

適用於 OpenStack Neutron 的 VMware NSX-T Data Center 外掛程式安裝指南

2019 年 9 月 19 日

VMware NSX-T Data Center 2.5



vmware®

您可以在 VMware 網站上找到最新的技術文件，網址如下：

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

如果您對於本文件有任何意見，歡迎寄至：

docfeedback@vmware.com

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

Copyright © 2019 VMware, Inc. 保留所有權利。 [版權與商標資訊](#)。

目錄

- 1 適用於 OpenStack Neutron 的 VMware NSX-T Data Center 外掛程式安裝指南 4
- 2 準備安裝適用於 OpenStack 的 NSX-T Data Center 外掛程式 5
 - 必要條件 5
 - 系統需求 5
 - Neutron 外掛程式比較 6
- 3 使用 NSX-T Data Center 外掛程式安裝 Neutron 基本服務 8
 - 在 Ubuntu 系統上安裝適用於 OpenStack 的 NSX-T Data Center 外掛程式 8
 - 在 Red Hat 系統上安裝適用於 OpenStack 的 NSX-T Data Center 外掛程式 9
- 4 針對 NSX-T Data Center 外掛程式設定 OpenStack 10
 - 設定 OpenStack Neutron 網路節點 10
 - 編輯 neutron.conf 和 nsx.ini 檔案 10
 - 啟用以用戶端憑證為基礎的驗證 11
 - 啟用 DHCP 和中繼資料 Proxy 服務 12
 - 適用於 OpenStack 的 NSX-T Data Center 外掛程式的範例組態檔案 14
 - OpenStack Nova 控制器組態 15
 - OpenStack Nova 運算組態檔案 15
- 5 使用適用於 OpenStack 的 NSX-T Data Center 外掛程式設定 Neutron 進階服務 16
 - 設定 OpenStack Octavia 負載平衡器即服務 (LBaaS) 17
 - 設定 OpenStack Neutron 的負載平衡器即服務 (LBaaS) 17
 - 設定 OpenStack Neutron 的防火牆即服務 (FWaaS) 18
 - 設定 OpenStack Neutron 的 IPSec VPN 即服務 (VPNaaS) 19
 - Neutron 進階服務的範例組態檔案 20
- 6 附錄：適用於 OpenStack 的 NSX-T Data Center 外掛程式組態內容 23

適用於 OpenStack Neutron 的 VMware NSX-T Data Center 外掛 程式安裝指南

1

本指南說明如何安裝和設定適用於 OpenStack Neutron 的 NSX-T Data Center 外掛程式。其中的資訊包含逐步的組態指示。

設定並執行後，VMware NSX-T Data Center 外掛程式會允許 OpenStack Neutron 在您的 NSX-T Data Center 部署中實現和管理虛擬網路資源。若要成功執行，您應該熟悉 NSX-T Data Center 和 OpenStack 元件與功能。

本指南提供適用於 NSX-T 原則和 NSX-T Manager 的 OpenStack Neutron 外掛程式的相關資訊。這是提供適用於 NSX-T 原則的 OpenStack 外掛程式的第一個 NSX-T Data Center 版本。針對此版本，NSX-T 原則外掛程式僅可用於全新安裝。

若要瞭解這些主題，請參閱：

- 《NSX-T Data Center 管理指南》
- OpenStack 說明文件

準備安裝適用於 OpenStack 的 NSX-T Data Center 外掛程式

2

本章節討論下列主題：

- 必要條件
- 系統需求
- Neutron 外掛程式比較

必要條件

VMware 為 OpenStack Neutron 外掛程式提供的支援套件僅包含 NSX-T 的特定構件。因此，必須先安裝您所選擇的 OpenStack 服務，然後再嘗試執行此安裝程序。

請遵循本文件中的程序來安裝和設定適用於 OpenStack Neutron 的 NSX-T Data Center 外掛程式，以與 NSX 部署整合。此程序假設已在 NSX-T 傳輸節點上安裝並設定 VMware NSX-T Data Center。

在 Neutron 服務安裝期間，需要網際網路連線或存取本機散發存放庫鏡像，以確保在安裝程序中可下載、安裝和設定適當的相依性。

系統需求

適用於 OpenStack 的 NSX-T Data Center 外掛程式的支援會以 Neutron 外掛程式形式實作。設定 Neutron 時所使用的 VMware NSX 外掛程式類別取決於您所使用的 NSX 版本。

《NSX-T Data Center 安裝指南》中會列出 vSphere 和 KVM 支援的 Hypervisor 版本 (Ubuntu、Red Hat Enterprise Linux、CentOS...)。

