


OpenStack网络

« (intro-nat.html)

» (fwaas.html)

 (https://bugs.launchpad.net/neutron/+filebug?field.title=OpenStack%20Networking%20in%20Neutron&field.comment=%0A%0A%0AThis bug tracker is for errors with the documentation, use the following as a template and remove or add fields as you see fit. Convert [] into [x] to check boxes.%0A%0A- [] This doc is inaccurate in this way: ____%0A- [] This is a doc addition request.%0A- [] I have a fix to the document that I can paste below including example: input and output. %0A%0AIf you have a troubleshooting or support issue, use the following resources.%0A%0A - Ask OpenStack: http://ask.openstack.org%0A - The mailing list: http://lists.openstack.org%0A - IRC: 'openstack' channel on Freenode%0A%0A-----%0ARelease:%2012.0.1.dev11%20on%202018-03-07%2021:05%0ASHA:%2043df2709acbdce86686a40b75fd34e96880427d0%0ASource:%20https://git.openstack.org/cgit/openstack/neutron/tree/doc/source/admin/intro-os-networking.rst%0AURL: https://docs.openstack.org/neutron/queens/admin/intro-os-networking.html&field.tags=doc)

更新日期：2018-03-07 21:05

OpenStack Networking允许您创建和管理其他OpenStack服务可以使用的网络对象，如网络，子网和端口。可以实现插件以适应不同的网络设备和软件，为OpenStack架构和部署提供灵活性。

网络服务，代号为neutron，提供了一个API，可让您定义云中的网络连接和寻址。网络服务使运营商能够利用不同的网络技术为其云网络提供支持。网络服务还提供一个API，用于配置和管理从L3转发和网络地址转换（NAT）到负载均衡，外围防火墙和虚拟专用网络等各种网络服务。

它包含以下组件：

API服务器

OpenStack Networking API包括对第2层网络和IP地址管理（IPAM）的支持，以及第3层路由器结构的扩展，使第2层网络和网关能够在外部网络之间进行路由。OpenStack Networking包含越来越多的插件，可以与包括路由器，交换机，虚拟交换机和软件定义网络（SDN）控制器在内的各种商用和开源网络技术实现互操作。

OpenStack Networking插件和代理

插拔端口，创建网络或子网，并提供IP地址。所选择的插件和代理根据特定云中使用的供应商和技术而有所不同。重要的是要提到一次只能使用一个插件。

消息队列

接受和路由由代理之间的RPC请求以完成API操作。在用于Open vSwitch和Linux网桥的ML2机制驱动程序中，消息队列用于在每个管理程序上运行的neutron服务器和neutron代理之间的RPC的ML2插件。

概念

要配置丰富的网络拓扑，您可以创建和配置网络和子网，并指示其他OpenStack服务（如计算）将虚拟设备连接到这些网络上的端口。OpenStack Compute是OpenStack Networking的主要消费者，为其实例提供连接。特别是，OpenStack Networking支持具有多个专用网络的每个项目，并使项目能够选择自己的IP寻址方案，即使这些IP地址与其他项目使用的IP地址重叠。有两种类型的网络，项目和提供商网络。作为网络创建过程的一部分，可以在项目之间共享任何这些类型的网络。

提供商网络

提供商网络为实例提供二层连接，并提供对DHCP和元数据服务的可选支持。这些网络连接或映射到数据中心内现有的第2层网络，通常使用VLAN（802.1q）标记来识别和分离它们。

提供商网络通常以牺牲灵活性为代价提供简单性，性能和可靠性。默认情况下，只有管理员可以创建或更新提供者网络，因为他们需要配置物理网络基础结构 可以使用以下参数更改允许创建或更新提供者网络的用户 `policy.json`：

- `create_network:provider:physical_network`
- `update_network:provider:physical_network`

▲ 警告

提供商网络的创建和修改可以使用物理网络资源，例如VLAN-s。只为受信任的项目启用这些更改。

此外，提供商网络仅处理实例的第2层连接，因此缺乏对路由器和浮动IP地址等功能的支持。

在许多情况下，已经熟悉依赖物理网络基础架构进行二层，三层或其他服务的虚拟网络体系结构的运营商可以无缝地部署OpenStack网络服务。特别是，提供商网络吸引希望从Compute网络服务（nova-network）迁移到OpenStack网络服务的运营商。随着时间的推移，运营商可以建立在这个最小的架构上，以实现更多的云网络功能

