**用户、配额管理**

用户管理

基本概念

用户在OpenStack中用于身份认证

管理员admin一般在packstack安装过程中创建

其他用户由管理员创建，并为器指定可以访问的项目

非管理员用户创建后，保存到mariadb中

非管理员用户具有以下权限

启动实例

创建卷和快照

创建镜像

分配浮动IP

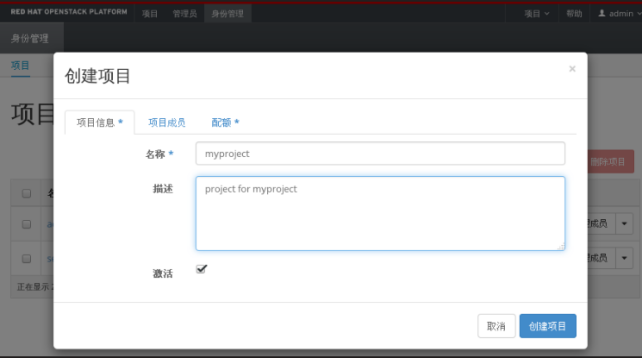
创建网络和路由器地址

创建防火墙以及规则、规则策略

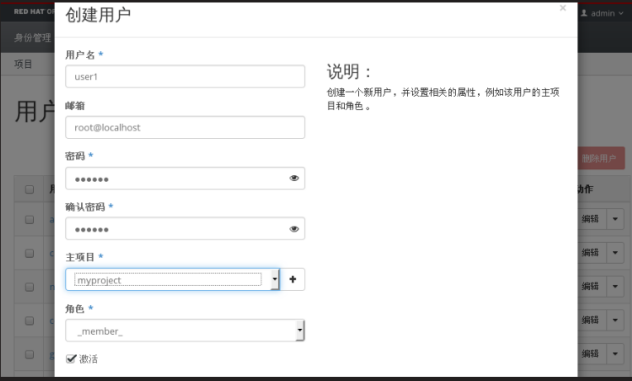
查看网络拓扑、项目使用情况等

通过horizon管理用户

首先创建名为myproject项目，保持默认配置



创建user1用户，指定项目位myproject



通过命令行管理用户

创建user2用户，指定密码位tedu.cn

[root@openstack~(keystone\_admin)]#openstack user create --password tedu.cn user2

设置user2的email地址

[root@openstack~(keystone\_admin)]#openstack user set --email [user2@tedu.cn](mailto:user2@tedu.cn) user2

列出所有用户

[root@openstack~(keystone\_admin)]#openstack user list

查看user2信息

[root@openstack~(keystone\_admin)]#openstack user show user2

指定user2可以访问myproject，角色为\_meber\_

[root@openstack~(keystone\_admin)]#openstack role add --user user2 --project myproject \_member\_

查看user2在myproject中的用户

[root@openstack~(keystone\_admin)]#openstack role list --projecct myproject --user user2

禁用用户

[root@openstack~(keystone\_admin)]#openstack user set --disable user2

激活用户

[root@openstack~(keystone\_admin)]#openstack user set --enable user2

修改user2的密码位redhat

[root@openstack~(keystone\_admin)]#openstack user set --password redhat user2



将user2从myproject中移除

[root@openstack~(keystone\_admin)]#openstack role remove --project myproject --user user2 \_member\_