適用於 OpenStack 的 NSX-T Data Center 外掛程式有下列有關相容 OpenStack 軟體版本的特定需求。

適用於 NSX-T 原則外掛程式的 OpenStack 發行版	版本
開放原始碼版本	Stein
適用於 NSX-T Manager 外掛程式的 OpenStack 發行版	版本
開放原始碼版本	Rocky
開放原始碼版本	Stein
Red Hat OpenStack 平台	含有 Red Hat Enterprise Linux 相關聯版本的 Red Hat OpenStack 版本 13。

Neutron 外掛程式比較

從 VMware NSX-T Data Center 2.5 開始，提供兩個外掛程式用於整合 OpenStack Neutron 與 NSX-T：

- NSX-T 原則外掛程式會使用基於意圖的 API 抽象，與 NSX-T Policy Manager 進行互動。這是新的外掛程式，並且是新安裝的建議選項。
- NSX-T Manager 外掛程式會使用命令式 API 與 NSX-T Manager 互動。這是現有的 NSX-T 外掛程式，必須用於現有的安裝以及 NSX-T 原則外掛程式未涵蓋的使用案例

表 2-1. 外掛程式功能比較

網路與安全性首頁	NSX-T MP 外掛程式	NSX-T 原則	說明
交換			
重疊的 IP 子網路支援	是	是	每個專案都可以動態建立專案專用的網路。這些網路可具有彼此重疊的 IP 子網路。
DHCP	是	是	執行個體會透過 DHCP 具有自動定址。
靜態 IPv6 位址繫結	否	是	
路由			
邏輯路由	是	是	在多個私人邏輯網路之間以及邏輯網路與外部網路之間啟用路由。
IPv6 邏輯路由	否	是	在多個專用 IPv6 邏輯網路之間以及邏輯網路與外部網路之間啟用路由
外部網路	是	是	對執行個體提供外部存取的網路。專用網路將透過路由器上行連結至外部網路，以提供對專用網路上執行個體的外部存取。
IPv6 外部網路	是	是	使用 IPv6 的外部網路。
靜態路由	是	是	插入靜態路由。
IPv6 靜態路由	否	是	使用 IPv6 的外部網路。
執行個體的浮動 IP	是	是	指派公用可路由的 IP 位址給執行個體，以啟用執行個體的外部存取。
無 NAT 路由器	是	是	無 NAT 路由器拓撲。
IPv6 無 NAT 路由器	否	是	無 NAT 拓撲是 OpenStack 搭配 IPv6 支援的唯一路由拓撲。不支援使用 NAT 搭配 IPv6。

表 2-1. 外掛程式功能比較 (續)

網路與安全性首頁	NSX-T MP 外掛程式	NSX-T 原則	說明
Neutron 路由器雙重堆疊介面	否	是	在 Neutron 路由器的相同介面上支援 IPv4 和 IPv6 雙重堆疊。
IPv6 SLAAC	否	是	支援無狀態位址自動組態。
安全性			
防火牆 - 安全群組	是	是	OpenStack 安全群組 (使用 NSX，會使用安全群組以及使用這些安全群組建立的 DFW 規則。這會允許微分割)
IPv6 防火牆 (安全群組)	否	是	Neutron 安全群組搭配 IPv6。
連接埠安全性	是	是	Neutron 連接埠安全性是使用 NSX SpoofGuard 功能來實作。
IPv6 連接埠安全性	否	是	Neutron 連接埠安全性是使用 NSX SpoofGuard 功能來實作。這會允許使用 <code>allowed_address_pairs</code> 和一個 IPv6 子網路對應至連接埠
防火牆 (L3 FWaaS)	是	是	
IPv6 防火牆 (L3 FWaaS)	否	是	
其他服務			
負載平衡	是	是	
服務品質	是	是	
DNS	是	是	
VPNaaS	是	否	

升級

從 OpenStack Neutron 搭配 NSX-T Manager 外掛程式到 OpenStack Neutron 搭配 NSX-T 原則外掛程式不存在任何移轉路徑。升級時，現有的安裝應持續執行 NSX-T Manager 外掛程式。在未來版本中，將提供從 NSX-T Manager 到 NSX-T 原則的移轉路徑。NSX-T 原則外掛程式是全新安裝的建議解決方案，因為它包含獨特功能 (IPv6)；此外，未來新功能將以獨佔方式提供 NSX-T 外掛程式使用。

