

适用于 OpenStack Neutron 的 VMware NSX-T Data Center 插件安装指南

2019 年 9 月 19 日

VMware NSX-T Data Center 2.5



vmware®

您可以从 VMware 网站下载最新的技术文档:

<https://docs.vmware.com/cn/>。

如果您对本文档有任何意见或建议, 请将反馈信息发送至:

docfeedback@vmware.com

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

威睿信息技术(中国)有限公司
北京办公室
北京市
朝阳区新源南路 8 号
启皓北京东塔 8 层 801
www.vmware.com/cn

上海办公室
上海市
淮海中路 333 号
瑞安大厦 804-809 室
www.vmware.com/cn

广州办公室
广州市
天河路 385 号
太古汇一座 3502 室
www.vmware.com/cn

版权所有 © 2019 VMware, Inc. 保留所有权利。 [版权和商标信息](#)

目录

1	适用于 OpenStack Neutron 的 VMware NSX-T Data Center 插件安装指南	4
2	准备安装适用于 OpenStack 的 NSX-T Data Center 插件	5
	必备条件	5
	系统要求	5
	Neutron 插件比较	6
3	使用 NSX-T Data Center 插件安装 Neutron 基础服务	8
	在 Ubuntu 系统上安装适用于 OpenStack 的 NSX-T Data Center 插件	8
	在 Red Hat 系统上安装适用于 OpenStack 的 NSX-T Data Center 插件	9
4	为 NSX-T Data Center 插件配置 OpenStack	10
	配置 OpenStack Neutron 网络节点	10
	编辑 neutron.conf 和 nsx.ini 文件	11
	启用基于客户端证书的身份验证	12
	启用 DHCP 和元数据代理服务	12
	适用于 OpenStack 的 NSX-T Data Center 插件配置文件示例	14
	OpenStack Nova 控制器配置	15
	OpenStack Nova 计算配置文件	15
5	使用适用于 OpenStack 的 NSX-T Data Center 插件配置 Neutron 高级服务	16
	配置 OpenStack Octavia 负载均衡器即服务 (LBaaS)	17
	配置 OpenStack Neutron 的负载均衡器即服务 (LBaaS)	17
	配置 OpenStack Neutron 的防火墙即服务 (FWaaS)	18
	配置 OpenStack Neutron 的 IPSec VPN 即服务 (VPNaaS)	19
	Neutron 高级服务的配置文件示例	20
6	附录：适用于 OpenStack 的 NSX-T Data Center 插件配置属性	23

适用于 OpenStack Neutron 的 VMware NSX-T Data Center 插件 安装指南

1

本指南介绍了如何安装和配置适用于 OpenStack Neutron 的 NSX-T Data Center 插件。该信息包括分步配置说明。

完成配置并运行后，VMware NSX-T Data Center 插件允许 OpenStack Neutron 在您的 NSX-T Data Center 部署中实现和管理虚拟网络连接资源。要成功执行这些操作，您应该熟悉 NSX-T Data Center 和 OpenStack 组件及功能。

本指南提供了有关适用于 NSX-T Policy 和 NSX-T Manager 的 Openstack Neutron 插件的信息。这是 NSX-T Data Center 的首个版本，它提供了适用于 NSX-T Policy 的 Openstack 插件。对于此版本，NSX-T Policy 插件仅可用于全新安装。

要了解这些主题，请参见：

- NSX-T Data Center 管理指南
- OpenStack 文档

准备安装适用于 OpenStack 的 NSX-T Data Center 插件

2

本章讨论了以下主题：

- 必备条件
- 系统要求
- Neutron 插件比较

必备条件

VMware 为 OpenStack Neutron 插件提供的支持软件包仅包含特定于 NSX-T 的工件。因此，尝试执行此安装过程前，必须先安装您所选的 OpenStack 服务。

遵循本文档中的过程安装并配置适用于 OpenStack Neutron 的 NSX-T Data Center 插件，以将其与您的 NSX 部署集成。此过程假定在 NSX-T 传输节点上已安装并配置 VMware NSX-T Data Center。

安装 Neutron 服务期间，需要 Internet 连接或者本地发行版存储库镜像的访问权，以确保在安装过程中可下载、安装并配置相应的依赖项。

系统要求

适用于 OpenStack 的 NSX-T Data Center 插件支持是作为 Neutron 插件来实现的。配置 Neutron 时使用的 VMware NSX 插件类取决于所使用的 NSX 版本。

