

云计算部署与管理

NSD CLOUD

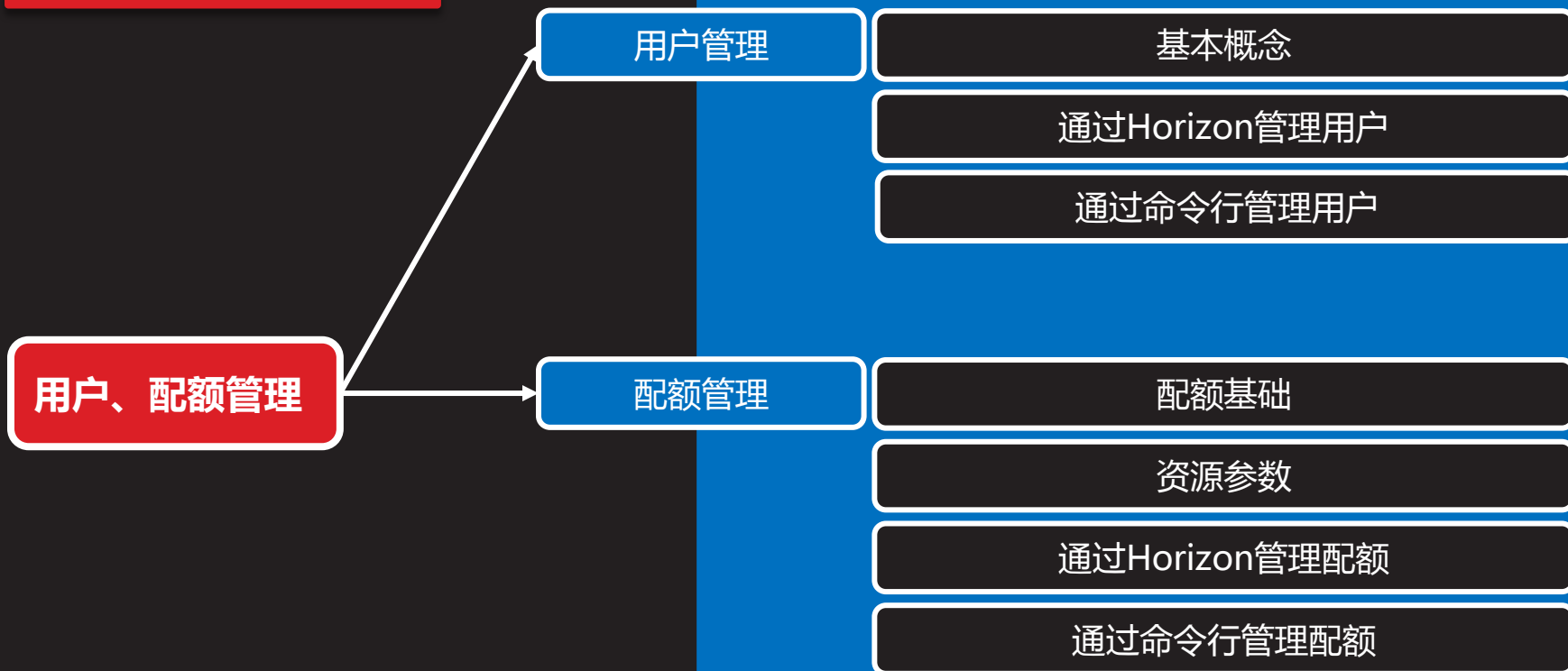
DAY02

内容

上午	09:00 ~ 09:30	作业讲解和回顾
	09:30 ~ 10:20	用户、配额管理
	10:30 ~ 11:20	云主机类型管理
	11:30 ~ 12:20	镜像管理
下午	14:00 ~ 14:50	网络管理
	15:00 ~ 15:50	安全和实例管理
	16:10 ~ 17:00	安装额外计算节点
	17:10 ~ 18:00	总结和答疑



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



基本概念（续1）

- 非管理员用户具有以下权限
 - 起动实例
 - 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

RED HAT OPENSTACK PLATFORM 项目 管理员 身份管理 项目 帮助 admin

身份管理

项目

创建项目

项目信息 * 项目成员 配额 *

名称 * myproject

描述 project for myproject

激活 ☒

取消 创建项目

通过Horizon管理用户（续1）

- 创建user1用户，指定项目为myproject

RED HAT OPENSTACK

身份管理

项目

用户

☐ 用户1
☐ 用户2
☐ 用户3
☐ 用户4
☐ 用户5
☐ 用户6
☐ 用户7
☐ 用户8
☐ 用户9
☐ 用户10

创建用户

用户名 *

user1

邮箱

root@localhost

密码 *

.....

