Tedu.cn
达内教育

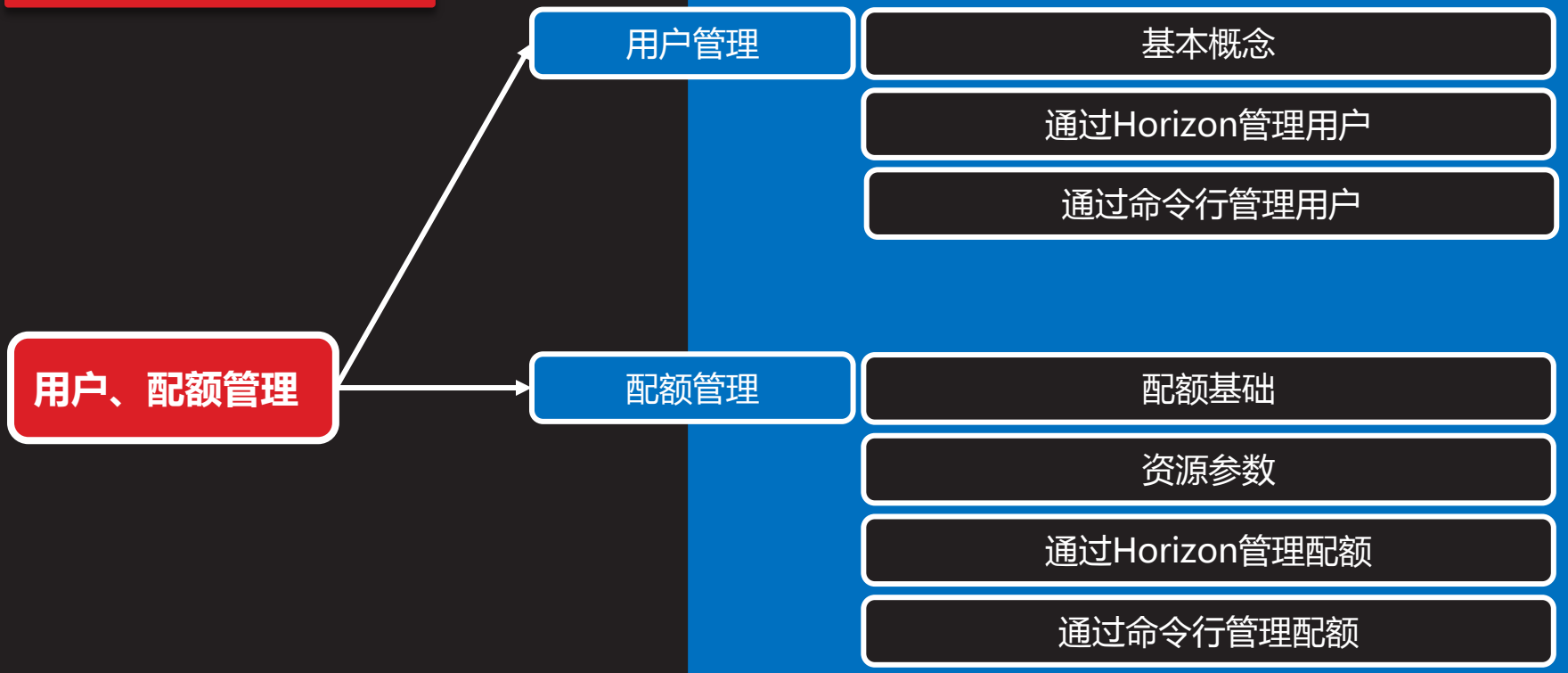
云计算部署与管理

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、配额管理
用户管理
基本概念
通过Horizon管理用户
通过命令行管理用户
配额管理
配额基础
资源参数
通过Horizon管理配额
通过命令行管理配额