NSX-T Data Center 安装指南 中列出了受支持的 vSphere 和 KVM 管理程序版本（Ubuntu、Red Hat Enterprise Linux、CentOS...）。

适用于 OpenStack 的 NSX-T Data Center 插件对于兼容的 OpenStack 软件版本存在如下具体需求。

适用于 NSX-T Policy 插件的 OpenStack 发行版	版本
开源版本	Stein
适用于 NSX-T Manager 插件的 OpenStack 发行版	版本
开源版本	Rocky
开源版本	Stein
Red Hat OpenStack 平台	Red Hat OpenStack V13（含关联的 Red Hat Enterprise Linux 版本）。

Neutron 插件比较

从 VMware NSX-T Datacenter 2.5 起，有两个插件可用于将 Openstack Neutron 与 NSX-T 相集成：

- **NSX-T Policy** 插件使用基于目的的 API 抽象与 NSX-T Policy Manager 进行交互。这是一个新插件，建议为全新安装选择该插件。
- **NSX-T Manager** 插件使用强制性 API 与 NSX-T Manager 进行交互。这是现有 NSX-T 插件，必须用于现有安装以及 NSX-T Policy 插件尚未涵盖的用例

表 2-1. 插件功能比较

网络与安全性功能	NSX-T MP 插件	NSX-T Policy	描述
交换			
支持 IP 子网重叠	是	是	每个项目均可动态创建项目专用的网络。这些网络可具有相互重叠的 IP 子网。
DHCP	是	是	实例通过 DHCP 自动寻址。
静态 IPv6 地址绑定	否	是	
路由			
逻辑路由	是	是	支持在多个专用逻辑网络之间进行路由，以及在逻辑网络与外部网络之间进行路由。
IPv6 逻辑路由	否	是	支持在多个专用 IPv6 逻辑网络之间进行路由，以及在逻辑网络与外部网络之间进行路由
外部网络	是	是	提供对实例的外部访问的网络。专用网络将通过路由器使用上行链路链接到外部网络，提供对专用网络上实例的外部访问。
IPv6 外部网络	是	是	使用 IPv6 的外部网络。
静态路由	是	是	插入静态路由。
IPv6 静态路由	否	是	使用 IPv6 的外部网络。
实例的浮动 IP	是	是	向实例分配公共可路由 IP 地址，以支持对实例的外部访问。
无 NAT 路由器	是	是	无 NAT 路由拓扑。
IPv6 无 NAT 路由器	否	是	无 NAT 拓扑是采用 IPv6 的 OpenStack 所支持的唯一路由拓扑。不支持采用 IPv6 的 NAT。

表 2-1. 插件功能比较（续）

网络与安全性功能	NSX-T MP 插件	NSX-T Policy	描述
Neutron 路由器双堆栈接口	否	是	在 Neutron 路由器的相同接口上支持 IPv4 和 IPv6 双堆栈。
IPv6 SLAAC	否	是	支持无状态地址自动配置。
安全			
启用防火墙 - 安全组	是	是	OpenStack 安全组（对于 NSX，使用安全组以及使用这些安全组创建的 DFW 规则。这样即可支持微分段）
启用 IPv6 防火墙（安全组）	否	是	采用 IPv6 的 Neutron 安全组。
端口安全	是	是	Neutron 端口安全是使用 NSX SpoofGuard 功能实现的。
IPv6 端口安全	否	是	Neutron 端口安全是使用 NSX SpoofGuard 功能实现的。这样即可允许设置 <code>allowed_address_pairs</code> 并将 IPv6 子网映射到端口
启用防火墙 (L3 FWaaS)	是	是	
启用 IPv6 防火墙 (L3 FWaaS)	否	是	
其他服务			
负载平衡	是	是	
服务质量	是	是	
DNS	是	是	
VPNaaS	是	否	

升级

不存在从含 NSX-T Manager 插件的 Openstack Neutron 到含 NSX-T Policy 插件的 Openstack Neutron 的迁移路径。升级时，现有安装应保持运行 NSX-T Manager 插件。未来发行版中将提供从 NSX-T Manager 到 NSX-T Policy 的迁移路径。NSX-T Policy 插件是为全新安装推荐的解决方案，因为它包含独有功能 (IPv6)；此外，将来将提供 NSX-T 插件专用的新功能。

使用 NSX-T Data Center 插件安装 Neutron 基础服务

3

本章讨论了以下主题：

- 在 Ubuntu 系统上安装适用于 OpenStack 的 NSX-T Data Center 插件
- 在 Red Hat 系统上安装适用于 OpenStack 的 NSX-T Data Center 插件

