# Openstack知识点汇总

**唯一正确的参考信息来源：openstack.org**

**一些零散的知识点**

1. **云计算提供的服务模式们**：

**基础设施即服务（IaaS）**：将网络（network）、存储（storage）、服务器（server）、虚拟化（virtualization）基础设施作为服务提供给用户。代表产品openstack。

**平台即服务（PaaS）**：追加操作系统（os）、中间件（middleware

）、运行环境（runtime）构建一个平台，作为服务提供给用户。用户需要自行注入数据，构建高级app。代表产品docker。

**软件即服务（SaaS）**：继续追加用户数据（data）、应用（application）彻底将特定功能实现，作为服务提供给用户。用户只需要一个浏览器就可以得到想要的程序。代表产品如一起写、页游。

这几种服务模式给用户的体验是定制化逐个升高，易用性与便捷性也在升高；给我等运维人员的体验是，用户的傻逼指数不断升高。

1. **常用虚拟化方案：**

KVM（linux虚拟化模块，集成于系统内核）+qemu（仿真器，其实也是一种虚拟化软件）

1. **常见镜像格式：**

Raw：原始镜像格式，模拟了裸设备，I/O性能突出，但是拷贝的时候是硬性大小，即磁盘设定多大，copy文件即多大。缺点还有不支持快照（snapshot）。

Qcow2（QEMU copy-on-write format）：来自QEMU，是KVM下的常用镜像格式，I/O特性低于Raw 25%左右，支持N多快照。

VMDK：来自VMware。

Vdi：来自于Virtual Box。

参考文档：http://blog.csdn.net/zhongbeida\_xue/article/details/53256520

**各大核心组件的知识点**

**Openstack核心组件：**keystone（认证服务）、nova（计算服务）、glance（镜像管理服务）、neutron（网络服务）、cinder（块存储服务）、horizon（图形化界面）

1. **keystone：**

openstack系统身份认证模块，该模块规模不大，但是非常重要，负责了整个系统中用户身份认证与其他模块之间相互认证的任务。在操作系统层面调用了linux的pam模块。由于keystone本身没有实体服务，是依托于http启动的，所以在这一层面，调用了http下的mod\_wsgi模块。默认监听端口为5000与35357。

后端：keystone的后端是数据库（DB），数据库里会写入整个openstack系统内的用户（user）、项目（project）、角色（role）、终端（endpoint）以及相互认证用的令牌（token）。值得注意的是，在所有其他组件的安装过程中，所有的角色、用户、项目创建都是在向keystone的数据库中写入数据。故此，keystone的删库重建是最为繁琐的。

令牌：令牌分为两种，fernet与UUID。二者之间的区别如下：UUID tokens

UUID是第一个令牌类型支持，是当前的默认令牌服务。UUID令牌长度是32字节，必须坚持在后端。客户必须通过UUID令牌为身份验证服务。默认情况下，重点支持UUID令牌使用SQL后台。副作用是，无论令牌的到期时间如何，数据库的大小都会随着时间而增长。过期的UUID令牌可以使用基本的命令行实用程序后台修剪

Fernet tokens

区别于UUID tokens只能持久化存入数据库，Fernet tokens完全不需要持久化。

简而言之，UUID安全性更高，但是消耗系统的资源。Fernet反之。常用fernet即可。

1. **nova**

作为openstack中最大的模块之一，nova在设计之初，就将自身拆解为若干小的模块进行编写。其主要作用是调度系统中的各种资源来创建虚拟机实例。向glance调用镜像，向neutron调用网络，向cinder调用块存储。在底层用系统命令调用KVM和QEMU来创建虚拟机。根据它所提供的子服务，可以分为以下几部分：

Nova-api：nova与其他模块通信、认证、相互调用的接口，也是相应用户的请求的接口。此服务支持OpenStack计算服务API，Amazon EC2 API，以及特殊的管理API用于赋予用户做一些管理的操作。它会强制实施一些规则，发起多数的编排活动，例如运行一个实例。

