

Installationshandbuch für VMware NSX-T Data Center Plug-in for OpenStack Neutron

19. September 2019

VMware NSX-T Data Center 2.5



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

Inhalt

1	Installationshandbuch für VMware NSX-T Data Center Plug-in for OpenStack Neutron	4
2	Vorbereiten der Installation von NSX-T Data Center Plug-in for OpenStack	5
	Voraussetzungen	5
	Systemvoraussetzungen	5
	Neutron-Plug-in-Vergleich	6
3	Installieren von Neutron Basic Services mit NSX-T Data Center-Plug-in	9
	Installieren von NSX-T Data Center Plug-in for OpenStack auf Ubuntu-Systemen	9
	Installieren von NSX-T Data Center Plug-in for OpenStack auf Red Hat-Systemen	10
4	Konfigurieren des OpenStack for NSX-T Data Center-Plug-ins	11
	Konfigurieren eines OpenStack Neutron-Netzwerkknotens	11
	Bearbeiten der neutron.conf- und nsx.ini-Dateien	12
	Aktivieren der Clientzertifikat-basierten Authentifizierung	13
	Aktivieren der DHCP- und Metadaten-Proxy-Dienste	14
	Beispielkonfigurationsdatei für NSX-T Data Center Plug-in for OpenStack	16
	OpenStack Nova Controller-Konfiguration	16
	OpenStack Nova Compute-Konfigurationsdatei	17
5	Konfigurieren von Neutron Advanced Services mit NSX-T Data Center Plug-in für OpenStack	18
	Konfigurieren von OpenStack Octavia Load Balancer-as-a-Service (LBaaS)	19
	Konfigurieren von OpenStack Neutron Octavia Load Balancer-as-a-Service (LBaaS)	20
	Konfigurieren der Firewall-as-a-Service (FWaaS) von OpenStack Neutron	21
	Konfigurieren der IPsec VPN-as-a-Service (VPNaaS) von OpenStack Neutron	22
	Beispiel-Konfigurationsdateien für erweiterte Neutron Advanced Services	23
6	Appendix: NSX-T Data Center Plug-in for OpenStack-Konfigurationseigenschaften	26

Installationshandbuch für VMware NSX-T Data Center Plug-in for OpenStack Neutron

1

In diesem Handbuch wird beschrieben, wie Sie das NSX-T Data Center Plug-in for OpenStack Neutron installieren und konfigurieren. Die Informationen enthalten Schritt-für-Schritt-Konfigurationsanweisungen.

Nach der Konfiguration wird das VMware NSX-T Data Center Plug-in ausgeführt und ermöglicht OpenStack Neutron die Realisierung und Verwaltung virtueller Netzwerkressourcen in Ihrer NSX-T Data Center-Bereitstellung. Für eine erfolgreiche Umsetzung sollten Sie mit den Komponenten und Funktionen von NSX-T Data Center und OpenStack vertraut sein.

Dieses Handbuch enthält Informationen zu OpenStack Neutron-Plug-ins für NSX-T Policy und NSX-T Manager. Dies ist die erste NSX-T Data Center-Version, die ein OpenStack-Plug-in für NSX-T Policy bereitstellt. Für diese Version kann das NSX-T Policy-Plug-in nur für neue Installationen verwendet werden.

Weitere Informationen zu diesen Themen finden Sie unter:

- *Administratorhandbuch für NSX-T Data Center*
- OpenStack-Dokumentation

Vorbereiten der Installation von NSX-T Data Center Plug-in for OpenStack

2

Dieses Kapitel enthält die folgenden Themen:

- [Voraussetzungen](#)
- [Systemvoraussetzungen](#)
- [Neutron-Plug-in-Vergleich](#)

Voraussetzungen

Das von VMware für das OpenStack Neutron-Plug-in bereitgestellte Support-Paket enthält nur NSX-T-spezifische Artefakte. Dies führt dazu, dass die OpenStack-Dienste Ihrer Wahl vor dem Versuch, diesen Installationsvorgang auszuführen, installiert werden müssen.

Befolgen Sie die Verfahren in diesem Dokument, um NSX-T Data Center Plug-in zu installieren und zu konfigurieren, damit OpenStack Neutron in Ihre NSX-Bereitstellung integriert werden können. Bei diesem Verfahren wird davon ausgegangen, dass VMware NSX-T Data Center auf den NSX-T-Transportknoten installiert und konfiguriert wurde.

Die Internetkonnektivität oder der Zugriff auf eine lokale Distributions-Repository-Spiegelung ist während der Neutron-Dienstinstallation erforderlich, um sicherzustellen, dass die entsprechenden Abhängigkeiten im Rahmen des Installationsvorgangs heruntergeladen, installiert und konfiguriert werden können.

Systemvoraussetzungen

Unterstützung von NSX-T Data Center Plug-in for OpenStack wird als Neutron-Plug-in implementiert. Die beim Konfigurieren von Neutron verwendete VMware NSX-Plug-in-Klasse hängt von der Version von NSX ab, die Sie verwenden.

Unterstützte Hypervisor-Versionen für vSphere und KVM (Ubuntu, Red Hat Enterprise Linux, CentOS...) sind in *Installationshandbuch für NSX-T Data Center* aufgeführt.

NSX-T Data Center Plug-in for OpenStack weist die folgenden spezifischen Anforderungen bezüglich kompatibler OpenStack-Softwareversionen auf.

OpenStack-Distribution für NSX-T Policy Plug-in	Version
Open Source-Edition	Stein

OpenStack-Distribution für NSX-T Manager Plug-in	Version
Open Source-Edition	Rocky
Open Source-Edition	Stein
Red Hat OpenStack-Plattform	Red Hat OpenStack-Version 13 mit der zugehörigen Version von Red Hat Enterprise Linux.

Neutron-Plug-in-Vergleich

Ab VMware NSX-T Data Center 2.5 sind zwei Plug-ins für die Integration von OpenStack Neutron mit NSX-T verfügbar:

- Das NSX-T Policy-Plug-in interagiert mit dem NSX-T-Richtlinienmanager unter Verwendung von absichtsbasierten API-Abstraktionen. Dies ist ein neues Plug-in und die empfohlene Wahl für neue Installationen.
- Das NSX-T Manager-Plug-in interagiert mit dem NSX-T Manager unter Verwendung von imperativen APIs. Dies ist das vorhandene NSX-T-Plug-in, es muss für vorhandene Installationen sowie für Anwendungsfälle verwendet werden, die noch nicht im NSX-T Policy-Plug-in abgedeckt sind.