一般而言，处理第3层操作的OpenStack Networking软件组件最能影响性能和可靠性。为了提高性能和可靠性，供应商网络将第3层操作转移到物理网络基础设施。

在一个特定的使用案例中，OpenStack部署驻留在一个混合环境中，使用传统的虚拟化和裸机主机，使用大量的物理网络基础设施。在OpenStack部署中运行的应用程序可能需要对部署以外的应用程序直接进行第2层访问（通常使用VLAN）。

路由的提供商网络

路由的提供商网络为实例提供三层连接。这些网络映射到数据中心中现有的第3层网络。更具体地说，网络映射到多个第2层段，其中每一个实质上都是提供商网络。每个都有一个连接到它的路由器网关，用于在它们之间和外部路由流量。网络服务不提供路由。

路由提供商网络提供的性能难以通过简单的提供商网络实现，但牺牲了保证的第2层连接。

有关更多信息，请参阅路由提供商网络 ([config-routed-networks.html#config-routed-provider-networks](#))。

自助服务网络

自助服务网络主要使普通（非特权）项目能够在不涉及管理员的情况下管理网络。这些网络完全是虚拟的，需要虚拟路由器与供应商和外部网络（如互联网）进行交互。自助服务网络通常还为实例提供DHCP和元数据服务。

在大多数情况下，自助服务网络使用覆盖协议，如VXLAN或GRE，因为它们可以支持比使用VLAN标记（802.1q）的第2层分段更多的网络。而且，VLAN通常需要额外配置物理网络基础设施。

IPv4自助服务网络通常使用私有IP地址范围（RFC1918），并通过虚拟路由器上的源NAT与提供商网络进行交互。浮动IP地址允许通过虚拟路由器上的目的地NAT从提供商网络访问实例。IPv6自助服务网络始终使用公共IP地址范围，并通过具有静态路由的虚拟路由器与提供商网络进行交互。

网络服务使用通常驻留在至少一个网络节点上的第3层代理实现路由器。与在第2层将实例连接到物理网络基础设施的提供商网络相反，自助服务网络必须遍历第3层代理。因此，三层代理或网络节点的超额预订或故障可能会影响大量的自助服务网络和使用它们的实例。考虑实施一个或多个高可用性功能以增加自助服务网络的冗余性和性能。