删除user2用户

[root@openstack~(keystone\_admin)]#openstack user delete user2

配额管理

配额基础

管理员可以通过配额限制，防止字元过度使用

配额基本项目，限制每个项目可以使用多少资源

这些操作上的功能的限制，赋予了管理员对每个项目的精准控制

资源参数

安全组规则：指定每个项目可用的规则数

核心：指定每个项可用的VCPU核心数

固定IP地址：指定每个项目可用的固定IP数

浮动IP地址：指定每个项目可用的浮动IP数

注入文件大小：指定每个项目内容大小

注入文件路径：指定每个项目注入的文件路径长度

注入文件：指定为个项目允许注入的文件数目

实例：指定每个项目课创建的虚拟机实例数目

密钥对：指定每个项目可创建的密钥数

元数据：指定每个项目可用的元数据数据数目

内存：指定每个项目可用的最大内存

安全组：指定每个项目课创建的安全组数目

通过horizon管理配额



通过命令行管理配额

列出项目的缺省配额

[root@openstack~(keystone\_admin)]#nova quota-defaults

列出myproject的配额

[root@openstack~(keystone\_admin)]#nova quota-show --tenant myproject

修改浮动IP地址配额

[root@openstack~(keystone\_admin)]#nova quota-update --floating-ips 20 myproject

**云主机类型管理**

云主机类型

基本概念

云主机类型就是资源的模版

它定义了一台云主机可以使用的资源，如内存大小、磁盘容量和CPU核心等

OpenStack提供了几个默认的云主机类型

管理员还可以自定义云主机类型

云主机类型参数

name：云主机类型名称

ID：云主机类型ID，系统会自动生成一个UUID

VCPUs：虚拟CPU数目

RAM(MB)：内存大小

ROOT disk(GB)：外围磁盘大小。如果希望使用本地磁盘，设置为0

临时磁盘：第二个外围磁盘

swap磁盘：交换磁盘大小

通过horizon管理云主机类型





通过命令行管理云主机类型

列出所有的云主机类型

[root@openstack~(keystone\_admin)]#openstack flavor list

创建一个云主机类型

[root@openstack~(keystone\_admin)]#openstack flavor create --public demo.tiny --id auto --ram 512 --disk 10 --vcpus 1

删除云主机类型

[root@openstack~(keystone\_admin)]#openstack flavor delete demo.tiny

**镜像管理**

镜像基础

基本概念

在红帽OpenStack平台中，镜像指的是虚拟磁盘文件，磁盘文件中应该已经安装了可启动的操作系统

镜像管理功能由glance服务提供

它形成了创建虚拟机实例最底层的块结构

镜像可由用户上传，也可以通过红帽站点官方下载

glance磁盘格式

raw：非结构化磁盘镜像格式

vhd：vmware、xen、microsoft、virualbox等均支持的通用磁盘格式

vmdk：另一个通用的磁盘格式

vdi：virtualbox虚拟机喝qemu支持磁盘格式

iso：光盘数据内容的归档格式

qcow2：qemu支持的磁盘格式。空间自动扩展，并支持写时复制

镜像服务

镜像服务提供了服务器镜像的拷贝、快照功能，可以作为模版快速建立，启动服务器

镜像服务维护了镜像的一致性

当上传镜像时，容器格式必须指定

容器格式指示磁盘文件格式是否包含了虚拟机元数据

镜像容器格式

bare：镜像中没有容器或元数据封装

ovf：一种开源的文件规范，描述了一个开源、安全、有效、可拓展的便携式虚拟打包以及软件分布格式

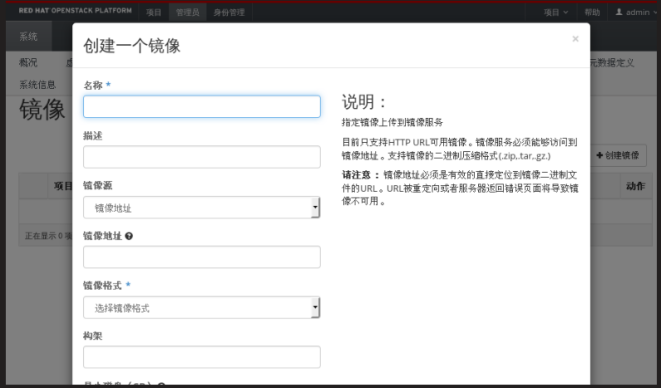
ova：OVA归档文件

aki：亚马逊内核镜像

ami：亚马逊主机镜像

镜像应用

通过horizon管理镜像





通过命令行管理镜像

上传镜像

[root@openstack~(keystone\_admin)]#openstack image create --disk-format qcow2 --min-disk 10 --min-ram 512 --file /root/small.img small\_rhel6

列出镜像

[root@openstack~(keystone\_admin)]#openstack image list

查看镜像详情

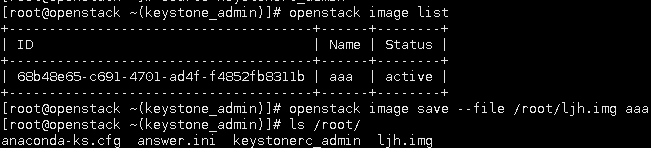
[root@openstack~(keystone\_admin)]#openstack image show small\_rhel6