Tabelle 2-1. Vergleich der Plug-in-Funktionen

Netzwerken und Sicherheit – Funktionen	NSX-T MP Plug-in	NSX-T Policy	Beschreibung
Switching			
Unterstützung von überlappenden IP-Subnetzen	Ja	Ja	Jedes Projekt kann dynamisch Netzwerke erstellen, die für das Projekt privat sind. Diese Netzwerke können über überlappende IP-Subnetze verfügen.
DHCP	Ja	Ja	Instanzen verfügen über automatische Adressierung über DHCP.
Statische IPv6-Adressbindung	Nein	Ja	
Routing			
Logisches Routing	Ja	Ja	Aktivieren Sie das Routing zwischen mehreren privaten logischen Netzwerken sowie zwischen einem logischen Netzwerk und einem externen Netzwerk.

Tabelle 2-1. Vergleich der Plug-in-Funktionen (Fortsetzung)

Netzwerken und Sicherheit – Funktionen	NSX-T MP Plug-in	NSX-T Policy	Beschreibung
Logisches IPv6-Routing	Nein	Ja	Aktivieren Sie das Routing zwischen mehreren privaten logischen IPv6-Netzwerken sowie zwischen einem logischen Netzwerk und einem externen Netzwerk.
Externe Netzwerke	Ja	Ja	Netzwerke, die externen Zugriff auf die Instanzen ermöglichen. Private Netzwerke werden per Uplink über einen Router mit dem externen Netzwerk verknüpft, um externen Zugriff auf die Instanzen in den privaten Netzwerken zu ermöglichen.
Externe IPv6-Netzwerke	Ja	Ja	Externes Netzwerk mit IPv6.
Statische Routen	Ja	Ja	Geben Sie eine statische Route an.
Statische IPv6-Routen	Nein	Ja	Externes Netzwerk mit IPv6.
Dynamische IP für Instanzen	Ja	Ja	Weisen Sie Instanzen öffentliche routingfähige IP-Adressen zu, um externen Zugriff auf die Instanzen zu ermöglichen.
No-NAT-Router	Ja	Ja	No-NAT-Routing-Topologie.
IPv6-No-NAT-Router	Nein	Ja	Die No-NAT-Topologie ist die einzige Routing-Topologie, die von OpenStack mit IPv6 unterstützt wird. NAT mit IPv6 wird nicht unterstützt.
Dual-Stack-Schnittstellen des Neutron-Routers	Nein	Ja	Unterstützung von IPv4- und IPv6-Dual-Stack auf denselben Schnittstellen eines Neutron-Routers.
IPv6-SLAAC	Nein	Ja	Unterstützung der statusfreien Adress-Autokonfiguration.
Sicherheit			
Firewall – Sicherheitsgruppen	Ja	Ja	OpenStack-Sicherheitsgruppen (mit NSX werden Sicherheitsgruppen verwendet und DFW-Regeln, die mit diesen SG erstellt wurden. Dies ermöglicht die Mikro-Segmentierung)

Tabelle 2-1. Vergleich der Plug-in-Funktionen (Fortsetzung)

Netzwerken und Sicherheit – Funktionen	NSX-T MP Plug-in	NSX-T Policy	Beschreibung
IPv6-Firewall (Sicherheitsgruppen)	Nein	Ja	Neutron-Sicherheitsgruppe mit IPv6.
Portsicherheit	Ja	Ja	Die Sicherheit des Neutron-Ports wird mithilfe der NSX-SpoofGuard-Funktionen implementiert.
IPv6-Port-Sicherheit	Nein	Ja	Die Sicherheit des Neutron-Ports wird mithilfe der NSX-SpoofGuard-Funktionen implementiert. Dies ermöglicht <code>allowed_address_pairs</code> und eine IPv6-Subnetz-Zuordnung zu einem Port.
Firewall (L3-FWaaS)	Ja	Ja	
IPv6-Firewall (L3-FWaaS)	Nein	Ja	
Andere Dienste			
Lastausgleich	Ja	Ja	
Servicequalität	Ja	Ja	
DNS	Ja	Ja	
VPNaas	Ja	Nein	

Upgrades

Es gibt keinen Migrationspfad von OpenStack Neutron mit NSX-T Manager-Plug-in für OpenStack Neutron mit dem NSX-T Policy-Plug-in. Beim Upgrade sollten vorhandene Installationen weiterhin das NSX-T Manager-Plug-in ausführen. Ein Migrationspfad von NSX-T Manager zu NSX-T Policy wird in zukünftigen Versionen verfügbar sein. Das NSX-T Policy-Plug-in ist die empfohlene Lösung für neue Installationen, da es eindeutige Funktionen (IPv6) enthält. Darüber hinaus wird das Verschieben neuer Funktionen ausschließlich für das NSX-T-Plug-in verfügbar sein.

Installieren von Neutron Basic Services mit NSX-T Data Center-Plug-in

3

Dieses Kapitel enthält die folgenden Themen:

- [Installieren von NSX-T Data Center Plug-in for OpenStack auf Ubuntu-Systemen](#)
- [Installieren von NSX-T Data Center Plug-in for OpenStack auf Red Hat-Systemen](#)

Installieren von NSX-T Data Center Plug-in for OpenStack auf Ubuntu-Systemen

Die NSX-T Data Center Plug-ins werden als Debian-Pakete(.deb) für Ubuntu-basierte Linux-Distributionen verteilt.

Voraussetzungen

Die NSX-T Data Center Plug-ins werden als Debian-Pakete(.deb) für Ubuntu-basierte Linux-Distributionen verteilt.

Die folgenden Anweisungen gelten sowohl für die NSX-T Manager- als auch für die NSX-T Policy-Plug-ins.

- Wenn die Installation des Debian-Pakets aufgrund von Abhängigkeitsfehlern fehlschlägt, ist es möglicherweise erforderlich, die Pakete `python-too` und `python-oslo.vmware` zu installieren. `Too` ist eine Python-Bibliothek, die Abstraktionen für verteilte Koordinationsprimitive bereitstellt. Ihr Hauptziel besteht darin, Gruppen und die Mitgliedschaft dieser Gruppen in verteilten Systemen zu verwalten. Die `Oslo VMWare`-Bibliothek bietet Unterstützung für gemeinsame VMWare-Vorgänge und-APIs. Beispiel: `sudo apt-get install python-oslo.vmware`.

Verfahren

- 1 Laden Sie die .deb-Dateien herunter: die NSX Neutron-Plug-ins und die gemeinsame NSX Neutron-Bibliothek.
- 2 Kopieren Sie die Dateien in den Neutron-Netzwerkknoten.
- 3 Installieren Sie das Paket mit dem Befehl `dpkg` im selben Verzeichnis wie die .deb-Datei.

Die Versionsnummern im folgenden Beispiel können je nach der beim Herunterladen ausgewählten Version unterschiedlich sein:

- `sudo dpkg -i python-vmware-nsxlib_12.0.0.9797177-1_all.deb`

- `sudo dpkg -i openstack-vmware-nsx_12.0.0.9797177-1_all.deb`

- 4 Installieren Sie das Firewall-as-a-Service(FWaaS)-Paket. Dies muss nach der Installation nicht aktiviert werden.

