgemäß konfiguriert sind, um Datenverkehr zuzulassen,

Um beispielsweise `ping` für eine VM zuzulassen, muss Folgendes richtig konfiguriert sein:

- Sicherheitsgruppe in AWS oder Microsoft Azure. Weitere Informationen hierzu finden Sie unter [Verwalten der Quarantäne-Richtlinie](#).
- NSX-T Data Center-DFW-Regeln Weitere Informationen finden Sie unter [Auf verwaltete Workload-VMs zugreifen](#).

- Windows-Firewall oder IPTables unter Linux.
- Versuchen Sie, das Problem zu beheben, indem Sie sich über SSH oder andere Methoden, wie z. B. die serielle Konsole in Microsoft Azure, bei der VM anmelden.
- Sie können die gesperrte VM neu starten.
- Wenn Sie immer noch nicht auf die VM zugreifen können, hängen Sie eine sekundäre NIC an die Arbeitslast-VM an, von der aus Sie auf diese Arbeitslast-VM zugreifen können.

Vorgänge und Verwaltung

17

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:

- [Hinzufügen eines Lizenzschlüssels](#)
- [Verwalten von Benutzerkonten und der rollenbasierten Zugriffssteuerung](#)
- [Einrichten von Zertifikaten](#)
- [Konfigurieren von Appliances](#)
- [Hinzufügen eines Berechnungsmanagers](#)
- [Tags verwalten](#)
- [Suchen nach Objekten](#)
- [Suchen nach dem SSH-Fingerabdruck eines Remote-Servers](#)
- [Sichern und Wiederherstellen von NSX Manager](#)
- [Verwalten von Appliances und Appliance-Clustern](#)
- [Protokollmeldungen](#)
- [Konfigurieren von IPFIX](#)
- [Nachverfolgen des Pfads eines Pakets mit Traceflow](#)
- [Anzeigen der Portverbindungsinformationen](#)
- [Überwachen der Aktivität eines Ports für einen logischen Switch](#)
- [Überwachen von Portspiegelungssitzungen](#)
- [Überwachen von Fabric-Knoten](#)
- [Anzeigen von Daten über Anwendungen, die auf virtuellen Maschinen ausgeführt werden](#)

- Erfassen von Support-Paketen
- Programm zur Verbesserung der Benutzerfreundlichkeit

Hinzufügen eines Lizenzschlüssels

Sie können mithilfe der NSX Manager-Benutzeroberfläche einen oder mehrere Lizenzschlüssel hinzufügen.

Die folgenden Typen von Nicht-Evaluierungslizenzen sind verfügbar:

- Standard
- Erweitert
- Enterprise

Bei der Installation von NSX Manager wird eine vorinstallierte Evaluierungslizenz aktiviert, die 60 Tage gültig ist. Die Evaluierungslizenz ermöglicht die Verwendung sämtlicher Funktionen einer Enterprise-Lizenz. Sie können eine Evaluierungslizenz nicht installieren oder deren Zuweisung aufheben.

Sie haben die Möglichkeit, eine oder mehrere Nicht-Evaluierungslizenzen zu installieren. Für jeden Typ lässt sich aber immer nur ein Schlüssel installieren. Wenn Sie eine Standard-, Erweiterte oder Enterprise-Lizenz installieren, ist die Evaluierungslizenz nicht mehr verfügbar. Sie können auch die Zuweisung von Nicht-Evaluierungslizenzen aufheben. Wenn Sie die Zuweisung aller Nicht-Evaluierungslizenzen aufheben, wird die Evaluierungslizenz wiederhergestellt.

Wenn Sie über mehrere Schlüssel des gleichen Lizenztyps verfügen und diese kombinieren möchten, müssen Sie zu <https://my.vmware.com> wechseln und dafür die Funktion Schlüssel kombinieren anwenden. In der Benutzeroberfläche von NSX Manager ist diese Funktion nicht verfügbar.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **System > Konfiguration > Lizenz** aus.
- 3 Klicken Sie auf **Hinzufügen**, um den Lizenzschlüssel einzugeben.
- 4 Klicken Sie auf **Speichern**.

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 konfigurieren, 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.

Ändern des CLI-Benutzerkennworts

Jede Appliance verfügt über zwei integrierte Benutzer („Admin“ und „Audit“), mit denen Sie sich anmelden und CLI-Befehle ausführen können. Sie können zwar das Kennwort für diese Benutzer ändern, aber keine Benutzer hinzufügen oder löschen.

Verfahren

- 1 Melden Sie sich bei der Appliance-CLI an.
- 2 Führen Sie den Befehl `set user` aus. Beispiel:

```
nsx> set user admin
Current password:
New password:
Confirm new password:
nsx>
```

Das Kennwort muss den folgenden Komplexitätsanforderungen genügen:

- Mindestens acht Zeichen lang
- Mindestens ein Großbuchstabe
- Mindestens ein Kleinbuchstabe
- Mindestens ein numerisches Zeichen
- mindestens ein Sonderzeichen

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-, NSX Controller- 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 Zertifikatfingerabdrucks von einem vIDM-Host

Bevor Sie die Integration von vIDM mit NSX-T konfigurieren, müssen Sie den Zertifikatfingerabdruck vom vIDM-Host abrufen.

Verfahren

- 1 Stellen Sie eine SSH-Verbindung mit dem vIDM-Host her, und melden Sie sich als **sshuser** an.
- 2 Führen Sie den folgenden Befehl aus, um **root**-Benutzer zu sein.

```
su root
```

- 3 Bearbeiten Sie der Datei `/etc/ssh/sshd_config`, und ändern Sie den Wert von `PermitRootLogin` in `yes` und den Wert von `StrictModes` in `no`.

```
PermitRootLogin yes
StrictModes no
```

- 4 Führen Sie den folgenden Befehl aus, um den `sshd`-Dienst neu zu starten.

```
service sshd restart
```

- 5 Melden Sie sich ab, und melden Sie sich als **root** an.
- 6 Führen Sie den folgenden Befehl aus, um den Director zu ändern.

```
cd /usr/local/horizon/conf
```

7 Führen Sie den folgenden Befehl aus, um den Fingerabdruck abzurufen.

```
openssl s_client -connect <FQDN of vIDM host>:443 < /dev/null 2>/dev/null | openssl x509 -sha256 -fingerprint -noout -in /dev/stdin
```

Beispiel:

```
openssl s_client -connect vidm.corp.local:443 < /dev/null 2>/dev/null | openssl x509 -sha256 -fingerprint -noout -in /dev/stdin
```

Verknüpfen eines vIDM-Hosts mit NSX-T

Um die Integration von NSX-T in vIDM zu ermöglichen, müssen Sie Informationen über den vIDM-Host angeben.

Der vIDM-Server sollte über ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat verfügen. Andernfalls funktioniert die Anmeldung bei vIDM über den NSX Manager möglicherweise nicht mit bestimmten Browsern wie Microsoft Edge oder Internet Explorer 11. Informationen zum Installieren eines CA-signierten Zertifikats auf vIDM finden Sie unter <https://docs.vmware.com/de/VMware-Identity-Manager/3.1/vidm-install/GUID-B76761BF-4B12-4CD5-9366-B0A1A2BF2A8B.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.

Voraussetzungen

- Stellen Sie sicher, dass Sie über den Fingerabdruck des Zertifikats vom vIDM-Host verfügen. Siehe [Abrufen des Zertifikatfingerabdrucks 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://www.vmware.com/support/pubs/identitymanager-pubs.html>.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **System > Benutzer** aus.
- 3 Klicken Sie auf die Registerkarte **Konfiguration**.
- 4 Klicken Sie auf **Bearbeiten**.

5 Geben Sie die folgenden Informationen an.

Parameter	Beschreibung
VMware Identity Manager-Appliance	Der vollqualifizierte Domänenname (FQDN) des vIDM-Hosts.
Client-ID	Die ID, die beim Registrieren von NSX Manager für den vIDM-Host erstellt wird.
Geheimer Client-Schlüssel	Der geheime Schlüssel, der beim Registrieren von NSX Manager für den vIDM-Host erstellt wird.
Fingerabdruck	Der Fingerabdruck des Zertifikats für den vIDM-Host.
NSX-Appliance	Die IP-Adresse oder der vollqualifizierte Domänenname (FQDN) von NSX Manager. 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.

6 Klicken Sie auf **Speichern**.

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>

Informationen zum Synchronisieren von virtuellen Maschinen mit dem Host finden Sie unter https://docs.vmware.com/de/VMware-vSphere/6.0/com.vmware.vsphere.vm_admin.doc/GUID-C0D8326A-B6E7-4E61-8470-6C173FDDF656.html. Auf den VMs werden möglicherweise NSX Manager, vIDM, Active Directory oder andere Dienstanbieter ausgeführt.

Drittanbieter-Infrastruktur

Konsultieren Sie die Dokumentation des Anbieters hinsichtlich der Synchronisierung von VMs und Hosts.

Konfigurieren von NTP auf dem vIDM-Server (nicht empfohlen)

Wenn das Synchronisieren der Zeit auf allen Hosts nicht möglich ist, können Sie die Synchronisierung mit dem Host deaktivieren und NTP auf dem vIDM-Server konfigurieren. Diese Methode wird jedoch nicht empfohlen, da hierfür UDP-Port 123 auf dem vIDM-Server geöffnet werden muss.

- Überprüfen Sie die Uhr auf dem vIDM-Server, um sich zu vergewissern, dass sie korrekt eingestellt ist.

```
# hwclock
Tue May 9 12:08:43 2017 -0.739213 seconds
```

- Bearbeiten Sie `/etc/ntp.conf` und fügen Sie die folgenden Einträge hinzu, sofern sie noch nicht vorhanden sind.

```
server server time.nist.gov
server server pool.ntp.org
server server time.is dynamic
```

- Öffnen Sie UDP-Port 123.

```
# iptables -A INPUT -p udp --dport 123 -j ACCEPT
```

Führen Sie den folgenden Befehl aus, um zu überprüfen, ob der Port geöffnet ist.

```
# iptables -L -n
```

- Starten Sie den NTP-Dienst.

```
/etc/init.d/ntp start
```

- Legen Sie fest, dass NTP nach einem Neustart automatisch ausgeführt wird.

```
# chkconfig --add ntp
# chkconfig ntp on
```

- Überprüfen Sie, ob der NTP-Server erreicht werden kann.

```
# ntpq -p
```

Die Spalte `reach` sollte nicht 0 anzeigen. Die Spalte `st` sollte eine Ziffer, nicht jedoch 16 anzeigen.

Rollenbasierte Zugriffssteuerung

Mit der rollenbasierten Zugriffssteuerung (RBAC) können Sie den Systemzugriff auf autorisierte Benutzer einschränken. Benutzern werden Rollen zugewiesen, und jede Rolle verfügt über bestimmte Berechtigungen.

Es gibt vier Arten von Berechtigungen:

- Vollzugriff
- Ausführen

- Lesen
- Keine

Vollzugriff gewährt dem Benutzer sämtliche Berechtigungen. Die Ausführungsberechtigung schließt die Leseberechtigung ein.

NSX-T Data Center hat die folgenden integrierten Rollen. Sie können keine neuen Rollen hinzufügen.

- Enterprise-Administrator
- Auditor
- Netzwerktechniker
- Netzwerkvorgänge
- Sicherheitstechniker
- Sicherheitsvorgänge
- Cloud-Dienstadministrator
- Cloud-Dienstauditor
- Load Balancer-Administrator
- Load Balancer-Auditor

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 17-1. Rollen und Berechtigungen](#) zeigt die Berechtigungen an, die die einzelnen Rollen für verschiedene Vorgänge haben. Die folgenden Abkürzungen werden verwendet:

- EA – Enterprise-Administrator
- A – Auditor
- NE – Netzwerktechniker
- NO – Netzwerkvorgänge
- SE – Sicherheitstechniker
- SO – Sicherheitsvorgänge
- CS Adm – Cloud-Dienstadministrator
- CS Aud – Cloud-Dienstauditor
- LB Adm – Load Balancer-Administrator
- LB Aud – Load Balancer-Auditor
- FA – Vollzugriff

■ E – Ausführen

■ R – Lesen

Tabelle 17-1. Rollen und Berechtigungen

Vorgang	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud
Tools > Portverbindung	E	R	E	E	E	E	E	R	E	E
Tools > Traceflow	E	R	E	E	E	E	E	R	E	E
Tools > Portspiegelung	FA	R	FA	FA	FA	FA	FA	R	Keine	Keine
Tools > IPFIX	FA	R	FA	R	FA	R	FA	R	Keine	Keine
Firewall > Allgemein	FA	R	R	R	FA	R	FA	R	Keine	Keine
Firewall > Konfiguration	FA	R	R	R	FA	R	FA	R	Keine	Keine
Verschlüsselung	FA	R	FA	R	FA	FA	Keine	Keine	Keine	Keine
Routing > Router	FA	R	FA	R	R	R	FA	R	R	R
Routing > NAT	FA	R	FA	R	FA	R	FA	R	R	R
DHCP > Serverprofile	FA	R	FA	R	FA	Keine	FA	R	Keine	Keine
DHCP > Server	FA	R	FA	R	FA	Keine	FA	R	Keine	Keine
DHCP > Relay-Profile	FA	R	FA	R	FA	Keine	FA	R	Keine	Keine
DHCP > Relay-Dienste	FA	R	FA	R	FA	Keine	FA	R	Keine	Keine
DHCP > Metadaten-Proxys	FA	R	FA	R	FA	Keine	Keine	Keine	Keine	Keine
IPAM	FA	R	FA	R	FA	Keine	Keine	Keine	Keine	Keine
Switching > Switches	FA	R	FA	FA	R	R	FA	R	R	R
Switching > Ports	FA	R	FA	FA	R	R	FA	R	R	R
Switching > Switching-Profile	FA	R	FA	FA	FA	FA	FA	R	R	R