用户创建项目网络以实现项目内的连接。默认情况下，它们完全隔离，不与其他项目共享。OpenStack Networking支持以下类型的网络隔离和覆盖技术。

平面

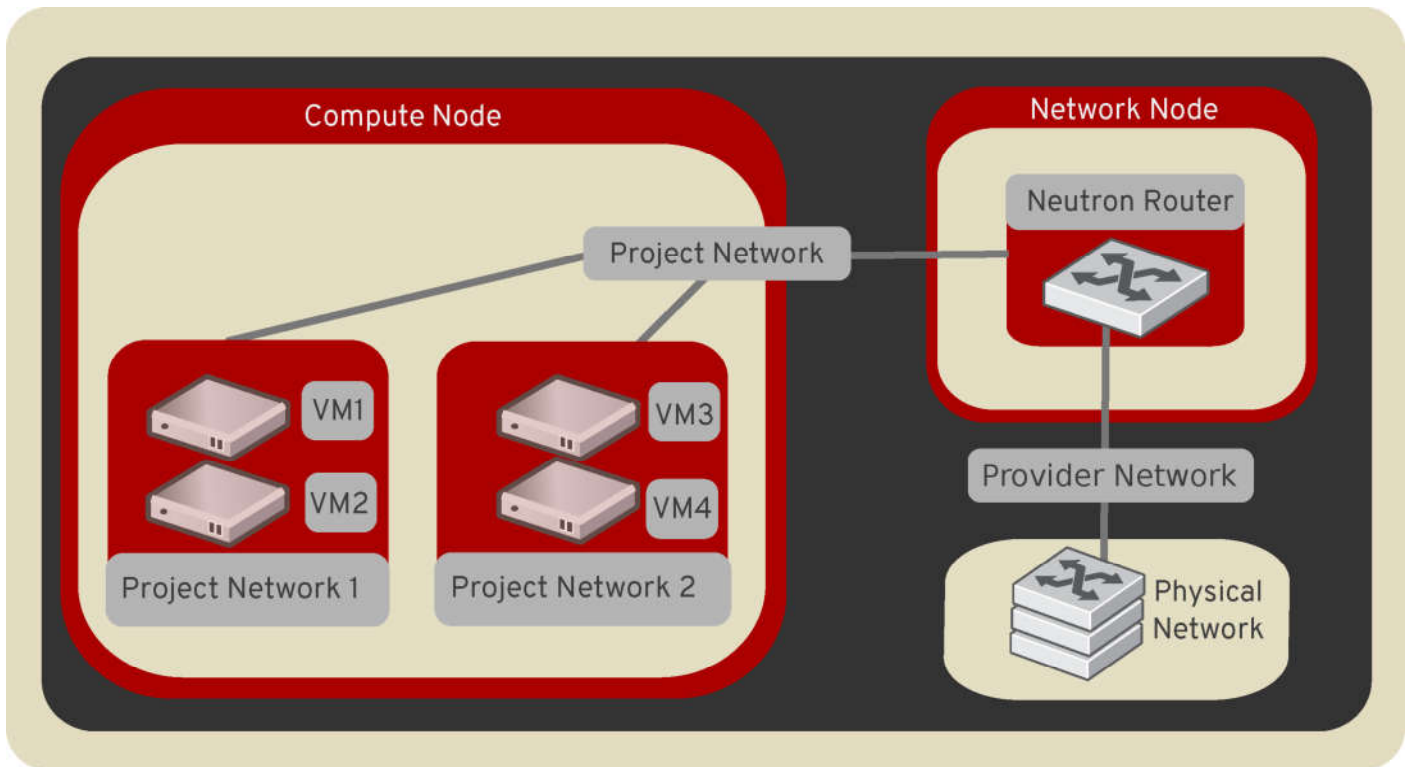
所有实例驻留在同一个网络上，也可以与主机共享。没有VLAN标记或其他网络隔离发生。

VLAN

网络允许用户使用与物理网络中存在的VLAN相对应的VLAN ID（802.1Q标记）来创建多个提供商或项目网络。这允许实例在整个环境中彼此通信。它们还可以与专用服务器，防火墙，负载均衡器和其他网络基础架构在同一个第2层VLAN上进行通信。

GRE和VXLAN

VXLAN和GRE是封装协议，它们创建覆盖网络来激活和控制计算实例之间的通信。网络路由器需要允许流量流出GRE或VXLAN项目网络。还需要路由器才能将直接连接的项目网络与包括Internet在内的外部网络相连接。路由器提供了使用浮动IP地址直接从外部网络连接到实例的功能。



(../images/NetworkTypes.png)

子网¹

一个IP地址块和相关的配置状态。这也被称为网络服务为项目和提供商网络提供的本地IPAM（IP地址管理）。当在网上创建新端口时，子网用于分配IP地址。

子网池¹

最终用户通常可以使用任何有效的IP地址创建子网，而不受其他限制。但是，在某些情况下，管理员或项目预先定义一个地址池以创建具有自动分配的子网是很好的选择。

使用子网池通过要求每个子网都在定义的池内限制可以使用的地址。它还防止地址重用或来自同一个池中的两个子网重叠。

有关更多信息，请参阅子网池 (config-subnet-pools.html#config-subnet-pools)。

端口¹

端口是用于将单个设备（如虚拟服务器的NIC）连接到虚拟网络的连接点。该端口还描述了相关的网络配置，例如要在该端口上使用的MAC和IP地址。

路由器¹

路由器在自助服务和提供商网络之间或属于项目的自助服务网络之间提供虚拟的第3层服务，如路由和NAT。网络服务使用第3层代理通过命名空间管理路由器。

安全组¹

安全组为虚拟防火墙规则提供了一个容器，用于控制端口级别的入口（进站到实例）和出站（从实例出站）网络流量。安全组使用默认的拒绝策略，并且只包含允许特定流量的规则。每个端口都可以以附加方式引用一个或多个安全组。防火墙驱动程序将安全组规则转换为基于数据包过滤技术的配置，例如iptables。

