#-----------------------------------------#

创建 2 个虚拟机

要求：

虚拟机1

8G 内存

2块网卡

第一块网卡连接虚拟交换机 vbr

第二块网卡连接虚拟交换机 private1

设置静态 IP，默认网关 192.168.1.254

/etc/sysconfig/network-scripts/ifcfg-ethX

BOOTPROTO="static"

IPADDR="192.168.1.xx"

PREFIX="24"

默认网关:

GATEWAY="192.168.1.254"

2块硬盘

其中 / 的 vda1 要求 50G

vdb 20G

虚拟机2

6G 内存

2块网卡

第一块网卡连接虚拟交换机 vbr

第二块网卡连接虚拟交换机 private1

设置静态 IP，默认网关 192.168.1.254

要求与第一台虚拟主机的两个 IP 都能 ping 通

硬盘

/ 的 vda1 要求 50G

testnode

test1 eth0 192.168.1.100 eth1 192.168.4.100 8G openstack

test2 eth0 192.168.1.101 eth1 192.168.4.101 6G nova

Openstack主要组件

• Horizon

– 用于管理Openstack各种服务的、基于web的管理接口

– 通过图形界面实现创建用户、管理网络、启动实例等操作

• Keystone

– 为其他服务提供认证和授权的集中身份管理服务

– 也提供了集中的目录服务

– 支持多种身份认证模式,如果密码认证、令牌认证、以及AWS(亚马逊Web服务)登陆

– 为用户和其他服务提供了SSO认证服务

• Neutron

– 一种软件定义网络服务

– 用于创建网络、子网、路由器、管理浮动IP地址

– 可以实现虚拟交换机、虚拟路由器

– 可用于在项目中创建VPN

• Cinder

– 为虚拟机管理存储卷的服务

– 为运行在Nova中的实例提供永久的块存储

– 可以通过快照进行数据备份

– 经常应用在实例存储环境中,如果数据库文件

• Nova

– 在节点上用于管理虚拟机的服务

– Nova是一个分布式的服务,能够不Keystone交互实现认证,不Glance交互实现镜像管理

– Nova被设计成在标准硬件上能够迚行水平扩展

– 启动实例时,如果有需要则下载镜像

• Glance

– 扮演虚拟机镜像注册的角色

– 允许用户为直接存储拷贝服务器镜像

– 这些镜像可以用于新建虚拟机的模板

NTP一定要有，而且不能和管理节点装在一起，否则服务起不来

DNS服务器一定要有，也不能和管理节点装在一起

除了Nova以外，其他组件都装在一台机，Nova多台

装12个YUM源，用下面3个光盘：

RHEL7-extras.iso CentOS7-1708.iso

RHEL7OSP-10.iso （有10个YUM源）

逻辑卷创建名为**cinder-volumes**的卷组，一定要叫该名

一、创建物理卷、卷组

pvcreate /dev/vdb pvs

vgcreate **cinder-volumes** /dev/vdb vgs

二、安装虚拟化服务器平台必备软件 (两台机都要安装 openstack nova)

yum -y install qemu-kvm libvirt-daemon libvirt-client libvirt-daemon-driver-qemu python-setuptools