Tedu.cn
达内教育

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

知识讲解

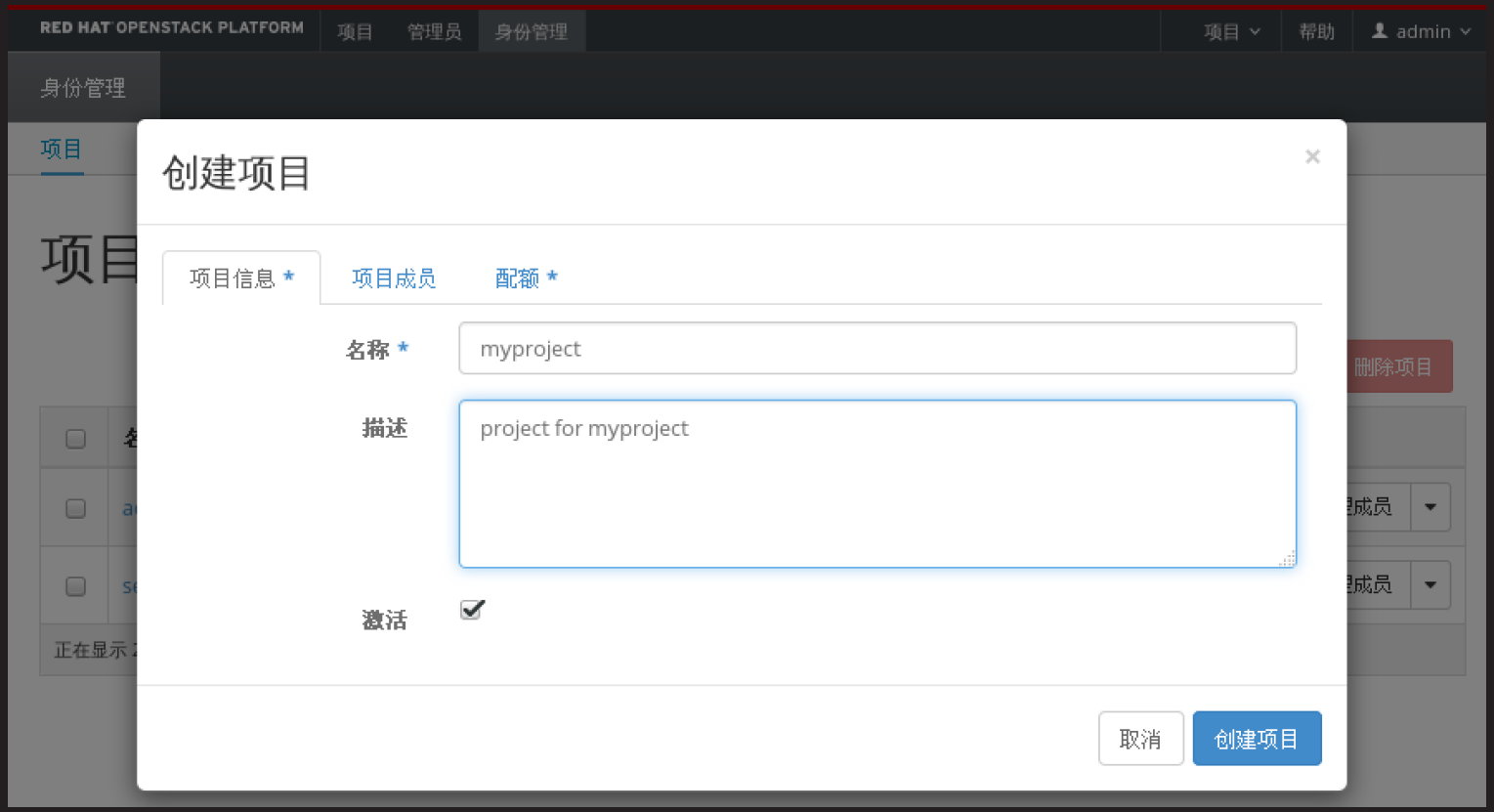
基本概念（续1）

- 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

知识讲解

通过Horizon管理用户

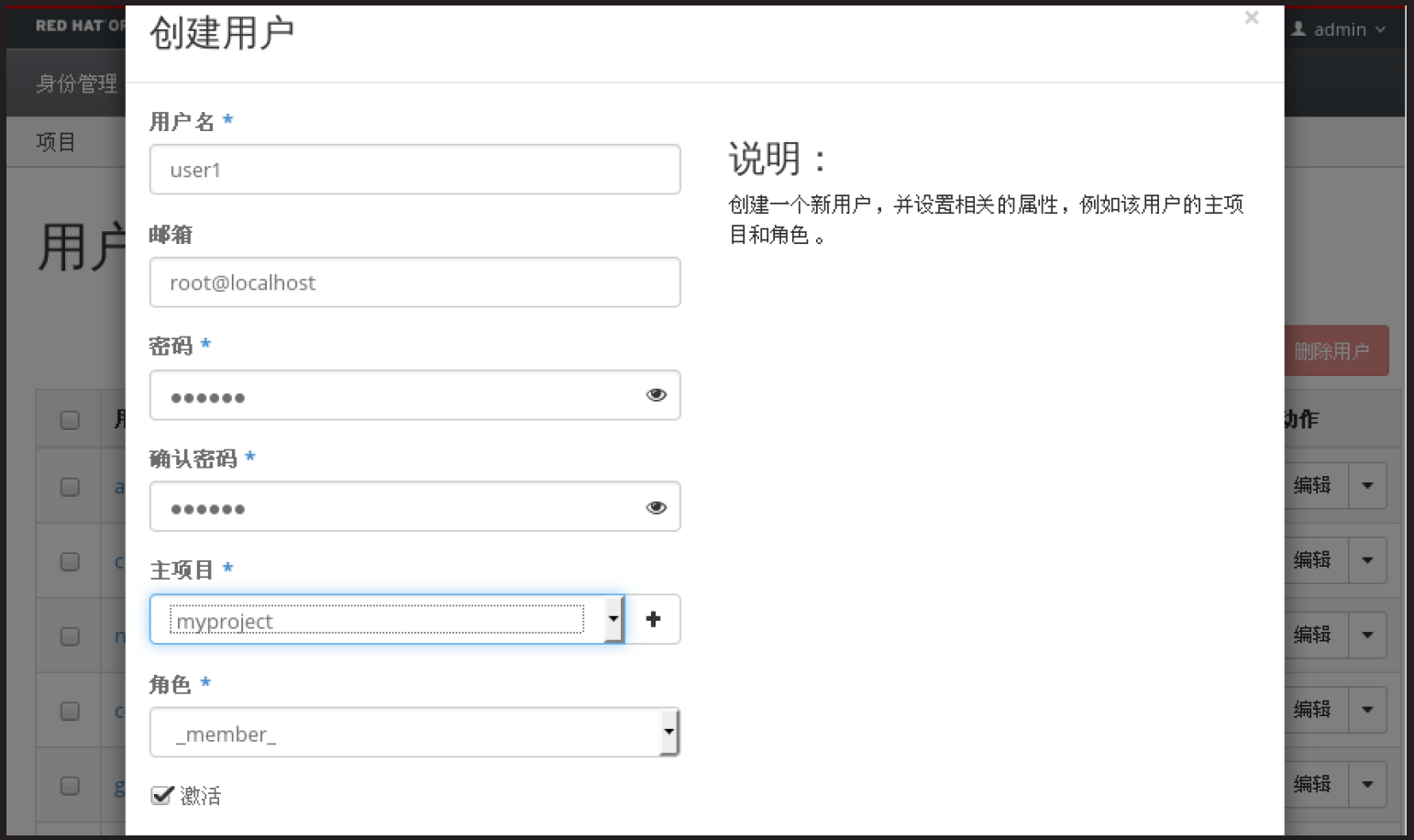
- 首先，创建名为myproject项目，保持默认配置



知识讲解

通过Horizon管理用户（续1）

- 创建user1用户，指定项目为myproject



知识讲解

通过命令行管理用户

知识讲解

- 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）

知识讲解

- 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）

知识讲解