每个项目都包含一个default安全组，允许所有出口流量并拒绝所有入口流量。您可以更改default安全组中的规则。如果您在未指定安全组的情况下启动实例，则default安全组会自动应用它。同样，如果您创建的端口未指定安全组，则default安全组会自动应用到该端口。

注意

如果使用元数据服务，则删除默认出站规则会拒绝访问169.254.169.254上的TCP端口80，从而阻止实例检索元数据。

安全组规则是有状态的。因此，允许用于安全外壳的入口TCP端口22自动创建允许返回出口流量和涉及那些TCP连接的ICMP错误消息的规则。

默认情况下，所有安全组都包含一系列执行以下操作的基本（完整性）和反欺骗规则：

- 只有在出口流量使用该端口的源MAC和IP地址，源MAC和IP组合**allowed-address-pairs**，或有效MAC地址（端口或 **allowed-address-pairs**）以及相关EUI64链路本地IPv6地址时，才允许出口流量。
- 允许使用实例的端口的源MAC地址和未指定的IPv4地址（0.0.0.0）的出口DHCP发现和请求消息。
- 允许从子网上的DHCP服务器进入DHCP和DHCPv6响应，以便实例可以获取IP地址。
- 拒绝出口DHCP和DHCPv6响应，以防止实例充当DHCP（v6）服务器。
- 允许入口/出口ICMPv6 MLD，邻居请求和邻居发现消息，以便实例可以发现邻居并加入组播组。
- 拒绝出口ICMPv6路由器通告以防止实例充当IPv6路由器并转发其他实例的IPv6通信。
- 允许使用特定实例的源MAC地址和未指定的IPv6地址（:）的出口ICMPv6 MLD报告（v1和v2）和邻居请求消息。重复地址检测（DAD）依赖于这些消息。
- 允许来自实例端口的MAC地址的出口非IP流量和实例端口上的任何其他MAC地址**allowed-address-pairs**。

虽然非IP流量，但安全组不会隐式地允许所有ARP流量。单独的ARP过滤规则可防止实例使用ARP拦截另一个实例的流量。您不能禁用或删除这些规则。

您可以通过设置端口属性禁用安全组包括基本和反欺骗的规则**port_security_enabled**来**False**。

扩展¹

OpenStack网络服务是可扩展的。扩展有两个目的：它们允许在API中引入新功能，而不需要更改版本，并允许引入供应商特定的利基功能。应用程序可以通过在**/extensions**URI上执行GET以编程方式列出可用的扩展。请注意，这是一个版本化的请求；也就是说，在一个API版本中可用的扩展可能在另一个版本中不可用。

DHCP ¹

可选的DHCP服务管理提供商和自助服务网络上的实例的IP地址。网络服务使用管理**qdhcp**命名空间和 **dnsmasq**服务的代理来实现DHCP 服务。