Die Versionsnummern im folgenden Beispiel können je nach der beim Herunterladen ausgewählten Version unterschiedlich sein:

- `sudo apt-get install python-neutron-fwaas`

Installieren von NSX-T Data Center Plug-in for OpenStack auf Red Hat-Systemen

Die Installations-NSX-T Data Center-Plug-ins für OpenStack sind als .rpm-Dateien für Red Hat-basierte Linux-Distributionen verpackt.

Die .rpm-Pakete finden Sie auf der Download-Seite von NSX-T Data Center unter **Treiber und Tools**. Diese Anweisungen gelten für Installationen, die TripleO nicht nutzen, andernfalls beziehen Sie sich auf den dedizierten Leitfaden für Red Hat OpenStack.

Verfahren

- 1 Laden Sie die .rpm-Dateien herunter: die NSX Neutron-Plug-ins und die gemeinsame NSX Neutron-Bibliothek.
- 2 Kopieren Sie sie in den Neutron-Netzwerkknoten, auf dem Sie das Plug-in installieren möchten.
- 3 Installieren Sie das Paket mit dem Befehl rpm im selben Verzeichnis wie die .rpm-Datei.

Die Versionsnummern im folgenden Beispiel können je nach der beim Herunterladen ausgewählten Version unterschiedlich sein:

- `sudo rpm -i python-vmware-nsxlib_12.0.0.9797177-1_all.rpm`
- `sudo rpm -i vmware-nsx-12.0.0.9797177-1.noarch.rpm`

- 4 Installieren Sie das Firewall-as-a-Service(FWaaS)-Paket. Dies muss nach der Installation nicht aktiviert werden.

- `sudo yum install python-neutron-fwaas`

Konfigurieren des OpenStack for NSX-T Data Center-Plug-ins

4

- [Konfigurieren eines OpenStack Neutron-Netzwerkknotts](#)

Die in diesem Abschnitt beschriebene Konfiguration entspricht der Konfiguration des Neutron-Netzwerkknotts.

- [Beispielkonfigurationsdatei für NSX-T Data Center Plug-in for OpenStack](#)

Konfigurationsdateien befinden sich in der Regel unter `/etc/neutron/plugins/vmware/nsx.ini`.

- [OpenStack Nova Controller-Konfiguration](#)

Die in diesem Abschnitt beschriebene Konfiguration ergänzt die Konfiguration der Nova Controller-Knoten mit Informationen zu NSX-T Data Center.

- [OpenStack Nova Compute-Konfigurationsdatei](#)

Zum Bearbeiten von Nova-Konfigurationsdateien verwenden Sie NSX-T.

Konfigurieren eines OpenStack Neutron-Netzwerkknotts

Die in diesem Abschnitt beschriebene Konfiguration entspricht der Konfiguration des Neutron-Netzwerkknotts.

Die Dokumentation bezieht sich auf das NSX-T Policy-Plug-in. In diesem Abschnitt werden jedoch auch die spezifischen Einstellungen für das NSX-T Manager-Plug-in hervorgehoben.

Zwei standardmäßige Konfigurationsdateipfade sind relevant:

- `/etc/neutron/neutron.conf` – Neutron-Konfigurationsdatei.
- `/etc/neutron/plugin/vmware/nsx.ini` – VMware NSX Neutron-Plug-in-Konfigurationsdatei.

- [Bearbeiten der `neutron.conf`- und `nsx.ini`-Dateien](#)

Diese Dateien müssen mit Informationen in Bezug auf die NSX-T-Umgebung bearbeitet werden, damit das Neutron-Plug-in mit der NSX-t-Bereitstellung interagieren kann.

- [Aktivieren der Clientzertifikat-basierten Authentifizierung](#)

Die auf dem Neutron-Clientzertifikat basierende Authentifizierung für NSX Manager wird unterstützt.

- [Aktivieren der DHCP- und Metadaten-Proxy-Dienste](#)

Mit dem NSX-T Data Center-Plug-in wird die OpenStack-Referenz-DHCP-Implementierung durch den nativen NSX-T Data Center-DHCP-Server ersetzt. Die NSX-T Data Center-Plattform bietet auch einen Proxy-Server für den Zugriff auf Nova-Metadaten.

Bearbeiten der neutron.conf- und nsx.ini-Dateien

Diese Dateien müssen mit Informationen in Bezug auf die NSX-T-Umgebung bearbeitet werden, damit das Neutron-Plug-in mit der NSX-t-Bereitstellung interagieren kann.

Verfahren

- 1 Bearbeiten Sie die `neutron.conf` -Datei, um das Neutron-Kern-Plug-in `[DEFAULT] core_plugin = vmware_nsxp` festzulegen. So aktivieren Sie das NSX-T Manager-Plug-in: `[DEFAULT] core_plugin = vmware_nsxv3`
- 2 Bearbeiten Sie die `nsx.ini` -Konfigurationsdatei, um das Plug-in für Ihre NSX-Bereitstellung zu konfigurieren.

Die Eigenschaften von NSX-T OpenStack Plugin finden Sie im Abschnitt „[nsx_p]“ der `nsx.ini`-Konfigurationsdatei.

Die unten aufgeführten Konfigurationseigenschaften gelten auch für das NSX-T Manager-Plug-in und werden im Abschnitt „[nsx_v3]-Konfiguration“ angegeben.

Die Konfigurationseigenschaften, die mindestens definiert werden müssen, sind:

Variable	Beschreibung
<code>nsx_api_managers</code>	Dieser Parameter ermöglicht eine Liste von kommagetrennten Manager-Endpoints.
<code>nsx_api_user</code>	Administrator-NSX-T Manager-Benutzername, normalerweise „admin“.
<code>nsx_api_password</code>	Administrator-Kennwort für NSX-T Manager.
<code>insecure</code>	Legen Sie diesen Wert auf „False“ fest, um die Verifizierung des NSX Manager-Serverzertifikats zu erzwingen. Standardeinstellung auf „True“.
<code>ca_file</code>	CA-Paketdateien, die bei der Überprüfung des NSX Manager-Serverzertifikats verwendet werden sollen. Diese Option wird ignoriert, wenn „unsicher“ auf „True“ festgelegt ist. Wenn „unsicher“ auf „False“ gesetzt und diese Option nicht festgelegt ist, werden die System-Root-CAs verwendet, um das Serverzertifikat zu überprüfen.
<code>nsx_api_managers</code>	Der Name oder die UUID der standardmäßigen NSX-Overlay-Transportzone, die zum Erstellen von Neutron-Netzwerken verwendet wird. Sie muss in NSX erstellt werden, bevor Neutron gestartet wird.
<code>default_tier0_router</code>	Hierbei muss es sich um einen Policy Manager NSX-T Tier0-Namens-Gateway-Router oder eine UUID handeln, mit der logische OpenStack-Router (NSX-T Tier1) in Zukunft verbunden werden (unter „Routing/Router“).
<code>dhcp_profile</code>	Geben Sie entweder eine UUID oder einen Namen ein. Siehe Erstellen eines DHCP-Profiles in NSX Manager .
<code>metadata_proxy</code>	Geben Sie entweder eine UUID oder einen Namen ein. Siehe Erstellen eines Metadaten-Proxys .

