CLOUD-day03

云平台部署与管理

# 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、规则策略

– 查看网络拓扑、项目使用概况等

## 通过Horizon管理用户

### • 首先,创建名为myproject项目,保持默认配置

身份管理-->项目-->创建项目-->名称(\*为必填项)-->配额-->(默认)-->创建项目

### • 创建user1用户,指定项目为myproject

身份管理-->用户-->创建用户-->用户名(\*为必填项)-->密码-->确认密码-->主项目(myproject)-->角色(\_member)-->创建用户

# 配额管理

## 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

## 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

# 云主机类型

## 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

## 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:第二个外围磁盘

• swap磁盘:交换磁盘大小

## 通过Horizon管理云主机类型

管理员-->云主机类型-->创建云主机类型-->名称(test01)-->VCPU-->内存-->根磁盘-->创建云主机类型

# 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劢的操作系统

• 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

• 镜像可以由用户上传,也可以通过红帽官方站点下载

## Glance磁盘格式

• raw:非结构化磁盘镜像格式

• vhd:VMware、Xen、Microsoft、VirtualBox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

## 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、起劢服务器

• 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

## 通过Horizon管理镜像

管理-->镜像-->创建镜像-->镜像名称-->文件-->镜像格式-->创建镜像（完成）

# 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的接口上

• 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

## 网络类型

• 项目网络:由Neutron提供的项目内部网络,网络间可用VLAN隔离

• 外部网络:可以让虚拟机接入外部网络,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,实现虚拟机实例不外部系统共享同一二层网络