使用 NSX-T Data Center 外掛程式 安裝 Neutron 基本服務

3

本章節討論下列主題：

- 在 Ubuntu 系統上安裝適用於 OpenStack 的 NSX-T Data Center 外掛程式
- 在 Red Hat 系統上安裝適用於 OpenStack 的 NSX-T Data Center 外掛程式

在 Ubuntu 系統上安裝適用於 OpenStack 的 NSX-T Data Center 外掛程式

針對以 Ubuntu 為基礎的 Linux 發行版，NSX-T Data Center 外掛程式會以 Debian (.deb) 套件的形式散佈。

必要條件

針對以 Ubuntu 為基礎的 Linux 發行版，NSX-T Data Center 外掛程式會以 Debian (.deb) 套件的形式散佈。

下列指示同時適用 NSX-T Manager 和 NSX-T 原則外掛程式。

- 如果由於相依性錯誤導致 Debian 套件安裝失敗，則可能需要安裝 `python-tooz` 和 `python-oslo.vmware` 套件。Tooz 是 Python 程式庫，可為分散式協調原始提供抽象。其主要目標是在分散式系統中處理群組和這些群組的成員資格。Oslo VMware 程式庫提供對通用 VMware 作業和 API 的支援。例如：`sudo apt-get install python-oslo.vmware`。

程序

- 1 下載 .deb 檔案：NSX Neutron 外掛程式和 NSX Neutron 通用程式庫。
- 2 將檔案複製到 Neutron 網路節點。
- 3 在與 .deb 檔案相同的目錄中，使用 `dpkg` 命令安裝套件。

根據下載時選取的版本，下列範例中的版本號碼可能會有所不同：

- `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 安裝防火牆即服務 (FWaaS) 套件。安裝後不需要啟用此功能。

根據下載時選取的版本，下列範例中的版本號碼可能會有所不同：

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

在 Red Hat 系統上安裝適用於 OpenStack 的 NSX-T Data Center 外掛程式

安裝適用於 OpenStack 的 NSX-T Data Center 外掛程式，封裝為以 Red Hat 為基礎的 Linux 發行版適用的 .rpm 檔案。

.rpm 套件可在 NSX-T Data Center 下載頁面的[驅動程式和工具](#)下找到。這些指示適用於未利用 TripleO 的安裝，否則請參閱 Red Hat OpenStack 的專用指南。

程序

- 1 下載 .rpm 檔案：NSX Neutron 外掛程式和 NSX Neutron 通用程式庫。
- 2 將其複製到您要在其上安裝外掛程式的 Neutron 網路節點上。
- 3 在與 .rpm 檔案所在相同的目錄中使用 rpm 命令安裝套件。

根據下載時選取的版本，下列範例中的版本號碼可能會有所不同：

- `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 安裝防火牆即服務 (FWaaS) 套件。安裝後不需要啟用此功能。

- `sudo yum install python-neutron-fwaas`

針對 NSX-T Data Center 外掛程式 設定 OpenStack

4

- 設定 [OpenStack Neutron](#) 網路節點
本節中所述的組態說明 Neutron 網路節點組態。
- 適用於 [OpenStack](#) 的 [NSX-T Data Center](#) 外掛程式的範例組態檔案
組態檔案通常位於 `/etc/neutron/plugins/vmware/nsx.ini`。
- [OpenStack Nova](#) 控制器組態
本節中所述的組態對 Nova 控制器節點組態進行補充，並提供有關 NSX-T Data Center 的資訊。
- [OpenStack Nova](#) 運算組態檔案
若要編輯 Nova 組態檔案，請使用 NSX-T。

設定 OpenStack Neutron 網路節點

本節中所述的組態說明 Neutron 網路節點組態。

本說明文件與 NSX-T 原則外掛程式相關。但是，此小節也會強調 NSX-T Manager 外掛程式的特定設定。

這兩個預設的組態檔案路徑是相關的：

- `/etc/neutron/neutron.conf` -- Neutron 的組態檔案。
- `/etc/neutron/plugin/vmware/nsx.ini` -- VMware NSX Neutron 外掛程式的組態檔案。
- 編輯 [neutron.conf](#) 和 [nsx.ini](#) 檔案
必須使用與 NSX-T 環境相關的資訊編輯這些檔案，才能讓 Neutron 外掛程式與 NSX-T 部署互動。
- 啟用以用戶端憑證為基礎的驗證
對 NSX Manager 支援以 Neutron 用戶端憑證為基礎的驗證。
- 啟用 [DHCP](#) 和中繼資料 [Proxy](#) 服務
使用 NSX-T Data Center 外掛程式時，OpenStack 參考 DHCP 實作會由 NSX-T Data Center 原生 DHCP 伺服器取代。NSX-T Data Center 平台也提供用於存取 Nova 中繼資料的 Proxy 伺服器。