Tabelle 17-1. Rollen und Berechtigungen (Fortsetzung)

Vorgang	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud
Lastausgleich > Load Balancer	FA	R	Keine	Keine	Keine	Keine	FA	R	FA	R
Lastausgleich > Virtuelle Server	FA	R	Keine	Keine	Keine	Keine	FA	R	FA	R
Lastausgleich > Profile > Anwendungsp rofile	FA	R	Keine	Keine	Keine	Keine	FA	R	FA	R
Lastausgleich > Profile > Persistenzprof ile	FA	R	Keine	Keine	Keine	Keine	FA	R	FA	R
Lastausgleich > Profile > SSL-Profil	FA	R	Keine	Keine	FA	R	FA	R	FA	R
Lastausgleich > Serverpools	FA	R	Keine	Keine	Keine	Keine	FA	R	FA	R
Lastausgleich > Überwachung en	FA	R	Keine	Keine	Keine	Keine	FA	R	FA	R
Bestand > Gruppen	FA	R	FA	R	FA	R	FA	R	R	R
Bestand > IP Sets	FA	R	FA	R	FA	R	FA	R	R	R
Bestand > IP- Pools	FA	R	FA	R	Keine	R	Keine	Keine	R	R
Bestand > MAC Sets	FA	R	FA	R	FA	R	FA	R	R	R
Bestand > Dienste	FA	R	FA	R	FA	R	FA	R	R	R
Bestand > Virtuelle Maschinen	R	R	R	R	R	R	R	R	R	R
Bestand > VM > Tags erstellen und zuweisen	FA	R	FA	FA	FA	FA	FA	R	R	R
Bestand > VM > Tags konfigurieren	FA	Keine	Keine	Keine	FA	Keine	Keine	Keine	Keine	Keine

Tabelle 17-1. Rollen und Berechtigungen (Fortsetzung)

Vorgang	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud
Fabric > Knoten > Hosts	FA	R	R	R	R	R	R	R	Keine	Keine
Fabric > Knoten > Knoten	FA	R	FA	R	FA	R	R	R	Keine	Keine
Fabric > Knoten > Edges	FA	R	FA	R	R	R	R	R	Keine	Keine
Fabric > Knoten > Edge-Cluster	FA	R	FA	R	R	R	R	R	Keine	Keine
Fabric > Knoten > Bridges	FA	R	FA	R	R	R	Keine	Keine	R	R
Fabric > Knoten > Transportknoten	FA	R	R	R	R	R	R	R	R	R
Fabric > Knoten > Tunnel	R	R	R	R	R	R	R	R	R	R
Fabric > Profile > Uplink-Profile	FA	R	R	R	R	R	R	R	R	R
Fabric > Profile > Edge-Cluster-Profile	FA	R	FA	R	R	R	R	R	R	R
Fabric > Profile > Konfiguration	FA	R	Keine	Keine	Keine	Keine	R	R	Keine	Keine
Fabric > Transportzone n > Transportzone n	FA	R	R	R	R	R	R	R	R	R
Fabric > Transportzone n > Transportzone nprofile	FA	R	R	R	R	R	R	R	R	R
Fabric > Berechnungs manager	FA	R	R	R	R	R	R	R	Keine	Keine

Tabelle 17-1. Rollen und Berechtigungen (Fortsetzung)

Vorgang	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud
System > Vertrauen	FA	R	Keine	Keine	FA	R	Keine	Keine	FA	R
System > Konfiguration	E	R	R	R	R	R	Keine	Keine	Keine	Keine
System > Dienstprogramme > Support-Paket	FA	R	R	R	R	R	R	R	Keine	Keine
System > Dienstprogramme > Sicherung	FA	R	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine
System > Dienstprogramme > Wiederherstellen	FA	R	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine
System > Dienstprogramme > Upgrade	FA	R	R	R	R	R	Keine	Keine	Keine	Keine
System > Benutzer > Rollenzuweisungen	FA	R	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine
System > Benutzer > Konfiguration	FA	R	Keine	Keine	Keine	Keine	Keine	Keine	Keine	Keine

Verwalten von Rollenzuweisungen

Sie können Rollenzuweisungen für Benutzer oder Benutzergruppen hinzufügen, ändern und löschen, wenn VMware Identity Manager in NSX-T Data Center integriert ist.

Voraussetzungen

- Stellen Sie sicher, dass ein vIDM-Host mit NSX-T verknüpft ist. Weitere Informationen finden Sie unter [Verknüpfen eines vIDM-Hosts mit NSX-T](#).

Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **System > Benutzer** aus.
- 3 Klicken Sie auf die Registerkarte **Rollenzuweisungen**, falls sie noch nicht ausgewählt ist.

4 Fügen Sie Rollenzuweisungen zu oder ändern oder löschen Sie sie.

Option	Aktionen
Hinzufügen von Rollenzuweisungen	Klicken Sie auf Hinzufügen , wählen Sie Benutzer oder Benutzergruppen aus, und wählen Sie Rollen aus.
Ändern von Rollenzuweisungen	Wählen Sie einen Benutzer oder eine Benutzergruppe aus und klicken Sie auf Bearbeiten .
Löschen von Rollenzuweisungen	Wählen Sie einen Benutzer oder eine Benutzergruppe aus und klicken Sie auf Löschen .

Anzeigen von Prinzipalidentitäten

Ein Prinzipal kann eine NSX-T Data Center-Komponente oder eine Drittanbieter-Anwendung wie ein OpenStack-Produkt sein. Ein Prinzipal mit einer Prinzipalidentität kann den Identitätsnamen dazu verwenden, ein Objekt zu erstellen und sicherzustellen, dass nur eine Einheit mit demselben Identitätsnamen das Objekt ändern oder löschen kann.

Eine Prinzipalidentität hat folgende Attribute:

- Name
- Knoten-ID
- Zertifikat
- RBAC-Rolle, welche die Zugriffsrechte des Prinzipals definiert
- Flag, das angibt, ob die von diesem Prinzipal erstellten Objekte geschützt sind

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 sie jedoch ändern und löschen. Ein Enterprise-Administrator-Benutzer kann geschützte Objekte nur mithilfe der NSX-T Data Center-API, aber nicht über die NSX Manager-Benutzeroberfläche löschen.

Eine Prinzipalidentität kann nur mithilfe der NSX-T-API erstellt oder gelöscht werden. Weitere Informationen finden Sie in der *NSX-T Data CenterAPI-Referenz*. Allerdings können Sie Prinzipalidentitäten über die NSX Manager-Benutzeroberfläche anzeigen.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **System > Benutzer** aus.
- 3 Klicken Sie auf die Registerkarte **Rollenzuweisungen**.

Anschließend werden Benutzer, Benutzergruppen und Prinzipalidentitäten angezeigt.

Einrichten von Zertifikaten

Sie können in NSX Manager eine Zertifikatsignieranforderung (CSR, Certificate Signing Request) generieren und diese an eine Zertifizierungsstelle (CA, Certificate Authority) senden, um ein Serverzertifikat abzurufen.

Die CSR kann auch für die Generierung von selbstsignierten Zertifikaten verwendet werden. Wenn Sie über ein vorhandenes Zertifikat oder über ein CA-Zertifikat verfügen, können Sie dieses importieren und anwenden. Sie haben auch die Möglichkeit, eine Zertifikatswiderrufsliste (CRL, Certificate Revocation List) mit widerrufenen Zertifikaten zu importieren.

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. 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.
- Stellen Sie sicher, dass die Paare für den öffentlichen und privaten Schlüssel verfügbar sind.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **System > Vertrauensstellung** aus.
- 3 Klicken Sie auf die Registerkarte **CSRS**.
- 4 Klicken Sie auf **CSR erzeugen**.
- 5 Vervollständigen Sie die Details für die CSR-Datei.

Option	Beschreibung
Name	Weisen Sie Ihrem Zertifikat einen Namen zu.
Allgemeiner Name	Geben Sie den vollqualifizierten Domännennamen (FQDN) Ihres Servers ein. Beispiel: test.vmware.de.
Name der Organisation	Geben Sie Ihren Organisationsnamen mit den erforderlichen Suffixen ein. Beispiel: VMware Global Inc.
Organisationseinheit	Geben Sie die Abteilung innerhalb Ihrer Organisation ein, die dieses Zertifikat verwaltet. Beispiel: IT-Abteilung.
Ort	Geben Sie die Stadt ein, in der Ihre Organisation ihren Standort hat. Beispiel: Unterschleissheim.

Option	Beschreibung
Bundesland	Geben Sie das Bundesland ein, in dem Ihre Organisation ihren Standort hat. Beispiel: Bayern.
Land	Geben Sie das Land ein, in dem Ihre Organisation ihren Standort hat. Beispiel: Deutschland.
Meldungsalgorithmus	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.
Schlüsselgröße	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.
Beschreibung	Geben Sie Informationen ein, mit denen sich dieses Zertifikat zu einem späteren Zeitpunkt einfach identifizieren lässt.

6 Klicken Sie auf **Speichern**.

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 als Interim-Zertifizierungsstelle für Ihr Unternehmen importieren. Nach dem Import des Zertifikats verfügen Sie über das Recht, Ihre eigenen Zertifikate zu signieren.

Voraussetzungen

Stellen Sie sicher, dass ein CA-Zertifikat verfügbar ist.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **System > Vertrauensstellung** aus.
- 3 Klicken Sie auf die Registerkarte **Zertifikate**.
- 4 Wählen Sie **Importieren > CA-Zertifikat importieren** aus, und geben Sie die Zertifikatdetails ein.

Option	Beschreibung
Name	Weisen Sie dem CA-Zertifikat einen Namen zu.
Zertifikatsinhalte	Wechseln Sie in das Verzeichnis der CA-Zertifikat-Datei auf Ihrem Computer und fügen Sie die Datei hinzu.
Beschreibung	Geben Sie eine zusammenfassende Beschreibung ein, was in diesem CA-Zertifikat enthalten ist.

- 5 Klicken Sie auf **Speichern**.

Ergebnisse

Sie können jetzt Ihre eigenen Zertifikate signieren.

Importieren eines Zertifikats

Sie können ein Zertifikat mit privatem Schlüssel zum Erstellen selbstsignierter Zertifikate importieren.

Voraussetzungen

Stellen Sie sicher, dass ein Zertifikat verfügbar ist.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **System > Vertrauensstellung** aus.
- 3 Klicken Sie auf die Registerkarte **Zertifikate**.
- 4 Wählen Sie **Importieren > Zertifikat importieren** aus, und geben Sie die Zertifikatdetails ein.

Option	Beschreibung
Name	Weisen Sie dem CA-Zertifikat einen Namen zu.
Zertifikatsinhalte	Wechseln Sie in das Verzeichnis der Zertifikatdatei auf Ihrem Computer und fügen Sie die Datei hinzu.

Option	Beschreibung
Privater Schlüssel	Wechseln Sie in das Verzeichnis der Datei für den privaten Schlüssel auf Ihrem Computer und fügen Sie die Datei hinzu.
Kennwort	Fügen Sie für dieses Zertifikat ein Kennwort hinzu.
Beschreibung	Geben Sie eine zusammenfassende Beschreibung ein, was in diesem Zertifikat enthalten ist.

5 Klicken Sie auf **Speichern**.

Ergebnisse

Sie haben jetzt die Möglichkeit, Ihre eigenen selbstsignierten Zertifikate zu erstellen.

Erstellen eines selbstsignierten Zertifikats

Die Verwendung von selbstsignierten Zertifikaten ist eventuell weniger sicher als die von vertrauenswürdigen Zertifikaten.

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 über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **System > Vertrauensstellung** aus.
- 3 Klicken Sie auf die Registerkarte **CSRS**.
- 4 Wählen Sie die vorhandene CSR aus.
- 5 Klicken Sie auf **Aktionen** und wählen Sie **Selbstsigniertes Zertifikat für CSR** im Dropdown-Menü aus.
- 6 Geben Sie die Anzahl der Tage ein, die das selbstsignierte Zertifikat gültig ist.
Der Standardzeitraum beträgt 10 Jahre.
- 7 Klicken Sie auf **Speichern**.

Ergebnisse

Das selbstsignierte Zertifikat wird in die Liste **Zertifikat** aufgenommen. Der Zertifikattyp ist als „selbstsigniert“ festgelegt.

Ersetzen eines Zertifikats

Wenn Sie ein vorhandenes Zertifikat ersetzen müssen, z. B. weil es abgelaufen ist, können Sie es mithilfe eines API-Aufrufs ersetzen.

Voraussetzungen

Stellen Sie sicher, dass ein Zertifikat in NSX Manager verfügbar ist. Siehe [Erstellen eines selbstsignierten Zertifikats](#) und [Importieren eines Zertifikats](#).

Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **System > Vertrauensstellung** aus.
- 3 Klicken Sie auf die Registerkarte **Zertifikate**.
- 4 Klicken Sie auf die ID des gewünschten Zertifikats und kopieren Sie die Zertifikat-ID aus dem Pop-up-Fenster.
- 5 Ersetzen Sie das vorhandene Zertifikat unter Verwendung des API-Aufrufs `POST /api/v1/node/services/http?action=apply_certificate`. Beispiel:

```
POST https://<nsx-mgr>/api/v1/node/services/http?
action=apply_certificate&certificate_id=e61c7537-3090-4149-b2b6-19915c20504f
```

Weitere Informationen finden Sie in der *Referenz zur NSX-T-API*.