确认密码 *

.....

主项目 *

myproject

角色 *

member

☒ 激活

说明：

创建一个新用户，并设置相关的属性，例如该用户的主项目和角色。

删除用户

动作

编辑

编辑

编辑

编辑

编辑

通过命令行管理用户

- 创建user2用户，指定密码为tedu.cn
`[root@vh02 ~(keystone_admin)]# openstack user create --password tedu.cn user2`
- 设置user2的email地址
`[root@vh02 ~(keystone_admin)]# openstack user set --email user2@tedu.cn user2`
- 列出所有用户
`[root@vh02 ~(keystone_admin)]# openstack user list`
- 查看user2信息
`[root@vh02 ~(keystone_admin)]# openstack user show user2`



通过命令行管理用户（续1）

- 指定user2可以访问myproject，角色为_member_
[root@vh02 ~(keystone_admin)]# openstack role add --user user2 --project myproject _member_
- 查看user2在myproject中的角色
[root@vh02 ~(keystone_admin)]# openstack role list --project myproject --user user2
- 禁用用户
[root@vh02 ~(keystone_admin)]# openstack user set --disable user2
- 激活用户
[root@vh02 ~(keystone_admin)]# openstack user set --enable user2



通过命令行管理用户（续2）

- 修改user2的密码为redhat
`[root@vh02 ~(keystone_admin)]# openstack user set --password redhat user2`
- 将user2从myproject中移除
`[root@vh02 ~(keystone_admin)]# openstack role remove --project myproject --user user2 _member_`
- 删除user2用户
`[root@vh02 ~(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
止的精准控制



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



资源参数（续1）

- 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



通过Horizon管理配额

RED HAT OPENSTACK PLATFORM 项目 管理员 身份管理 项目 ▾ 帮助 admin ▾

身份管理

项目

项目

正在显示

删除项目

管理成员 ▾

管理成员 ▾

管理成员 ▾

编辑项目

项目信息 *

项目成员

配额 *

元数据条目 *

128

虚拟内核 *

20

实例 *

10

注入的文件 *

5

已注入文件内容 (Bytes) *

10240

云硬盘 *

10

云硬盘快照 *

10

云硬盘和快照的总大小

1000



通过命令行管理配额

- 列出项目的缺省配额

```
[root@vh02 ~(keystone_admin)]# nova quota-defaults
```

- 列出myproject的配额

```
[root@vh02 ~(keystone_admin)]# nova quota-show --tenant  
myproject
```

- 修改浮动IP地址配额

```
[root@vh02 ~(keystone_admin)]# nova quota-update --floating-ips  
20 myproject
```



案例1：用户和配额管理

1. 创建myproject项目
2. 通过Horizon创建user1用户
3. 通过CLI创建user2用户，练习相关用户管理命令
4. 通过Horizon和CLI对myproject进行配额调整



云主机类型管理

云主机类型管理

云主机类型

基本概念

云主机类型参数

通过Horizon管理云主机类型

通过命令行管理云主机类型

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

RED HAT OPENSTACK PLATFORM

项目 管理员 身份管理

项目 帮助 admin

系统

概況 虚拟机管理器 主机集合 实例 云硬盘 云主机类型 镜像 网络 路由 默认值

元数据定义 系统信息

云主机类型

筛选

+ 创建云主机类型

删除主机类型

<input type="checkbox"/>	云主机类型名称	虚拟内核	内存	根磁盘	临时磁盘	交换盘空间	ID	公有	元数据	动作
<input type="checkbox"/>	m1.tiny	1	512MB	1GB	0GB	0 MB	1	True	{}	编辑云主机类型
<input type="checkbox"/>	m1.small	1	2GB	20GB	0GB	0 MB	2	True	{}	编辑云主机类型
<input type="checkbox"/>	m1.medium	2	4GB	40GB	0GB	0 MB	3	True	{}	编辑云主机类型
<input type="checkbox"/>	m1.large	4	8GB	80GB	0GB	0 MB	4	True	{}	编辑云主机类型
<input type="checkbox"/>	m1.xlarge	8	16GB	160GB	0GB	0 MB	5	True	{}	编辑云主机类型