編輯 neutron.conf 和 nsx.ini 檔案

必須使用與 NSX-T 環境相關的資訊編輯這些檔案，才能讓 Neutron 外掛程式與 NSX-T 部署互動。

程序

- 1 編輯 `neutron.conf` 檔案來設定核心 Neutron 外掛程式

[DEFAULT] core_plugin = vmware_nsxp。若要啟用 NSX-T Manager 外掛程式：

[DEFAULT] core_plugin = vmware_nsxv3

- 2 編輯 `nsx.ini` 組態檔案以設定用於 NSX 部署的外掛程式。

NSX-T OpenStack 外掛程式內容位於 `nsx.ini` 組態檔案的 `[nsx_p]` 區段下。

下方的組態內容也適用 NSX-T Manager 外掛程式，並且是在 `[nsx_v3]` 組態區段中指定。

需要定義的最小組態內容集如下：

變數	說明
<code>nsx_api_managers</code>	此參數會允許以逗點分隔的 Manager 端點清單。
<code>nsx_api_user</code>	管理員 NSX-T Manager 使用者名稱，通常為 <code>admin</code> 。
<code>nsx_api_password</code>	管理員 NSX-T Manager 密碼。
<code>insecure</code>	設定為 <code>False</code> 可強制驗證 NSX Manager 伺服器憑證。預設值為 <code>True</code> 。
<code>ca_file</code>	用於驗證 NSX Manager 伺服器憑證的 CA 服務包檔案。如果「 <code>insecure</code> 」設為 <code>True</code> ，則會忽略此選項。如果「 <code>insecure</code> 」設為 <code>False</code> 且此選項未設定，則會使用系統根 CA 來驗證伺服器憑證。
<code>nsx_api_managers</code>	將用於建立 Neutron 網路的預設 NSX 覆蓋傳輸區域的名稱或 UUID。必須先在 NSX 中建立，然後才能啟動 Neutron。
<code>default_tier0_router</code>	這必須是將連線到未來 OpenStack 邏輯路由器 (NSX-T 第 1 層) 的 Policy Manager NSX-T 第 0 層名稱開道路由器或 UUID (位於「路由/路由器」下方)。
<code>dhcp_profile</code>	輸入 UUID 或名稱。請參閱在 NSX Manager 中建立 DHCP 設定檔 。
<code>metadata_proxy</code>	輸入 UUID 或名稱。請參閱 建立中繼資料 Proxy 。

- 3 執行下列命令重新啟動 Neutron，以提取 `nsx.ini` 檔案中的變更：`ps-aux |grep neutron`。
- 4 確認 `nsx.ini` 和 `neutron.conf` 存在輸出中。請注意，Neutron 可在命令列中接受一或多個組態檔案。剖析組態時會合併這些檔案，以便組態檔案結構可以反映特定使用者的喜好設定。

```
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
```

啟用以用戶端憑證為基礎的驗證

對 NSX Manager 支援以 Neutron 用戶端憑證為基礎的驗證。

以用戶端憑證為基礎的驗證可讓 Neutron 外掛程式以企業管理員角色登入主體身分識別。其他主體身分識別無法編輯 Neutron 主體身分識別建立的資源，因此可防止意外錯誤，例如刪除與 Neutron 路由器相關聯的邏輯路由器。請參閱《NSX-T for Data Center 管理指南》中的「檢視主體身分識別」以取得詳細資訊。

