**14\_Cloud\_3用户+配额管理+云主机类型管理+镜像管理+网络管理+安全和实例管理+计算节点扩容**

**一 用户\配额管理-项目管理**

**1.1 基本概念**

**1.1.1 项目**: 一组隔离的的资源和对象.由一组关联的用户进行管理

在旧版里,也用租户(tenant[ˈtenənt])来表示

根据配置的需求,项目对应一个组织\一个公司或是一个使用客户等

项目中可以有多个用户,项目中的用户可以在该项目中创建\管理虚拟资源

具有admin角色的用户可以创建项目

项目相关信息保存到mariadb中

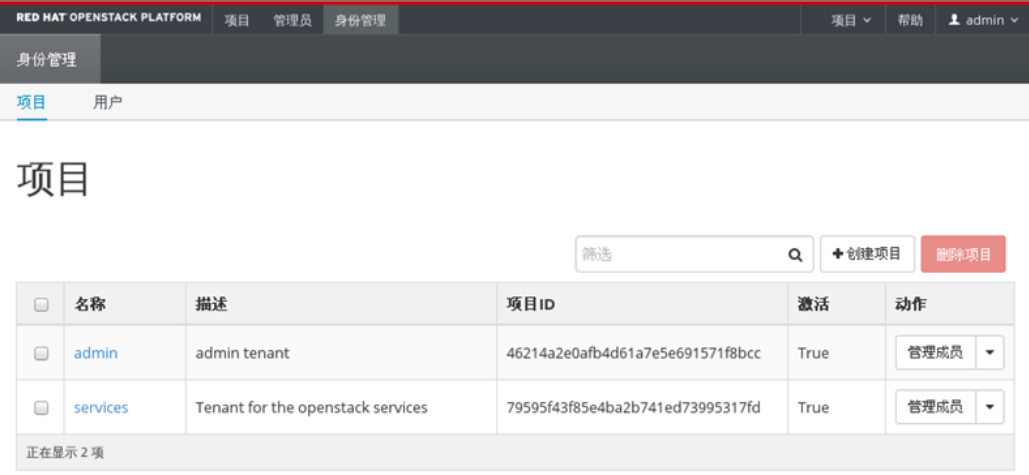
缺省情况下,packstack安装的openstack中有两个独立的项目

admin: 为admin账户创建的项目

services: 与安装的各个服务相关联

**1.2创建项目**

通过Horizon可以进行项目的创建和删除



**1.3 通过命令行管理项目**

**创建名为myproject项目**

**openstack project create** myproject

**列出所有项目**

**openstack project list**

**查看myproject详细信息**

**openstack project show** myproject

**禁用与激活项目**

**openstack project set-disable\enable** myproject

**查看项目配额**

**nova quota-show --tenant** myproject

**更新可用的vcpu数目为30**

**nova quota-update --cores** 30

**删除myproject**

**openstack project delete** myproject

**1.4 用户基本概念**

用户在openstack中用于身份认证

管理员用户admin一般在packstack安装过程中创建

其他用户由管理员用户创建,并指定可以访问的项目

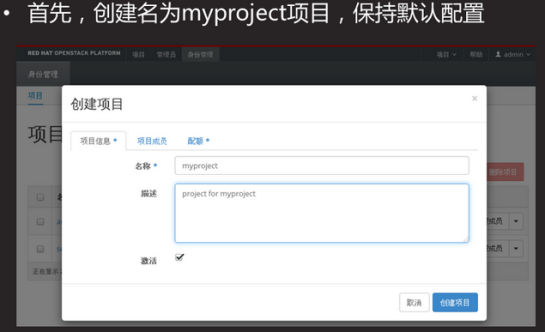
非管理员用户创建后,保存到mariadb中

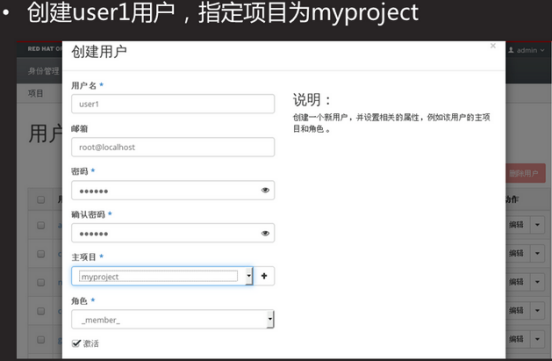
非管理员用户具有以下权限:

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\创建防

火墙以及规则策略\查看网络拓扑,项目使用概况等

**1.5 通过Horizon管理用户**





**1.6 通过命令行管理用户**

创建user2用户,指定密码为tedu.cn

openstack user create --password tedu.cn user2

设置user2的email地址

openstack user set --email [user2@tedu.cn](mailto:user2@tedu.cn) user2

列出所有用户

openstack user list

查看user2信息

openstack user show user2

指定user2可以访问myproject,角色为\_member\_

openstack role add --user user2 --project myproject \_

禁用\激活用户

openstack user set --disable\enable user2

修改user2的密码为redhat

openstack user set --password redhat user2

将user2从myproject中移除

openstack role remove --project myproject --user user2 \_member\_

删除user2用户

openstack user delete user2

**二 用户\配额管理-配额管理**

**2.1 配额基础**

管理员可以通过配额限制,防止资源的过度使用

配额基本项目,限制每个项目可以使用多少资源

这些操作上的功能限制,赋予了管理员对每个项目的精准控制

2.2 资源参数

安全组规则: 指定每个项目可用的规则数

核心: 指定每个项可用额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: 指定每个项目允许注入的文件数目

实例: 指定每个项目可创建的虚拟机实例数目

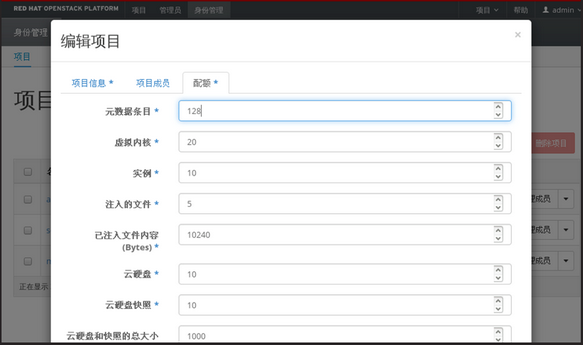
密钥对: 指定每个项目可创建的密钥数

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: 指定每个项目可创建的安全组数目

**2.3 通过Horizon管理配额**



**2.4 通过命令行管理配额**

列出项目的缺省配额

nova quota-defaults

列出myproject的配额

nova quota-show --tenant

修改浮动IP地址配额

nova quota-update --floating-ips 20 myproject

**三 云主机类型管理**

**3.1 基本概念**

云主机类型就是资源的模板

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核心数等

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

**3.2 云主机类型参数**

name: 云主机类型名称

ID: 云主机类型ID,系统自动生成一个UUID

VCPUs: 虚拟CPU数目

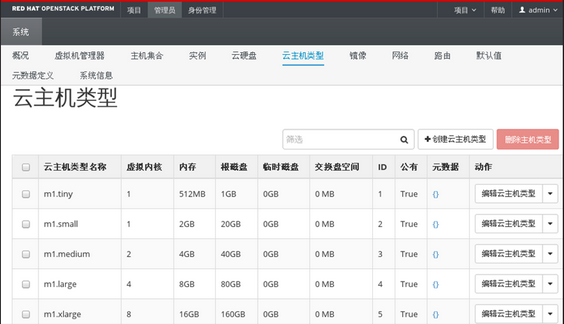
RAM(MB): 内存大小

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: 第二哥外围磁盘

swap磁盘: 交换磁盘大小

**3.3 通过Horizon管理云主机类型**



**3.4 通过命令行管理云主机类型**

列出所有的云主机类型

openstack flavor[ˈfleɪvə] list

创建一个云主机类型

openstack flavor create --public demo.tiny --id auto --ram 512 --disk 10 --vcpus 1