## 通过Horizon创建网络

### • 项目网络由租户在自己的项目中创建

管理员-->网络-->创建网络-->名称-->项目-->供应商(flat)-->物理网络-->共享的-->外部网络-->提交

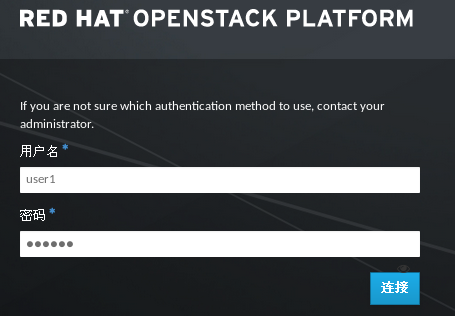
## 通过Horizon设置外部网络

### • 外部网络只有管理员有权限设置

管理员-->网络-->public-->创建子网-->子网名称-->网络地址-->网关IP-->下一步-->去掉激活DHCP-->分配地址池-->已创建

## 切换普通用户user1进一步配置



## 配置路由器

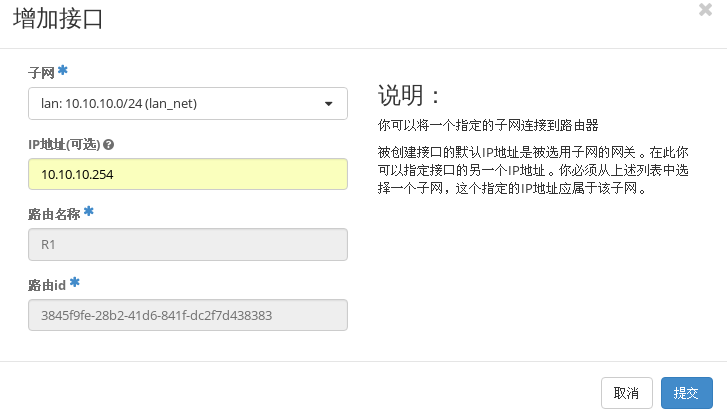
### • 内外网通过路由器连接起来

项目-->网络-->网络拓扑-->新建路由-->路由名称-->外部网络-->新建路由



### 为路由器增加接口：





## 创建网络

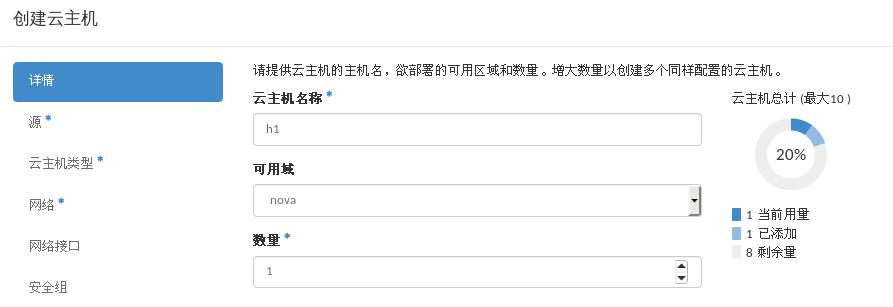
### 项目-->网络-->网络拓扑-->创建网络-->网络名称-->下一步-->子网名称-->网络地址-->网关-->下一步-->分配地址池-->已创建







## 在Horizon中创建云主机



在可用一栏中选择

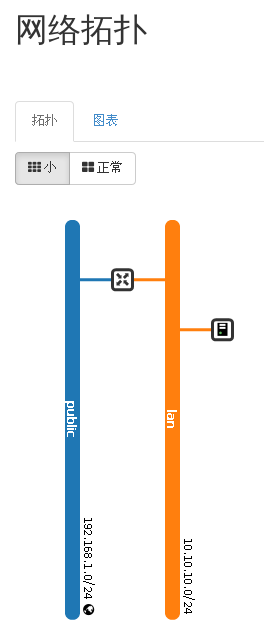
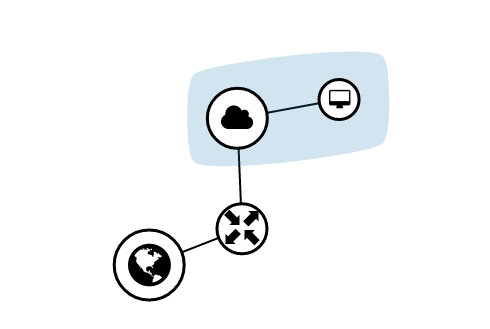


云主机类型在可用中选择自己创建的test01；网络选择lan网-->配置之后点击创建云主机即可创建完成





## 云主机创建成功之后的网络拓扑图如下：

网络拓扑图表模式

# 浮动IP地址

## 浮动IP地址的作用

### • 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,浮劢IP地址池被定义

### • 虚拟机实例起动后,可以为其关联一个浮动IP地址

### • 虚拟机实例也可以解除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



绑定浮动IP地址-->+号-->ip地址的选择-->关联



# 安全管理

## 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,但是阻止所有对虚拟机实例的访问

# 安装额外计算节点

## 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

• 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

• 停止并禁用NetworkManager

### 检查ifcfg-eth0 ifcfg-eth1能ping 通openstack主机

检查/etc/resolv.conf

检查 chronyc sources -v

检查 NTP时间同步

### 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,所以要提前安装上,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

[root@openstack ~]# vim answer.ini

98 CONFIG\_COMPUTE\_HOSTS=192.168.1.10,192.168.1.11

102 CONFIG\_NETWORK\_HOSTS=192.168.1.10,192.168.1.11

### 安装节点

• 在第一台节点上执行安装命令

[root@vh02 ~] # packstack --answer-file answer.txt

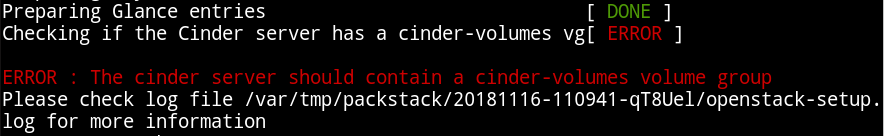
• 按提示,输入进程主机root密码

• 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

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

**出现** \*\*\*\* Installation completed successfully \*\*\*\*\*\* **即成功**

若出现以下错误，查看openstack上的vg卷是否存在



若不存在，则创建：

[root@openstack ~]# pvcreate /dev/vdb

[root@openstack ~]# vgcreate cinder-volumes /dev/vdb