在 Ubuntu 系统上安装适用于 OpenStack 的 NSX-T Data Center 插件

对于基于 Ubuntu 的 Linux 发行版，NSX-T Data Center 插件作为 debian (.deb) 软件包进行分发。

前提条件

对于基于 Ubuntu 的 Linux 发行版，NSX-T Data Center 插件作为 debian (.deb) 软件包进行分发。

以下说明适用于 NSX-T Manager 和 NSX-T Policy 插件。

- 如果由于依赖关系错误导致 debian 软件包安装失败，那么可能需要安装 python-tooz 和 python-oslo.vmware 软件包。Tooz 是一个 Python 库，可为分布式协调原语提供抽象。其主要目标是在分布式系统中对分组和这些分组的成员资格进行处理。Oslo VMware 库可以为常用 VMware 操作和 API 提供支持。例如：`sudo apt-get install python-oslo.vmware`。

步骤

- 1 下载 .deb 文件：NSX Neutron 插件和 NSX Neutron 常用库。
- 2 将文件复制到 Neutron 网络节点。
- 3 在 .deb 文件所在目录中使用 `dpkg` 命令安装软件包。

以下示例中的版本号可能因下载时所选版本而异：

- `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 安装防火墙即服务 (FWaaS) 软件包。安装后无需启用。

以下示例中的版本号可能因下载时所选版本而异：

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

在 Red Hat 系统上安装适用于 OpenStack 的 NSX-T Data Center 插件

对于基于 Red Hat 的 Linux 发行版，安装适用于 OpenStack 的 NSX-T Data Center 插件已打包为 .rpm 文件。

这些 .rpm 软件包可在 NSX-T Data Center 下载页面的[驱动程序和工具](#)下找到。这些说明适用于不使用 TripleO 的安装，否则请参见 Red Hat OpenStack 的专用指南。

步骤

- 1 下载 .rpm 文件：NSX Neutron 插件和 NSX Neutron 常用库。
- 2 将其复制到要安装插件的 Neutron 网络节点上。
- 3 在 .rpm 文件所在目录中使用 rpm 命令安装该软件包。

以下示例中的版本号可能因下载时所选版本而异：

- `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 安装防火墙即服务 (FWaaS) 软件包。安装后无需启用。

- `sudo yum install python-neutron-fwaas`

为 NSX-T Data Center 插件配置 OpenStack

- [配置 OpenStack Neutron 网络节点](#)
本节中所述的配置描述了 Neutron 网络节点配置。
- [适用于 OpenStack 的 NSX-T Data Center 插件配置文件示例](#)
配置文件通常位于：`/etc/neutron/plugins/vmware/nsx.ini`。
- [OpenStack Nova 控制器配置](#)
本部分中描述的配置是对 Nova 控制器节点配置的补充，其中包含有关 NSX-T Data Center 的信息。
- [OpenStack Nova 计算配置文件](#)
要编辑 Nova 配置文件，请使用 NSX-T。

配置 OpenStack Neutron 网络节点

本节中所述的配置描述了 Neutron 网络节点配置。

本文档主要围绕 NSX-T Policy 插件展开。但是，本节还将着重介绍特定于 NSX-T Manager 插件的设置。

有两条相关的默认配置文件路径：

- `/etc/neutron/neutron.conf`：Neutron 配置文件。
- `/etc/neutron/plugin/vmware/nsx.ini`：VMware NSX Neutron 插件配置文件。
- [编辑 neutron.conf 和 nsx.ini 文件](#)
必须使用与 NSX-T 环境相关的信息来编辑这些文件，以使 Neutron 插件能够与 NSX-T 部署进行交互。
- [启用基于客户端证书的身份验证](#)
支持对 NSX Manager 执行基于 Neutron 客户端证书的身份验证。
- [启用 DHCP 和元数据代理服务](#)
对于 NSX-T Data Center 插件，OpenStack 引用 DHCP 实现已替换为 NSX-T Data Center 本机 DHCP 服务器。NSX-T Data Center 平台还提供了用于访问 Nova 元数据的代理服务器。

