

从今天开始，我们将学习 OpenStack 的 Networking Service，Neutron。  
Neutron 的难度会比前面所有模块都大一些，内容也多一些。  
为了帮助大家更好的掌握 Neutorn，CloudMan 也会分析地更详细一些。

**Neutron 概述**

传统的网络管理方式很大程度上依赖于管理员手工配置和维护各种网络硬件设备；而云环境下的网络已经变得非常复杂，特别是在多租户场景里，用户随时都可能需要创建、修改和删除网络，网络的连通性和隔离已经不太可能通过手工配置来保证了。

如何快速响应业务的需求对网络管理提出了更高的要求。传统的网络管理方式已经很难胜任这项工作，而“软件定义网络（software-defined networking, SDN）”所具有的灵活性和自动化优势使其成为云时代网络管理的主流。

Neutron 的设计目标是实现“网络即服务（Networking as a Service）”。为了达到这一目标，在设计上遵循了基于 SDN 实现网络虚拟化的原则，在实现上充分利用了 Linux 系统上的各种网络相关的技术。

在这一章，我们将讨论 Neutron 的功能和它的各个组件，学习部署和配置 OpenStack 网络的不同方法，会涉及软件和硬件设备多个层面。

**Neutron 功能**

Neutron 为整个 OpenStack 环境提供网络支持，包括二层交换，三层路由，负载均衡，防火墙和 VPN 等。Neutron 提供了一个灵活的框架，通过配置，无论是开源还是商业软件都可以被用来实现这些功能。

**二层交换 Switching**

Nova 的 Instance 是通过虚拟交换机连接到虚拟二层网络的。

Neutron 支持多种虚拟交换机，包括 Linux 原生的 Linux Bridge 和 Open vSwitch。

Open vSwitch（OVS）是一个开源的虚拟交换机，它支持标准的管理接口和协议。

利用 Linux Bridge 和 OVS，Neutron 除了可以创建传统的 VLAN 网络，还可以创建基于隧道技术的 Overlay 网络，比如 VxLAN 和 GRE（Linux Bridge 目前只支持 VxLAN）。

在后面章节我们会学习如何使用和配置 Linux Bridge 和 Open vSwitch。

**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。router 通过 IP forwarding，iptables 等技术来实现路由和 NAT。

我们将在后面章节讨论如何在 Neutron 中配置 router 来实现 instance 之间，以及与外部网络的通信。

**负载均衡 Load Balancing**

Openstack 在 Grizzly 版本第一次引入了 Load-Balancing-as-a-Service（LBaaS），提供了将负载分发到多个 instance 的能力。LBaaS 支持多种负载均衡产品和方案，不同的实现以 Plugin 的形式集成到 Neutron，目前默认的 Plugin 是 HAProxy。

我们也将在后面章节学习 LBaaS 的使用和配置。

**防火墙 Firewalling**

Neutron 通过下面两种方式来保障 instance 和网络的安全性。

**Security Group**通过 iptables 限制进出 instance 的网络包。

**Firewall-as-a-Service**  
FWaaS，限制进出虚拟路由器的网络包，也是通过 iptables 实现。

我们将在后面章节详细讨论 Security 和 FWaaS。  
  
下一节我们会讨论 Neutron 网络涉及的一些基本概念，便于后面深入学习。