- 3 Starten Sie Neutron neu, um die Änderungen in der `nsx.ini`-Datei zu übernehmen, indem Sie den Befehl `ps -aux |grep neutron` ausführen.
- 4 Stellen Sie sicher, dass `nsx.ini` und `neutron.conf` in der Ausgabe vorhanden sind. Beachten Sie, dass Neutron eine oder mehrere Konfigurationsdateien in der Befehlszeile akzeptiert. Diese Dateien werden zusammengeführt, wenn die Konfiguration analysiert wird, sodass die Konfigurationsdateistruktur die Einstellungen eines bestimmten Benutzers widerspiegeln kann.

```
ps -aux |grep neutron
stack      7688  0.0  1.8 311332 148904 ?        Ss   Nov26  21:10
/usr/bin/python /usr/local/bin/neutron-server --config-file
/etc/neutron/neutron.conf --config-file
/etc/neutron/plugins/vmware/nsx.ini
```

Aktivieren der Clientzertifikat-basierten Authentifizierung

Die auf dem Neutron-Clientzertifikat basierende Authentifizierung für NSX Manager wird unterstützt.

Die Clientzertifikat-basierte Authentifizierung ermöglicht es dem Neutron-Plug-in, sich als Prinzipalidentität mit der Rolle „Enterprise-Administrator“ anzumelden. Andere Prinzipalidentitäten können Ressourcen, die von der Neutron-Prinzipalidentität erstellt wurden, nicht bearbeiten. Somit sind diese vor versehentlichen Fehlern wie dem Löschen eines logischen Routers, der einem Neutron-Router zugeordnet ist, geschützt. Weitere Informationen finden Sie unter „Prinzipalidentität anzeigen“ im NSX-T for Data Center-Administratorhandbuch.

Verfahren

- 1 Um die Clientzertifikatauthentifizierung zu aktivieren, definieren Sie Folgendes in der Datei `nsx.ini`:
 - `nsx_use_client_auth = True`
 - `nsx_client_cert_storage = nsx-db`
 - `nsx_client_cert_file = <file to store certificate and private key>`
- 2 Starten Sie Neutron neu, um die Änderungen in der `nsx.ini`-Datei zu übernehmen, indem Sie den Befehl `service neutron-server restart` ausführen.

Stellen Sie sicher, dass der Neutron-Server die `neutron.conf` und `nsx.ini`-Dateien verwendet, indem Sie den folgenden Befehl ausführen:

- `ps -aux |grep neutron`

Stellen Sie sicher, dass `nsx.ini` und `neutron.conf` in der Ausgabe vorhanden sind. Beispiel:

```
ps -aux |grep neutron
stack      7688  0.0  1.8 311332 148904 ?        Ss   Nov26  21:10
/usr/bin/python /usr/local/bin/neutron-server --config-file
/etc/neutron/neutron.conf --config-file
/etc/neutron/plugins/vmware/nsx.ini
```

Aktivieren der DHCP- und Metadaten-Proxy-Dienste

Mit dem NSX-T Data Center-Plug-in wird die OpenStack-Referenz-DHCP-Implementierung durch den nativen NSX-T Data Center-DHCP-Server ersetzt. Die NSX-T Data Center-Plattform bietet auch einen Proxy-Server für den Zugriff auf Nova-Metadaten.

Diese Vorgänge müssen unabhängig vom im vorherigen Schritt konfigurierten NSX-T Plug-in durchgeführt werden.

- **Erstellen eines DHCP-Profiles in NSX Manager**

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.

- **Erstellen eines Metadaten-Proxys**

Mit einem Metadaten-Proxyserver können VM-Instanzen instanzenspezifische Metadaten von einem OpenStack Nova-API-Server abrufen.

- **Bearbeiten der `nsx.ini`-Datei**

Die neuen Variablen `native_dhcp_metadata`, `metadata_proxy` und `dhcp_profile` müssen in `nsx.ini` angegeben werden, die diese Profile konsumiert.

Erstellen eines DHCP-Profiles in NSX Manager

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.

Voraussetzungen

Um den nativen DHCP-Server von NSX-T Data Center zu aktivieren, muss ein DHCP-Profil in NSX-T Data Center erstellt und an die Neutron-Plug-in-Konfiguration in `nsx.ini` übergeben werden. Stellen Sie sicher, dass der Neutron DHCP-Dienst (q-DHCP in devstack) und der Metadaten-Agent (q-Meta in devstack) nicht aktiv sind. Legen Sie in der Datei `neutron.conf` auf `False` fest.

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 **Netzwerk und Sicherheit – Erweitert > DHCP** aus dem Navigationsbereich aus.
- 3 Wählen Sie **Serverprofile** und dann **Hinzufügen**.
- 4 Geben Sie einen Namen und optional eine Beschreibung ein.
- 5 Wählen Sie im Dropdown-Menü einen **Edge-Cluster** aus.
- 6 Klicken Sie auf **Hinzufügen**.

Erstellen eines Metadaten-Proxys

Mit einem Metadaten-Proxyserver können VM-Instanzen instanzenspezifische Metadaten von einem OpenStack Nova-API-Server abrufen.

Die NSX-Plattform bietet einen Proxy-Server für den Zugriff auf Nova-Metadaten. Der Proxy erfasst alle an der 169.254.269.254-Adresse vorgenommenen Anforderungen und leitet sie an den in der NSX-T-Metadaten-Proxy-Konfiguration angegebenen Nova-Metadaten-Server-Endpoint weiter.

Voraussetzungen

Der für den Metadaten-Proxy verwendete Edge-Knoten muss über IP-Konnektivität der Verwaltungs-IP-Adressen zum Metadatenserver verfügen.

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 **Netzwerk – Erweitert > DHCP** aus dem Navigationsbereich aus.
- 3 Wählen Sie **Metadaten-Proxys** und dann **Hinzufügen** aus.
- 4 Geben Sie einen **Namen** und optional eine Beschreibung ein.
- 5 Geben Sie die **Nova-Server-URL** als `http://<openstack_controller>:8775` ein. Wenn der Metadaten-Proxy-Server einen anderen als den standardmäßigen Port 8775 überwacht, aktualisieren Sie die URL mit dem richtigen Port. Ports befinden sich auf dem Controller-Knoten in der Nova-API-Konfigurationsdatei `/etc/nova.conf`. Suchen Sie dabei nach dem Parameter `metadata_listen_port`. Wenn die Konfiguration geändert werden muss, starten Sie den `n-api`-oder Nova-Server neu.
- 6 Geben Sie den **geheimen** Parameter ein.
- 7 Wählen Sie im Dropdown-Menü einen **Edge-Cluster** aus.
- 8 Klicken Sie auf **Hinzufügen**.