编辑 neutron.conf 和 nsx.ini 文件

必须使用与 NSX-T 环境相关的信息来编辑这些文件，以使 Neutron 插件能够与 NSX-T 部署进行交互。

步骤

- 1 编辑 `neutron.conf` 文件以设置 Neutron 核心插件 `[DEFAULT] core_plugin = vmware_nsxp`。要启用 NSX-T Manager 插件：`[DEFAULT] core_plugin = vmware_nsxv3`
- 2 编辑 `nsx.ini` 配置文件，以便为 NSX 部署配置该插件。

NSX-T OpenStack 插件属性位于 `nsx.ini` 配置文件的 `[nsx_p]` 部分下。

以下配置属性同样适用于 NSX-T Manager 插件，并在 `[nsx_v3]` 配置部分中指定。

需要定义的最小配置属性集为：

变量	说明
<code>nsx_api_managers</code>	此参数支持逗号分隔的管理器端点列表。
<code>nsx_api_user</code>	管理员 NSX-T Manager 用户名，通常为 <code>admin</code> 。
<code>nsx_api_password</code>	管理员 NSX-T Manager 密码。
<code>insecure</code>	设置为 <code>False</code> 以强制验证 NSX Manager 服务器证书。默认值为 <code>True</code> 。
<code>ca_file</code>	在验证 NSX Manager 服务器证书时要使用的 CA 包文件。如果“ <code>insecure</code> ”设置为 <code>True</code> ，那么忽略该选项。如果“ <code>insecure</code> ”设置为 <code>False</code> 并且未设置该选项，那么将使用系统根 CA 来验证服务器证书。
<code>nsx_api_managers</code>	将用于创建 Neutron 网络的默认 NSX 覆盖网络传输区域的名称或 UUID。需要先在 NSX 中创建此名称或 UUID，然后才能启动 Neutron。
<code>default_tier0_router</code>	这必须为将来 OpenStack 逻辑路由器 (NSX-T Tier-1) 将连接到的 Policy Manager NSX-T Tier-0 网关路由器名称或 UUID（位于“路由/路由器”下）。
<code>dhcp_profile</code>	输入 UUID 或名称。请参见在 NSX Manager 中创建 DHCP 配置文件 。
<code>metadata_proxy</code>	输入 UUID 或名称。请参见 创建元数据代理 。

- 3 通过运行以下命令重新启动 Neutron 以应用 `nsx.ini` 文件中的更改：`ps-aux |grep neutron`。
- 4 验证输出中是否存在 `nsx.ini` 和 `neutron.conf`。请注意，Neutron 在命令行中可接受一个或多个配置文件。解析配置时会合并这些文件，以便配置文件结构可反映用户的特定偏好。

```
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
```

启用基于客户端证书的身份验证

支持对 NSX Manager 执行基于 Neutron 客户端证书的身份验证。

基于客户端证书的身份验证支持 Neutron 插件以企业管理员角色作为主体身份进行登录。其他主体身份无法编辑由 Neutron 主体身份创建的资源，因此可避免发生诸如删除与 Neutron 路由器关联的逻辑路由器之类的意外错误。请参见《NSX-T for Data Center 管理指南》中的“查看主体身份”以获取更多信息。

步骤

- 1 要启用客户端证书身份验证，请在 `nsx.ini` 文件中完成如下定义：

- `nsx_use_client_auth = True`
- `nsx_client_cert_storage = nsx-db`
- `nsx_client_cert_file = <file to store certificate and private key>`

- 2 通过运行以下命令重新启动 Neutron 以应用 `nsx.ini` 文件中的更改：`service neutron-server restart`。

通过运行以下命令验证 Neutron 服务器是否正在使用 `neutron.conf` 和 `nsx.ini` 文件：

- `ps -aux |grep neutron`

验证输出中是否存在 `nsx.ini` 和 `neutron.conf`。例如：

```
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
```

启用 DHCP 和元数据代理服务

对于 NSX-T Data Center 插件，OpenStack 引用 DHCP 实现已替换为 NSX-T Data Center 本机 DHCP 服务器。NSX-T Data Center 平台还提供了用于访问 Nova 元数据的代理服务器。

无论上一步中是否已配置 NSX-T 插件，都必须执行这些操作。

- 在 [NSX Manager](#) 中创建 DHCP 配置文件

DHCP 服务器配置文件用于指定 NSX Edge 群集或 NSX Edge 群集的成员。具有此配置文件的 DHCP 服务器可处理来自逻辑交换机上虚拟机的 DHCP 请求，这些逻辑交换机已连接到配置文件中指定的 NSX Edge 节点。

- [创建元数据代理](#)