通过命令行管理云主机类型

- 列出所有的云主机类型

```
[root@vh02 ~(keystone_admin)]# openstack flavor list
```

- 创建一个云主机类型

```
[root@vh02 ~(keystone_admin)]# openstack flavor create --public  
demo.tiny --id auto --ram 512 --disk 10 --vcpus 1
```

- 删除云主机类型

```
[root@vh02 ~(keystone_admin)]# openstack flavor delete demo.tiny
```



案例2：新建云主机类型

- 分别通过Horizon和CLI练习创建云主机类型
 1. 名字：m2.tiny
 2. ID：自动
 3. 虚拟内核：1个
 4. 内存：512M
 5. 根磁盘：10GB
 6. 临时磁盘和swap无要求



镜像管理

镜像管理

镜像基础

基本概念

Glance磁盘格式

镜像服务

镜像容器格式

镜像应用

通过Horizon管理镜像

通过命令行管理镜像

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 : 另一个通用的磁盘格式
- 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

知识讲解

RED HAT OPENSTACK PLATFORM

项目

管理员

身份管理

项目

帮助

admin

系统

概况

系统信息

镜像

正在显示 0 项

创建镜像

名称 *

描述

镜像源

镜像地址

镜像地址

镜像格式 *

选择镜像格式

构架

说明：

指定镜像上传到镜像服务

目前只支持HTTP URL可用镜像。镜像服务必须能够访问到镜像地址。支持镜像的二进制压缩格式(.zip,.tar,.gz.)

请注意：镜像地址必须是有效的直接定位到镜像二进制文件的URL。URL被重定向或者服务器返回错误页面将导致镜像不可用。



通过命令行管理镜像

- 上传镜像

```
[root@vh02 ~(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@vh02 ~(keystone_admin)]# openstack image list
```

- 查看镜像详情

```
[root@vh02 ~(keystone_admin)]# openstack image show small_rhel6
```



通过命令行管理镜像（续1）

- 修改镜像属性

```
[root@vh02 ~(keystone_admin)]# openstack image set --public  
small_rhel6
```

- 另存镜像为本地文件

```
[root@vh02 ~(keystone_admin)]# openstack image save --file  
/tmp/small_rhel6.img small_rhel6
```

- 删除镜像

```
[root@vh02 ~(keystone_admin)]# openstack image delete small_rhel6
```



案例3：上传镜像

1. 将本机上的rhel6磁盘镜像文件small.img上传
2. 上传到Openstack的名称为small_rhel6
3. 设置镜像属性为public
4. 镜像最小磁盘大小为10GB，最小内存为512MB



网络管理

网络管理

网络和路由

Openstack网络工作原理

网络类型

通过Horizon创建网络

通过Horizon设置外部网络

配置路由器

通过命令行管理网络

浮动IP地址

浮动IP地址的作用

在Horizon中管理浮动IP地址

通过命令行管理浮动IP地址

通过命令行管理项目

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：项目拥有的网络由Neutron提供。网络间采用VLAN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创建网络

- 项目网络由租户在自己的项目中创建

RED HAT OPENSTACK PLATFORM 项目 身份管理 项目 ▾ 帮助 user1 ▾

计算 ▾

网络拓扑

网络

正在显示 0 项

创建网络

网络 子网 子网详情

网络名称

创建新网络。另外，关联到网络的子网在下一面板中被创建。

网络描述

管理员状态 ⓘ

上

☒ 创建子网

取消 « 后退 后页 »