Ergebnisse

Der API-Aufruf startet den HTTP-Dienst neu, damit der Dienst von nun an das neue Zertifikat verwenden kann. Wenn die POST-Anforderung erfolgreich war, erhalten Sie den Antwortcode 200 Accepted (200 Akzeptiert).

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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **System > Vertrauensstellung** aus.
- 3 Klicken Sie auf die Registerkarte **CRLS**.
- 4 Klicken Sie auf **Importieren** und fügen Sie die CRL-Details hinzu.

Option	Beschreibung
Name	Weisen Sie der CRL einen Namen zu.
Zertifikatsinhalte	<p>Kopieren Sie alle Elemente in der CRL und fügen Sie sie in diesem Abschnitt ein.</p> <p>Beispiel-CRL</p> <pre>-----BEGIN X509 CRL----- MIIBODCB4zANBgkqhkiG9w0BAQQFADBGMQswCQYDVQQGEwJBVTEMMAoGA1UECBM D UUxEMRkwFwYDVQQKEwBNaw5jb20gUHR5LiBMdGQuMQswCQYDVQQLEwJDUzEhMBk G A1UEAxMSU1NMZW5IGRlbW8gc2VydmVyFw0wMTAxMTUxNjI2NTdaFw0wMTAyMTQ x NjI2NTdaMFIwEgIBARcNOTUxMDA5MjMzMjA1WjASAgEDFw05NTEyMDEwMTAwMD a MBMCAhI0Fw0wMTAxMTUxNjE5NDdaMBMCAhI1Fw0wMTAxMTUxNjIzNDZaMA0GCSq G SIb3DQEBAUAA0EAHPjQ3M93Q0j8Ufi+jZM7Y78TfAzG4jJn/ E6MYBPFVQFY0/Gp UZexfjSVo5CIyyS0tYscz8o07avwBxTiMpDEQg== -----END X509 CRL-----</pre>
Beschreibung	Geben Sie eine Übersicht über den Inhalt dieser CRL ein.

- 5 Klicken Sie auf **Speichern**.

Ergebnisse

Die importierte CRL wird als Link angezeigt.

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 über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **System > Vertrauensstellung** aus.
- 3 Klicken Sie auf die Registerkarte **CSRS**.
- 4 Wählen Sie die vorhandene CSR aus.
- 5 Klicken Sie auf **Aktionen**, und wählen Sie im Dropdown-Menü **Zertifikat für CSR importieren** aus.
- 6 Wechseln Sie in das Verzeichnis der signierten Zertifikatsdatei auf Ihrem Computer, und fügen Sie die Datei hinzu.
- 7 Klicken Sie auf **Speichern**.

Ergebnisse

Das selbstsignierte Zertifikat wird in die Liste **Zertifikat** aufgenommen. Der Zertifikattyp ist als „selbstsigniert“ festgelegt.

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 17-2. Befehle und API-Anforderungen für die Systemkonfiguration.

Aufgabe	Befehlszeile (NSX Manager, NSX Controller, NSX Edge)	API-Anforderung (nur NSX Manager)
Systemzeitzone festlegen	<code>set timezone <timezone></code>	PUT <code>https://<nsx-mgr>/api/v1/node</code>
NTP-Server festlegen	<code>set ntp-server <ntp-server></code>	PUT <code>https://<nsx-mgr>/api/v1/node/services/ntp</code>
DNS-Server festlegen	<code>set name-servers <dns-server></code>	PUT <code>https://<nsx-mgr>/api/v1/node/network/name-servers</code>
DNS-Suchdomäne festlegen	<code>set search-domains <domain></code>	PUT <code>https://<nsx-mgr>/api/v1/node/network/search-domains</code>

Hinzufügen eines Berechnungsmanagers

Ein Berechnungsmanager, z. B. vCenter Server, ist eine Anwendung, die Ressourcen wie Hosts und virtuellen Maschinen verwaltet. NSX-T Data Center fragt Berechnungsmanager ab, um Informationen zu Änderungen wie hinzugefügten oder entfernten Hosts oder virtuellen Maschinen zu erhalten, und aktualisiert die Bestandsliste entsprechend. Optional haben Sie die Möglichkeit, einen Berechnungsmanager hinzuzufügen, denn NSX-T erhält Bestandslisteninformationen auch ohne Berechnungsmanager, zum Beispiel von eigenständigen Hosts und VMs.

In dieser Version unterstützt diese Funktion Folgendes:

- vCenter Server Version 6.5 Update 1, Version 6.5 Update 2 und Version 6.7.
- IPv6- und IPv4-Kommunikation mit vCenter Server.
- Maximal 5 Berechnungsmanager.

Verfahren

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

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

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

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

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

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

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

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

Wenn eine bestehende Registrierung vorhanden ist, wird sie ersetzt.

Ergebnisse

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

Tags verwalten

Sie können Objekten Tags hinzufügen, um die Suche zu erleichtern. Beim Angeben eines Tags können Sie auch einen Geltungsbereich festlegen.

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

Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://nsx-manager-ip-address` mit Administratorrechten bei einem NSX Manager an.
- 2 Navigieren Sie zu einer Objektkategorie.
Navigieren Sie beispielsweise zu **Switching > Switches**.
- 3 Klicken Sie auf den Namen eines Switches.
- 4 Wählen Sie die Menüoption **Aktionen > Tags verwalten** aus oder klicken Sie neben „Tags“ auf **Verwalten**.
- 5 Fügen Sie Tags hinzu bzw. löschen Sie Tags.

Option	Aktion
Tag hinzufügen	Klicken Sie auf Hinzufügen , um ein Tag und optional einen Geltungsbereich anzugeben.
Tag löschen	Wählen Sie ein vorhandenes Tag aus und klicken Sie auf Löschen .

Ein Objekt kann maximal 30 Tags aufweisen. Tags dürfen höchstens 256 Zeichen enthalten. Bereiche dürfen höchstens 128 Zeichen enthalten.

- 6 Klicken Sie auf **Speichern**.

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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager 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.