Nova-api-metadata：接受来自虚拟机发送的元数据请求。

Nova-scheduler：该服务用于调度计算节点，即决定由哪一台计算节点创建虚拟机。这里要掺杂许多算法知识，工作原理是filter+weight。在filter中指定特定的过滤器，可以实现在特定的计算节点或一组计算节点上创建指定的虚拟机（主机聚合）。

Nova-conductor:该服务作用于nova-compute与数据库之间。是nova服务读写数据库的服务，故而实际工作中，遇到nova与数据库之间的不搭调、报错，就去找conductor的报错信息（/var/log/nova/nova-conductor.log）。

Nova-console：

以上的诸项服务都是无状态的服务，使用高可用的时候，用keepalived一类即可了。

Nova-compute：该服务运行于计算节点上，通过Hypervior的API来创建与销毁虚拟机实例，对于我们目前的环境，该Hypervior即指的是KVM或者QEMU的libvirt。该服务本身就已经分布式部署在各个计算节点上，故而不必做高可用，使用后端共享存储，某个计算节点宕机后，可以使用疏散功能。

1. **glance：**

openstack中管理镜像的服务。它接受磁盘镜像或服务器镜像API请求，和来自终端用户或OpenStack计算组件的元数据定义。它也支持包括OpenStack对象存储在内的多种类型仓库上的磁盘镜像或服务器镜像存储。包括以下俩个组件：

glance-api：接受镜像API的调用，诸如镜像的发现、恢复、存储。

glance-registry：存储、处理和恢复镜像的元数据，元数据包括大小、类型等。其实该服务面向的是后端数据库。

1. **neutron：**

允许创建、插入接口设备，这些设备由其他的OpenStack服务管理。插件式的实现可以容纳不同的网络设备和软件，为OpenStack架构与部署提供了灵活性。

物理网络：tcp/ip7层模型

Neutron服务包含了很多的代理和插件，如下：

L3-agent：工作在三层的代理，实际理解为虚拟路由器（VRouter）。这一代理解决了北向数据流，即数据流由实例与外部网络间的传输，并由浮动IP解决外部网络访问内部实例的问题。

L2-agent：工作在二层的代理，实际理解为虚拟的交换机。常用的为linuxbridgeagent，该代理原生，简单，可靠。可作为L2-agent的默认选择。还有一种openvswitch（OVS），作为第三方的L2-agent，可以模拟一些特定厂商的交换机，但是一般用不上。

Dhcp-agent：提供dhcp功能。

Metadata-agent：配合nova-metadata-service，转发用户定制信息给上述nova模块，实现用户数据注入。

FWaaS：防火墙即服务。

LBaaS：负载均衡即服务。

VPNaaS：VPN即服务。这三个是neutron的三大高级特性。

在这些代理与插件中，dhcp与LBaaS会耗费一些资源，其他的对于系统资源的占用很低。

1. **cinder**

块存储服务，块存储提供一个基础设施为了管理卷，以及和OpenStack计算服务交互，为实例提供卷。此服务也会激活管理卷的快照和卷类型的功能。

块存储的特点：简言之，块存储设备就是一个可以装OS的盘。具备bootable的特性。

块存储服务常包含以下组件：

cinder-api：接受API请求，并将其路由到``cinder-volume``执行。

cinder-volume：与块存储服务和例如cinder-scheduler的进程进行直接交互。它也可以与这些进程通过一个消息队列进行交互。cinder-volume服务响应送到块存储服务的读写请求来维持状态。它也可以和多种存储提供者在驱动架构下进行交互。

cinder-scheduler：选择最优存储提供节点来创建卷。其与``nova-scheduler``组件类似。

cinder-backup：提供任何种类备份卷到一个备份存储提供者。就像``cinder-volume``服务，它与多种存储提供者在驱动架构下进行交互。

消息队列：在块存储的进程之间路由信息。

1. **horizon**

一个web接口，使得云平台的管理者可以用图形化的界面管理不同的资源以及服务。该服务没有自己的实体服务，是依托于HTTP启动的。其配置文件的格式和其他openstack的配置文件并不相同，需要根据它特定的情况配置。