+ 创建网络

动作



通过Horizon设置外部网络

- 外部网络只有管理员有权限设置

RED HAT OPENSTACK PLATFORM 项目 管理员 身份管理 项目 ▾ 帮助 admin ▾

系统

概况 虚拟机管理器 主机集合 实例 云硬盘 云主机类型 镜像 网络 路由 默认值 元数据定义

系统信息

网络

正在显示 2 项

编辑网络

名称
WAN

ID *
3c9cdf25-c9e6-4564-807b-60cfa517b50a

管理员状态 *
上

☐ 共享的
☒ 外部网络

说明：
更新您的网络名称

取消 保存

配置路由器

- 内外网通过路由器连接起来

RED HAT OPENSTACK PLATFORM

项目 身份管理

项目 ▾ 帮助 user1 ▾

计算 ▾

网络拓扑

路由

正在显示 0 项

路由名称 *

router1

管理员状态

上 ▾

外部网络

WAN ▾

说明 :

基于特殊参数创建一路由。

取消

新建路由

+ 新建路由

动作



配置路由器（续1）

- 创建路由接口，与内网相连

RED HAT OPENSTACK PLATFORM 项目 身份管理 项目 ▾ 帮助 user1 ▾

计算 ▾ 网络

网络拓扑 网络

路由详情

概况 接口

名称
正在显示 0 项

增加接口

子网 *

LAN: 192.168.100.0/24 (subnet1)

IP地址(可选) ⓘ

192.168.100.1

路由名称 *

router1

路由id *

dfa2aff6-aaa9-4dc9-b966-2ea708965234

说明：

你可以将一个指定的子网连接到路由器

被创建接口的默认IP地址是被选用子网的网关。在此你可以指定接口的另一个IP地址。你必须从上述列表中选择一个子网，这个指定的IP地址应属于该子网。

取消 增加接口



通过命令行管理网络

- 创建网络

```
[root@vh02 ~(keystone_admin)]# openstack network create --project myproject --enable internal
```

- 创建子网

```
[root@vh02 ~(keystone_admin)]# neutron subnet-create --name subnet3 --gateway 192.168.200.1 --allocation-pool start=192.168.200.101,end=192.168.200.200 --enable-dhcp internal 192.168.200.0/24 --tenant-id ff387162978643f894cdd1c98597160c
```



通过命令行管理网络（续1）

- 查看网络详情

```
[root@vh02 ~(keystone_admin)]# openstack network show internal
```

- 新建路由器

```
[root@vh02 ~(keystone_admin)]# neutron router-create --tenant-id  
ff387162978643f894cdd1c98597160c router2
```

- 删除网络

```
[root@vh02 ~(keystone_admin)]# openstack network delete internal  
[root@vh02 ~(keystone_admin)]# neutron router-delete router2
```



案例4：创建网络

1. 在myproject中创建两个网络
 - 一个内网，将来用于连接实例
 - 一个外网，将来有于对外通信
2. 创建一个路由器，将两个网络连接起来



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

The screenshot displays the Horizon OpenStack Platform interface. At the top, the navigation bar includes 'RED HAT OPENSTACK PLATFORM', '项目' (Project), '身份管理' (Identity Management), '项目' (Project) with a dropdown, '帮助' (Help), and 'user1' with a dropdown. The main navigation tabs are '计算' (Compute), '网络' (Network), '概况' (Overview), '实例' (Instances), '云硬盘' (Volumes), '镜像' (Images), and '访问 & 安全' (Access & Security). The '访问 & 安全' tab is active, showing a sub-tab '安全组' (Security Groups). A modal dialog titled '分配浮动IP' (Allocate Floating IP) is open. It features a '资源池 *' (Resource Pool) dropdown menu with 'WAN' selected. To the right, a '说明:' (Note) section states: '从指定的浮动IP池中分配一个浮动IP。' (Allocate a floating IP from the specified floating IP pool.). Below this, the '项目配额' (Project Quota) section shows '浮动IP (0)' (Floating IP (0)) and a progress bar indicating '50 可用配额' (50 available quota). At the bottom right of the dialog are '取消' (Cancel) and '分配IP' (Allocate IP) buttons.