程序

1 若要啟用用戶端憑證驗證，請在 `nsx.ini` 檔案中定義下列項目：

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

2 執行下列命令重新啟動 Neutron，以提取 `nsx.ini` 檔案中的變更：`service neutron-server restart`。

透過執行下列命令，確認 Neutron 伺服器正在使用 `neutron.conf` 和 `nsx.ini` 檔案：

- `ps -aux |grep neutron`

確認 `nsx.ini` 和 `neutron.conf` 存在輸出中。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
```

啟用 DHCP 和中繼資料 Proxy 服務

使用 NSX-T Data Center 外掛程式時，OpenStack 參考 DHCP 實作會由 NSX-T Data Center 原生 DHCP 伺服器取代。NSX-T Data Center 平台也提供用於存取 Nova 中繼資料的 Proxy 伺服器。

無論在上一步驟中設定的 NSX-T 外掛程式為何，都必須執行這些作業。

■ 在 NSX Manager 中建立 DHCP 設定檔

DHCP 伺服器設定檔會指定 NSX Edge 叢集或 NSX Edge 叢集的成員。具有此設定檔的 DHCP 伺服器會為來自邏輯交換器上虛擬機器的 DHCP 要求提供服務，而該交換器會連線至設定檔中所指定的 NSX Edge 節點。

■ 建立中繼資料 Proxy

中繼資料 Proxy 伺服器讓虛擬機器執行個體能夠從 OpenStack Nova API 伺服器，擷取執行個體特定的中繼資料。

■ 編輯 `nsx.ini` 檔案

必須在使用這些設定檔的 `nsx.ini` 中指定新變數 `native_dhcp_metadata`、`metadata_proxy` 和 `dhcp_profile`。

在 NSX Manager 中建立 DHCP 設定檔

DHCP 伺服器設定檔會指定 NSX Edge 叢集或 NSX Edge 叢集的成員。具有此設定檔的 DHCP 伺服器會為來自邏輯交換器上虛擬機器的 DHCP 要求提供服務，而該交換器會連線至設定檔中所指定的 NSX Edge 節點。

必要條件

若要啟用 NSX-T Data Center 的原生 DHCP 伺服器，必須在 NSX-T Data Center 中建立 DHCP 設定檔，並將其傳遞至 `nsx.ini` 中的 Neutron 外掛程式組態。確定 Neutron DHCP 服務 (DevStack 中的 `q-dhcp`) 和中繼資料代理程式 (DevStack 中的 `q-meta`) 不在執行中。在 `neutron.conf` 檔案中，設定為 `False`。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://nsx-manager-ip-address`。
- 2 選取導覽面板中的**進階網路與安全性 > DHCP**。
- 3 選取**伺服器設定檔**，然後按一下**新增**。
- 4 輸入名稱和 (選用) 說明。
- 5 從下拉式功能表中選取 **Edge 叢集**。
- 6 按一下**新增**。

建立中繼資料 Proxy

中繼資料 Proxy 伺服器讓虛擬機器執行個體能夠從 OpenStack Nova API 伺服器，擷取執行個體特定的中繼資料。

NSX 平台提供用於存取 Nova 中繼資料的 Proxy 伺服器。Proxy 將擷取在 169.254.269.254 位址進行的所有要求，並將其轉送到在 NSX-T 中繼資料 Proxy 組態中指定的 Nova 中繼資料伺服器端點

必要條件

用於中繼資料 Proxy 的 Edge 節點必須從其管理 IP 位址具有中繼資料伺服器的 IP 連線。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://nsx-manager-ip-address`。
- 2 選取導覽面板中的**進階網路 > DHCP**。
- 3 選取**中繼資料 Proxy**，然後按一下**新增**。
- 4 輸入**名稱**和選用的說明。
- 5 輸入 `http://<openstack_controller>:8775` 做為 **Nova 伺服器 URL**。如果中繼資料 Proxy 伺服器正在接聽預設 8775 以外的連接埠，請將 URL 更新為正確的連接埠。您可以在控制器節點上的 Nova API 組態檔案 `/etc/nova.conf` 中找到連接埠，請查詢 `metadata_listen_port` 參數。如果需要變更組態，請將 `n-api` 或 Nova 伺服器重新啟動。
- 6 輸入**密碼**參數。

7 從下拉式功能表中選取 **Edge 叢集**。

8 按一下**新增**。

編輯 nsx.ini 檔案

必須在使用這些設定檔的 nsx.ini 中指定新變數 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

適用於 OpenStack 的 NSX-T Data Center 外掛程式的範例組態檔案

組態檔案通常位於 /etc/neutron/plugins/vmware/nsx.ini。

以下是範例組態檔案：

```
[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 控制器組態

本節中所述的組態對 Nova 控制器節點組態進行補充，並提供有關 NSX-T Data Center 的資訊。

以下是 Nova 控制器範例組態檔案，通常位於控制節點的 `/etc/nova/nova.conf` 上。

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

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

OpenStack Nova 運算組態檔案

若要編輯 Nova 組態檔案，請使用 NSX-T。

本節中所述的組態對 Nova 運算節點組態進行補充，並提供有關 NSX-T Data Center 的資訊。

以下是 Nova 運算範例組態檔案，通常位於運算節點的 `/etc/nova/nova.conf` 上。

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

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

使用適用於 OpenStack 的 NSX-T Data Center 外掛程式設定 Neutron 進階服務

5

OpenStack Neutron 的負載平衡器即服務 (LBaaS)、防火牆即服務 (FWaaS) 和 IPSec VPN 即服務 (VPNaaS) 也稱為 Neutron 進階服務。