删除云主机类型

openstack flavor delete demo.tiny

**四 镜像管理-镜像基础**

**4.1 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

镜像管理功能有Glance服务提供

它形成了创建虚拟机实例最底层的块结构

镜像可以用用户上传,也可用通过红帽官方站点下载

**4.2 Glance磁盘格式**

raw: 非结构化磁盘镜像格式

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

vmdk: 是vmware的虚拟磁盘格式

vdi: virtualbox虚拟机和QEMU支持的磁盘格式

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copy-on-write

**4.3 镜像服务**

镜像服务提供了服务器镜像的拷贝\快照功能,可以作为模板快速建立\启动服务器

镜像服务维护了镜像的一致性

当上传镜像是,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

**4.4 镜像容器格式**

bare: 镜像中没有容器或元数据封装

ovf: 一种开元的文件规范,描述了一个开源\安全\有效\可扩展的便携式虚拟打包以

及软件分布格式

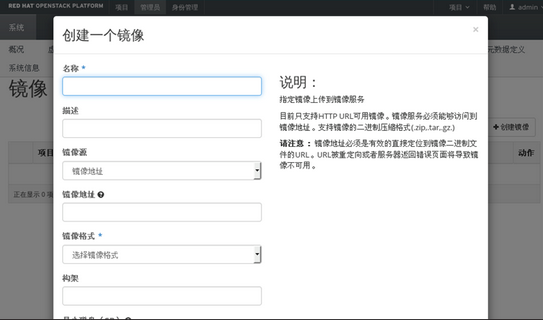
ova: OVA归档文件

aki: 亚马逊内核镜像

ami: 亚马逊主机镜像

**五 镜像管理-镜像应用**

**5.1 过Horizon管理镜像**

** 通**

**5.2 通过命令行管理镜像**

上传镜像

openstack image create --disk-format qcow2 --min-disk 10 --min-ram 512 --file /root/small.img small\_rhel6

列出镜像

openstack image list

查看镜像详情

openstack image show small\_rhel6

修改镜像属性

openstack image set -public small\_rhel6

另存镜像为本地文件

openstack image save --file /tmp/small\_rhel6.img small\_rhel6

删除镜像

openstack image delete small\_6

**六 网络管理-网络和路由**

**6.1 openstack网络工作原理**

实例被分配到子网中,以实现网络连通性

每个项目可以有一到多个子网

在红帽的openstack平台中,openstack网络服务是缺省的网络选项,nova网络服务作为备用

管理员能够配置丰富的网络,将其他openstack服务连接到这些网络接口上

每个项目都能拥有多个私有网络,各个项目的私有网络互相不受干扰

**6.2 网络类型**

项目网络: 由nertorn提供的项目内部网络,网络间可用vlan隔离

外部网络: 可以让虚拟机介入网络网络,但需要配置浮动IP地址

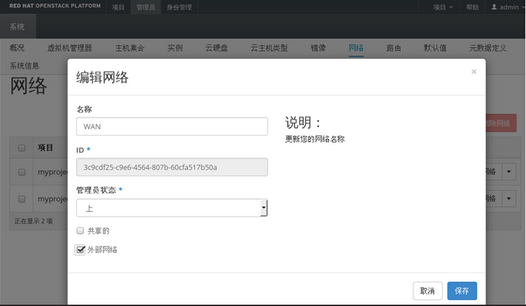
提供商网络: 将实例连接到现有网络,实现虚拟机实例与外部系统共享同一二层网络

**6.3 通过Horizon创建网络**



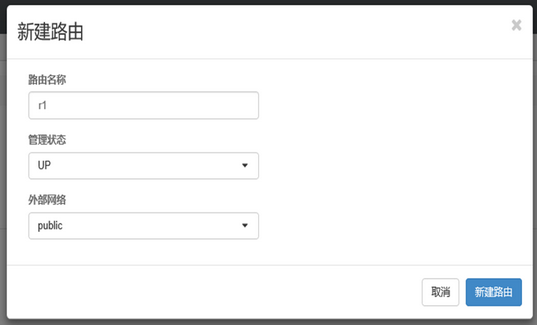
**6.4 通过Horizon设置外部网络**

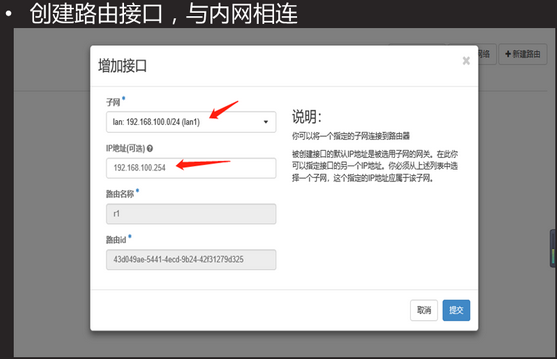
外部网络只有管理员有权限设置



**6.5 配置路由器**

**内外网通过路由器连接起来**





**6.6 通过命令行管理网络**

创建网络

openstack network create --project myproject --enable internal

创建子网

neutron subnet-create --name subnet3 --gateway 192.168.1.254 --allocation-pool start=192.168.4.100,end=192.168.1.200