修改镜像属性

[root@openstack~(keystone\_admin)]#openstack image set --public small\_rhel6

另存镜像为本地文件

[root@openstack~(keystone\_admin)]#openstack image save --file /tmp/small\_rhel6.img small\_rhel6



删除镜像

[root@openstack~(keystone\_admin)]#openstack image delete small\_rhel6

**网络管理**

网络和路由

OpenStack网络工作原理

实例被分配到子网中，以实现网络联通性

每个项目科一有一到多个子网

在红帽的OpenStack平台中，OpenStack网络服务是默认的网络选项，Nova网络服务作为备用

管理员能够配置丰富的网络，讲其它OpenStack服务连接到这些接口上

每个项目都能拥有多个私有网络，每个项目的私有网络互相不受干扰

网络类型

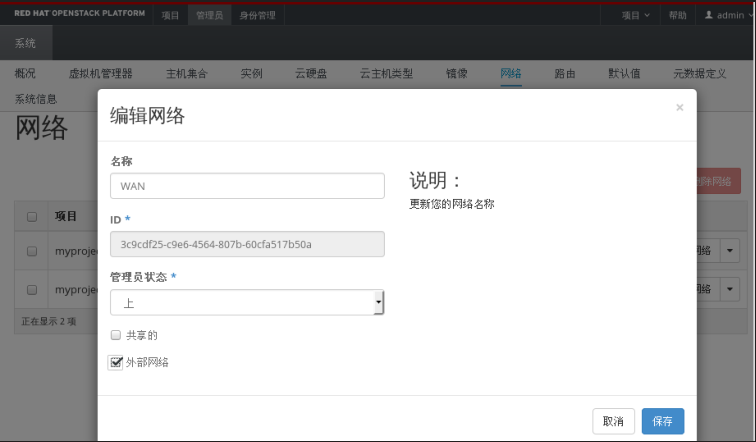
项目网络：项目拥有的网络由neutron提供。网络间才用vxlan隔离

外部网络：访问虚拟机实例的流量通过外部网络进入。实例需要配置浮动IP地址

提供商网络：将实例连接到现有网络，实现虚拟机实例与外部系统共享同一二层网络

通过horizon设置外部网络

外部网络只有管理员有权限设置

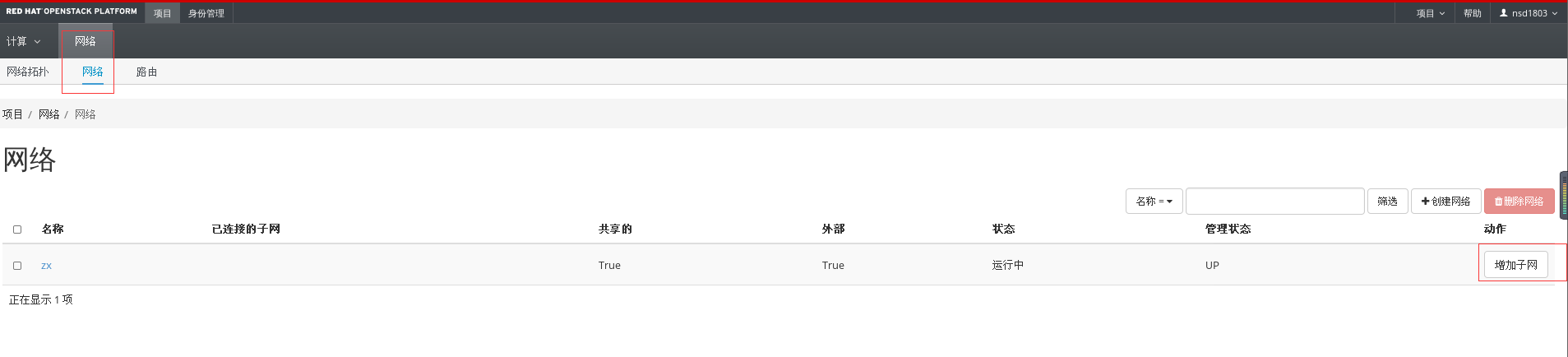




通过horizon创建网络

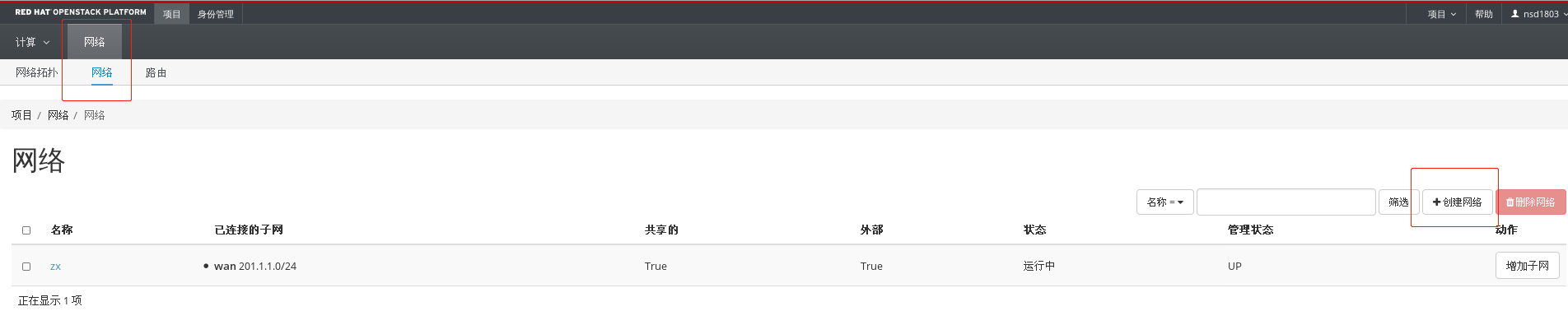
项目网络由租户在自己的项目中创建







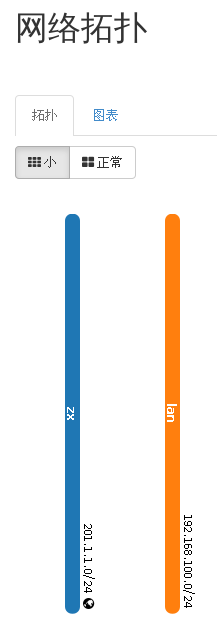




创建内网