RED HAT OPENSTACK PLATFORM 项目 身份管理 项目 帮助 user1

计算 网络

概况 实例 云硬盘 镜像 访问 & 安全

访问 & 安全

安全组

分配浮动IP

资源池 *

WAN

说明：

从指定的浮动IP池中分配一个浮动IP。

项目配额

浮动IP (0) 50 可用配额

取消 分配IP



通过命令行管理浮动IP地址

- 分配地址

```
[root@vh02 ~(keystone_admin)]# neutron floatingip-create --tenant-id  
ff387162978643f894cdd1c98597160c WAN
```

- 查看地址

```
[root@vh02 ~(keystone_admin)]# neutron floatingip-list
```



案例5：管理浮动IP地

- 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



安全和实例管理

安全和实例管理

安全管理

安全组

安全组规则

创建安全组及规则

实例管理

云主机实例要求

在Horizon中创建云主机

绑定浮动IP地址

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



创建安全组及规则

- 创建安全组

RED HAT OPENSTACK PLATFORM
项目
身份管理
项目
帮助
user1

计算
网络

概况
实例
云硬盘
镜像
访问 & 安全

访问 & 安全

安全组

名称 *

描述

说明：

安全组是IP过滤规则的集合，可被应用到虚拟机的网络设置中。在安全组创建后，你可以给安全组增加规则。

取消

创建安全组

创建安全组及规则（续1）

- 点击新建安全组的管理规则，进行规则定义

RED HAT OPENSTACK PLATFORM 项目 身份管理 项目 ▾ 帮助 user1 ▾

计算 网络 存储 安全 监控 日志 告警 备份 恢复 迁移 部署 运维 管理

管理 a573

正在显示 2 项

添加规则

规则 *
HTTPS

远程 * ⓘ
CIDR

CIDR ⓘ
0.0.0.0/0

说明：

云主机可以关联安全组，组中的规则定义了允许哪些访问到达被关联的云主机。安全组由以下三个主要组件组成：

规则：你可以指定期望的规则模板或者使用定制规则，选项有定制TCP规则、定制UDP规则或定制ICMP规则。

打开端口/端口范围：你选择的TCP和UDP规则可能会打开一个或一组端口。选择“端口范围”将为你提供开始和结束端口的范围。对于ICMP规则你需要指定ICMP类型和所提供的空间里面的代码。

远程：你必须指定允许通过该规则的来访源。可以通过以下两种方式实现：IP地址黑名单(CIDR，)或者源地址组(安全组)。如果选择一个安全组作为来访源地址，则该安全组中的任何云主机实例都被允许使用该规则访问任一其它云主机。

取消 添加

删除规则

动作

删除规则

删除规则



案例6：创建安全组及规则

- 新建一个安全组
- 添加规则，允许任意主机都可以通过SSH访问虚拟机实例
- 添加规则，允许任意主机都可以通过HTTPS访问虚拟机实例
- 添加规则，只允许本组内主机可以通过HTTP访问虚拟机实例



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
- 将云主机接入到内部网络



在Horizon中创建云主机

RED HAT OPENSTACK

计算 网络 实例 云主

正在显示 0 项

详情 * 访问 & 安全 网络 * 创建后 高级选项

可用域
nova

云主机名称 *
small_rhel6

云主机类型 * ?
m2.tiny
Some flavors not meeting minimum image requirements have been disabled.

云主机数量 * ?
1

云主机启动源 * ?
从镜像启动

镜像名称 *
small_rhel6 (101.6 MB)