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 17-3. 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
```

Sichern und Wiederherstellen von NSX Manager

Wenn NSX Manager nicht mehr funktionsfähig ist, können Sie es aus einer Sicherung wiederherstellen. Während NSX Manager nicht mehr funktionsfähig ist, ist die Datenebene nicht betroffen, aber Sie können keine Änderungen an der Konfiguration vornehmen.

Es gibt drei Sicherungstypen:

Clustersicherung	Diese Sicherung umfasst den gewünschten Zustand des virtuellen Netzwerks.
Knotensicherung	Hierbei handelt es sich um eine Sicherung des NSX Manager-Knotens.
Bestandssicherung	Diese Sicherung umfasst das Set an ESX- und KVM-Hosts und -Edges. Diese Informationen werden bei Wiederherstellungsvorgängen zum Erkennen und Beheben von Diskrepanzen zwischen dem gewünschten Zustand der Managementebene und diesen Hosts verwendet.

Es gibt zwei Sicherungsmethoden:

Manuelle NSX Manager-Knotensicherung und -Clustersicherung	Manuelle Knoten- und Clustersicherungen können jederzeit nach Bedarf durchgeführt werden.
Automatische NSX Manager-Knotensicherung, -Clustersicherung und Bestandssicherung	Automatische Sicherungen werden nach einem von Ihnen festgelegten Zeitplan durchgeführt. Automatische Sicherungen werden dringend empfohlen. Siehe Zeitplan für automatische Sicherungen erstellen .

Um sicherzustellen, dass Ihre Sicherungen stets aktuell sind, sollten Sie automatische Sicherungen konfigurieren. Das regelmäßige Durchführen von Cluster- und Bestandssicherungen ist wichtig.

Sie können NSX-T Data Center-Konfigurationen wieder in den Zustand versetzen, der bei einer beliebigen Clustersicherung gespeichert wurde. Sicherungen müssen auf einer neuen NSX Manager-Appliance wiederhergestellt werden, die in derselben NSX Manager-Version ausgeführt wird wie die Appliance, die gesichert wurde.

Sichern der NSX Manager-Konfiguration

Die Sicherung der NSX Manager-Konfiguration besteht aus der Sicherung des NSX Manager-Knoten, Clusters und Bestands.

Verfahren

1 Sicherungsspeicherort konfigurieren

Sicherungen werden auf einem Dateiserver gespeichert, auf den NSX Manager zugreifen kann. Bevor eine Sicherung erfolgen kann, müssen Sie den Speicherort für diesen Server konfigurieren.

2 Zeitplan für automatische Sicherungen erstellen

Erstellen Sie einen Zeitplan für regelmäßige Sicherungen, damit Sie nicht funktionierende NSX Manager und die entsprechenden Konfigurationsdaten wiederherstellen können. Automatische Sicherungen sind standardmäßig deaktiviert. Sie können automatische Sicherungen für spezielle Wochentage oder in einem bestimmten Intervall einrichten. Sicherungen mit Zeitplan werden dringend empfohlen.

Sicherungsspeicherort konfigurieren

Sicherungen werden auf einem Dateiserver gespeichert, auf den NSX Manager zugreifen kann. Bevor eine Sicherung erfolgen kann, müssen Sie den Speicherort für diesen Server konfigurieren.

Hinweis Sicherungskopien auf dem Backup-Dateiserver werden von NSX Manager standardmäßig nicht gelöscht. Sie müssen die Backup-Rotation verwalten und sicherstellen, dass der Server über genügend Festplattenspeicher für Backups verfügt. Sie können ein Skript ausführen, das alte Backups automatisch löscht.

Voraussetzungen

Stellen Sie sicher, dass Sie über den SSH-Fingerabdruck des Sicherungsdateiservers verfügen. Nur ein SHA256-gehashter ECDSA-Schlüssel wird als Fingerabdruck akzeptiert. Siehe [Suchen nach dem SSH-Fingerabdruck eines Remote-Servers](#).

Verfahren

- 1 Melden Sie sich in einem Browser unter `https://<nsx-manager-ip-address>` als Administrator bei NSX Manager an.
- 2 Klicken Sie auf **System > Dienstprogramme > Sicherung**.
- 3 Um dem Sicherungsspeicherort die Anmeldedaten für den Zugriff zur Verfügung zu stellen, klicken Sie oben rechts auf der Seite auf **Bearbeiten**.
- 4 Klicken Sie auf den Umschalter **Automatische Sicherung**, um diesen zu aktivieren.
- 5 Geben Sie die IP-Adresse oder den Hostnamen des Sicherungsdateiservers ein.
- 6 Bearbeiten Sie den Standardport, falls erforderlich.
- 7 Geben Sie den Benutzernamen und das Kennwort ein, die für die Anmeldung beim Sicherungsdateiserver erforderlich sind.

- 8 Geben Sie im Feld **Zielverzeichnis** den absoluten Verzeichnispfad ein, unter dem die Sicherungen gespeichert werden sollen.

Das Verzeichnis muss bereits vorhanden sein. Wenn Sie über mehrere Bereitstellungen von NSX-T Data Center verfügen, verwenden Sie für jede Bereitstellung ein eigenes Verzeichnis.
- 9 Geben Sie die Passphrase zur Entschlüsselung der Sicherungsdaten ein.

Diese Passphrase wird benötigt, um eine Sicherung wiederherzustellen. Wenn Sie die Sicherungspassphrase vergessen, können Sie keine Sicherungen wiederherstellen.
- 10 Geben Sie den SSH-Fingerabdruck des Servers ein, auf dem die Sicherungen gespeichert werden. Siehe [Suchen nach dem SSH-Fingerabdruck eines Remote-Servers](#).
- 11 Klicken Sie auf **Speichern**.
- 12 Klicken Sie unten auf der Seite auf **Jetzt sichern**, um zu bestätigen, dass die Dateien auf den Sicherungsdateiserver geschrieben werden können.

Nächste Schritte

Erstellen Sie einen Zeitplan für automatische Sicherungen.

Zeitplan für automatische Sicherungen erstellen

Erstellen Sie einen Zeitplan für regelmäßige Sicherungen, damit Sie nicht funktionierende NSX Manager und die entsprechenden Konfigurationsdaten wiederherstellen können. Automatische Sicherungen sind standardmäßig deaktiviert. Sie können automatische Sicherungen für spezielle Wochentage oder in einem bestimmten Intervall einrichten. Sicherungen mit Zeitplan werden dringend empfohlen.

Voraussetzungen

- Bestimmen Sie ein angemessenes Sicherungsverzeichnis. Wählen Sie ein Verzeichnis, das Schutz vor einzelnen Fehlerquellen bietet. Speichern Sie die Sicherungen beispielsweise nicht in demselben Dateispeicher wie die Appliances. Wenn dieser Dateispeicher ausfällt, kann sich das sowohl auf die Appliances als auch auf deren Sicherungen auswirken.
- Suchen Sie den SSH-Fingerabdruck des Servers, auf dem die Sicherungen gespeichert sind. Siehe [Suchen nach dem SSH-Fingerabdruck eines Remote-Servers](#). Für die Anforderungen der Sicherungs- und Wiederherstellungs-API dürfen die SSH-Fingerabdrücke keine Doppelpunkte enthalten.

Verfahren

- 1 Melden Sie sich in einem Browser unter `https://<nsx-manager-ip-address>` als Administrator bei NSX Manager an.
- 2 Klicken Sie auf **System > Dienstprogramme > Sicherung**.
- 3 Klicken Sie in der oberen rechten Ecke auf der Seite auf **Bearbeiten**.
- 4 Klicken Sie auf **Dateiserver** und stellen Sie sicher, dass automatische Sicherungen aktiviert sind.
- 5 Klicken Sie oben auf der Seite auf **Zeitplan**.

- 6 Klicken Sie für Knoten-/Clustersicherungen auf **Wöchentlich** und legen Sie dann den Tag/die Tage und die Uhrzeit für die Sicherung auf den SFTP-Server fest, oder klicken Sie auf **Intervall** und legen Sie die Uhrzeit für die Sicherung fest.
- 7 Bestandssicherungen werden standardmäßig alle 5 Minuten ausgeführt und sollten regelmäßig erstellt werden. Akzeptieren oder ändern Sie die Standardeinstellung nach Bedarf.
- 8 Klicken Sie auf **Speichern**.

Ergebnisse

Hinweis Die erste wöchentliche Sicherung wird am festgelegten Wochentag zur angegebenen Zeit durchgeführt. Die erste Intervallsicherung wird direkt nach dem Speichern der Sicherungskonfiguration mit aktivierten automatischen Sicherungen durchgeführt.

Es werden drei separate Sicherungsdateien vom NSX Manager gespeichert: auf Knotenebene, auf Clusterebene und vom Bestand. Die Sicherungsdateien werden auf dem SFTP-Server in dem in der Sicherungskonfiguration angegebenen Verzeichnis gespeichert. Innerhalb dieses Verzeichnisses werden die Dateien in den folgenden Verzeichnissen gespeichert:

- /<user specified directory>/cluster-node-backups (Cluster- und Knotensicherungen)
- /<user specified directory>/inventory-summary (Bestandssicherungen)

Wiederherstellen der NSX Manager-Konfiguration

Wenn NSX Manager nicht mehr funktionsfähig ist, können Sie es aus einer Sicherung wiederherstellen. Dazu müssen Sie die Passphrase eingeben, die beim Erstellen der Sicherung angegeben wurde.

Hinweis Das Wiederherstellen einer Sicherung auf derselben NSX Manager-Appliance, auf der die Sicherung erstellt wurde, wird nicht unterstützt.

Verfahren

1 Vorbereiten der Wiederherstellung aus einer NSX Manager-Sicherung

Um NSX Manager-Sicherungen wiederherstellen zu können, müssen Sie erst eine neue NSX Manager-Appliance installieren. Der neue NSX Manager muss mit der gleichen Verwaltungs-IP-Adresse bereitgestellt werden wie der bisherige NSX Manager.

2 Wiederherstellen einer Sicherung

Das Wiederherstellen einer Sicherung führt zu Wiederherstellung des Netzwerkzustand zum Zeitpunkt der Sicherung, zum Wiederherstellen der von NSX Manager verwalteten Konfigurationen und zum Abgleichen von Änderungen, z. B. dem Hinzufügen oder Löschen von Knoten, die seit der Sicherung an der Fabric vorgenommen wurden.

3 Entfernen der NSX-T Data Center-Erweiterung aus vCenter Server

Wenn Sie einen Berechnungsmanager hinzufügen, fügt NSX Manager seine Identität als Erweiterung in vCenter Server hinzu. Wenn dieser vCenter Server nicht in einer NSX-T Data Center-Installation registriert werden soll, können Sie die Erweiterung über den Browser für verwaltete Objekte (Managed Object Browser, MOB) von vCenter Server entfernen.

Vorbereiten der Wiederherstellung aus einer NSX Manager-Sicherung

Um NSX Manager-Sicherungen wiederherstellen zu können, müssen Sie erst eine neue NSX Manager-Appliance installieren. Der neue NSX Manager muss mit der gleichen Verwaltungs-IP-Adresse bereitgestellt werden wie der bisherige NSX Manager.

Hinweis Das Wiederherstellen einer Sicherung auf derselben NSX Manager-Appliance, auf der die Sicherung erstellt wurde, wird nicht unterstützt.

Voraussetzungen

- Ermitteln Sie die Version des NSX Managers, die für die Erstellung der Sicherungen verwendet wurde, und halten Sie eine entsprechende Installationsdatei (OVA, OVF oder QCOW2) dieser Version bereit.
- Ermitteln Sie die IP-Adresse, die NSX Manager für die Erstellung der Knotensicherung zugewiesen wurde.
- Stellen Sie sicher, dass keine Änderungen der Konfiguration von NSX Manager durchgeführt werden, solange der Wiederherstellungsvorgang nicht abgeschlossen ist.

Verfahren

- 1 Wenn die alte NSX Manager-Appliance weiterhin ausgeführt wird (z. B., wenn Sie mit der Wiederherstellung ein Upgrade rückgängig machen möchten), fahren Sie diese herunter.
- 2 Installieren Sie eine neue NSX Manager-Appliance.
 - Die Version der neuen NSX Manager-Appliance muss mit der Version identisch sein, mit der die Sicherungen erstellt wurden.
 - Diese Appliance müssen Sie mit der der Manager-Sicherung entsprechenden IP-Adresse konfigurieren.

Unter *Installationshandbuch für NSX-T Data Center* finden Sie weitere Informationen und Anweisungen zu diesen Schritten.

Nächste Schritte

Stellen Sie die Sicherung wieder her.

Wiederherstellen einer Sicherung

Das Wiederherstellen einer Sicherung führt zu Wiederherstellung des Netzwerkzustand zum Zeitpunkt der Sicherung, zum Wiederherstellen der von NSX Manager verwalteten Konfigurationen und zum

Abgleichen von Änderungen, z. B. dem Hinzufügen oder Löschen von Knoten, die seit der Sicherung an der Fabric vorgenommen wurden.

Hinweis Das Wiederherstellen einer Sicherung auf derselben NSX Manager-Appliance, auf der die Sicherung erstellt wurde, wird nicht unterstützt.

Voraussetzungen

- Stellen Sie sicher, dass Sie über den SSH-Fingerabdruck des Sicherungsdateiservers verfügen. Nur ein SHA256-gehashter ECDSA-Schlüssel wird als Fingerabdruck akzeptiert. Siehe [Suchen nach dem SSH-Fingerabdruck eines Remote-Servers](#).
- Stellen Sie sicher, dass eine Passphrase der Knoten- und Clustersicherungsdateien vorhanden ist.
- Stellen Sie sicher, dass Sie über eine neue Installation von NSX Manager verfügen, für die kein Objekt konfiguriert wurde. Siehe [Vorbereiten der Wiederherstellung aus einer NSX Manager-Sicherung](#).

Verfahren

- 1 Melden Sie sich über einen Browser beim neu installierten NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **System > Dienstprogramme** aus.
- 3 Klicken Sie auf die Registerkarte **Wiederherstellen**.
- 4 Klicken Sie auf **Bearbeiten**, um den Sicherungsdateiserver zu konfigurieren.
- 5 Geben Sie die IP-Adresse oder den Hostnamen ein.
- 6 Ändern Sie die Portnummer, falls erforderlich.
Die Standardeinstellung ist 22.
- 7 Geben Sie den Benutzernamen und das Kennwort zur Anmeldung beim Server ein.
- 8 Geben Sie im Feld **Zielverzeichnis** den absoluten Verzeichnispfad ein, unter dem die Sicherungen gespeichert werden.
- 9 Geben Sie die zur Verschlüsselung der Sicherungsdaten verwendete Passphrase ein.
- 10 Geben Sie den SSH-Fingerabdruck des Servers ein, auf dem die Sicherungen gespeichert sind.
- 11 Klicken Sie auf **Speichern**.
- 12 Wählen Sie eine Sicherung aus.
- 13 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.

Nachdem der Wiederherstellungsvorgang abgeschlossen ist, wird der Bildschirm „Wiederherstellung abgeschlossen“ angezeigt. Er zeigt das Ergebnis der Wiederherstellung, den Zeitstempel der Sicherungsdatei und die Start- und Endzeit des Wiederherstellungsvorgangs. Wenn die Wiederherstellung fehlgeschlagen ist, wird auf dem Bildschirm der Schritt angezeigt, in dem der Fehler aufgetreten ist, z. B. `Current Step: Restoring Cluster (DB)` oder `Current Step: Restoring Node`. Wenn entweder nur die Cluster- oder Knotenwiederherstellung fehlgeschlagen ist, liegt der Fehler möglicherweise nur vorübergehend vor. In diesem Fall müssen Sie nicht auf **Wiederholen** klicken. Sie können den Manager neu starten. Daraufhin wird die Wiederherstellung fortgesetzt.

Sie können auch bestimmen, ob bei der Cluster- oder Knotenwiederherstellung ein Fehler aufgetreten ist, indem Sie den folgenden CLI-Befehl ausführen, um die Systemprotokolldatei anzuzeigen und nach den Zeichenfolgen `Cluster-Wiederherstellung fehlgeschlagen` und `Knotenwiederherstellung fehlgeschlagen` zu suchen.

```
get log-file syslog
```

Führen Sie zum Neustarten des Managers den folgenden CLI-Befehl aus:

```
restart service manager
```

Führen Sie zum Neustarten des Managers den folgenden CLI-Befehl aus:

```
reboot
```

Ergebnisse

Hinweis Wenn Sie nach der Sicherung einen Berechnungsmanager hinzugefügt haben und nach der Wiederherstellung versuchen, den Berechnungsmanager erneut hinzuzufügen, erhalten Sie eine Fehlermeldung über die fehlgeschlagene Registrierung. Sie können den Fehler beheben und den Berechnungsmanager erfolgreich hinzufügen. Weitere Informationen finden Sie in Schritt 5 unter [Hinzufügen eines Berechnungsmanagers](#). Wenn Sie die in einem vCenter Server gespeicherten Informationen zu NSX-T Data Center entfernen möchten, führen Sie die Schritte unter [Entfernen der NSX-T Data Center-Erweiterung aus vCenter Server](#) aus.

Entfernen der NSX-T Data Center-Erweiterung aus vCenter Server

Wenn Sie einen Berechnungsmanager hinzufügen, fügt NSX Manager seine Identität als Erweiterung in vCenter Server hinzu. Wenn dieser vCenter Server nicht in einer NSX-T Data Center-Installation registriert werden soll, können Sie die Erweiterung über den Browser für verwaltete Objekte (Managed Object Browser, MOB) von vCenter Server entfernen.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client als Administrator an.
- 2 Wählen Sie den ESXi-Host aus.
- 3 Klicken Sie auf die Registerkarte **Verwalten > Einstellungen**.
- 4 Wählen Sie im Menü **Erweiterte Systemeinstellungen** aus.

- 5 Aktivieren Sie die Option **Config.HostAgent.plugins.solo.enableMob**.
- 6 Melden Sie sich beim MOB an.
- 7 Klicken Sie auf den Link **content**, der den Wert für die Eigenschaft **content** in der Tabelle „Eigenschaften“ darstellt.
- 8 Klicken Sie auf den Link **ExtensionManager**, der den Wert der Eigenschaft **extensionManager** aus der Tabelle „Eigenschaften“ darstellt.
- 9 Klicken Sie auf den Link **UnregisterExtension** in der Tabelle „Methoden“.
- 10 Geben Sie **com.vmware.nsx.management.nsx** im Textfeld **Wert** ein.
- 11 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.
- 12 Stellen Sie sicher, dass die Erweiterung entfernt wurde, indem Sie auf der vorherigen Seite auf die Methode **FindExtension** klicken und sie durch Eingabe desselben Werts für die Erweiterung aufrufen.
Das Ergebnis sollte `void` sein.

Wiederherstellen eines NSX Controller-Clusters

Kann ein NSX Controller-Cluster nicht wiederhergestellt werden oder müssen Sie mindestens einen Controller aufgrund von Änderungen bei der Clustermitgliedschaft ersetzen, sollten Sie den gesamten Controller-Cluster wiederherstellen.

Vor der Wiederherstellung eines Controller-Clusters stellen Sie zunächst fest, ob Änderungen bei der Steuerungscluster-Mitgliedschaft bezüglich der Informationen auf Managementebene und der Informationen zur eigentlichen Mitgliedschaft auf Controllerebene vorliegen. Die Mitgliedschaft kann abweichen, wenn nach einer Sicherung Änderungen vorgenommen wurden.

- Kann der gesamte Cluster nicht wiederhergestellt werden, finden Sie Informationen unter [Erneute Bereitstellung des NSX Controller-Clusters](#).
- Befolgen Sie die Schritte unten, um festzustellen, ob sich die Clustermitgliedschaft geändert hat. Sollte dies der Fall sein, stellen Sie den Cluster aus einer Sicherung wieder her.

Voraussetzungen

- Stellen Sie sicher, dass Sie über eine aktuelle Sicherung verfügen.
- Führen Sie eine Wiederherstellung aus. Siehe [Wiederherstellen einer Sicherung](#).

Verfahren

- 1 Melden Sie sich bei der CLI eines NSX Manager an und führen Sie den Befehl `get management-cluster status` aus.
- 2 Melden Sie sich bei der CLI eines NSX Controller an und führen Sie den Befehl `get managers` aus, um sicherzustellen, dass der Controller beim Manager registriert ist.

- 3 Führen Sie den Befehl `get control-cluster status` aus.
- 4 Um festzustellen, ob Änderungen bei der Mitgliedschaft vorliegen, vergleichen Sie die IP-Adressen der `get management-cluster status`-Befehlsausgabe mit dem Befehl `get control-cluster status`.

Sind die IP-Adressen im Set dieselben, ist keine weitere Aktion erforderlich. Weicht mindestens eine der IP-Adressen ab, fahren Sie mit den weiteren Schritten fort, um den gesamten Controller-Cluster wiederherzustellen.
- 5 Melden Sie sich bei der CLI der NSX Controller an, um mithilfe des Befehls `get control-cluster status` festzustellen, welcher der Master-Controller ist.

Die Ausgabe des Master-Controllers ist `is master: true`.
- 6 Führen Sie den Befehl `stop service <controller>` auf einem anderen als dem Master-Controller aus.
- 7 Melden Sie sich beim Master-Controller an und führen Sie den Befehl `detach control-cluster <ip-address[:port]>` aus, um den Controller aus dem vorherigen Schritt, bei dem es sich nicht um den Master-Controller handelt, zu trennen.
- 8 (Optional) Führen Sie den Befehl `detach controller <uuid>` auf dem NSX Manager zum Trennen dieses Controllers nur aus, wenn dieser Controller durch den Befehl `get management-cluster status` auf dem NSX Manager angezeigt wird.
- 9 Melden Sie sich bei der CLI des NSX Controllers an und führen Sie den Befehl `deactivate control-cluster` aus.
- 10 Entfernen Sie die Bootstrap- und die UUID-Datei mit den folgenden Befehlen: `rm -r /opt/vmware/etc/bootstrap-config` und `rm -r /config/vmware/node-uuid`
- 11 Führen Sie die Schritte 6–10 für die übrigen Controller aus, die keine Master-Controller sind.
- 12 Melden Sie sich bei der CLI des Master-Controllers an, und führen Sie den Befehl `stop service <controller>` aus.
- 13 Führen Sie den Befehl `detach controller <uuid>` auf dem NSX Manager aus, um diesen Controller zu trennen.
- 14 Melden Sie sich bei der CLI des Master-Controllers an, und führen Sie den Befehl `deactivate control-cluster` aus.
- 15 Entfernen Sie die Bootstrap- und die UUID-Datei mit den folgenden Befehlen: `rm -r /opt/vmware/etc/bootstrap-config` und `rm -r /config/vmware/node-uuid`
- 16 Führen Sie den Befehl `get management-cluster status` über den NSX Manager aus. Werden in der Ausgabe weiterhin Controller angezeigt, führen Sie den Befehl `detach controller <uuid>` aus, um die restlichen zu entfernen.

Nächste Schritte

Führen Sie die folgenden Aufgaben in der aufgeführten Reihenfolge aus.

- 1 Führen Sie eine Wiederherstellung aus.
- 2 Treten Sie über die Managementebene den NSX Controllern bei, wie im *Installationshandbuch für NSX-T* beschrieben.
- 3 Stellen Sie den NSX Controller-Cluster erneut bereit, wie im *Installationshandbuch für NSX-T* beschrieben.

Verwalten von Appliances und Appliance-Clustern

Jede Installation von NSX-T Data Center erfordert und unterstützt nur eine Instanz von NSX Manager. NSX Controller-Cluster müssen über drei Mitglieder verfügen. NSX Edge-Cluster müssen über mindestens zwei Mitglieder verfügen.

Wenn eine Appliance in einem NSX Controller- oder NSX Edge-Cluster nicht mehr funktionsfähig ist oder wenn Sie diese aus irgendeinem Grund entfernen müssen, können Sie diese durch eine neue Appliance ersetzen.

Wichtig Wenn Sie die Clustermitgliedschaft von NSX Controller oder NSX Edge ändern, müssen Sie die Clustersicherung nach der Sicherung der neuen Konfiguration durchführen. Siehe [Sichern und Wiederherstellen von NSX Manager](#).

Verwalten von NSX Manager

Sie können den Status von NSX Manager überprüfen und ihn neu starten, falls sie nicht mehr funktioniert.

Abrufen des Status von NSX Manager

Sie können den Status von NSX Manager über die NSX Manager-Benutzeroberfläche anzeigen oder mit einem CLI-Befehl abrufen.

Verfahren

- 1 Melden Sie sich über einen Browser unter `http://<nsx-manager-ip-address>` bei NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **System > Komponenten** aus.
Der Status von NSX Manager wird angezeigt.
- 3 Alternativ können Sie sich bei der CLI von NSX Manager anmelden.
- 4 Führen Sie den Befehl `get management-cluster status` aus. Beispiel:

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 10.172.121.217 (UUID 42191561-79dc-710a-74f1-d15f10cd2c40) Online

Management cluster status: STABLE
```

```

Number of nodes in control cluster: 3
- 10.172.121.91    (UUID ab35851f-e616-4760-8d7a-c4386c537382)
- 10.172.122.187  (UUID d159b758-c320-411f-aa67-1e2fd35f5ef2)
- 10.172.122.138  (UUID 12a3b19d-26a0-492e-836e-e9a3cc25e799)

Control cluster status: DEGRADED