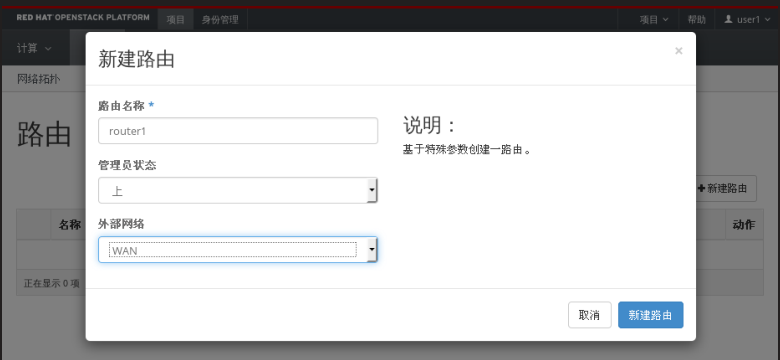




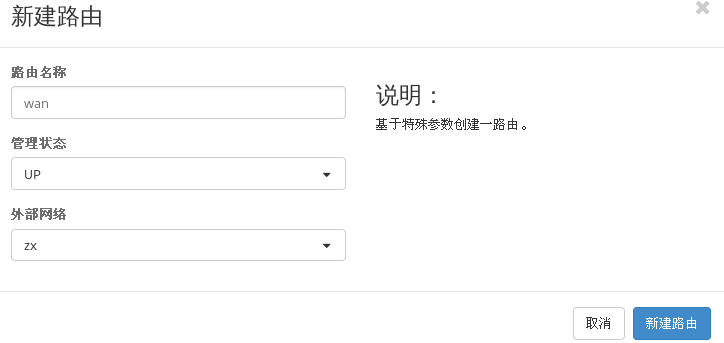


配置路由器

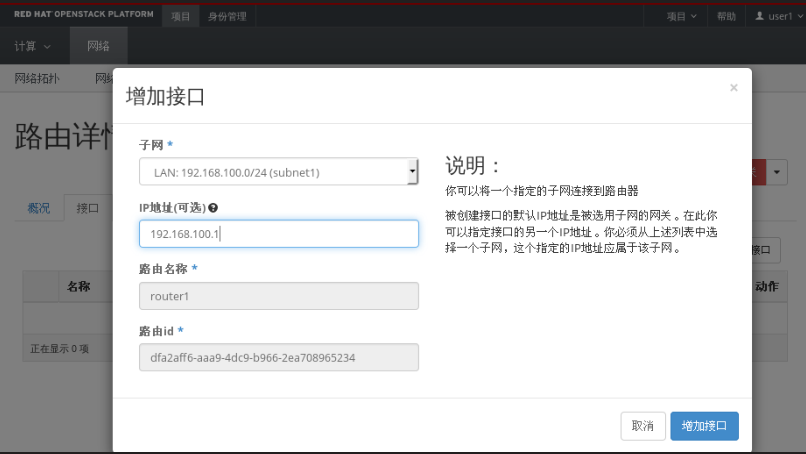
内外网通过路由器连接起来（用户）

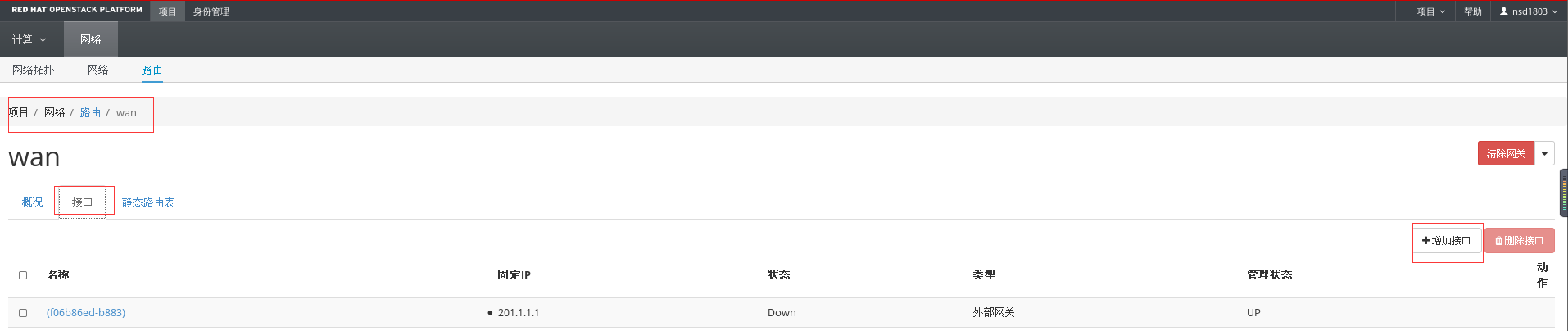


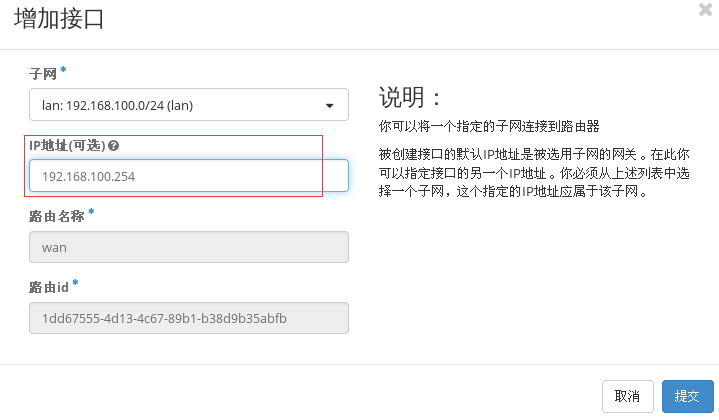


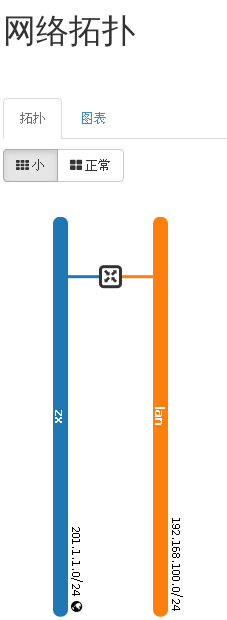


创建路由接口，与内网相连





ip地址为刚才子网指定的IP



通过命令行管理网络

创建网络

[root@openstack~(keystone\_admin)]#openstack network create --project myproject --enable internal