指定创建云主机的详细信息
详细说明启动云主机的情况,下面的图表显示此项目所使用的资源和关联的项目配额。

方案详情

名称	m2.tiny
虚拟内核	1
根磁盘	10 GB
临时磁盘	0 GB
磁盘总计	10 GB
内存	512 MB

项目限制

云主机数量 10 中的 0 已使用

虚拟CPU数量 20 中的 0 已使用

内存总计 51200 中的 0 MB已使用



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

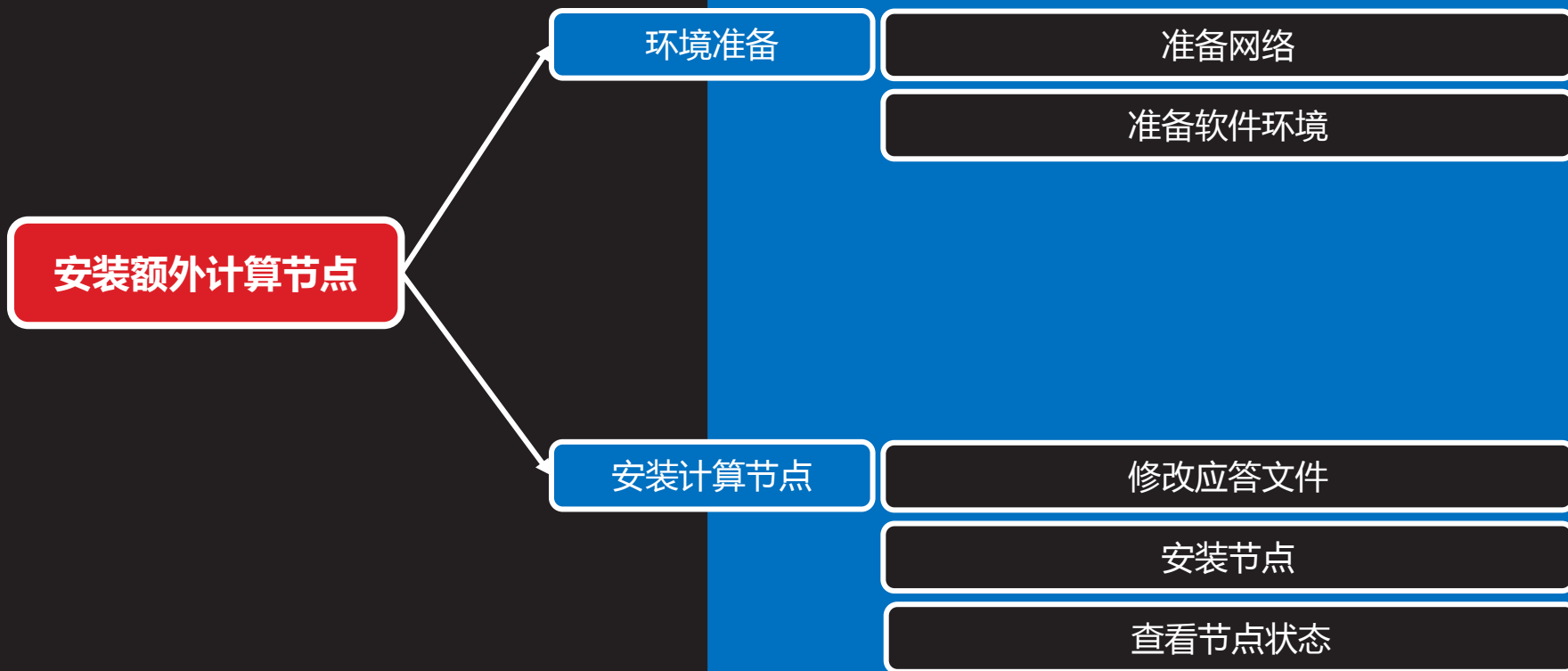


案例7：创建云主机

- 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



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



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@vh02 ~] # vim answer.txt  
CONFIG_COMPUTE_HOST=192.168.1.10,192.168.1.11  
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

RED HAT OPENSTACK PLATFORM
项目
管理员
身份管理
项目
帮助
admin

系统

概况
虚拟机管理器
主机集合
实例
云硬盘
云主机类型
镜像
网络
路由
默认值
元数据定义

系统信息

主机集合

主机集合

筛选
+ 创建主机集合

名称	可用域	主机	元数据	动作
没有要显示的条目。				

正在显示 0 项

可用域

筛选

可用域名称	主机	可用配额
internal	vh02.tedu.cn (服务已运行)	True
nova	vh03.tedu.cn (服务已运行) vh02.tedu.cn (服务已运行)	True



案例8：安装额外计算节点

- 新主机要求如下：
 1. 添加两块网卡，均能与第一个节点通信
 2. 能够准确地进行DNS解析
 3. 配置yum仓库
 4. 安装计算节点



总结和答疑



无法配置外部网络

问题现象

- 在Horizon界面中，希望将网络WAN设置为“外部网络”，可是找不到设置外部网络的入口



故障分析及排除

- 原因分析
 - 外部网络只有管理员才能设置
- 解决办法
 - 注销当前用户，使用管理员admin设置外部网络



云主机无法PING通

问题现象

- 已经为云主机分配了浮动IP地址
- 可以通过SSH连接到云主机
- 远程PING云主机时，却请求超时



故障分析及排除

- 原因分析
 - 能够通过ssh通信，证明网络是通畅的
 - PING不通需要检查安全配置
- 解决办法
 - 设置安全组规则，允许ICMP协议进入