從 NSX-T Data Center 2.5 NSX-T 外掛程式 (原則和 Manager 兩者) 開始支援 Octavia 負載平衡服務，該服務會取代已淘汰的 Neutron LBaaS 服務。

下列資訊假設您有 NSX-T Data Center 2.4 以及 OpenStack Stein 14.0。

系統需求中列出目前支援的版本。

若要啟用 Neutron 進階服務 NSX-T Data Center，應在 Neutron 組態中指定下列項目：

- 啟用特定服務的服務外掛程式
- 設定服務的服務提供者
- 提供 NSX-T Data Center 驅動程式 (如果適用)，以及 NSX-T Data Center 的特定組態項目

這些選項是在 Neutron 組態檔案中指定，通常可在 `/etc/neutron` 中找到 (附註：外掛程式特定的組態檔案通常可在 `/etc/neutron/plugins/vmware` 中找到)。Neutron 可在命令列中接受一或多個組態檔案。剖析組態時會合併這些檔案，以便組態檔案結構可以反映特定使用者的喜好設定。通常會採用下列結構：

- `neutron.conf` - 核心 Neutron 選項、基本組態參數 (例如：API Manager 端點、傳輸區域識別碼)、服務外掛程式清單。
- `neutron_lbass.conf` - 負載平衡服務提供者和選項。
- `Octavia.conf` - 負載平衡提供者和 MQ 主題。僅支援 Octavia 負載平衡器服務。此檔案通常位於 `/etc/Octavia/Octavia.conf`，並由 Octavia 服務載入。
- `neutron_fwass.conf` - 防火牆服務提供者、驅動程式和驅動程式選項。
- `neutron_vpnaas.conf` - VPN 服務提供者和其他選項。

服務提供者是使用 `service_provider` 選項指定。此選項可在 Neutron 組態中對不同類型的服務重複多次，但指定服務類型不能有一個以上的預設服務提供者。

Service_provider 組態屬性結構：<SERVICE_TYPE>:<PROVIDER_CLASS>:[<DEFAULT>]。

- 設定 OpenStack Octavia 負載平衡器即服務 (LBaaS)

這些指示用於設定 NSX-T Data Center 負載平衡器搭配 Octavia 的 OpenStack 耗用量。

- 設定 OpenStack Neutron 的負載平衡器即服務 (LBaaS)

- 設定 OpenStack Neutron 的防火牆即服務 (FWaaS)

這些指示適用於設定 FWaaS v2。

- 設定 OpenStack Neutron 的 IPsec VPN 即服務 (VPNaaS)

此服務可讓 OpenStack 使用者使 Neutron 網路可供透過安全的 VPN 通道的遠端站台存取。

- Neutron 進階服務的範例組態檔案

設定 OpenStack Octavia 負載平衡器即服務 (LBaaS)

這些指示用於設定 NSX-T Data Center 負載平衡器搭配 Octavia 的 OpenStack 耗用量。

相同指示同時適用 NSX-T 原則和 NSX-T Manager 外掛程式。

如需有關 Octavia 負載平衡器服務的一般資訊，請參閱官方說明文件。

程序

- 1 在 `/etc/neutron/neutron.conf` 中，請確定未設定用於 NSX-T Data Center 的負載平衡服務外掛程式，例如，`service_plugins` 清單中不應存在 `vmware_nsx_lbaasv2`。如果有對 `neutron.conf` 檔案進行任何變更，請重新啟動 Neutron 服務
- 2 在 `/etc/octavia/octavia.conf` 中，指定下列項目：
 - a 在 `[api_settings]` 組態設定中，指定 NSX-T 提供者：`default_provider_driver = vmwareedge`
`enabled_provider_drivers = vmwareedge:NSX`
 - b 在 `[oslo_messaging]` 區段中，指定用於 Octavia 和 NSX-T 驅動程式之間的通訊主題，這會在 Neutron 程序空間中執行。
- 3 重新啟動 Octavia API 服務。

設定 OpenStack Neutron 的負載平衡器即服務 (LBaaS)

這些指示用於設定 NSX-T Data Center 負載平衡器搭配 LBaaS v2 的 OpenStack 耗用量。相同指示同時適用 NSX-T 原則和 NSX-T Manager 外掛程式。

程序

- 1 在預設的組態區段中，編輯 `/etc/neutron/neutron.conf`，以新增 NSX-T Data Center 的負載平衡服務外掛程式：`service_plugins = vmware_nsx_lbaasv2,[...]`