创建子网

[root@openstack~(keystone\_admin)]#neutron subnet-create --name subnet3 --gateway 192.168.200.1 --enable-dhcp internal 192.168.200.0/24 --tenant-id ff38716297863f894cdd1c98597160c

查看网络详情

[root@openstack~(keystone\_admin)]#openstack network show internal

新建路由器

[root@openstack~(keystone\_admin)]#neutron router-create --tenant-id ff387162978643f894cdd1c98597160c router2

删除网络

[root@openstack~(keystone\_admin)]#openstack network delete internal

[root@openstack~(keystone\_admin)]#neutron router-delete router2

浮动IP地址

浮动IP地址作用

浮动IP地址用于从外界访问虚拟机实例

浮动IP地址只能从现有浮动IP地址池中分配

创建外部网络时，浮动IP地址被定义

虚拟机实例启动后，可以为其关联一个浮动IP地址

虚拟机实例也可以解绑IP地址绑定

解除绑定后，再绑定时，不保证绑定原来的IP地址

在horizon中管理浮动IP地址



通过命令行管理浮动IP地址

分配地址

[root@openstack~(keystone\_admin)]#neutron floatingip-create --tenant-id ff387162978943cdd1c98597160c WAN

查看地址

[root@openstack~(keystone\_admin)]#neutron floatingip-list

**安全和实例管理**

安全管理

安全组

安全组用于空值对虚拟机实例的访问

安全组在高层定义了哪些网络及哪些协议是被授权可以访问虚拟机实例的

每个项目都可以自己定义安全组

项目成员可以编辑默认的安全规则，也可以添加新的安全规则

所有的项目都有一个默认的default安全组

安全组规则

安全组规则定义了如何处理网络访问

规则基于网络或协议定义

每个规则都有出和入两个方向

规则也可以指定ip协议版本

默认的安全组规则，允许虚拟机实例对外访问，但是禁止所有对虚拟机的实例访问

创建安全组及规则

创建安全组



点击新建安全组的管理规则，进行规则定义



实例管理

云主机实例要求

使用m2.tiny云主机类型

云主机处于新建的安全组中

将云主机接入内部网络

在horizon中创建云主机



绑定浮动IP

远程主机通过浮动IP地址来访问云主机



安装额外计算节点

1. 检查nova主机能否与openstack互相ping通（两块网卡都要测试）
2. 检查selinux是否禁用（getenforce）
3. 检查firewalld是否卸载（rpm -qa | grep firewalld）
4. 检查NetworkManager是否卸载（rpm -qa | grep NetworkManager）
5. 检查yum源（yum repolist）
6. 检查系统yum源是否导入公钥（gpgcheck=1）
7. 检查时间服务器（chronyc sources -v）
8. 检查OpenStack和本机的主机名能否ping通（往Hosts里面添加主机名和ip,管理节点和Nova节点都要）

环境准备

准备网络

配置两块网卡，与第一台OpenStack服务器的两块网卡对应，能ping通

一块网卡用于主机间通信，另一块网卡用于隧道

DNS地址指向正确的服务器地址

停用并禁用NetworkManager

准备软件环境

配置好yum，能够使用rhel7光盘和OpenStack光盘提供的仓库源

由于安装过程中有些依赖包没有在Yum源中，所以要提前安上，依赖的软件包

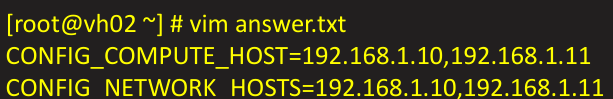
导入签名信息

安装计算节点

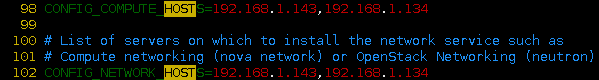
修改应答文件

安装额外节点，只需要在第一台OpenStack服务器上进行即可

修改配置文件







安装节点

在第一台节点上执行安装命令

packstack --answer-file answer.ini



按提示，输入远程主机root密码

本机已安装服务，不会被覆盖，只有改动后的选项才需要重新配置

查看节点状态

安装后的状态如图所示





云主机热迁移