--enable-dhcp internal 192.168.1.0/24 --tenant-id UUID字符串

查看网络详情

openstack network show internal

新建路由器

neutron router-create --tenant-id UUID字符串

删除网络

openstack network delete internal

neutron router-delete r2

**七 网络管理-浮动IP地址**

**7.1 浮动IP地址的作用**

浮动IP一般是花钱购买的

浮动IP地址用于从外界访问虚拟机实例

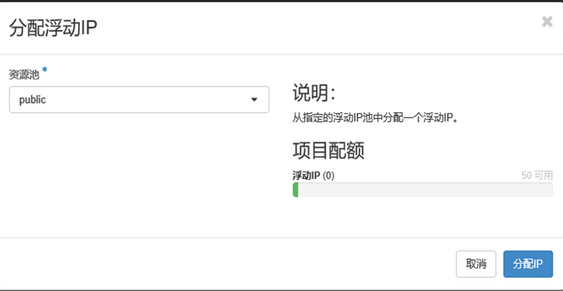
浮动IP地址只能从现有浮动IP地址池中分配

创建外部网络时,浮动IP地址池被定义

虚拟机实例启动后,可以为其关联一个浮动IP地址

虚拟机实例可以解除IP地址绑定

**7.2 在Horizon中管理浮动IP地址**



**7.3 通过命令行管理浮动IP地址**

分配地址

neutron floatingip-create --tenant-id UUID字符串

查看地址

neutron floatingip-list

**八 安全和实例-安全管理**

**8.1 安全组**

安全组用于控制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

每个项目都可以定义自己的安全组

项目成员可以编辑默认的安全规则,也可以天剑新的安全规则

所有的项目都有一个默认的default安全组

**8.2 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,运行虚拟机实例对外访问,但是阻止所有对虚拟机实例的访问

**8.3 创建安全组及规则**





**九 安全和实例管理-实例管理**

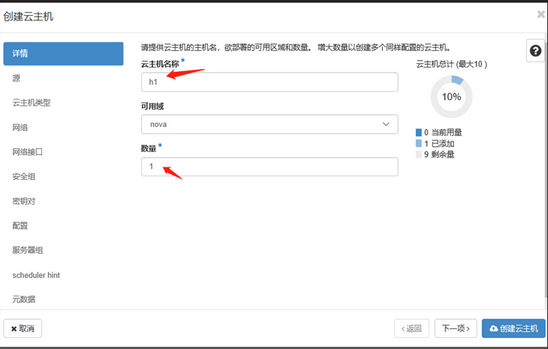
**9.1 云主机实例要求**

使用m2.tiny云主机类型

云主机处于新建的安全组中

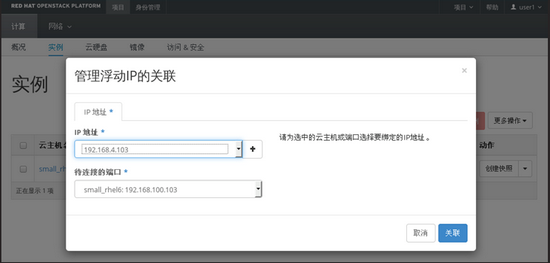
将云主机介入到内部网络

**9.2 在Horizon中创建云主机**



**9.3 绑定浮动IP地址**

远程主机通过访问浮动IP地址来访问云主机



**十 计算节点扩容-环境准备**

**10.1 准备扩容主机**

准备主机nova2

配置静态IP:192.168.1.12,及主机名

保证与openstack,和nova1能相互ping通

配置/etc/resolv.conf,删除serach开头行

配置时间同步/etc/chrony.conf

配置yum源,软件仓库一共4个(10670)

