1. Neutron
2. Neutron介绍

传统的网络管理方式依赖于管理员手工配置和维护各种网络硬件设备，而云环境下的网络非常复杂，在多租户的场景下，用户可能随时需要创建，修改和删除网络，因此需要自动地对网络进行修改。软件定义网络（SDN）所具有的灵活性和自动化优势成为了云时代的网络管理的主流方式。Neutron的设计目标是“网络即服务“，在设计上遵循了基于SDN实现网络虚拟化的原则，充分利用了Linux系统上的各种网络相关技术。

1. Neutron功能

Neutron为整个Openstack环境提供了网络支持，包括二层交换，三层路由，负载均衡，防火墙和VPN等功能。

1. 二层交换Switching

Nova的Instance是通过虚拟交换机连接到虚拟的二层网络上的，Neutron支持多种虚拟交换机，包括Linux原生的Linux Bridge和Open vSwitch（OVS）。利用虚拟交换机，Neutron除了可以创建传统的VLAN网络外，还可以创建基于隧道技术的Overlay网络，如VxLan和GRE。

1. 三层路由Routing

Instance可以配置不同网段的IP，Neutron的router（虚拟路由器）实现Instance 跨网段通信。虚拟路由器会通过IP forwading，iptables等技术实现路由和NAT。

1. 负载均衡Load Balancing

Openstack在Grizzly版本引入了Load-Balancing-as-a-service(LBaaS)，提供将负载分发到多个Instance的能力。

1. 防火墙Firewalling

Neutron通过两种方式来保障instance和网络的安全性。

1. Security Group

通过iptables限制进出instance的网络包。

1. Firewall-as-a-Service

限制进出虚拟路由器的网络包，通过iptables实现。

1. Neutron网络的基本概念

Neutron管理的网络资源包括network, subnet和port：

1.network

network是一个隔离的二层广播域，Neutron支持多种类型的network，包括local, fla, VLAN, VxLAN和GRE。不同的network在二层上是隔离的，但是如果借助了路由器的haunt，则network可以在三层之上通信。

注意，network必须属于某个Project（Tenant租户），一个Project可以创建多个network。

（1）local

local网络与其他网络和节点隔离，local网络中的instance只能与位于同一节点上的同一网络的instance通信，local主要用于单机测试。

（2）flat

flat网络是无vlan tagging的网络，其中的instance能够与同一网路中的instance通信，并且可以跨越多个节点。

（3）vlan

vlan是一个二层的广播域，同一个vlan的instance可以通信，不同的vlan只能够通过router通信，vlan网络可以跨节点，是应用最广的网络类型。

（4）vxlan

vxlan是基于隧道技术的overlay网络。

（5）gre

gre也是overlay网络，使用的是IP包进行封装。

2.subnet

subnet是一个IPV4或IPV6地址段，即子网。instance的IP从subnet中分配，每个subnet需要定义IP地址的范围和掩码。一个subnet只能够属于某个network，一个network可以有多个subnet，这些subnet可以是不同的IP段，但是每个subnet的CIDR不能重叠。如下所示：

network A

subnet A-a : 10.10.1.0/24 {“start” : “10.10.1.1”, “end” : “10.10.1.50”}

subnet A-b : 10.10.1.0/24 {“start” : “10.10.1.51”, “end” : “10.10.1.100”}

虽然两个子网的IP地址没有重叠，但是它们的子网段都是10.10.1.0/24，因此是重叠的。

如果subnet在不同的network中，则CIDR和IP都是可以重叠的。那么这样不就会造成IP冲突了吗？

答案是不会的，因为Neutron的router是通过Linux network namespace实现的，network namespace是一种网络隔离机制，通过它，每个router有自己独立的路由表。因此，如果两个subnet是通过同一个router路由，根据router的配置，只有指定的一个subnet可以被路由；如果两个subnet是通过不同的router路由的，因为router的路由表是独立的，所以两个subnet都可以被路由。

3.port

port是虚拟交换机上的一个端口，定义了MAC地址和IP地址，当instance的虚拟网卡VIF（virtual Interface）绑定到port时，port会将MAC和IP分配给VIF。一个port必须属于某个subnet，一个subnet可以有多个port。

4.Project，Network，Subnet，Port和VIP的关系