Bearbeiten der nsx.ini-Datei

Die neuen Variablen `native_dhcp_metadata`, `metadata_proxy` und `dhcp_profile` müssen in `nsx.ini` angegeben werden, die diese Profile konsumiert.

- `dhcp_profile = <UUID or name – DHCP>`
- `native_dhcp_metadata = True`
- `metadata_proxy = <UUID or name – MetaData Proxy>`
- `native_metadata_route = 169.254.169.254/31`

Beispielkonfigurationsdatei für NSX-T Data Center Plug-in for OpenStack

Konfigurationsdateien befinden sich in der Regel unter `/etc/neutron/plugins/vmware/nsx.ini`.

Nachfolgend finden Sie eine Beispielkonfigurationsdatei:

```
[nsx_p]
# NSX-T credentials
nsx_api_managers = 192.168.10.5
nsx_api_user = admin
nsx_api_password = VMware1!
insecure = True
# NSX-T objects information
default_tier0_router = 0fd8b97f-315d-4461-a80b-adb489b6cfbc
default_overlay_tz_ = 4d3fcd4f-0946-4b08-ab6b-5463c571463d
default_vlan_tz = f74b5dab-dad3-47d2-b46e-57a1eeb5fde3
# DHCP and Metadata Proxy offered by NSX-T
dhcp_profile = 153637ce-657a-4ff9-a2f2-ffab62441abc
metadata_proxy = 32cf4708-7b1f-4932-b4ca-9f7029c9a7a2
```

```
[nsx_v3]
# NSX-T credentials
nsx_api_managers = 192.168.10.5
nsx_api_user = admin
nsx_api_password = VMware1!
insecure = True
# NSX-T objects information
default_tier0_router_uuid = 0fd8b97f-315d-4461-a80b-adb489b6cfbc
default_overlay_tz_uuid = 4d3fcd4f-0946-4b08-ab6b-5463c571463d
# DHCP and Metadata Proxy offered by NSX-T
dhcp_profile = 153637ce-657a-4ff9-a2f2-ffab62441abc
metadata_proxy = 32cf4708-7b1f-4932-b4ca-9f7029c9a7a2
```

OpenStack Nova Controller-Konfiguration

Die in diesem Abschnitt beschriebene Konfiguration ergänzt die Konfiguration der Nova Controller-Knoten mit Informationen zu NSX-T Data Center.

Im Folgenden finden Sie eine Beispielkonfigurationsdatei für den Nova Controller, die sich normalerweise auf `/etc/nova/nova.conf` im Controller-Knoten befindet.

```
[DEFAULT]
firewall_driver = nova.virt.firewall.NoopFirewallDriver
use_neutron = True

[neutron]
metadata_proxy_shared_secret = VMware1!
service_metadata_proxy = True
```


OpenStack Nova Compute-Konfigurationsdatei

Zum Bearbeiten von Nova-Konfigurationsdateien verwenden Sie NSX-T.

Die in diesem Abschnitt beschriebene Konfiguration ergänzt die Konfiguration der Nova Compute-Knoten mit Informationen zu NSX-T Data Center.

Im Folgenden finden Sie eine Beispielfunktionsdatei für Nova Compute, die sich normalerweise auf `/etc/nova/nova.conf` in Compute-Knoten befindet.

```
[DEFAULT]
firewall_driver = nova.virt.firewall.NoopFirewallDriver
use_neutron = True

[neutron]
#for KVM
ovs_bridge = nsx-managed
```

Konfigurieren von Neutron Advanced Services mit NSX-T Data Center Plug-in für OpenStack

5

OpenStack Neutron Load Balancer-as-a-Service (LBaaS), Firewall-as-a-Service (FWaaS) und IPSec VPN-as-a-Service (VPNaaS) werden auch als Neutron Advanced Services bezeichnet.

Ab NSX-T Data Center 2.5 unterstützen NSX-T-Plug-ins (sowohl Policy als auch Manager) den Load Balancer-Dienst von Octavia, der den stillgelegten Neutron LBaaS-Dienst ersetzt.

Bei den folgenden Informationen wird davon ausgegangen, dass Sie über NSX-T Data Center 2.4 und OpenStack Stein 14.0 verfügen.

Die unterstützten aktuellen Versionen sind in den [Systemvoraussetzungen](#) aufgeführt.

Um Neutron Advanced Services NSX-T Data Center zu aktivieren, muss Folgendes in der Neutron-Konfiguration eingestellt werden:

- Aktivieren des Dienst-Plug-ins für den spezifischen Dienst
- Konfigurieren von Dienstanbietern für den Dienst
- Ggf. Angeben des NSX-T Data Center-Treibers und der für NSX-T Data Center spezifischen Konfigurationseinträge

Diese Optionen werden in Neutron-Konfigurationsdateien angegeben, in der Regel zu finden in `/etc/neutron` (Hinweis: Plug-in-spezifische Konfigurationsdateien sind in der Regel in `/etc/neutron/plugins/vmware` zu finden. Neutron akzeptiert eine oder mehrere Konfigurationsdateien in der Befehlszeile. Diese Dateien werden zusammengeführt, wenn die Konfiguration analysiert wird, sodass die Konfigurationsdateistruktur die Einstellungen eines bestimmten Benutzers widerspiegeln kann. Die folgende Struktur wird normalerweise verwendet:

- `neutron.conf` – Neutron-Kernoptionen, grundlegende Konfigurationsparameter (z. B. API-Manager-Endpoint, Transportzonen-Bezeichner), Service-Plug-in-Liste.
- `neutron_lbass.conf` – Load Balancing-Dienstanbieter und -Optionen.
- `octavia.conf` – Load Balancing-Anbieter und MQ Topic. Nur für den Octavia Load Balancer-Dienst. Diese Datei befindet sich in der Regel in `/etc/octavia/octavia.conf` und wird vom Octavia-Dienst geladen.
- `neutron_fwass.conf` – Firewall-Dienstanbieter, -Treiber und -Treiberoptionen.
- `neutron_vpnaas.conf` – VPN-Dienstanbieter und andere Optionen.

Dienstanbieter werden mit der Option `service_provider` angegeben. Diese Option kann in einer Neutron-Konfiguration für verschiedene Arten von Diensten mehrmals wiederholt werden, aber es darf nicht mehr als einen Standarddienstanbieter für einen bestimmten Dienstyp geben.