通过使用元数据代理服务器，虚拟机实例可以从 OpenStack Nova API 服务器中检索实例特定的元数据。

- [编辑 nsx.ini 文件](#)

在使用这些配置文件的 `nsx.ini` 中应指定新变量 `native_dhcp_metadata`、`metadata_proxy` 和 `dhcp_profile`。

在 NSX Manager 中创建 DHCP 配置文件

DHCP 服务器配置文件用于指定 NSX Edge 群集或 NSX Edge 群集的成员。具有此配置文件的 DHCP 服务器可处理来自逻辑交换机上虚拟机的 DHCP 请求，这些逻辑交换机已连接到配置文件中指定的 NSX Edge 节点。

前提条件

要启用 NSX-T Data Center 的本地 DHCP 服务器，必须在 NSX-T Data Center 中创建 DHCP 配置文件，并将其传递到 `nsx.ini` 中的 Neutron 插件配置。确保 `neutron dhcp` 服务（`devstack` 中的 `q-dhcp`）和元数据代理（`devstack` 中的 `q-meta`）未在运行。在 `neutron.conf` 文件中，将 `dhcp` 设置为 `False`。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 `https://nsx-manager-ip-address` 中的 NSX Manager。
- 2 从导航面板中选择 **高级网络和安全 > DHCP**。
- 3 选择 **服务器配置文件**，然后单击 **添加**。
- 4 输入名称和可选的说明。
- 5 从下拉菜单中选择 **Edge 群集**。
- 6 单击 **添加**。

创建元数据代理

通过使用元数据代理服务器，虚拟机实例可以从 OpenStack Nova API 服务器中检索实例特定的元数据。

NSX 平台提供了用于访问 Nova 元数据的代理服务器。此代理将捕获在 `169.254.269.254` 地址上提交的所有请求，并将其转发到 NSX-T 元数据代理配置中指定的 Nova 元数据服务器端点。

前提条件

用于元数据代理的 Edge 节点必须具有从其管理 IP 地址到元数据服务器的 IP 连接。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 `https://nsx-manager-ip-address` 中的 NSX Manager。
- 2 从导航面板中选择 **高级网络 > DHCP**。
- 3 选择 **元数据代理**，并单击 **添加**。
- 4 输入 **名称**和可选的说明。
- 5 输入以下 **Nova 服务器 URL**：`http://<openstack_controller>:8775`。如果元数据代理服务器正在侦听默认端口 `8775` 以外的其他端口，请使用正确的端口更新 URL。可在 Nova API 配置文件 `/etc/nova.conf` 中的控制器节点上通过查找 `metadata_listen_port` 参数找到这些端口。如果需要更改配置，请重新启动 `n-api` 或 `nova` 服务器。
- 6 输入 **Secret** 参数。
- 7 从下拉菜单中选择 **Edge 群集**。