請注意，`service_plugins` 為清單選項。可透過以逗點分隔其完整類別名稱或捷徑的方式來指定多個服務外掛程式。

2 使用下列方式編輯 `/etc/neutron/neutron-lbaas.conf` 檔案：

- a 透過在 `service_providers` 組態區段中設定 `service_provider` 選項，設定 NSX-T Data Center 的負載平衡器服務驅動程式：`service_plugins = LOADBALANCERV2:VMwareEdge:neutron_lbaas.drivers.vmware.edge_driver_v2.EdgeLoadBalancerDriverV2:default`。
- b 設定 Keystone 驗證參數 (若尚未設定)。`neutron-lbaas` 服務會使用這些參數，且與 NSX-T Data Center 整合無關。請注意，應提供 Keystone 端點的位置。

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

3 確定已將檔案 `/etc/neutron/neutron-lbaas.conf` 新增至 Neutron 伺服器命令列。這可透過執行命令 `ps -aux | grep neutron` 並確認輸出中是否存在 `/etc/neutron/neutron-lbaas.conf` 來驗證。

如果未包含該檔案，則應編輯 Neutron 服務啟動器。服務啟動器的位置和結構取決於所使用的特定 OpenStack 發行版。

4 重新啟動 Neutron 服務。確切的服務名稱取決於所使用的 OpenStack 發行版。

設定 OpenStack Neutron 的防火牆即服務 (FWaaS)

這些指示適用於設定 FWaaS v2。

程序

1 在預設的組態區段中，編輯 `/etc/neutron/neutron.conf`，以將防火牆新增為 NSX-T Data Center 的服務外掛程式：`service_plugins = firewall_v2`

`Service_plugins` 為清單選項。可透過以逗點分隔其完整類別名稱或捷徑的方式來指定多個服務外掛程式。

2 使用下列方式編輯 `/etc/neutron/neutron-fwaas.conf` 檔案：

- a 透過在 `service_providers` 組態區段中設定 `service_provider` 選項，將防火牆設定為 NSX-T Data Center 的服務驅動程式。`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
```

此選項的值具有特定結構：`<service_type>:<service_name>:<driver_class>:`

`[<default>]`。`service_provider` 是「多字串」選項。每次指定該選項時，都會將選項的值新增至清單。可透過為每個服務提供者設定 `service_provider` 選項來指定多個服務提供者。

- b 透過在 FWaaS 組態區段中設定 `enabled = True`，將防火牆即服務切換為開啟。
 - c 在 FWaaS 組態區段中設定 `driver = vmware_nsxp_edge_v2`，設定 NSX-T Data Center 的 FWaaS 裝置驅動程式。
 - d 透過在 FWaaS 組態區段中設定 `driver = vmware_nsxv3_edge_v2`，設定 NSX Manager 外掛程式的 FWaaS 裝置驅動程式。
- 3 檢查已將檔案 `/etc/neutron/neutron-fwaas.conf` 新增至 Neutron 伺服器命令列。這可透過執行 `ps -aux | grep neutron` 並確認輸出中是否存在 `/etc/neutron/neutron-fwaas.conf` 來驗證。如果未包含該檔案，則應編輯 Neutron 服務啟動器。服務啟動器的位置和結構取決於所使用的特定 OpenStack 發行版。

- 4 重新啟動 Neutron 服務。特定的服務名稱取決於所使用的 OpenStack 發行版。

設定 OpenStack Neutron 的 IPsec VPN 即服務 (VPNaaS)

此服務可讓 OpenStack 使用者使 Neutron 網路可供透過安全的 VPN 通道的遠端站台存取。

VPNaaS 驅動程式無法用於 NSX-T 原則外掛程式。下列指示僅適用 NSX-T Manager 外掛程式。

程序

- 1 在預設的組態區段中，編輯 `/etc/neutron/neutron.conf`，以將 IPsec VPN 新增為 NSX-T Data Center 的服務外掛程式：`service_plugins = vmware_nsx_vpnaas, [...]`

`service_plugins` 為清單選項。可透過以逗點分隔其完整類別名稱或捷徑的方式來指定多個服務外掛程式。

- 2 以下列方式編輯 `/etc/neutron/neutron-vpnaas.conf` 檔案：設定 NSX-T Data Center 的載入 VPNservice 驅動程式，方法是在 `service_providers` 組態區段中設定 `service_provider` 選項。
`service_provider =`
`VPN:vmware:vmware_nsx.services.vpnaas.nsxv3.ipsec_driver.NSXv3IPsecVpnDriver:default`

此選項的值具有特定結構：`<service_type>:<service_name>:<driver_class>:[<default>]`。
`service_provider` 是「多字串」選項。每次指定該選項時，都會將選項的值新增至清單。可透過為每個服務提供者設定 `service_provider` 選項來指定多個服務提供者。

- 3 確定已將檔案 `/etc/neutron/neutron-vpnaas.conf` 新增至 Neutron 伺服器命令列。這可透過執行 `ps -aux | grep neutron` 並確認輸出中是否存在 `/etc/neutron/neutron-vpnaas.conf` 來驗證。
 如果未包含該檔案，則應編輯 Neutron 服務啟動器。服務啟動器的位置和結構取決於所使用的特定 OpenStack 發行版。
- 4 重新啟動 Neutron 服務。特定的服務名稱取決於所使用的 OpenStack 發行版。

Neutron 進階服務的範例組態檔案