Service_provider-Konfigurationsattributstruktur: `<SERVICE_TYPE>:<PROVIDER_CLASS>:[<DEFAULT>]`.

- [Konfigurieren von OpenStack Octavia Load Balancer-as-a-Service \(LBaaS\)](#)

Diese Anweisungen dienen zur Konfiguration der OpenStack-Nutzung von NSX-T Data Center Load Balancer mit Octavia.

- [Konfigurieren von OpenStack Neutron Octavia Load Balancer-as-a-Service \(LBaaS\)](#)

- [Konfigurieren der Firewall-as-a-Service \(FWaaS\) von OpenStack Neutron](#)

Diese Anweisungen gelten für die Konfiguration von FWaaS v2.

- [Konfigurieren der IPsec VPN-as-a-Service \(VPNaaS\) von OpenStack Neutron](#)

Mit diesem Dienst können OpenStack-Benutzer Neutron-Netzwerke über sichere VPN-Tunnel für die Remotesite zugänglich machen.

- [Beispiel-Konfigurationsdateien für erweiterte Neutron Advanced Services](#)

Konfigurieren von OpenStack Octavia Load Balancer-as-a-Service (LBaaS)

Diese Anweisungen dienen zur Konfiguration der OpenStack-Nutzung von NSX-T Data Center Load Balancer mit Octavia.

Dieselben Anweisungen gelten sowohl für das NSX-T Policy- als auch für das NSX-T Manager-Plug-in.

Allgemeine Informationen zum Load Balancer-Dienst von Octavia finden Sie in der offiziellen Dokumentation.

Verfahren

- 1 Stellen Sie sicher, dass das Plug-in für den Load Balancer-Dienst für NSX-T Data Center in `/etc/neutron/neutron.conf` nicht konfiguriert ist. `vmware_nsx_lbaasv2` sollte also in der Liste der `service_plugins` nicht vorhanden sein. Wenn Änderungen an der Datei `neutron.conf` vorgenommen werden, starten Sie den Neutron-Dienst neu.
- 2 Geben Sie in `/etc/octavia/octavia.conf` Folgendes an:
 - a Geben Sie in der Konfigurationseinstellung `[api_settings]` den NSX-T-Anbieter an:
`default_provider_driver = vmwareedge` `enabled_provider_drivers = vmwareedge:NSX`
 - b Geben Sie im Abschnitt `[oslo_messaging]` ein Thema für die Kommunikation zwischen Octavia und dem NSX-T-Treiber an, der im Neutron-Prozessbereich ausgeführt wird.
- 3 Starten Sie den Octavia API-Dienst neu.

Konfigurieren von OpenStack Neutron Octavia Load Balancer-as-a-Service (LBaaS)

Diese Anweisungen dienen zur Konfiguration der OpenStack-Nutzung von NSX-T Data Center Load Balancer mit LBaaSV2. Dieselben Anweisungen gelten sowohl für das NSX-T Policy- als auch für das NSX-T Manager-Plug-in.

Verfahren

- 1 Bearbeiten Sie `/etc/neutron/neutron.conf`, um das Load Balancing-as-a-Service-Plug-in für NSX-T Data Center hinzuzufügen, im Abschnitt „Standardkonfiguration“: `service_plugins = vmware_nsx_lbaaSv2, [...]`

Beachten Sie, dass `service_plugins` eine Listenoption ist. Es ist möglich, mehrere Dienst-Plug-ins anzugeben, indem die vollständigen Klassennamen oder Verknüpfungen mit einem Komma getrennt werden.

- 2 Bearbeiten Sie die Datei `/etc/neutron/neutron-lbaas.conf` mit den folgenden Optionen:

- a Legen Sie den Treiber für den Load Balancer-Dienst für NSX-T Data Center fest, indem Sie die Einstellung „`service_provider`“ im Abschnitt „`service_providers-Konfiguration`“ festlegen:


```
service_plugins =
LOADBALANCERV2:VMWareEdge:neutron_lbaaS.drivers.vmware.edge_driver_v2.EdgeLoadBalancerDriverV2:default
```
- b Konfigurieren Sie die Keystone-Authentifizierungsparameter, sofern sie noch nicht konfiguriert sind. Diese werden vom Neutron-lbaas-Dienst verwendet und beziehen sich nicht auf die NSX-T Data Center-Integration. Beachten Sie, dass der Speicherort des Keystone-Endpoints angegeben werden muss.

```
[service_auth]
auth_version = 3
admin_password = password
admin_user = admin
admin_tenant_name = admin
auth_url = http://<keystone_endpoint>/identity/v3
```

- 3 Stellen Sie sicher, dass die Datei `/etc/neutron/neutron-lbaas.conf` zur Neutron-Serverbefehlszeile hinzugefügt wird. Dies kann durch das Ausführen des Befehls `ps -aux | grep neutron` überprüft werden und durch das Prüfen, ob `/etc/neutron/neutron-lbaas.conf` in der Ausgabe vorhanden ist.

Wenn die Datei nicht enthalten ist, sollte der Neutron-Dienst-Launcher bearbeitet werden. Speicherort und die Struktur von Dienst-Launchern hängen von der jeweilig verwendeten OpenStack-Verteilung ab.

- 4 Starten Sie den Neutron-Dienst neu. Der genaue Dienstname hängt von der verwendeten OpenStack-Distribution ab.

Konfigurieren der Firewall-as-a-Service (FWaaS) von OpenStack Neutron

Diese Anweisungen gelten für die Konfiguration von FWaaS v2.

Verfahren

- 1 Bearbeiten Sie `/etc/neutron/neutron.conf`, um das Firewall-as-a-Service-Plug-in für NSX-T Data Center hinzuzufügen, im Abschnitt „Standardkonfiguration“: `service_plugins = firewall_v2`

`Service_plugins` ist eine Listenoption. Es können mehrere Dienst-Plug-ins angegeben werden, indem ihre vollständigen Klassennamen oder Verknüpfungen mit einem Komma getrennt werden.

- 2 Bearbeiten Sie die Datei `/etc/neutron/neutron-fwaas.conf` mit den folgenden Optionen:

- a Legen Sie den Firewall-as-a-Service-Treiber für NSX-T Data Center fest, indem Sie die Einstellung `service_provider` im Abschnitt „service_providers-Konfiguration“ festlegen.


```
service_provider = FIREWALL_V2:fwaas_db:neutron_fwaas.services.firewall.service_drivers.agents.agents.FirewallAgentDriver:default
```

```
[service_auth]
auth_version = 3
admin_password = password
admin_user = admin
admin_tenant_name = admin
auth_url = http://<keystone_endpoint>/identity/v3
```

Der Wert dieser Option weist eine bestimmte Struktur auf:

`<service_type>:<service_name>:<driver_class>:[<default>]`. `service_provider` ist eine „Multi-String“-Option. Jedes Mal, wenn sie angegeben wird, wird der Wert der Option zu einer Liste hinzugefügt. Mehrere Dienstanbieter können durch Festlegen der Einstellung `service_provider` für jeden angegeben werden.