元数据¹

可选的元数据服务为实例提供API以获取元数据（如SSH密钥）的API。

服务和组件层次结构¹

服务器¹

- 提供API，管理数据库等。

插件¹

- 管理代理商

代理¹

- 为实例提供第2/3层连接
- 处理物理 - 虚拟网络转换
- 处理元数据等

第2层（以太网和交换）¹

- Linux桥
- OVS

第3层（IP和路由）¹

- L3
- DHCP

杂项¹

- 元数据

服务¹

路由服务¹

VPNaaS ¹

虚拟专用网络即服务（VPNaaS）是引入VPN功能集的中子扩展。


LBaaS ¹

负载均衡器即服务（LBaaS）API提供并配置负载均衡器。参考实现基于HAProxy软件负载均衡器。


FWaaS ¹


防火墙即服务（FWaaS）API是一种实验性API，可使早期采用者和供应商测试其网络实施。

« (intro-nat.html) » (fwaas.html) 🐞 (https://bugs.launchpad.net/neutron/+filebug?field.title=OpenStack%20Networking%20in%20Neutron&field.comment=%0A%0A%0AThis bug tracker is for errors with the documentation, use the following as a template and remove or add fields as you see fit. Convert [] into [x] to check boxes:%0A%0A- [] This doc is inaccurate in this way: ____%0A- [] This is a doc addition request.%0A- [] I have a fix to the document that I can paste below including example: input and output. %0A%0AIf you have a troubleshooting or support issue, use the following resources:%0A%0A - Ask OpenStack: http://ask.openstack.org%0A - The mailing list: http://lists.openstack.org%0A - IRC: 'openstack' channel on Freenode%0A%0A-----%0ARelease:%2012.0.1.dev11%20on%202018-03-07%2021:05%0ASHA:%2043df2709acbdce86686a40b75fd34e96880427d0%0ASource:%20https://git.openstack.org/cgit/openstack/neutron/tree/doc/source/admin/intro-os-networking.rst%0AURL: https://docs.openstack.org/neutron/queens/admin/intro-os-networking.html&field.tags=doc)



<https://creativecommons.org/licenses/by/3.0/>
除另有说明外，本文档受 [Creative Commons Attribution 3.0](https://creativecommons.org/licenses/by/3.0/) 许可的授权 (<https://creativecommons.org/licenses/by/3.0/>)。查看所有 [OpenStack](http://www.openstack.org/legal) 法律文件 (<http://www.openstack.org/legal>)。

 发现错误？报告错误 (<https://bugs.launchpad.net/neutron/+filebug?field.title=OpenStack%20networking%20in%20neutron&field.comment=%0A%0A%0Athis%20bug%20tracker%20is%20for%20errors%20with%20the%20documentation%2C%20use%20the%20following%20as%20a%20template%20and%20remove%20or%20add%20fields%20as%20you%20see%20fit%20convert%20%5B%5D%20into%20%5BX%5D%20to%20check%20boxes%3A%0A%0A-%5B%5D%20this%20doc%20is%20inaccurate%20in%20this%20way%3A%0A-%5B%5D%20this%20is%20a%20doc%20addition%20request.%0A-%5B%5D%20i%20have%20a%20fix%20to%20the%20document%20that%20i%20can%20paste%20below%20including%20example%3A%0A%0Ainput%20and%20output.%0A%0Aif%20you%20have%20a%20troubleshooting%20or%20support%20issue%2C%20use%20the%20following%20resources%3A%0A%0A-%20ask%20openstack%3A%20http%3A%2F%2Fask.openstack.org%0A-%20the%20mailing%20list%3A%20http%3A%2F%2Flists.openstack.org%0A-%20irc%3A%20%27openstack%27%20channel%20on%20freenode%0A%0A-----%0ARELEASE%3A%2012.0.1.dev11%20ON%202018-03-07%2021:05%0ASHA%3A2043df2709acbdce86686a40b75fd34e96880427d0%0ASOURCE%3A%20https%3A%2F%2Fgit.openstack.org%2Fcg%2Fopenstack%2Fneutron%2Ftree%2Fdoc%2Fsource%2Fadmin%2Fintro-os-networking.rst%0AURL%3Ahttps%3A%2F%2Fdocs.openstack.org%2Fneutron%2Fqueens%2Fadmin%2Fintro-os-networking.html&field.tags=DOC>)

 问题吗？ (<http://ask.openstack.org>)



OpenStack文档 ▾

Neutron 12.0.1

(../index.html)

安装指南 (../install/index.html)

OpenStack网络指南 (index.html)

- 介绍 (intro.html)
- 组态 (config.html)
- 部署示例 (deploy.html)
- 操作 (ops.html)
- 移民 (migration.html)
- 杂 (misc.html)
- 存档的内容 (archives/index.html)

中子配置选项 (../configuration/index.html)

命令行界面参考 (../cli/index.html)

中子特征分类 (../feature_classification/index.html)

贡献者指南 (../contributor/index.html)

页面内容

概念

- 提供商网络
- 路由的提供商网络
- 自助服务网络
- 子网
- 子网池
- 端口
- 路由器
- 安全组
- 扩展
- DHCP
- 元数据

服务和组件层次结构

- 服务器
- 插件
- 代理
 - 第2层（以太网和交换）
 - 第3层（IP和路由）
 - 杂
- 服务
 - 路由服务
 - VPNaaS
 - LBaaS
 - FWaaS