**10.2 准备软件环境**

安装软件依赖包:qemu-kvm libvirt-client libvirt-daemon

libvirt-daemon-driver-qemu python-setuptools

nova2 ~]# systemctl status libvirtd　　＃此服务基于以上４个依赖包

**十一 计算节点扩容-安装计算节点**

**11.1 修改应答文件**

openstack计算几点采用远程安装

即在openstack上执行指令,远程安全nova2

远程安装使用ssh指令,从openstack上必须能够通过ssh命令登录nova2

在openstack上修改配置文件

openstack ~]# vim answer.ini

98 CONFIG\_COMPUTE\_HOST=192.168.1.11,**192.168.1.12**

102 CONFIG\_NETWORK\_HOSTS=192.168.1.10,192.168.1.11,192.168.12

**11.2 安装节点**

在openstack上重新执行安装命令

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,只有改动后的选项猜需要重新配置

安装后,apache配置已被还原,需要重新添加

WSGIApplicationGroup %{GLOBAL}

**11.3 查看节点状态**

安装后的状态如图所示



1 案例1：管理项目

1.1 问题

本案例要求：

通过Horizon完成以下操作

创建名为tedu的项目

创建用户 uu 来管理这个项目

1.2 步骤

实现此案例需要按照如下步骤进行。

步骤一：创建项目

1）创建tedu项目，如图-1所示：

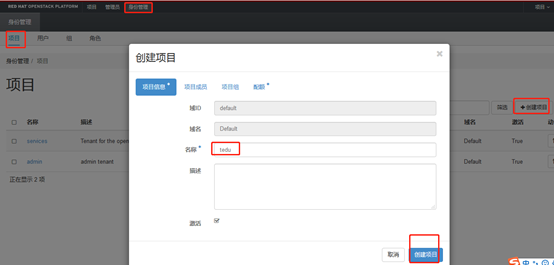


图-1

2）创建uu用户，如图-2所示：

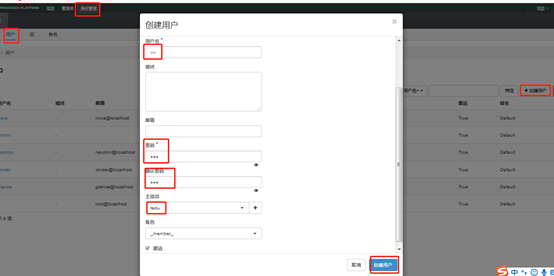


图-2

4）通过Horizon进行配额调整，如图-3所示：



图-3

2 案例2：新建云主机类型

2.1 问题

本案例要求通过命令和Horizon创建云主机类型：

名字：m2.tiny

ID：自动

虚拟内核：1个

内存：512M

根磁盘：10GB

临时磁盘和swap无要求

2.2 步骤

实现此案例需要按照如下步骤进行。

步骤一：新建云主机类型

1）通过Horizon创建云主机类型，如图-4所示：



图-4

3 案例3：上传镜像