```

Hinweis Auch wenn als Ergebnis Verwaltungscluster ausgegeben wird, kann es sich nur um eine Instanz von NSX Manager handeln.

Neustart von NSX Manager

Sie können NSX Manager mit einem CLI-Befehl neu starten, um die Appliance nach kritischen Fehlern wiederherzustellen.

Verfahren

- 1 Melden Sie sich bei der CLI von NSX Manager an.
- 2 Führen Sie den Befehl `reboot` aus. Beispiel:

```

nsx-manager> reboot
Are you sure you want to reboot (yes/no): y

```

Verwalten von NSX Controller-Clustern

In Produktionsbereitstellungen muss der NSX Controller-Cluster über drei Mitglieder verfügen, um Ausfälle im Hinblick auf die NSX-Steuerungskomponente zu vermeiden. Jeder Controller muss auf einem eindeutigen Hypervisor-Host platziert werden (insgesamt drei physische Hypervisor-Hosts), um die Beeinträchtigung der NSX-Steuerungskomponente durch den Ausfall eines einzelnen physischen Hypervisors zu vermeiden. In Bereitstellungen für Labor- und Testumgebungen ohne Produktionsarbeitslasten ist die Ausführung eines einzelnen Controllers zur Einsparung von Ressourcen akzeptabel.

Ein NSX Controller-Cluster muss über die Mehrheit verfügen, damit er ordnungsgemäß funktioniert. Wenn zwei von drei Mitgliedern online sind, besitzt der Cluster weiterhin die Mehrheit. Sie müssen den Cluster mit den drei Mitgliedern wiederherstellen, indem Sie den Offline-NSX Controller aktivieren. Wenn dies nicht möglich ist, können Sie ihn ersetzen. Siehe [Ersetzen eines Mitglieds des NSX Controller-Clusters](#).

Wenn nur eines von drei Mitgliedern online ist, verfügt der Cluster nicht mehr über die Mehrheit und funktioniert nicht ordnungsgemäß. Wenn Sie keines der Mitglieder, die offline sind, aktivieren können, können Sie die fehlgeschlagenen NSX Controller ersetzen oder den NSX Controller-Cluster erneut bereitstellen. Siehe [Erneute Bereitstellung des NSX Controller-Clusters](#).

Voraussetzungen

Stellen Sie anhand der Fehlerbehebung sicher, dass die Appliances nicht wiederhergestellt werden können. Durch diese Schritte können Sie die Appliances z. B. eventuell wiederherstellen, ohne sie ersetzen zu müssen.

- Stellen Sie sicher, dass die Appliances über Netzwerkkonnektivität verfügen und beheben Sie dies, falls nicht.
- Starten Sie die Appliances neu.

Nächste Schritte

Rufen Sie den Clusterstatus von NSX Controller ab. Siehe [Abrufen des Clusterstatus des NSX Controller](#).

Abrufen des Clusterstatus des NSX Controller

Sie haben die Möglichkeit, den Status des NSX Controller-Clusters des NSX Manager zu ermitteln. Sie können auch den Status jedes NSX Controller von seiner Befehlszeilenschnittstelle aus überprüfen.

Das Abrufen des Clusterstatus des NSX Controller und der Clustermitglieder bietet eine Unterstützung bei der Ermittlung der Ursache eines Problems mit dem NSX Controller-Cluster.

Tabelle 17-4. Clusterstatus des NSX Controller

	Ist mindestens ein Controller beim NSX Manager registriert?	Verfügt der NSX Controller-Cluster über die Mehrheit?	Wurden Clustermitglieder von NSX Controller heruntergefahren?
NO_CONTROLLERS	Nein	Nicht verfügbar	Nicht verfügbar
UNAVAILABLE	Unbekannt	Unbekannt	Unbekannt
STABLE	Ja	Ja	Nein
DEGRADED	Ja	Ja	Ja
UNSTABLE	Ja	Nein	Nein

Verfahren

- 1 Melden Sie sich bei der NSX Manager-Befehlszeilenschnittstelle (CLI) an.
- 2 Führen Sie den Befehl `get management-cluster status` aus.

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.52 (UUID 1228c336-3932-4b5b-b87e-9f66259cebcd)
- 192.168.110.53 (UUID f5348a2e-2d59-4edc-9618-2c05ac073fd8)
- 192.168.110.51 (UUID 03fad907-612f-4068-8109-efdf73002038)

Control cluster status: STABLE
```

- 3 Melden Sie sich bei der NSX Controller-Befehlszeilenschnittstelle (CLI) an.
- 4 Führen Sie den Befehl `get control-cluster status` aus.

```
nsx-controller-1> get control-cluster status
uuid: 03fad907-612f-4068-8109-efdf73002038
is master: true
in majority: true


| uuid                                 | address        | status |
|--------------------------------------|----------------|--------|
| 03fad907-612f-4068-8109-efdf73002038 | 192.168.110.51 | active |
| 1228c336-3932-4b5b-b87e-9f66259cebcd | 192.168.110.52 | active |
| f5348a2e-2d59-4edc-9618-2c05ac073fd8 | 192.168.110.53 | active |


```

Neustarten von NSX Controller-Clustermitgliedern

Wenn Sie mehrere Mitglieder Ihres NSX Controller-Clusters neu starten möchten, müssen Sie jedes Mitglied einzeln starten. Ein Cluster mit drei Mitgliedern kann über die Mehrheit verfügen, wenn ein Mitglied offline ist. Wenn zwei Mitglieder offline sind, verliert der Cluster die Mehrheit und funktioniert nicht mehr ordnungsgemäß.

Verfahren

- 1 Melden Sie sich an der Befehlszeilenschnittstelle (CLI) des NSX Manager an.
- 2 Rufen Sie den Status der Verwaltungs- und Controller-Cluster ab.

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.53 (UUID f5348a2e-2d59-4edc-9618-2c05ac073fd8)
- 192.168.110.51 (UUID 03fad907-612f-4068-8109-efdf73002038)
- 192.168.110.52 (UUID 1228c336-3932-4b5b-b87e-9f66259cebcd)

Control cluster status: STABLE
```

- 3 Melden Sie sich an der Befehlszeilenschnittstelle (CLI) des NSX Controller an, der neu gestartet werden muss, und führen Sie den Neustart durch.

```
nsx-controller-2> reboot
Are you sure you want to reboot (yes/no): y
```

- 4 Rufen Sie den Status der Verwaltungs- und Controller-Cluster erneut ab. Warten Sie, bis der Controller-Cluster über den Status STABLE (Stabil) verfügt, bevor Sie weitere Mitglieder neu starten.

In diesem Beispiel wird der NSX Controller 192.168.110.53 neu gestartet, der Status des Controller-Clusters lautet auf DEGRADED (Herabgestuft). Das bedeutet, dass der Cluster in der Mehrheit ist, aber ein Mitglied heruntergefahren wurde. Unter [Abrufen des Clusterstatus des NSX Controller](#) finden Sie weitere Informationen über den Clusterstatus des NSX Controllers.

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.53 (UUID f5348a2e-2d59-4edc-9618-2c05ac073fd8)
- 192.168.110.52 (UUID 1228c336-3932-4b5b-b87e-9f66259cebcd)
- 192.168.110.51 (UUID 03fad907-612f-4068-8109-efdf73002038)

Control cluster status: DEGRADED
```

Erreicht der NSX Controller-Cluster den Status STABLE (Stabil), können Sie auf sichere Weise weitere Mitglieder neu starten.

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.53 (UUID f5348a2e-2d59-4edc-9618-2c05ac073fd8)
- 192.168.110.51 (UUID 03fad907-612f-4068-8109-efdf73002038)
- 192.168.110.52 (UUID 1228c336-3932-4b5b-b87e-9f66259cebcd)

Control cluster status: STABLE
```

- 5 Wenn Sie weitere Informationen zum Status der einzelnen NSX Controller-Appliance benötigen, melden Sie sich beim NSX Controller an und führen Sie den Befehl `get control-cluster status` aus.

```
nsx-controller-1> get control-cluster status
uuid: 03fad907-612f-4068-8109-efdf73002038
is master: true
in majority: true

  uuid                                address                status
  ----                                -
03fad907-612f-4068-8109-efdf73002038 192.168.110.51         active
1228c336-3932-4b5b-b87e-9f66259cebcd 192.168.110.52         active
f5348a2e-2d59-4edc-9618-2c05ac073fd8 192.168.110.53         not active
```

- 6 Wiederholen Sie die Schritte zum Neustart weiterer NSX Controller-Appliances bei Bedarf.

Ersetzen eines Mitglieds des NSX Controller-Clusters

Ein NSX Controller-Cluster muss über mindestens drei Mitglieder verfügen. Wenn eine NSX Controller-Appliance nicht mehr funktionsfähig ist oder Sie sie aus einem anderen Grund aus dem Cluster entfernen möchten, müssen Sie zuerst eine neue NSX Controller-Appliance für einen Cluster mit vier Mitgliedern hinzufügen. Wenn das vierte Mitglied hinzugefügt wurde, können Sie eine NSX Controller-Appliance aus dem Cluster entfernen.

Voraussetzungen

- Stellen Sie anhand der Fehlerbehebung sicher, dass die Appliances nicht wiederhergestellt werden können. Durch diese Schritte können Sie die Appliances z. B. eventuell wiederherstellen, ohne sie ersetzen zu müssen.
 - Stellen Sie sicher, dass die Appliances über Netzwerkkonnektivität verfügen und beheben Sie dies, falls nicht.
 - Starten Sie die Appliances neu.
- Ermitteln Sie die Version des NSX Controllers, den Sie ersetzen möchten, und halten Sie eine entsprechende Installationsdatei (OVA, OVF oder QCOW2) dieser Version bereit.