- b Schalten Sie die Firewall-as-a-Service ein, indem Sie `enabled = True` im Abschnitt „FWaaS-Konfiguration“ festlegen.
 - c Legen Sie den FWaaS-Gerätetreiber für NSX-T Data Center fest, indem Sie `driver = vmware_nsxp_edge_v2` im Abschnitt „FWaaS-Konfiguration“ festlegen.
 - d Legen Sie den FWaaS-Gerätetreiber für das NSX Manager-Plug-in fest, indem Sie `driver = vmware_nsxv3_edge_v2` im Abschnitt „FWaaS-Konfiguration“ festlegen.
- 3 Stellen Sie sicher, dass die Datei `/etc/neutron/neutron-fwaas.conf` zur Neutron Server-Befehlszeile hinzugefügt wurde. Dies kann durch das Ausführen von `ps -aux | grep neutron` überprüft werden und durch das Prüfen, ob `/etc/neutron/neutron-fwaas.conf` in der Ausgabe vorhanden ist.

Wenn die Datei nicht enthalten ist, sollte der Neutron-Dienst-Launcher bearbeitet werden. Der Speicherort und die Struktur von Dienst-Launchern hängen von der jeweilig verwendeten OpenStack-Verteilung ab.

- 4 Starten Sie den Neutron-Dienst neu. Der spezifische Dienstname hängt von der verwendeten OpenStack-Verteilung ab.

Konfigurieren der IPSec VPN-as-a-Service (VPNaaS) von OpenStack Neutron

Mit diesem Dienst können OpenStack-Benutzer Neutron-Netzwerke über sichere VPN-Tunnel für die Remotesite zugänglich machen.

Der VPNaaS-Treiber ist für das NSX-T Policy-Plug-in nicht verfügbar. Die folgenden Anweisungen gelten nur für das NSX-T Manager-Plug-in.

Verfahren

- 1 Bearbeiten Sie `/etc/neutron/neutron.conf`, um das IPSec VPN-as-a-Service-Plug-in für NSX-T Data Center hinzuzufügen, im Abschnitt „Standardkonfiguration“: `service_plugins = vmware_nsx_vpnaas, [...]`

`service_plugins` ist eine Listenoption. Es ist möglich, mehrere Dienst-Plug-ins anzugeben, indem die vollständigen Klassennamen oder Verknüpfungen mit einem Komma getrennt werden.

- 2 Bearbeiten Sie die Datei `/etc/neutron/neutron-vpnaas.conf` mit Folgendem: Legen Sie den VPNservice-Treiber zum Laden für NSX-T Data Center fest, indem Sie die Einstellung `service_provider` im Abschnitt „service_providers-Konfiguration“ festlegen. `service_provider = VPN:vmware:vmware_nsx.services.vpnaas.nsxv3.ipsec_driver.NSXv3IPsecVpnDriver:default`

Der Wert dieser Option weist eine bestimmte Struktur auf:

`<service_type>:<service_name>:<driver_class>:[<default>]`. `service_provider` ist eine „Multi-String“-Option. Jedes Mal, wenn sie angegeben wird, wird der Wert der Option zu einer Liste hinzugefügt. Mehrere Dienstanbieter können durch Festlegen der Einstellung `service_provider` für jeden angegeben werden.

- 3 Stellen Sie sicher, dass die Datei `/etc/neutron/neutron-vpnaas.conf` zur Neutron-Serverbefehlszeile hinzugefügt wird. Dies kann durch das Ausführen von `ps -aux | grep neutron` überprüft werden und durch das Prüfen, ob `/etc/neutron/neutron-vpnaas.conf` in der Ausgabe vorhanden ist.

Wenn die Datei nicht enthalten ist, sollte der Neutron-Dienst-Launcher bearbeitet werden. Der Speicherort und die Struktur von Dienst-Launchern hängen von der jeweilig verwendeten OpenStack-Verteilung ab.

- 4 Starten Sie den Neutron-Dienst neu. Der spezifische Dienstname hängt von der verwendeten OpenStack-Verteilung ab.

Beispiel-Konfigurationsdateien für erweiterte Neutron Advanced Services

```
[DEFAULT]
ovs_integration_bridge = nsxvswitch
dhcp_agent_notification = False
notify_nova_on_port_data_changes = True
notify_nova_on_port_status_changes = True
core_plugin = vmware_nsxv3
service_plugins =
vmware_nsx_lbaasv2,vmware_nsx_vpnaas,neutron_fwaas.services.firewall.fwaas_plugin_v2.FirewallPluginV2
[...]
neutron_vpnaas.conf
[DEFAULT]
[service_providers]
service_provider =
VPN:vmware:vmware_nsx.services.vpnaas.nsxv3.ipsec_driver.NSXv3IPsecVpnDriver:default
neutron_fwaas.conf
[DEFAULT]
[quotas]
# Number of firewalls allowed per tenant. A negative value means unlimited.
# (integer value)
#quota_firewall = 10
# Number of firewall policies allowed per tenant. A negative value means
# unlimited. (integer value)
#quota_firewall_policy = 10
# Number of firewall rules allowed per tenant. A negative value means
# unlimited. (integer value)
#quota_firewall_rule = 100

[service_providers]
service_provider =
FIREWALL_V2:fwaas_db:neutron_fwaas.services.firewall.service_drivers.agents.agents.FirewallAgentDriver:default
[fwaas]
enabled = True
driver = vmware_nsxv3_edge_v2
neutron_lbaas.conf
[DEFAULT]
[quotas]
# Number of LoadBalancers allowed per tenant. A negative value
# means unlimited. (integer value)
#quota_loadbalancer = 10

# Number of Loadbalancer Listeners allowed per tenant. A negative
# value means unlimited. (integer value)
#quota_listener = -1
# Number of pools allowed per tenant. A negative value means
# unlimited. (integer value)
#quota_pool = 10
# Number of pool members allowed per tenant. A negative value means
# unlimited. (integer value)
#quota_member = -1
```

```
# Number of health monitors allowed per tenant. A negative value
# means unlimited. (integer value)
#quota_healthmonitor = -1
[service_auth]
auth_version = 3
admin_password = password
admin_user = admin
admin_tenant_name = admin
auth_url = http://<keystone_ip>/identity/v3
[service_providers]
service_provider =
LOADBALANCERV2:VMWareEdge:neutron_lbaas.drivers.vmware.edge_driver_v2.EdgeLoadBalancerDriverV2:default
```

```
Octavia.conf
[DEFAULT]
verbose = True
transport_url = rabbit://<amqp_user>:<amqp_password>@<amqp_node>:5672/
debug = True

[api_settings]
default_provider_driver = vmwareedge
enabled_provider_drivers = vmwareedge:NSX
bind_port = 9875
api_handler = queue_producer
bind_host = 0.0.0.0

[database]
connection = mysql+pymysql://root:<db_password?@<db_node>:3306/octavia

[keystone_auth_token]
signing_dir =
memcached_servers = <memcached_node>:11211
cafile = <cabundle_path>
project_domain_name = Default
project_name = service
user_domain_name = Default
password = <password>
username = octavia
auth_url = http://<keystone_node>/identity
auth_type = password

[certificates]
server_certs_key_passphrase = insecure-key-do-not-use-this-key
ca_private_key_passphrase = foobar
ca_private_key = /etc/octavia/certs/private/cakey.pem
ca_certificate = /etc/octavia/certs/ca_01.pem

[controller_worker]
amp_ssh_key_name = octavia_ssh_key
amp_image_tag = amphora
network_driver = allowed_address_pairs_driver
compute_driver = compute_nova_driver
amphora_driver = amphora_haproxy_rest_driver
```



```
workers = 2
amp_active_retries = 100
amp_active_wait_sec = 2

[oslo_messaging]
topic = vmwarensxv_edge_lb
rpc_thread_pool_size = 2

[house_keeping]
load_balancer_expiry_age = 3600

[service_auth]
memcached_servers = <memcached_node>:11211
cafile = <cabundle_path>
project_domain_name = Default
project_name = admin
user_domain_name = Default
password = openstack
username = admin
```