3.1 问题

本案例要求上传一个镜像：

将本机上的rhel6磁盘镜像文件small.img上传

上传到Openstack的名称为small\_rhel6

设置镜像属性为public

镜像最小磁盘大小为10GB，最小内存为512MB

3.2 步骤

实现此案例需要按照如下步骤进行。

步骤一：上传镜像，如图-5所示：

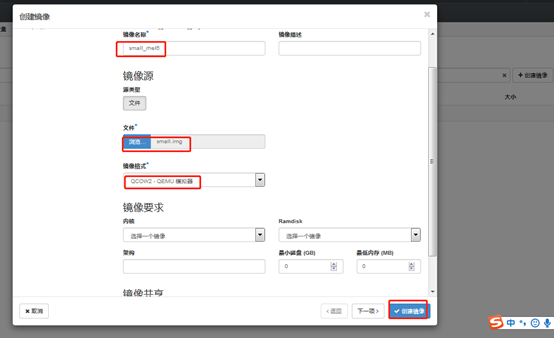


图-5

4 案例4：创建网络

4.1 问题

本案例要求：

在tedu项目中创建两个网络，一个内网，用于连接实例，一个外网，用于对外通信

创建一个路由器，将两个网络连接起来

4.2 步骤

实现此案例需要按照如下步骤进行。

步骤一：创建网络

1）登陆admin用户，创建外网public，如图-6所示：



图-6

2）退出admin用户 ，登陆uu用户，创建public的子网wan，如图-7所示：

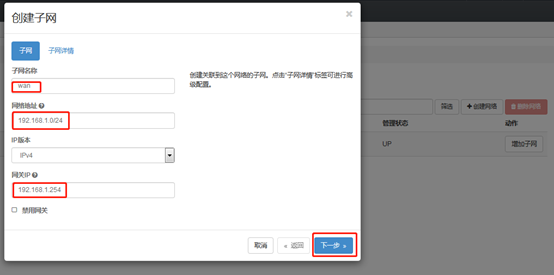


图-7

3）public外网不需要激活DHCP，如图-8所示：



图-8

4）创建内网lan，如图-9所示：

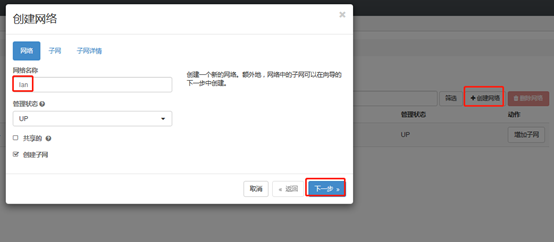


图-9

5）创建lan的子网，如图-10所示：

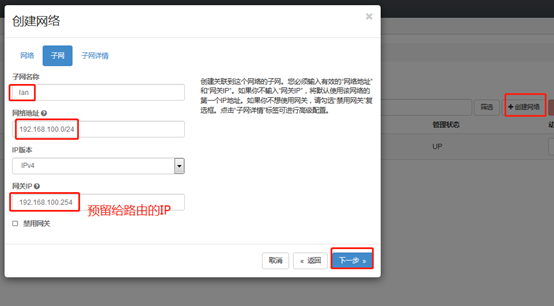


图-10

7）给内网分配地址池，如图-11所示：

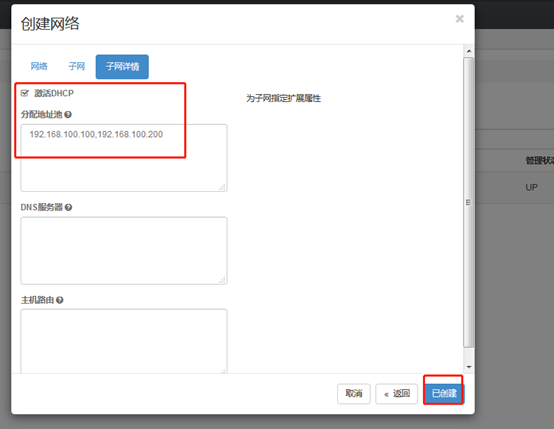


图-11

8）新建路由，如图-12所示：



图-12

9）选择路由子网，如图-13所示：

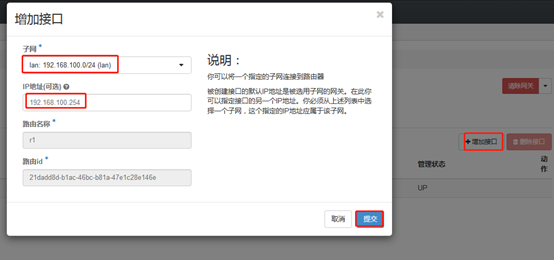


图-13

5 案例5：管理浮动IP地址

5.1 问题

本案例要求：

通过Horizon创建一个浮动IP地址

通过命令行创建一个浮动IP地址

5.2 步骤

实现此案例需要按照如下步骤进行。

步骤一：创建浮动IP

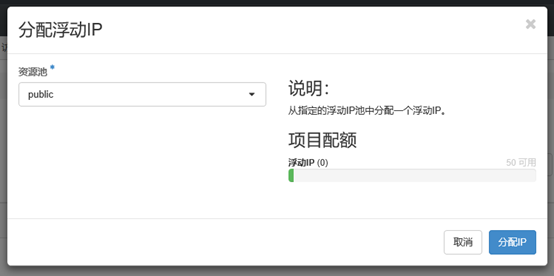


图-14

6 案例6：创建安全组及规则

6.1 问题

本案例要求：

新建一个安全组

添加规则，允许任意主机可以通过SSH访问虚拟机实例

添加规则，允许任意主机可以通过HTTPS访问虚拟机实例

添加规则，只允许本组内的主机可以通过HTTP访问到虚拟机实例

6.2 步骤

实现此案例需要按照如下步骤进行。

步骤一：建立安全组



图15