- 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

Tedu.cn
达内教育

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

知识讲解

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

知识讲解

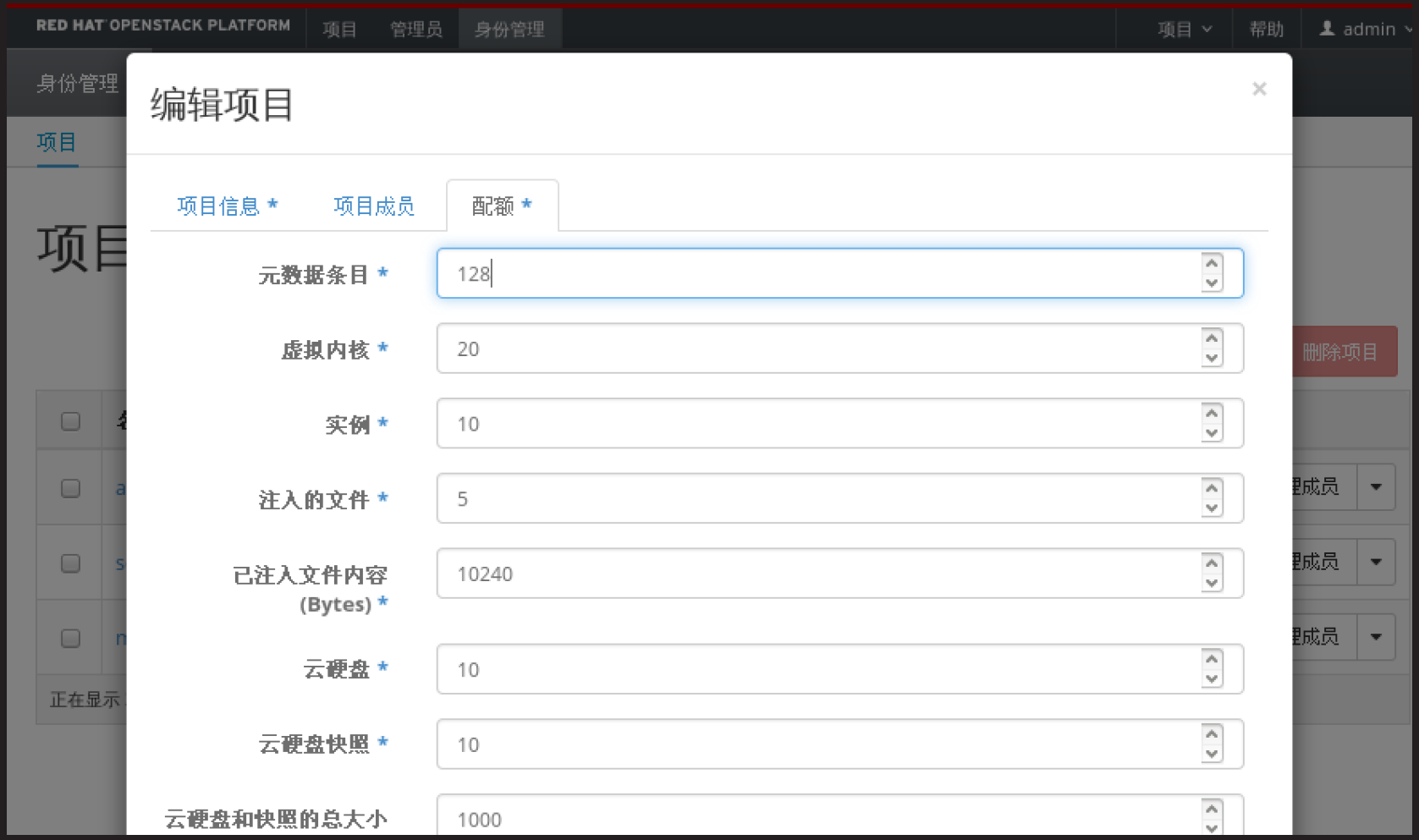
资源参数（续1）

- 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

知识讲解

通过Horizon管理配额

知识讲解



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

知识讲解

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

课堂练习

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

Tedu.cn
达内教育

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

知识讲解

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

知识讲解

通过Horizon管理云主机类型

知识讲解

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
m1.tiny	1	512MB	1GB	0GB	0 MB	1	True	{}	编辑云主机类型
m1.small	1	2GB	20GB	0GB	0 MB	2	True	{}	编辑云主机类型
m1.medium	2	4GB	40GB	0GB	0 MB	3	True	{}	编辑云主机类型
m1.large	4	8GB	80GB	0GB	0 MB	4	True	{}	编辑云主机类型
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