8 单击添加。

编辑 nsx.ini 文件

在使用这些配置文件的 nsx.ini 中应指定新变量 native_dhcp_metadata、metadata_proxy 和 dhcp_profile。

- 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

适用于 OpenStack 的 NSX-T Data Center 插件配置文件示例

配置文件通常位于：/etc/neutron/plugins/vmware/nsx.ini。

以下是配置文件示例：

```
[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 控制器配置

本部分中描述的配置是对 Nova 控制器节点配置的补充，其中包含有关 NSX-T Data Center 的信息。

以下是 Nova 控制器配置文件示例，此文件通常位于控制节点上的 `/etc/nova/nova.conf` 中。

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

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

OpenStack Nova 计算配置文件

要编辑 Nova 配置文件，请使用 NSX-T。

本部分中描述的配置是对 Nova 计算节点配置的补充，其中包含有关 NSX-T Data Center 的信息。

以下是 Nova 计算配置文件示例，此文件通常位于计算节点上的 `/etc/nova/nova.conf` 中。

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

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

使用适用于 OpenStack 的 NSX-T Data Center 插件配置 Neutron 高级服务

5

OpenStack Neutron 的负载均衡器即服务 (LBaaS)、防火墙即服务 (FWaaS) 和 IPSec VPN 即服务 (VPNaaS) 也称为 Neutron 高级服务。

从 NSX-T Data Center 2.5 起，NSX-T 插件（包括 Policy 和 Manager）支持 Octavia 负载均衡服务，此服务用于替代已淘汰的 Neutron LBaaS 服务。

以下信息假定您已拥有 NSX-T Data Center 2.4 和 OpenStack Stein 14.0。

[系统要求](#) 中列出了受支持的最新版本。

要启用 Neutron 高级服务 NSX-T Data Center，应在 Neutron 配置中指定以下内容：

- 为特定服务启用服务插件
- 为服务配置服务提供程序
- 提供 NSX-T Data Center 驱动程序（如适用）和特定于 NSX-T Data Center 的配置条目

在 Neutron 配置文件中指定了这些选项，这些文件通常位于 `/etc/neutron` 中（注：特定于插件的配置文件通常位于 `/etc/neutron/plugins/vmware` 中）。Neutron 在命令行中可接受一个或多个配置文件。解析配置时会合并这些文件，以便配置文件结构可反映用户的特定偏好。通常采用以下结构：

- **neutron.conf**：Neutron 核心选项、基本配置参数（例如，API Manager 端点、传输区域标识）和服务插件列表。
- **neutron_lbass.conf**：负载均衡服务提供程序和选项。
- **Octavia.conf**：负载均衡提供程序和 MQ 主题。仅适用于 Octavia 负载均衡器服务。此文件通常位于 `/etc/Octavia/Octavia.conf` 中，并且通过 Octavia 服务进行加载。
- **neutron_fwass.conf**：防火墙服务提供程序、驱动程序和驱动程序选项。
- **neutron_vpnaas.conf**：VPN 服务提供程序和其他选项。

服务提供程序是使用 `service_provider` 选项指定的。在 Neutron 配置中可为不同种类的服务多次重复使用此选项，但任一给定服务类型不得包含多个默认服务提供程序。

Service_provider 配置属性结构：<SERVICE_TYPE>:<PROVIDER_CLASS>:[<DEFAULT>]。

- [配置 OpenStack Octavia 负载均衡器即服务 \(LBaaS\)](#)

这些说明适用于配置 OpenStack 如何将 NSX-T Data Center 负载均衡器与 Octavia 配合使用。

- [配置 OpenStack Neutron 的负载均衡器即服务 \(LBaaS\)](#)

- [配置 OpenStack Neutron 的防火墙即服务 \(FWaaS\)](#)

这些说明用于配置 FWaaS v2。

- [配置 OpenStack Neutron 的 IPsec VPN 即服务 \(VPNaaS\)](#)

此服务支持 OpenStack 用户在远程站点上通过安全的 VPN 隧道访问 Neutron 网络。

- [Neutron 高级服务的配置文件示例](#)

配置 OpenStack Octavia 负载均衡器即服务 (LBaaS)

这些说明适用于配置 OpenStack 如何将 NSX-T Data Center 负载均衡器与 Octavia 配合使用。

这些说明同样适用于 NSX-T Policy 和 NSX-T Manager 插件。

有关 Octavia 负载均衡器服务的一般信息，请参见官方文档。

步骤

- 1 在 `/etc/neutron/neutron.conf` 中，确保未配置 NSX-T Data Center 的负载均衡服务插件，即 `service_plugins` 列表中不应存在 `vmware_nsx_lbaasv2`。如果已对 `neutron.conf` 文件执行任何更改，请重新启动 Neutron 服务
- 2 在 `/etc/octavia/octavia.conf` 中，指定以下操作：
 - a 在 `[api_settings]` 配置设置中，指定 NSX-T 提供程序：`default_provider_driver = vmwareedge` `enabled_provider_drivers = vmwareedge:NSX`
 - b 在 `[oslo_messaging]` 部分中，为 Octavia 与 Neutron 进程空间中运行的 NSX-T 驱动程序之间的通信指定一个主题。
- 3 重新启动 Octavia API 服务。

配置 OpenStack Neutron 的负载均衡器即服务 (LBaaS)

这些说明适用于配置 OpenStack 如何将 NSX-T Data Center 负载均衡器与 LBaaS v2 配合使用。这些说明同样适用于 NSX-T Policy 和 NSX-T Manager 插件。

步骤

- 1 编辑 `/etc/neutron/neutron.conf`，在以下默认配置部分中为 NSX-T Data Center 添加负载均衡服务插件：`service_plugins = vmware_nsx_lbaasv2, [...]`

请注意，`service_plugins` 是一个列表选项。可指定多个服务插件，使用逗号分隔其完整类名或快捷方式。

2 按如下方式编辑 `/etc/neutron/neutron-lbaas.conf` 文件：

- a 通过在 `service_providers` 配置部分中设置 `service_provider` 选项，为 NSX-T Data Center 设置负载均衡器服务驱动程序：`service_plugins = LOADBALANCERV2:VMwareEdge:neutron_lbaas.drivers.vmware.edge_driver_v2.EdgeLoadBalancerDriverV2:default`。
- b 如果尚未配置 **Keystone** 身份验证参数，请完成配置。这些参数供 `neutron-lbaas` 服务使用，与 NSX-T Data Center 集成不相关。请注意，应提供 **Keystone** 端点的位置。

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

3 确保 `/etc/neutron/neutron-lbaas.conf` 文件已添加到 **Neutron** 服务器命令行。可通过运行 `ps -aux | grep neutron` 命令并验证输出中是否存在 `/etc/neutron/neutron-lbaas.conf` 来完成此验证过程。

如果其中不包含此文件，那么应编辑 **Neutron** 服务启动程序。服务启动程序的位置和结构取决于所使用的特定 **Openstack** 发行版。

4 重新启动 **Neutron** 服务。确切的服务名称取决于所使用的 **OpenStack** 发行版。

配置 OpenStack Neutron 的防火墙即服务 (FWaaS)

这些说明用于配置 FWaaS v2。

步骤

1 编辑 `/etc/neutron/neutron.conf`，在以下默认配置部分中为 NSX-T Data Center 添加防火墙即服务插件：`service_plugins = firewall_v2`

`Service_plugins` 是一个列表选项。可指定多个服务插件，使用逗号分隔其完整类名或快捷方式。

2 按如下方式编辑 `/etc/neutron/neutron-fwaas.conf` 文件：

- a 通过在 `service_providers` 配置部分中设置 `service_provider` 选项，为 NSX-T Data Center 设置防火墙即服务驱动程序。`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
```