```
[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_authtoken]
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
```

附錄：適用於 OpenStack 的 NSX-T Data Center 外掛程式組態內容

6

表 6-1. 組態內容

區段	變數	說明
nsx_p	nsx_api_managers	一或多個 NSX Manager 的 IP 位址 (以逗點分隔)。IP 位址應採用下列格式：[<scheme>://<ip_address>[:<port>]。如果未提供配置，則會使用 https。如果未提供連接埠，則會對 http 使用連接埠 80，並對 https 使用連接埠 443。
	nsx_use_client_auth	布林值。設為 True 以啟用用戶端憑證驗證
	nsx_client_cert_file	包含用戶端憑證和私密金鑰之檔案的路徑 (採用 PEM 格式)。
	nsx_client_cert_pk_password	(選用) 用於加密私密金鑰的密碼。
	nsx_api_user	用於存取 NSX Manager API 的使用者名稱。
	nsx_api_password	用於存取 NSX Manager API 的密碼。
	dns_domain	用於建立主機名稱的網域。
	default_overlay_tz	default_edge_cluster
	default_vlan_tz	(選用) 僅在建立 VLAN 或一般提供者網路時需要。用於橋接 Neutron 網路之間的預設 NSX VLAN 傳輸區域的 UUID 或名稱 (如果未指定任何實體網路)。
	edge_cluster	(選用) 為要連線的第 1 層路由器指定 Edge 叢集 (不同於所連線的 Edge 叢集)。
	retries	(選用) 失效修訂版本錯誤時要重試 API 要求的次數上限。
	ca_file	(選用) 指定用於驗證 NSX Manager 伺服器憑證的 CA 服務包檔案。如果「insecure」設為 True，則會忽略此選項。如果「insecure」設為 False 且 ca_file 未設定，則會使用系統根 CA 來驗證伺服器憑證。
	insecure	(選用) 如果為 true，則不會驗證 NSX Manager 伺服器憑證。如果為 false，則會使用透過「ca_file」指定的 CA 服務包，或如果未設定，則將使用的預設系統根 CA。

表 6-1. 組態內容 (續)

區段	變數	說明
	http_timeout	(選用) 中止對 NSX Manager 的 HTTP 連線之前的時間 (以秒為單位)。
	http_read_timeout	(選用) 中止來自 NSX Manager 的 HTTP 讀取回應之前的時間 (以秒為單位)。
	http_retries	(選用) 重試 HTTP 連線的次數上限。
	concurrent_connections	(選用) 對每個 NSX Manager 的連線數目上限。
	conn_idle_timeout	(選用) 在未使用 Manager 連線的情況中，確保與 NSX Manager 的連線需等待的時間 (以秒為單位)。
	default_tier0_router	(選用) 用於連線至第 1 層邏輯路由器及設定外部網路的預設第 0 層路由器的 UUID 或名稱。
	metadata_on_demand	(選用) 如果為 True，則僅當路由器連結至已停用 DHCP 的子網路時，才會為路由器建立內部中繼資料網路。
	dhcp_profile	(選用) 用於啟用原生 DHCP 服務的 NSX DHCP 設定檔的 UUID。必須先在 NSX 中建立，然後才能使用 NSX 外掛程式啟動 Neutron。
	locking_coordinator_url	(選用) 用於鎖定管理員的分散式鎖定協調資源 URL。此值會做為參數傳遞至 tooz 協調器。依預設，此值為「無」，且 oslo_concurrency 會用於單一節點鎖定管理。
	realization_max_attempts	(選用) 等待資源實現時，允許的重試嘗試次數上限。預設值：50
	realization_wait_sec	(選用) 實現資源的嘗試之間的秒數。預設值：1 秒