Appendix: NSX-T Data Center Plug-in for OpenStack-Konfigurationseigenschaften

6

Tabelle 6-1. Konfigurationseigenschaften

Abschnitt	Variable	Beschreibung
nsx_p	nsx_api_managers	Die IP-Adresse mindestens eines NSX Managers, ggf. kommasetrennt. Die IP-Adresse muss folgendes Format aufweisen: [<scheme>://]<ip_adress>[:<port>]. Wenn Schema nicht angegeben ist, wird HTTPS verwendet. Wenn kein Port angegeben wird, wird Port 80 für HTTP und Port 443 für HTTPS verwendet.
	nsx_use_client_auth	Boolesch. Auf „true“ festlegen, um die Clientzertifikatauthentifizierung zu aktivieren
	nsx_client_cert_file	Pfad zu einer Datei, die das Clientzertifikat und den privaten Schlüssel enthält, im PEM-Format.
	nsx_client_cert_pk_password	Optionales Kennwort für die Entschlüsselung des privaten Schlüssels.
	nsx_api_user	Der Benutzername, der für den Zugriff auf die NSX Manager-API verwendet wird.
	nsx_api_password	Das für den Zugriff auf die NSX Manager-API verwendete Kennwort.
	dns_domain	Domäne, die zum Aufbau der Hostnamen verwendet werden soll.
	default_overlay_tz	default_edge_cluster
	default_vlan_tz	(Optional) Nur bei der Erstellung von VLAN- oder Flat-Anbieternetzwerken erforderlich. Die UUID oder der Name der standardmäßigen NSX-VLAN-Transportzone, die für die Überbrückung zwischen Neutron-Netzwerken verwendet wird, wenn kein physisches Netzwerk angegeben wurde.

Tabelle 6-1. Konfigurationseigenschaften (Fortsetzung)

Abschnitt	Variable	Beschreibung
	edge_cluster	(Optional) Angeben eines Edge-Clusters für Tier1-Router, mit dem eine Verbindung hergestellt werden soll, außer dem Edge-Cluster, mit dem er verbunden ist.
	Wiederholungen	(Optional) Die maximale Anzahl der Wiederholungen von API-Anforderungen bei veralteten Revisionsfehlern.
	ca_file	(Optional) Geben Sie eine CA-Paketdatei an, die bei der Überprüfung des NSX Manager-Serverzertifikats verwendet werden soll. Diese Option wird ignoriert, wenn „unsicher“ auf „True“ festgelegt ist. Wenn „unsicher“ auf „False“ gesetzt und ca_file nicht festgelegt ist, werden die System-Root-CAs verwendet, um das Serverzertifikat zu überprüfen.
	unsicher	(Optional) Bei Einstellung auf „true“ wird das NSX Manager-Serverzertifikat nicht verifiziert. Bei Einstellung auf „false“ wird das über „ca_file“ angegebene CA-Paket verwendet, oder wenn die Standardsystem-Root-CAs nicht verwendet werden.
	http_timeout	(Optional) Die Zeit in Sekunden, bevor eine HTTP-Verbindung zu einem NSX Manager abgebrochen wird.
	http_read_timeout	(Optional) Die Zeit in Sekunden, bevor eine HTTP-Leseantwort von einem NSX Manager abgebrochen wird.
	http_retries	(Optional) Maximale Anzahl der Wiederholungsversuche einer HTTP-Verbindung.
	concurrent_connections	(Optional) Maximale Anzahl der Verbindungen zu jedem NSX Manager.
	conn_idle_timeout	(Optional) Der Zeitraum in Sekunden, der gewartet wird, bevor die Konnektivität mit dem NSX Manager sichergestellt wird, wenn keine Manager-Verbindung verwendet wurde.
	default_tier0_router	(Optional) Die UUID oder der Name des standardmäßigen Tier-0-Routers, der für die Verbindung mit logischen Tier 1-Routern und das Konfigurieren externer Netzwerke verwendet wird.

Tabelle 6-1. Konfigurationseigenschaften (Fortsetzung)

Abschnitt	Variable	Beschreibung
	metadata_on_demand	(Optional) Wenn „True“ festgelegt ist, wird ein internes Metadaten-Netzwerk nur dann für einen Router erstellt, wenn der Router mit einem DHCP-deaktivierten Subnetz verbunden ist.
	dhcp_profile	(Optional) Die UUID des NSX-DHCP-Profiles, das zum Aktivieren des nativen DHCP-Diensts verwendet wird. Sie muss in NSX erstellt werden, bevor Neutron mit dem NSX-Plug-in gestartet wird.
	locking_coordinator_url	(Optional) URL der Koordinationsressource für verteilte Sperrungen für Sperr-Manager. Dieser Wert wird als Parameter an den tooz-Koordinator übergeben. Standardmäßig ist der Wert „Ohne“ und oslo_concurrency wird für die Verwaltung von Einzelknotensperren verwendet.
	realization_max_attempts	(Optional) Maximal zulässige Anzahl von Wiederholungsversuchen während des Wartens auf die Realisierung einer Ressource. Standard: 50
	realization_wait_sec	(Optional) Anzahl der Sekunden zwischen den Versuchen, eine Ressource zu realisieren. Standard: 1 Sekunde