该选项的值采用如下特殊结构：`<service_type>:<service_name>:<driver_class>:<default>`。 `service_provider` 是一个“多字符串”选项。每次指定该选项时，都会将该选项的值添加到列表中。可通过为每个服务提供程序都设置 `service_provider` 选项来指定多个服务提供程序。

- b 通过在 FWaaS 配置部分中设置 `enabled = True` 来开启防火墙即服务。
 - c 通过在 FWaaS 配置部分中设置 `driver = vmware_nsxp_edge_v2`，为 NSX-T Data Center 设置 FWaaS 设备驱动程序。
 - d 通过在 FWaaS 配置部分中设置 `driver = vmware_nsxv3_edge_v2`，为 NSX Manager 插件设置 FWaaS 设备驱动程序。
- 3** 检查 `/etc/neutron/neutron-fwaas.conf` 文件是否已添加到 Neutron 服务器命令行中。可通过运行 `ps -aux | grep neutron` 并验证输出中是否存在 `/etc/neutron/neutron-fwaas.conf` 来完成此验证过程。

如果其中不包含此文件，那么应编辑 Neutron 服务启动程序。服务启动程序的位置和结构取决于所使用的特定 OpenStack 发行版。

- 4** 重新启动 Neutron 服务。具体服务名称取决于所使用的 OpenStack 发行版。

配置 OpenStack Neutron 的 IPSec VPN 即服务 (VPNaaS)

此服务支持 OpenStack 用户在远程站点上通过安全的 VPN 隧道访问 Neutron 网络。

VPNaaS 驱动程序不可供 NSX-T Policy 插件使用。以下说明仅适用于 NSX-T Manager 插件。

步骤

- 1** 编辑 `/etc/neutron/neutron.conf`，在以下默认配置部分中为 NSX-T Data Center 添加 IPSec VPN 即服务插件：`service_plugins = vmware_nsx_vpnaas,[...]`

`service_plugins` 是一个列表选项。可指定多个服务插件，使用逗号分隔其完整类名或快捷方式。

- 2 如下所示编辑 `/etc/neutron/neutron-vpnaas.conf` 文件：通过在 `service_providers` 配置部分中设置 `service_provider` 选项，为 NSX-T Data Center 设置加载 VPNservice 驱动程序。

```
service_provider =
```

```
VPN:vmware:vmware_nsx.services.vpnaas.nsxv3.ipsec_driver.NSXv3IPsecVpnDriver:default
```

该选项的值采用如下特殊结构：<service_type>:<service_name>:<driver_class>:

[<default>]。`service_provider` 是一个“多字符串”选项。每次指定该选项时，都会将该选项的值添加到列表中。可以通过为每个服务提供程序设置 `service_provider` 选项来指定多个服务提供程序。