Verfahren

- 1 Installieren und konfigurieren Sie einen neuen NSX Controller.

Unter *Installationshandbuch für NSX-T Data Center* finden Sie weitere Informationen und Anweisungen zu diesen Schritten.

- a Installieren Sie eine neue NSX Controller-Appliance.

Die Version des neuen NSX Controllers muss mit jener des ersetzten NSX Controllers identisch sein.

- b Verbinden Sie den neuen NSX Controller mit der Verwaltungskomponente.
- c Verbinden Sie den neuen NSX Controller mit dem Controller-Cluster.

- 2 Fahren Sie den NSX Controller herunter, der aus dem Cluster entfernt werden soll.
- 3 Melden Sie sich bei einem anderen NSX Controller an und prüfen Sie, ob der NSX Controller, den Sie entfernen möchten, den Status Nicht aktiv besitzt.

```
nsx-controller-1> get control-cluster status
uuid: e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b
is master: true
in majority: true

```

uuid	address	status
06996547-f50c-43c0-95c1-8bb644dea498	192.168.110.53	active
471e5ac0-194b-437c-9359-564cea845333	192.168.110.54	active
e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b	192.168.110.51	active
863f9669-509f-4eba-b0ac-61a9702a242b	192.168.110.52	not active

4 Trennen Sie den Controller vom Cluster.

```
nsx-controller-1> detach control-cluster 192.168.110.52
Successfully detached node from the control cluster.
```

5 Trennen Sie den Controller von der Verwaltungskomponente.

```
nsx-manager-1> detach controller 863f9669-509f-4eba-b0ac-61a9702a242b
The detach operation completed successfully
```

6 Stellen Sie sicher, dass die Controller aktiv sind und der Controller-Cluster stabil ist.

Von einem NSX Controller aus:

```
nsx-controller-1> get control-cluster status
uuid: e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b
is master: true
in majority: true
```

uuid	address	status
06996547-f50c-43c0-95c1-8bb644dea498	192.168.110.53	active
471e5ac0-194b-437c-9359-564cea845333	192.168.110.54	active
e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b	192.168.110.51	active

Von einem NSX Manager aus:

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 4213216E-F93A-71B2-DA20-AFE5E714644F) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.51 (UUID e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b)
- 192.168.110.53 (UUID 06996547-f50c-43c0-95c1-8bb644dea498)
- 192.168.110.54 (UUID 471e5ac0-194b-437c-9359-564cea845333)

Control cluster status: STABLE
```

Ergebnisse

Hinweis Der Controller, der mit dem Befehl `detach` entfernt wurde, behält weiterhin einige Konfigurationsinformationen bei. Wenn Sie den Controller erneut mit einem Controller-Cluster verbinden möchten, müssen Sie den folgenden CLI-Befehl auf dem Controller ausführen, um die veralteten Informationen zu entfernen:

```
deactivate control-cluster
```

Erneute Bereitstellung des NSX Controller-Clusters

Wenn durch das Ersetzen eines Controllers NSX Controller-Clusterprobleme nicht behoben werden konnten oder wenn mehrere NSX Controller-Appliances nicht wiederhergestellt werden können, lässt sich

der gesamte Cluster neu bereitstellen. Der NSX Manager enthält die gesamte gewünschte Konfiguration und kann zum erneuten Erstellen Ihres NSX Controller-Clusters verwendet werden.

Die Datenpfadverbindungen werden während der Wiederherstellung des NSX Controller-Clusters nicht unterbrochen.

Voraussetzungen

- Stellen Sie anhand der Fehlerbehebung sicher, dass die Appliances nicht wiederhergestellt werden können. Durch diese Schritte können Sie die Appliances z. B. eventuell wiederherstellen, ohne sie ersetzen zu müssen.
 - Stellen Sie sicher, dass die Appliances über Netzwerkkonnektivität verfügen und beheben Sie dies, falls nicht.
 - Starten Sie die Appliances neu.
- Ermitteln Sie die Version des NSX Controllers, den Sie ersetzen möchten, und halten Sie eine entsprechende Installationsdatei (OVA, OVF oder QCOW2) dieser Version bereit.
- Ermitteln Sie die IP-Adressen, die den NSX Controller-Appliances zugewiesen wurden.

Verfahren

- 1 Fahren Sie alle Controller im NSX Controller-Cluster herunter.
- 2 Trennen Sie die Controller von NSX Manager.
 - a Melden Sie sich bei der NSX Manager-Befehlszeilenschnittstelle (CLI) an.
 - b Rufen Sie mit dem Befehl `get management-cluster status` eine Liste der Controller ab.

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 422EC8D8-B43F-D206-5048-781A5AECDC6) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.53 (UUID c28d0ac7-3107-4548-817a-50d76db007ab)
- 192.168.110.51 (UUID 4a0916c7-2f4d-48c2-81b6-29b7b3758ef4)
- 192.168.110.52 (UUID 1a409f24-9b9a-431e-a03a-1929db74bf00)

Control cluster status: UNSTABLE
```

- c Trennen Sie mit dem Befehl `detach controller` die Controller.

```
nsx-manager-1> detach controller 1a409f24-9b9a-431e-a03a-1929db74bf00
The detach operation completed successfully
nsx-manager-1> detach controller 4a0916c7-2f4d-48c2-81b6-29b7b3758ef4
The detach operation completed successfully
nsx-manager-1> detach controller c28d0ac7-3107-4548-817a-50d76db007ab
The detach operation completed successfully
```

3 Installieren Sie drei NSX Controller-Appliances und erstellen Sie einen neuen NSX Controller-Cluster.

Unter *Installationshandbuch für NSX-T Data Center* finden Sie weitere Informationen und Anweisungen zu diesen Schritten.

- a Installieren Sie drei NSX Controller-Appliances.
 - Die Version der neuen NSX Controller-Appliances muss mit jener der ersetzten NSX Controller-Appliances identisch sein.
 - Weisen Sie die neuen Controller der gleichen IP-Adresse zu, die für die alten Controller verwendet wurde.
- b Verbinden Sie die NSX Controller-Appliances mit der Verwaltungskomponente.
- c Initialisieren Sie auf einer NSX Controller-Apliance den Controller-Cluster.
- d Verbinden Sie die beiden anderen Controller mit dem Controller-Cluster.

Verwalten von NSX Edge-Clustern

Sie können ein NSX Edge ersetzen, z. B., wenn es nicht mehr funktionsfähig ist oder wenn Sie die Hardware ändern müssen. Nachdem Sie einen neuen NSX Edge installiert und einen neuen Transportknoten angelegt haben, können Sie den NSX Edge-Cluster so modifizieren, dass er den alten Transportknoten durch den neuen ersetzt.

Hinweis Wenn Sie einen Tier-1-NSX Edge-Cluster entfernen, ist die Instanz des verteilten Tier-1-Routers (Distributed Router, DR) kurzzeitig außer Betrieb.

Verfahren

- 1 Wenn das NSX Edge, das Sie ersetzen möchten, noch in Betrieb ist, können Sie es in den Wartungsmodus versetzen, um die Ausfallzeit zu minimieren. Wenn die Hochverfügbarkeit auf den zugeordneten logischen Routern aktiviert ist, verwenden diese nach dem Wechsel in den Wartungsmodus ein anderes NSX Edge-Cluster-Mitglied. Wenn NSX Edge nicht mehr funktionsfähig ist, ist dies nicht erforderlich.
 - a Rufen Sie die Fabric-Knoten-ID des fehlgeschlagenen Fabric-Knotens ab.

```
https://192.168.110.201/api/v1/fabric/nodes
...
  "resource_type": "EdgeNode",
  "id": "a0f4fa74-e77c-11e5-8701-005056aeed61",
  "display_name": "edgenode-02a",
...
```

- b Versetzen Sie den fehlgeschlagenen NSX Edge-Knoten in den Wartungsmodus.

```
POST https://192.168.110.201/api/v1/fabric/nodes/a0f4fa74-e77c-11e5-8701-005056aeed61?
action=enter_maintenance_mode
```

2 Installieren Sie ein neues NSX Edge.

Unter *Installationshandbuch für NSX-T Data Center* finden Sie weitere Informationen und Anweisungen zu diesen Schritten.

3 Verbinden Sie mit dem Befehl `join management-plane` das neue NSX Edge mit der Verwaltungskomponente.

Unter *Installationshandbuch für NSX-T Data Center* finden Sie weitere Informationen und Anweisungen zu diesen Schritten.

4 Konfigurieren Sie NSX Edge als Transportknoten.

Unter *Installationshandbuch für NSX-T Data Center* finden Sie weitere Informationen und Anweisungen zu diesen Schritten.

Sie können die Konfiguration des Transportknotens der fehlgeschlagenen NSX Edge-Appliance von der API abrufen und damit einen neuen Transportknoten erstellen.

a Rufen Sie die Fabric-Knoten-ID des neuen Fabric-Knotens ab.

```
https://192.168.110.201/api/v1/fabric/nodes
...
  "resource_type": "EdgeNode",
  "id": "d61c8d86-f4b8-11e5-b1b2-005056ae3c10",
  "display_name": "edgenode-03a",
  ...
```

b Rufen Sie die Transportknoten-ID des fehlgeschlagenen Transportknotens ab.

```
GET https://192.168.110.201/api/v1/transport-nodes
...
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "73cb00c9-70d0-4808-abfe-a12a43251133",
  "display_name": "TN-edgenode-01a",
  ...
```

- c Rufen Sie die Transportknotenkonfiguration des fehlgeschlagenen Transportknotens ab.

```
GET https://192.168.110.201/api/v1/transport-nodes/73cb00c9-70d0-4808-abfe-a12a43251133
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "73cb00c9-70d0-4808-abfe-a12a43251133",
  "display_name": "TN-edgenode-01a",
  "tags": [],
  "transport_zone_endpoints": [
    ...
  ],
  "host_switches": [
    ...
  ],
  "node_id": "a0f4fa74-e77c-11e5-8701-005056aeed61",
  "_create_time": 1457696199196,
  "_last_modified_user": "admin",
  "_last_modified_time": 1457696225606,
  "_create_user": "admin",
  "_revision": 2
}
```

- d Erstellen Sie mit POST /api/v1/transport-nodes den neuen Transportknoten.

Geben Sie im Anforderungstext die folgenden Informationen für den neuen Transportknoten an:

- description für den neuen Transportknoten (optional)
- display_name für den neuen Transportknoten
- node_id des Fabric-Knotens für das Erstellen des neuen Transportknotens

Kopieren Sie die folgenden Informationen des fehlgeschlagenen Transportknotens in den Anforderungstext:

- transport_zone_endpoints
- host_switches
- tags (optional)

```
POST https://192.168.110.201/api/v1/transport-nodes
{
  "description": "",
  "display_name": "TN-edgenode-03a",
  "tags": [
    ...
  ],
  "transport_zone_endpoints": [
    ...
  ],
  "host_switches": [
```

```
...  
],  
"node_id": "d61c8d86-f4b8-11e5-b1b2-005056ae3c10"  
}
```

- 5 Bearbeiten Sie den NSX Edge-Cluster und ersetzen Sie den fehlgeschlagenen Transportknoten durch den neuen Transportknoten.

- a Rufen Sie die ID des neuen Transportknotens und des fehlgeschlagenen Transportknotens ab. Das Feld `id` enthält die Transportknoten-ID.

```
GET https://192.168.110.201/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",
```

- b Rufen Sie die ID des NSX Edge-Clusters ab. Das Feld `id` enthält die NSX Edge-Cluster-ID. Rufen Sie die Mitglieder des NSX Edge-Clusters vom Array `members` ab.

```
GET https://192.168.110.201/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"
    }
  ],
```

- c Bearbeiten Sie den NSX Edge-Cluster und ersetzen Sie den fehlgeschlagenen Transportknoten durch den neuen Transportknoten. Der Wert für `member_index` muss mit dem Index des fehlgeschlagenen Transportknotens übereinstimmen.

Vorsicht Wenn NSX Edge weiter in Betrieb ist, wird dieser durch diese Aktion unterbrochen. Dadurch werden alle logischen Routerports vom fehlgeschlagenen Transportknoten zum neuen Transportknoten übertragen.