三、环境验证

1. 禁用 selinux sestatus:disabled

2. 卸载 firewalld rpm -qn | grep firewalld

3. 卸载 NetworkManager rpm -qn | grep Network

4. 配置主机IP地址 ping 192.168.4.254

5. 配置主机yum客户端 yum repolist 10731

6. 创建cinder-volumes的卷组 vgs

7. 导入公钥 只有CentOS7-1708源gpg＝1，要导入公钥

8. 安装依赖的软件包 virsh

openstack会自己接管防火墙和网络配置

安装openstack

1. 配置packstack（openstack主机）
2. 装包

]# yum install -y openstack-packstack

]# packstack --gen-answer-file answer.ini

1. 修改应答文件

]# vim answer.ini

CONFIG\_DEFAULT\_PASSWORD=Taren1 //默认密码 11

CONFIG\_SWIFT\_INSTALL=n //y使用共享 n使用本地硬盘 42

CONFIG\_NTP\_SERVERS=192.168.1.254 //同步NTP时间服务 75

ONFIG\_COMPUTE\_HOSTS=192.168.1.100 //nova节点的IP 98

CONFIG\_NETWORK\_HOSTS=192.168.1.100

//把哪些主机网络变成openstack支持的网络 102

CONFIG\_CINDER\_VOLUMES\_CREATE=n

//禁止自动创建cinder-volumes卷组 554

CONFIG\_CINDER\_VOLUMES\_SIZE=20G //创建的卷要>20

CONFIG\_NEUTRON\_ML2\_TYPE\_DRIVERS=flat,vxlan

//flat 出口网卡，用来出外网 | vxlan是用软件划分vlan，局域网 840

CONFIG\_NEUTRON\_ML2\_VXLAN\_GROUP=239.1.1.5 //组播地址 876

CONFIG\_NEUTRON\_OVS\_BRIDGE\_MAPPINGS=physnet1:br-ex

//网桥，虚拟交换机 910

CONFIG\_NEUTRON\_OVS\_BRIDGE\_IFACES=br-ex:eth0 //把网卡模拟成虚拟交换机的VAN口，让虚拟交换机和真实交换机通讯，使用eth0连接 921

CONFIG\_NEUTRON\_OVS\_TUNNEL\_IF=eth1

//用eth1网卡，使用trunk或tun隧道进行通讯，把两张网卡连接起来 936

CONFIG\_PROVISION\_DEMO=n //1179

3.安装openstack

]# packstack --answer-file answer.ini

4.验证OVS配置 （OVS虚拟交换机）

1） ovs-vsctl show

2） ip -o addr show

cat /etc/sysconfig/network-scripts/ifcfg-br-ex

ONBOOT=yes

IPADDR=192.168.1.100

PREFIX=24

GATEWAY=192.168.1.254

DEVICE=br-ex

NAME=br-ex

DEVICETYPE=ovs

OVSBOOTPROTO=static

TYPE=OVSBridge

cat /etc/sysconfig/network-scripts/ifcfg-eth0

DEVICE=eth0

NAME=eth0

DEVICETYPE=ovs

TYPE=OVSPort

OVS\_BRIDGE=br-ex

ONBOOT=yes

BOOTPROTO=none

eth0变成了虚拟交换机的一个端口和真实虚拟机连通

Openstack操作基础

Horizon

• Horizon BUG 处理

• 安装虽然没有报错,但默认无法打开 Horizon,这是一个软件的配置 BUG

]# vim /etc/httpd/conf.d/15-horizon\_vhost.conf

WSGIProcessGroup apache 下面一行添加

WSGIApplicationGroup %{GLOBAL} <--- 这里添加

修改完重新载入配置 apachectl graceful

cd ~

cat keystonerc\_admin 查看页面初始用户名密码

unset OS\_SERVICE\_TOKEN

export OS\_USERNAME=admin

export OS\_PASSWORD=6b12592bbdc949e6 //修改完密码修改文件，密码真正存储在数据库中，再执行认证

export OS\_AUTH\_URL=http://192.168.1.100:5000/v2.0

export PS1='[\u@\h \W(keystone\_admin)]\$ '