- 3 确保 `/etc/neutron/neutron-vpnaas.conf` 文件已添加到 Neutron 服务器命令行。可通过运行 `ps -aux | grep neutron` 并验证输出中是否存在 `/etc/neutron/neutron-vpnaas.conf` 来完成此验证过程。

如果其中不包含此文件，那么应编辑 Neutron 服务启动程序。服务启动程序的位置和结构取决于所使用的特定 OpenStack 发行版。

- 4 重新启动 Neutron 服务。具体服务名称取决于所使用的 OpenStack 发行版。

Neutron 高级服务的配置文件示例

```
[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 =
LOADBALANCER_V2: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
```

附录：适用于 OpenStack 的 NSX-T Data Center 插件配置属性

6

表 6-1. 配置属性

区域	变量	说明
nsx_p	nsx_api_managers	一个或多个 NSX Manager 的 IP 地址（由逗号分隔）。IP 地址应采用以下格式： [<scheme>://]<ip_address>[:<port>]。如果未提供方案，将使用 https。如果未提供端口，那么对于 http 将使用端口 80，对于 https 则使用端口 443。
	nsx_use_client_auth	Boolean 设置为 True 以启用客户端证书身份验证
	nsx_client_cert_file	包含客户端证书和私钥的 PEM 格式文件的路径。
	nsx_client_cert_pk_password	（可选）用于对私钥进行解密的密码。
	nsx_api_user	用于访问 NSX Manager API 的用户名。
	nsx_api_password	用于访问 NSX Manager API 的密码。
	dns_domain	用于构建主机名的域。
	default_overlay_tz	default_edge_cluster
	default_vlan_tz	（可选）仅当创建 VLAN 或扁平化提供者网络时才需要。默认 NSX VLAN 传输区域的 UUID 或名称，用于在未指定任何物理网络的情况下桥接 Neutron 网络。
	edge_cluster	（可选）为 Tier-1 路由器指定要连接到的 Edge 群集，而不是已连接到的 Edge 群集。
	retries	（可选）表示出现失效修订错误时，可重试 API 请求的最大次数。
	ca_file	（可选）指定在验证 NSX Manager 服务器证书时要使用的 CA 包文件。如果“insecure”设置为 True，那么忽略该选项。如果“insecure”设置为 False 并且未设置 ca_file，那么将使用系统根 CA 来验证服务器证书。

表 6-1. 配置属性（续）

区域	变量	说明
	<code>insecure</code>	（可选）如果设置为 <code>true</code> ，那么不会验证 NSX Manager 服务器证书。如果设置为 <code>false</code> ，那么将使用通过“ <code>ca_file</code> ”指定的 CA 包，如果未设置，则使用默认系统根 CA。
	<code>http_timeout</code>	（可选）在中止与 NSX Manager 的 HTTP 连接之前等待的时间（秒）。
	<code>http_read_timeout</code>	（可选）在中止来自 NSX Manager 的 HTTP 读响应之前等待的时间（秒）。
	<code>http_retries</code>	（可选）HTTP 连接的最大重试次数。
	<code>concurrent_connections</code>	（可选）与每个 NSX Manager 建立的最大连接数。
	<code>conn_idle_timeout</code>	（可选）在未使用任何 NSX Manager 连接的情况下，确认与 NSX Manager 连接之前等待的时间量（秒）。
	<code>default_tier0_router</code>	（可选）用于连接到 Tier-1 逻辑路由器和配置外部网络的默认 Tier-0 路由器的 UUID 或名称。
	<code>metadata_on_demand</code>	（可选）如果设置为 <code>True</code> ，那么仅当路由器连接到已禁用 DHCP 的子网时，才会为路由器创建内部元数据网络。
	<code>dhcp_profile</code>	（可选）用于启用本机 DHCP 服务的 NSX DHCP 配置文件的 UUID。需要先在 NSX 中创建此 UUID，然后才能使用 NSX 插件启动 Neutron。
	<code>locking_coordinator_url</code>	（可选）用于锁定管理器的分布式锁定协调资源的 URL。该值将作为参数传递到 <code>tooz</code> 协调程序。默认情况下，该值为 <code>None</code> ，并使用 <code>oslo_concurrency</code> 进行单节点锁定管理。
	<code>realization_max_attempts</code>	（可选）等待实现资源时允许的最大重试次数。默认值：50
	<code>realization_wait_sec</code>	（可选）为实现资源所进行尝试之间间隔的秒数。默认值：1 秒