2）允许ssh访问，如图-16



图-16

3）允许HTTPS访问，如图-17所示：

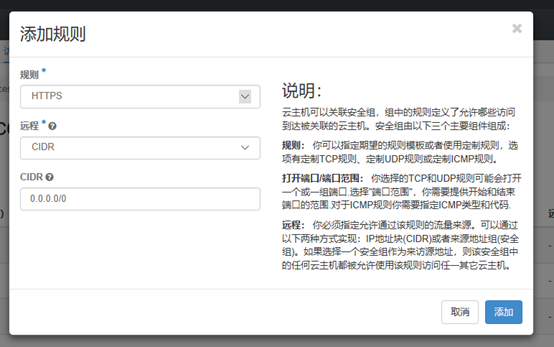


图-17

7 案例7：创建云主机

7.1 问题

本案例要求：

使用m2.tiny云主机类型

将云主机加入到内部网络

设置安全规则，允许外界ping通云主机

设置外界可以ssh到云主机

7.2 步骤

实现此案例需要按照如下步骤进行。

步骤一：创建云主机

1）创建云主机，如图-18所示：



图-18



图-19

4）云主机类型，如图-20所示：

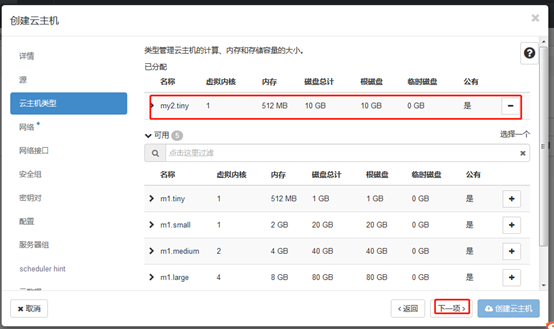


图-20

5）云主机网络，如图-21所示：



图-21

步骤二：设置安全组规则，允许外界ping通云主机

1）添加规则，如图-22所示：



图-22

2）增加ping规则，如图-23所示

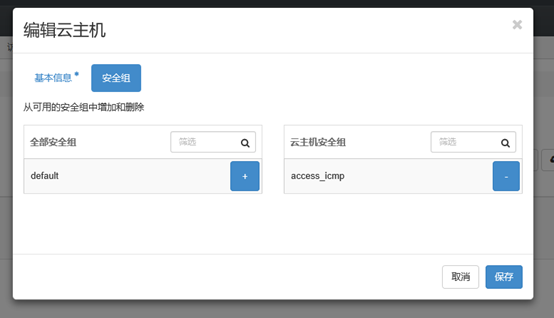


图-23

7）进入控制台，配置dns的ip为192.168.1.254，浮动ip在案例5已经设置，这里不再重复，通过浮动ip可以ssh连接，如图-24所示：

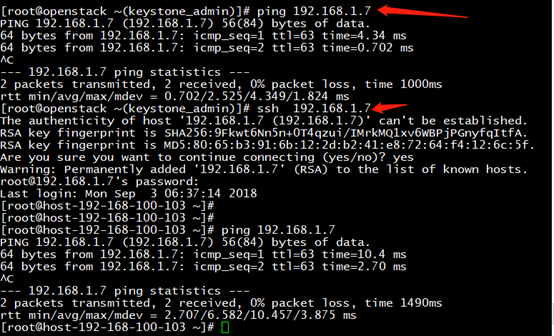


图-24

8 案例8：安装额外计算节点

8.1 问题

本案例要求安装额外的计算节点：

nova02 请参考 nova01 的配置步骤

8.2 步骤

实现此案例需要按照如下步骤进行。

步骤一：安装计算节点

1）更改answer.ini文件

[root@openstack ~]# vim answer.ini        //在openstack上面操作

98 CONFIG\_COMPUTE\_HOSTS=192.168.1.11,192.168.1.12

102 CONFIG\_NETWORK\_HOSTS=192.168.1.10,192.168.1.11,192.168.1.12

[root@openstack ~]# packstack --answer-file answer.ini

\*\*\*\* Installation completed successfully \*\*\*\*\*\*

2）这时浏览器访问时不出现页面，15-horizon\_vhost.conf文件被还原，需要重新修改这个文件

[root@openstack ~]# cd /etc/httpd/conf.d/