In diesem Beispiel ist der Transportknoten TN-edgenode-01a (73cb00c9-70d0-4808-abfe-a12a43251133) fehlgeschlagen und wurde 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://192.168.110.201/api/v1/edge-clusters/9a302df7-0833-4237-af1f-4d826c25ad78?
action=replace_transport_node
{
  "member_index": 0,
  "transport_node_id" : "890f0e3c-aa81-46aa-843b-8ac25fe30bd3"
}
```

6 (Optional) Löschen Sie den fehlgeschlagenen Transportknoten und den NSX Edge-Knoten.

Protokollmeldungen

Protokollmeldungen aller NSX-T Data Center-Komponenten einschließlich den auf ESXi-Hosts ausgeführten entsprechen dem Syslog-Format gemäß RFC 5424. Protokollmeldungen von KVM-Hosts sind im RFC-3164-Format. Die Protokolldateien befinden sich im Verzeichnis `/var/log`.

Auf NSX-T Data Center-Appliances können Sie den folgenden NSX-T Data Center-CLI-Befehl zum Anzeigen der Protokolle ausführen:

```
get log-file <auth.log | http.log | kern.log | manager.log | node-mgmt.log | syslog> [follow]
```

Auf Hypervisoren können Sie Linux-Befehle wie z. B. `tac`, `tail`, `grep` oder `more` verwenden, um die Protokolle anzuzeigen. Diese Befehle können Sie auch auf NSX-T Data Center--Appliances verwenden.

Weitere Informationen zu RFC 5424 finden Sie unter <https://tools.ietf.org/html/rfc5424>. Weitere Informationen zu RFC 3164 finden Sie unter <https://tools.ietf.org/html/rfc3164>.

RFC 5424 legt für Protokollmeldungen das folgende Format fest:

```
<facility * 8 + severity> version UTC-TZ hostname APP-NAME procid MSGID [structured-data] msg
```

Beispiel für eine Protokollmeldung:

```
<187>1 2016-03-15T22:53:00.114Z nsx-manager NSX - SYSTEM [nsx@6876 comp="nsx-manager"
errorCode="MP4039" subcomp="manager"] Connection verification failed for broker '10.160.108.196'.
Marking broker unhealthy.
```

Jede Nachricht enthält Komponentendetails (`comp`) und Unterkomponentendetails (`subcomp`), die es erleichtern, die Quelle der Nachricht zu identifizieren.

NSX-T Data Center erstellt reguläre Protokolle („facility local6“ mit einem numerischen Wert von 22) und Überwachungsprotokolle („facility local7“ mit einem numerischen Wert von 23). Alle API-Aufrufe lösen ein Überwachungsprotokoll aus.

Ein Eintrag im Überwachungsprotokoll, der einem API-Aufruf zugeordnet ist, enthält die folgende Informationen:

- Den Parameter `entId` mit einer Element-ID zur Identifizierung des Objekts der-API.
- Den Parameter `req-id` mit einer Anforderungs-ID zur Identifizierung eines bestimmten API-Aufrufs.
- Den Parameter `ereqId` mit einer ID, die auf eine externe Anforderung verweist, wenn der API-Aufruf den Header `X-NSX-EREQID: <string>` enthält.
- Den Parameter `euser` der auf einen externen Benutzer verweist, wenn der API-Aufruf den Header `X-NSX-EUSER: <string>` enthält.

RFC 5424 definiert die folgenden Ebenen für den Schweregrad:

Schweregrad	Beschreibung
0	Notfall: Das System steht nicht zur Verfügung
1	Ernste Warnung: Es muss sofort reagiert werden
2	Kritisch: Kritische Bedingungen
3	Fehler: Fehlerbedingungen
4	Warnung: Warnbedingungen
5	Hinweis: Normale, aber signifikante Bedingung
6	Information: Informationsmeldungen
7	Debug: Meldungen auf Debug-Ebene

Alle Protokolle mit dem Schweregrad „Notfall“, „Ernste Warnung“, „Kritisch“ und „Fehler“ enthalten einen eindeutigen Fehlercode im Abschnitt der strukturierten Daten der Protokollmeldung. Der Fehlercode besteht aus einer Zeichenfolge und einer Dezimalzahl. Die Zeichenfolge steht für ein bestimmtes Modul.

Das MSGID-Feld identifiziert den Meldungstyp. Eine Liste der Meldungs-IDs finden Sie unter [Protokollmeldungs-IDs](#).

Konfigurieren der Remoteprotokollierung

Sie können NSX-T Data Center-Appliances und -Hypervisoren für das Senden von Meldungen zu einem Server für Remoteprotokollierung konfigurieren.

Remoteprotokollierung wird auf NSX Manager-, NSX Controller-, NSX Edge- und Hypervisor-Knoten unterstützt. Sie müssen die Remoteprotokollierung auf jedem Knoten einzeln konfigurieren.

Auf einem KVM-Host konfiguriert das NSX-T Data Center-Installationspaket den rsyslog-Daemon automatisch, indem es entsprechende Konfigurationsdateien im Verzeichnis `/etc/rsyslog.d` platziert.

Voraussetzungen

- Konfigurieren Sie einen Protokollierungsserver für den Empfang der Protokolle.

Verfahren

1 So konfigurieren Sie die Remoteprotokollierung auf einer NSX-T Data Center-Appliance:

- a Führen Sie den folgenden Befehl aus, um einen Protokollserver zu konfigurieren und festzulegen, welche Arten von Meldungen an den Protokollserver gesendet werden sollen. Mehrere facility- oder messageid-Parameter können, durch Kommas ohne Leerzeichen getrennt, als Liste angegeben werden.

```
set logging-server <hostname-or-ip-address[:port]> proto <proto> level <level> [facility <facility>] [messageid <messageid>] [certificate <filename>] [structured-data <structured-data>]
```

Weitere Informationen zu diesem Befehl finden Sie in der *Referenz zur NSX-T-CLI*. Sie haben die Möglichkeit, den Befehl mehrmals zum Hinzufügen mehrerer Konfigurationen für Protokollierungsserver auszuführen. Beispiel:

```
nsx> set logging-server 192.168.110.60 proto udp level info facility syslog messageid SYSTEM,FABRIC
nsx> set logging-server 192.168.110.60 proto udp level info facility auth,user
```

- b Sie können die Protokollierungskonfiguration mit dem Befehl `get logging-server` anzeigen. Beispiel:

```
nsx> get logging-servers
192.168.110.60 proto udp level info facility syslog messageid SYSTEM,FABRIC
192.168.110.60 proto udp level info facility auth,user
```

2 So konfigurieren Sie die Remoteprotokollierung auf einem ESXi-Host:

- a Führen Sie die folgenden Befehle aus, um Syslog zu konfigurieren und eine Testnachricht zu senden:

```
esxcli network firewall ruleset set -r syslog -e true
esxcli system syslog config set --loghost=udp://<log server IP>:<port>
esxcli system syslog reload
esxcli system syslog mark -s "This is a test message"
```

- b Sie können die Konfiguration durch Ausführen des folgenden Befehls anzeigen:

```
esxcli system syslog config get
```

3 So konfigurieren Sie die Remoteprotokollierung auf einem KVM-Host:

- a Bearbeiten Sie die Datei `/etc/rsyslog.d/10-vmware-remote-logging.conf`, um sie an Ihre Umgebung anzupassen.
- b Fügen Sie der Datei die folgende Zeile hinzu:

```
*.* @<ip>:514;RFC5424fmt
```

- c Führen Sie den folgenden Befehl aus:

```
service rsyslog restart
```

Protokollmeldungs-IDs

In einer Protokollmeldung identifiziert das Meldungs-ID-Feld den Meldungstyp. Sie können den Parameter `messageid` im Befehl `set logging-server` verwenden, um zu filtern, welche Protokollmeldungen an den Protokollierungsserver gesendet werden.

Tabelle 17-5. Protokollmeldungs-IDs

Meldungs-ID	Beispiele
FABRIC	Hostknoten Hostvorbereitung Edge-Knoten Transportzone Transportknoten Uplink-Profil Clusterprofil Edge-Cluster Bridge-Cluster und -Endpoints
SWITCHING	Logischer Switch Ports für logischen Switch Switching-Profil Funktionen der Switch-Sicherheit
ROUTING	Logischer Router Logische Routerports Statisches Routing Dynamisches Routing NAT
FIREWALL	Firewallregeln Firewallregelabschnitte
FIREWALL-PKTLOG	Protokolle der Firewallverbindung Protokolle des Firewallpakets

Tabelle 17-5. Protokollmeldungs-IDs (Fortsetzung)

Meldungs-ID	Beispiele
GROUPING	IP Sets MAC Sets NS-Gruppen NS-Dienste NS-Dienstgruppen VNI-Pool IP-Pool
DHCP	DHCP-Relay
SYSTEM	Appliance-Verwaltung (remote syslog, ntp, etc.) Clusterverwaltung Vertrauensverwaltung Lizenzierung Benutzer und Rollen Aufgabenverwaltung Installation (NSX Manager, NSX Controller) Upgrade (NSX Manager, NSX Controller, NSX Edge und Upgrades für Hostpakete) Umsetzung Tags
MONITORING	SNMP Portverbindung Traceflow
-	Alle anderen Protokollmeldungen

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.

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

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.

Voraussetzungen

- Installieren Sie mindestens einen IPFIX-Collector.
- Stellen Sie sicher, dass die IPFIX-Collectors über Netzwerkkonnektivität zu den Hypervisors verfügen.
- Stellen Sie sicher, dass alle relevanten Firewalls, einschließlich der ESXi-Firewall, den Datenverkehr auf den IPFIX-Collector-Ports zulassen.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **Tools > IPFIX** aus.
- 3 Klicken Sie für die Switch-IPFIX-Konfiguration auf die Registerkarte **Switch-IPFIX-Collectors**.
- 4 Klicken Sie auf **Hinzufügen**.
- 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 **Speichern**.

Konfigurieren von Switch-IPFIX-Profilen

Sie können IPFIX-Profile für Switches konfigurieren.

Verfahren

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

- 2 Wählen Sie im Navigationsbereich die Option **Tools > IPFIX** aus.
- 3 Klicken Sie auf die Registerkarte **Switch-IPFIX-Profile**.
- 4 Klicken Sie auf **Hinzufügen**, um ein Profil hinzuzufügen.

Einstellung	Beschreibung
Name und Beschreibung	Geben Sie einen Namen und optional eine Beschreibung ein.
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.
Sampling-Wahrscheinlichkeit (%)	Der Prozentsatz der Pakete, die abgetastet werden (ungefähr) Wenn Sie diese Einstellung erhöhen, kann sich dies auf die Leistung der Hypervisors und Collectors auswirken. Wenn alle Hypervisors mehr IPFIX-Pakete an den Collector senden, kann der Collector möglicherweise nicht alle Pakete erfassen. Indem Sie die Wahrscheinlichkeit auf dem Standardwert von 0,1 % belassen, bleibt die Auswirkung auf die Leistung gering.
Beobachtungsdomänen-ID	Mit der Beobachtungsdomänen-ID wird festgelegt, aus welcher Beobachtungsdomäne die Netzwerk-Flows stammen. Geben Sie 0 ein, um keine bestimmte Beobachtungsdomäne anzugeben.
Collector-Profil	Wählen Sie einen Switch-IPFIX-Collector aus, den Sie im vorherigen Schritt konfiguriert haben.
Priorität	Dieser Parameter dient zur Behebung von Konflikten, wenn mehrere Profile anwendbar sind. IPFIX-Exporter verwendet nur das Profil mit der höchsten Priorität. Ein niedrigerer Wert bedeutet eine höhere Priorität.

- 5 Klicken Sie auf **Angewendet auf**, um das Profil auf ein oder mehrere Objekte anzuwenden.

Die Objekttypen sind logische Ports, logische Switches und NS-Gruppen. Wenn Sie eine NS-Gruppe auswählen, muss sie einen oder mehrere logische Switches oder logische Ports enthalten. Wenn die NS-Gruppe nur IP Sets oder MAC Sets enthält, wird sie ignoriert.

- 6 Klicken Sie auf **Speichern**.

Konfigurieren von Firewall-IPFIX-Collectors

Sie können IPFIX-Collectors für Firewalls konfigurieren.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **Tools > IPFIX** aus.
- 3 Klicken Sie auf die Registerkarte **Firewall-IPFIX-Collectors**.
- 4 Geben Sie einen Namen und optional eine Beschreibung ein.

- 5 Klicken Sie auf **Hinzufügen** und geben Sie die IP-Adresse und den Port eines Collectors ein.
Sie können bis zu 4 Collectors hinzufügen.
- 6 Klicken Sie auf **Speichern**.

Konfigurieren von Firewall-IPFIX-Profilen

Sie können IPFIX-Profile für Firewalls konfigurieren.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **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.
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 **Angewendet auf**, um das Profil auf ein oder mehrere Objekte anzuwenden.
Die Objekttypen sind logische Ports, logische Switches und NS-Gruppen. Wenn Sie eine NS-Gruppe auswählen, muss sie einen oder mehrere logische Switches oder logische Ports enthalten. Wenn die NS-Gruppe nur IP Sets oder MAC Sets enthält, wird sie ignoriert.
- 6 Klicken Sie auf **Speichern**.

ESXi-IPFIX-Vorlagen

Ein ESXi-Host-Transportknoten unterstützt acht IPFIX-Flow-Vorlagen.

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()
```

IPFIX-Vorlagen für KVM

Ein KVM-Hosttransportknoten unterstützt 88 IPFIX-Flow-Vorlagen und eine Vorlage für Optionen.

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 (e 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 (e 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.

Nachverfolgen des Pfads eines Pakets mit Traceflow

Mit Traceflow können Sie den Pfad prüfen, den ein Paket von einem logischen Port im logischen Netzwerk zu einem anderen logischen Port im selben Netzwerk nimmt. Traceflow verfolgt den Transportpfad eines Pakets auf Knotenebene nach, das an einem logischen Port eingefügt wurde. 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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wechseln Sie zum Traceflow-Bildschirm. Es stehen die beiden nachfolgend aufgeführten Optionen zur Verfügung.
 - Wählen Sie im Navigationsbereich **Tools > Traceflow** aus.
 - Wählen Sie im Navigationsbereich **Switching** aus, klicken Sie auf die Registerkarte **Ports**, wählen Sie einen VIF-angefügten Port aus und klicken Sie auf **Aktionen > Traceflow**
- 3 Wählen Sie einen Datenverkehrstyp aus.
Es stehen die Optionen „Unicast“, „Multicast“ und „Broadcast“ zur Verfügung.
- 4 Geben Sie die Quell- und Zielinformationen gemäß dem Datenverkehrstyp an.