页面访问：192.168.1.100

项目

• 一组隔离的资源和对象。由一组关联的用户进行管理

• 项目中可以有多个用户,项目中的用户可以在该项目创建、管理虚资资源

• 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

配额：

VCPU数量 （所有主机总CPU数量）

云主机数量

内存

浮动IP（花钱买的公网IP）

关于 /root/keystone\_admin 文件的注意事项：

1、该文件只是一个文本，里面记录了 admin 的用户名和密码，与认证无关

2、不能通过修改该文件达到修改 admin 密码的目的

3、修改 admin 密码请使用 web 页面登录后，在web页面中修改

修改后，keystone\_admin 中的密码通用要修改成新的密码才可以继续使用

4、该文件可以作为命令行的登录文件使用，使用方式 source ~/keystone\_admin

5、如果你安装完成 openstack 后，没有修改过 admin 的密码

keystone\_admin 文件不小心被更改了

我们可以通过查找应答文件 answer.ini 中的变量 CONFIG\_KEYSTONE\_ADMIN\_PW 来找到默认安装密码

命令行创建

]# openstack project list

Missing value auth-url required for auth plugin password //未认证

]# source ~/keystonerc\_admin //执行认证

]# openstack help ----帮助

]# openstack user set + 回车 ----命令具体帮助

]# openstack project list

]# openstack user list

用户管理

• 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,并为其指定可以访问的项目

• 非管理员用户创建后,保存到MariaDB中

修改user2的密码为redhat（不用知道原始密码）也可以修改admin密码

(keystone\_admin)]# openstack user set --password redhat user2

配额管理

• 管理员可以通过配额限制,防止资源过度使用

• 配额基本项目,限制每个项目可以使用多少资源

• 这些操作上的功能上的限制,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据目

• 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

云主机类型管理 （资源模板）

云主机类型参数

• Name:云主机类型名称

• ID:云主机类型ID,系统自劢生成一个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

云主机类型 ----定义xml

demo.xml 模板

用模板规范用户创建云主机

界面：管理员－系统-云主机类型

镜像管理 （后端盘）

• 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

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

镜像应用

界面：管理员-镜像

另存镜像为本地文件

~(keystone\_admin)]# openstack image list

备份到哪个路径

~(keystone\_admin)]# openstack image save --file /tmp/small\_rhel6.img small\_rhel6(镜像名)

网络管理 （创建虚拟交换机）

通过Horizon创建网络

1. 由管理员创建外部网络 admin用户

界面：管理员－网络

flat physnet1：物理网络标识，在配置文件中有 （如果选错了，云主机会上不了网）

1. 由租户自己创建项目中的私有网络 u1用户

1）增加外网的子网

界面：网络－网络－选择外网增加子网

不能激活DHCP，因为IP是买的

1. 创建内网

界面：网络－网络－创建网络

3）创建路由

界面：网络－路由

外网

创建完路由，编辑 增加接口 选内网 192.168.100.254

查看拓朴

创建虚拟云主机

root redhat

浮动IP地址

• 将真实IP映射给虚拟云主机，并不是真正配置到虚拟主机上

• 分配浮动IP类似于DHCP随机分配

• 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

把云主机发布到公网中

选择一台云主机－绑定浮动IP

设置完此时网络还是不通，要再设置添加新的安全组

安全组 （防火墙）openstack要对防火墙有控制权，所以和本机的防火墙冲突，底层还是调用firewalld

• 每个规则都有出和入两个方向

默认是default组，不允许任务人访问

界面：项目－计算－访问和安全

出口 0.0.0.0

添加规则 入口 ALL\_ICMP

添加规则 入口 TCP 22

有多条就新增多条规则

添加规则 入口 其他协议 （不作任何限制）

编辑安全组，把新建的安全组放在default前面

cd /var/log/nova

Nova安装

添加nova节点主机

环境验证

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 (sestatus)

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 10731包)

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 是否能 ping 通

vim /etc/hosts

192.168.1.100 openstack

192.168.1.101 nova

openstack主机 修改：

]# vim answer.ini

ONFIG\_COMPUTE\_HOSTS=192.168.1.100,192.168.1.101

//openstack IP 和nova节点的IP 98

CONFIG\_NETWORK\_HOSTS=192.168.1.100,192.168.1.101

//把哪些主机网络变成openstack支持的网络，openstack IP 和nova节点的IP 102

执行：packstack --answer-file=answer.ini

（会连接nova节点的22端口，输入nova主机密码）

virsh dumpxml 虚拟机

systemctl restart libvirtd openstack-nova-compute管理libvirtd