[root@openstack conf.d]# vi 15-horizon\_vhost.conf

35 WSGIProcessGroup apache

36 WSGIApplicationGroup %{GLOBAL} //添加这一行

[root@openstack conf.d]# apachectl graceful //重新载入配置文件

3）浏览器访问，出现页面

[root@openstack conf.d]# firefox 192.168.1.10

[root@localhost conf.d]# cd

[root@localhost ~]# ls

answer.ini keystonerc\_admin

[root@openstack ~]# cat keystonerc\_admin

unset OS\_SERVICE\_TOKEN

export OS\_USERNAME=admin

export OS\_PASSWORD=1bb4c987345c45ba

4）安装后的节点状态，如图-25所示：



图-25

5）云主机热迁移，没有迁移之前云主机是在nova01上面。如图-26所示：



图-26

热迁移选择，如图-27所示：

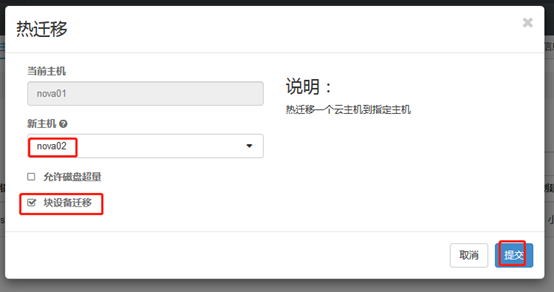


图-27

迁移状态，如图-28所示：



图-28

迁移结果，如图-29所示：

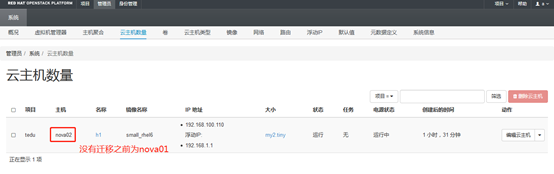


图-29

openstack错误分析：

1）进入控制台不显示内容，如图-30所示：

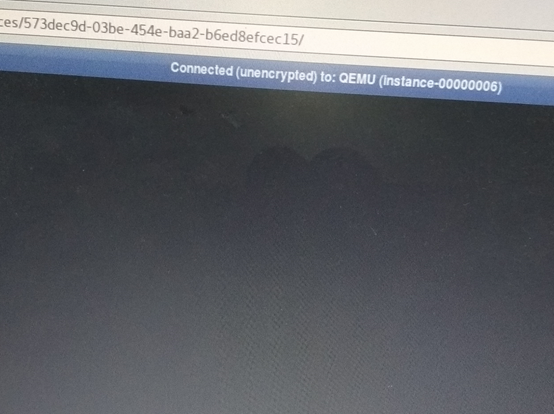


图-30

解决办法：可以重新启动一下openstack-nova-console

2）若出现云主机处于错误状态，如图-31所示：

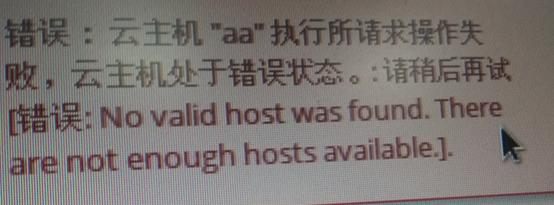


图-31

解决办法：

可能是主机down掉

可能是内存不足

可能是内网出现了问题，检查内网，或者把内网删除（不会建立的可以参考案例4），重新建立，之后重新启动openstack

[root@openstack ~]# systemctl restart openstack-nova-compute

3）云主机热迁移失败

解决办法：查看主机名是否ping通，还可以查看qemu-kvm-rhev这个包有没有安装

4）云主机迁移错误。如图-32所示：

IMG_287

图-32

创建的云主机有问题，不用共享存储，必须使用 镜像 文件