Datenverkehrstyp	Festlegen der Quellinformationen	Festlegen der Zielinformationen
Unicast	<p>Wählen Sie eine VM und eine virtuelle Schnittstelle aus. 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 im Dropdown-Menü aus.</p> <p>Wenn die IP-Adresse und die MAC-Adresse nicht angezeigt werden, geben Sie die IP-Adresse und die MAC-Adresse in die Textfelder ein.</p> <p>Dies gilt auch für die Datenverkehrstypen „Multicast“ und „Broadcast“.</p>	<p>Wählen Sie entweder „VM-Name“ oder „IP-MAC“ aus dem Dropdown-Menü „Typ“ aus.</p> <ul style="list-style-type: none"> ■ Wenn Sie „VM-Name“ ausgewählt haben, wählen Sie eine VM und eine virtuelle Schnittstelle aus. Wählen Sie eine IP-Adresse und eine MAC-Adresse aus oder geben Sie diese ein. ■ Wenn Sie „IP-MAC“ ausgewählt haben, wählen Sie den Nachverfolgungstyp aus (Schicht 2 oder Schicht 3). Wenn Sie für den Nachverfolgungstyp „Schicht 2“ ausgewählt haben, geben Sie eine IP-Adresse und eine MAC-Adresse ein. Wenn Sie für den Nachverfolgungstyp „Schicht 3“ ausgewählt haben, geben Sie eine IP-Adresse ein.
Multicast	Siehe „Unicast“.	Geben Sie eine IP-Adresse ein. Es muss sich um eine Multicast-Adresse von 224.0.0.0 bis 239.255.255.255 handeln.
Broadcast	Siehe „Unicast“.	Geben Sie die Länge des Subnetzpräfixes ein.

- 5 (Optional) Klicken Sie auf **Erweitert**, um die erweiterten Optionen einzublenden.

- 6 (Optional) Geben Sie in die linke Spalte die gewünschten Werte oder Angaben für die folgenden Felder ein:

Option	Beschreibung
Frame-Größe	Beispiel: 128
TTL	Beispiel: 64
Zeitüberschreitung (ms)	Beispiel: 10000
Ethernet-Typ	Beispiel: 2048
Nutzlasttyp	Wählen Sie eine Option aus dem Dropdown-Menü aus.
Nutzlastdaten	Nutzlastdaten, die auf der Grundlage des ausgewählten Nutzlasttyps (Base64, Hex, Unformatierter Text, Binär oder Dezimal) formatiert sind

- 7 (Optional) Wählen Sie in der linken Spalte unter „Protokoll“ ein Protokoll aus dem Dropdown-Menü „Typ“ aus.
- 8 (Optional) Führen Sie auf der Basis des ausgewählten Protokolls die in der folgenden Tabelle aufgeführten zugeordneten Schritte aus.

Protokoll	Schritt 1	Schritt 2	Schritt 3
TCP	Geben Sie einen Quellport ein.	Geben Sie einen Zielport ein.	Wählen Sie die gewünschten TCP-Flags im Dropdown-Menü aus.
UDP	Geben Sie einen Quellport ein.	Geben Sie einen Zielport ein.	Nicht verfügbar
ICMP	Geben Sie eine ICMP-ID ein.	Geben Sie einen Folgewert ein.	Nicht verfügbar

- 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.

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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.

- 2 Wählen Sie im Navigationsbereich die Option **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.

Überwachen der Aktivität eines Ports für einen logischen Switch

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 Port für den logischen Switch konfiguriert ist. Siehe [Verbinden einer VM mit einem logischen Switch](#).

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich **Netzwerk > Switching**.
- 3 Klicken Sie auf die Registerkarte **Ports**.
- 4 Klicken Sie auf den Namen eines Ports.
- 5 Klicken Sie auf die Registerkarte **Überwachen**.

Der Portstatus und Statistiken werden angezeigt.

- 6 Um eine CSV-Datei von den MAC-Adressen herunterzuladen, die vom Host abgerufen wurden, klicken Sie auf **MAC-Tabelle herunterladen**.
- 7 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 Port für den logischen Switch angefügt wurden.

Ergebnisse

Wenn Sie feststellen, dass Pakete wegen einer Netzwerküberlastung verworfen wurden, können Sie ein QoS-Switching-Profil für den logischen Switch-Port konfigurieren, um einen Datenverlust bei bevorzugten Paketen zu vermeiden. Siehe [Grundlegendes zum QoS-Switching-Profil](#).

Überwachen von Portspiegelungssitzungen

Sie können Portspiegelungssitzungen für die Fehlerbehebung und für andere Zwecke überwachen.

Hinweis zu NSX Cloud Wenn Sie NSX Cloud verwenden, finden Sie unter [Verwendung von NSX-T Data Center-Funktionen mit der Public Cloud](#) eine Liste der automatisch generierten logischen Elemente, 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.
- Ein Zielport kann nur gespiegelten Datenverkehr empfangen.
- 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.
- Die Quell- und Zielports der Spiegelungssitzung müssen sich 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-Portspiegelungssitzung 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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **Tools > Portspiegelungssitzung** aus.
- 3 Klicken Sie auf **Hinzufügen** und wählen Sie einen Sitzungstyp aus.
Folgende Typen sind verfügbar: **Lokale SPAN**, **Remote-SPAN**, **Remote-L3 SPAN** und **Logische SPAN**.
- 4 Geben Sie einen Namen und optional eine Beschreibung für die Sitzung ein.

5 Geben Sie zusätzliche Parameter an.

Sitzungstyp	Parameter
Lokale SPAN	<ul style="list-style-type: none"> ■ Transportknoten – wählen Sie einen Transportknoten aus. ■ Richtung – wählen Sie Bidirektional, Eingehend oder Ausgehend aus. ■ Paketkürzung – wählen Sie einen Wert für die Paketkürzung aus.
Remote-SPAN	<ul style="list-style-type: none"> ■ Sitzungstyp – wählen Sie RSPAN-Quellsitzung oder RSPAN-Zielsitzung aus. ■ Transportknoten – wählen Sie einen Transportknoten aus. ■ Richtung – wählen Sie Bidirektional, Eingehend oder Ausgehend aus. ■ Paketkürzung – wählen Sie einen Wert für die Paketkürzung aus. ■ Gekapselte VLAN-ID VLAN-ID – geben Sie eine gekapselte VLAN-ID an. ■ Ursprungs-VLAN beibehalten – Legen Sie fest, ob die ursprüngliche VLAN-ID beibehalten werden soll.
Remote-L3 SPAN	<ul style="list-style-type: none"> ■ Kapselung – wählen Sie GRE, ERSPAN TWO oder ERSPAN THREE aus. ■ GRE-Schlüssel – geben Sie einen GRE-Schlüssel an, wenn Sie für „Kapselung“ die Option GRE ausgewählt haben. ■ Transportknoten – geben Sie einen Transportknoten an, wenn Sie für „Kapselung“ eine der Optionen ERSPAN TWO oder ERSPAN THREE ausgewählt haben. ■ ERSPAN-ID – geben Sie eine ERSPAN-ID an, wenn Sie für „Kapselung“ eine der Optionen ERSPAN TWO oder ERSPAN THREE ausgewählt haben. ■ Richtung – wählen Sie Bidirektional, Eingehend oder Ausgehend aus. ■ Paketkürzung – wählen Sie einen Wert für die Paketkürzung aus.
Logische SPAN	<ul style="list-style-type: none"> ■ Logischer Switch – wählen Sie einen logischen Switch aus. ■ Richtung – wählen Sie Bidirektional, Eingehend oder Ausgehend aus. ■ Paketkürzung – wählen Sie einen Wert für die Paketkürzung aus.

6 Klicken Sie auf **Weiter**.

7 Geben Sie Quellinformationen an.

Sitzungstyp	Parameter
Lokale SPAN	<ul style="list-style-type: none"> ■ Wählen Sie einen N-VDS aus. ■ Wählen Sie physische Schnittstellen aus. ■ Aktivieren oder deaktivieren Sie die Kapselung von Paketen. ■ Wählen Sie virtuelle Maschinen aus. ■ Wählen Sie virtuelle Schnittstellen aus.
Remote-SPAN	<ul style="list-style-type: none"> ■ Wählen Sie virtuelle Maschinen aus. ■ Wählen Sie virtuelle Schnittstellen aus.
Remote-L3 SPAN	<ul style="list-style-type: none"> ■ Wählen Sie virtuelle Maschinen aus. ■ Wählen Sie virtuelle Schnittstellen aus. ■ Wählen Sie einen logischen Switch aus.
Logische SPAN	<ul style="list-style-type: none"> ■ Wählen Sie logische Ports aus.

8 Klicken Sie auf **Weiter**.

9 Geben Sie Zielinformationen an.

Sitzungstyp	Parameter
Lokale SPAN	<ul style="list-style-type: none"> ■ Wählen Sie virtuelle Maschinen aus. ■ Wählen Sie virtuelle Schnittstellen aus.
Remote-SPAN	<ul style="list-style-type: none"> ■ Wählen Sie einen N-VDS aus. ■ Wählen Sie physische Schnittstellen aus.
Remote-L3 SPAN	<ul style="list-style-type: none"> ■ Geben Sie eine IPv4-Adresse an.
Logische SPAN	<ul style="list-style-type: none"> ■ Wählen Sie logische Ports aus.

10 Klicken Sie auf **Speichern**.

Die Quelle und das Ziel können nach dem Speichern der Portspiegelungssitzung nicht mehr geändert werden.

Überwachen von Fabric-Knoten

Sie können Fabric-Knoten wie Hosts, Edges, NSX Edge-Cluster, Bridges und Transportknoten mithilfe der Benutzeroberfläche von NSX Manager überwachen.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **Fabric > Knoten** aus.
- 3 Wählen Sie eine der nachfolgend aufgeführten Registerkarten aus.
 - Hosts
 - Edges
 - Edge-Cluster
 - Bridges
 - Transportknoten

Ergebnisse

Hinweis Sie können den LCP-Konnektivitätsstatus im Bildschirm „Hosts“ ignorieren, wenn für den MPA-Konnektivitätsstatus eines Hosts „Nicht vorhanden“ oder „Unbekannt“ angegeben wird, da dieser möglicherweise fehlerhaft ist.

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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **Bestand > Gruppen** aus.
- 3 Klicken Sie auf den Namen einer NSGroup.
- 4 Klicken Sie auf die Registerkarte **Anwendungen**.
- 5 Klicken Sie auf **ANWENDUNGSDATEN ERFASSEN**.

Dieser Vorgang kann einige Minuten in Anspruch nehmen. Wenn der Vorgang abgeschlossen ist, werden die folgenden Informationen angezeigt:

- Die Gesamtzahl Prozesse.
 - Verschiedene Ebenen repräsentierende Kreise, z. B. Web-, Datenbank- und Anwendungsebene. Zudem wird die Anzahl Prozesse in den einzelnen Ebenen angezeigt.
- 6 Klicken Sie auf einen Kreis, um weitere Informationen über die Prozesse in der jeweiligen Ebene anzuzeigen.

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 Navigieren Sie im Browser zu <https://nsx-manager-ip-address> und melden Sie sich mit Administratorrechten bei NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **System > Dienstprogramme** aus.
- 3 Klicken Sie auf die Registerkarte **Support-Paket**.
- 4 Wählen Sie die Zielknoten aus.

Bei den verfügbaren Knotentypen handelt es sich um Verwaltungsknoten, Controller-Knoten, Edges, Hosts und Public Cloud Gateways (PCGs).

- 5 (Optional) Geben Sie den Protokollierungszeitraum in Tagen an, um Protokolle auszuschließen, die vor der festgelegten Anzahl an Tagen erstellt wurden.

- 6 (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.

- 7 (Optional) Aktivieren Sie das entsprechende Kontrollkästchen, um die Pakete auf einen Dateiserver hochzuladen.
- 8 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.
- 9 Überwachen Sie den Status des Erfassungsvorgangs.
Das Statusfeld zeigt in Prozenten an, für wie viele Knoten die Erfassung des Support-Pakets durchgeführt wurde.
- 10 Wenn die Option für das Senden des Pakets an einen Dateiserver nicht aktiviert ist, klicken Sie auf **Herunterladen**, um das Paket herunterzuladen.

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, an denen die Informationen gesammelt werden, sowie die Proxyserver-Konfiguration festlegen.

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 über Ihren Browser unter <https://nsx-manager-ip-address> mit Administratorrechten bei einem NSX Manager an.
- 2 Wählen Sie **System > Konfiguration > Eigenschaften** aus.
- 3 Klicken Sie im Abschnitt „Status und Statistiken“ auf **Bearbeiten**.
- 4 Klicken Sie auf die Menüoption **Datenerfassung**.
- 5 Klicken Sie im Abschnitt „Programm zur Verbesserung der Benutzerfreundlichkeit“ auf **Bearbeiten**.
- 6 Klicken Sie auf die Menüoption **Am VMware-Programm zur Verbesserung der Benutzerfreundlichkeit teilnehmen**.
- 7 (Optional) Konfigurieren Sie die Einstellungen zur Datenerfassung und zur Wiederholung der Uploads.
- 8 (Optional) Klicken Sie auf die Registerkarte **Proxy**.
- 9 Klicken Sie auf die Menüoption **Proxy**, um Proxyserver-Einstellungen für das Senden von Daten zu konfigurieren.

Option	Beschreibung
Hostname	Geben Sie den FQDN oder die IP-Adresse des Proxyservers ein.
Port	Geben Sie den Proxyserver-Port ein.
Benutzername	(Optional) Geben Sie den Benutzernamen ein, der zur Authentifizierung durch den Proxyserver verwendet werden soll.
Kennwort	(Optional) Geben Sie das Kennwort ein, das zur Authentifizierung durch den Proxyserver verwendet werden soll.
Schema	Legen Sie im Dropdown-Menü das vom Proxyserver akzeptierte HTTP- oder HTTPS-Schema fest.

- 10 Klicken Sie auf **Speichern**.