知识讲解

- 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

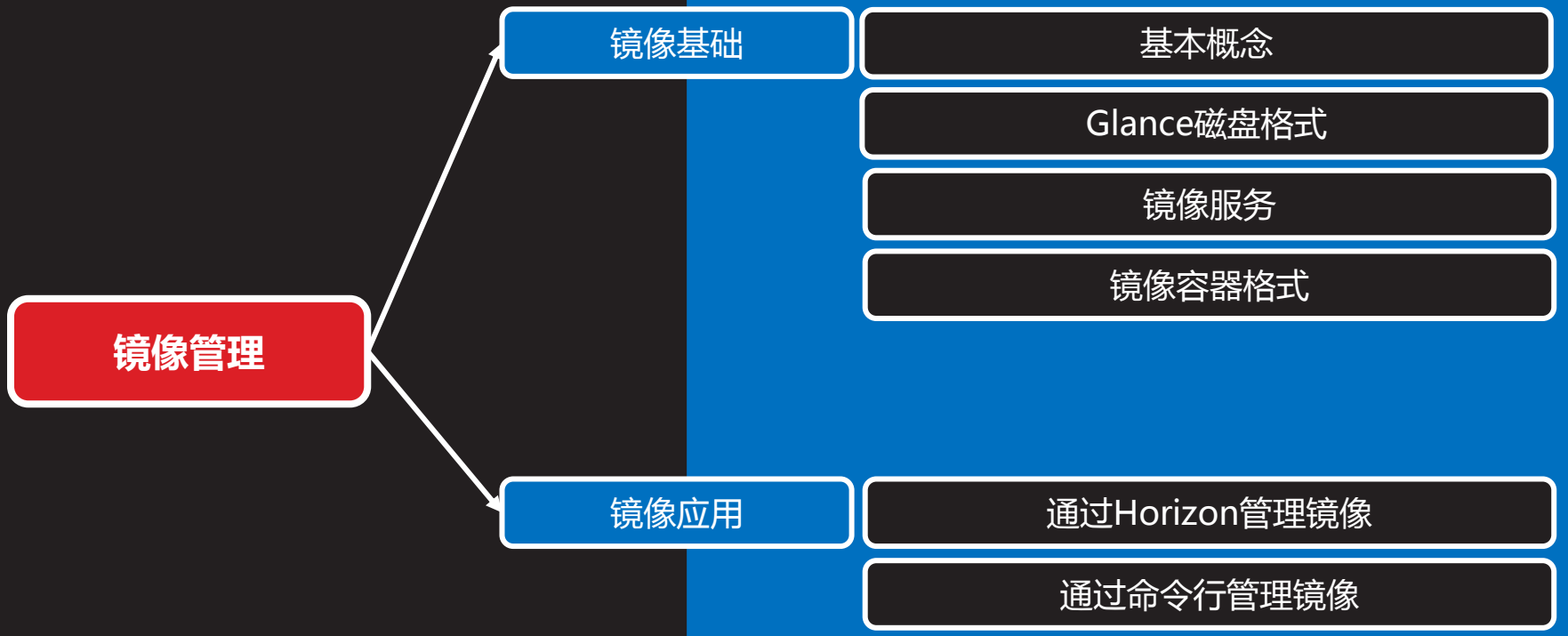
  [root@vh02 ~(keystone_admin)]# openstack flavor delete demo.tiny

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

课堂练习

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

Tedu.cn
达内教育

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

知识讲解

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

知识讲解

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

知识讲解

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

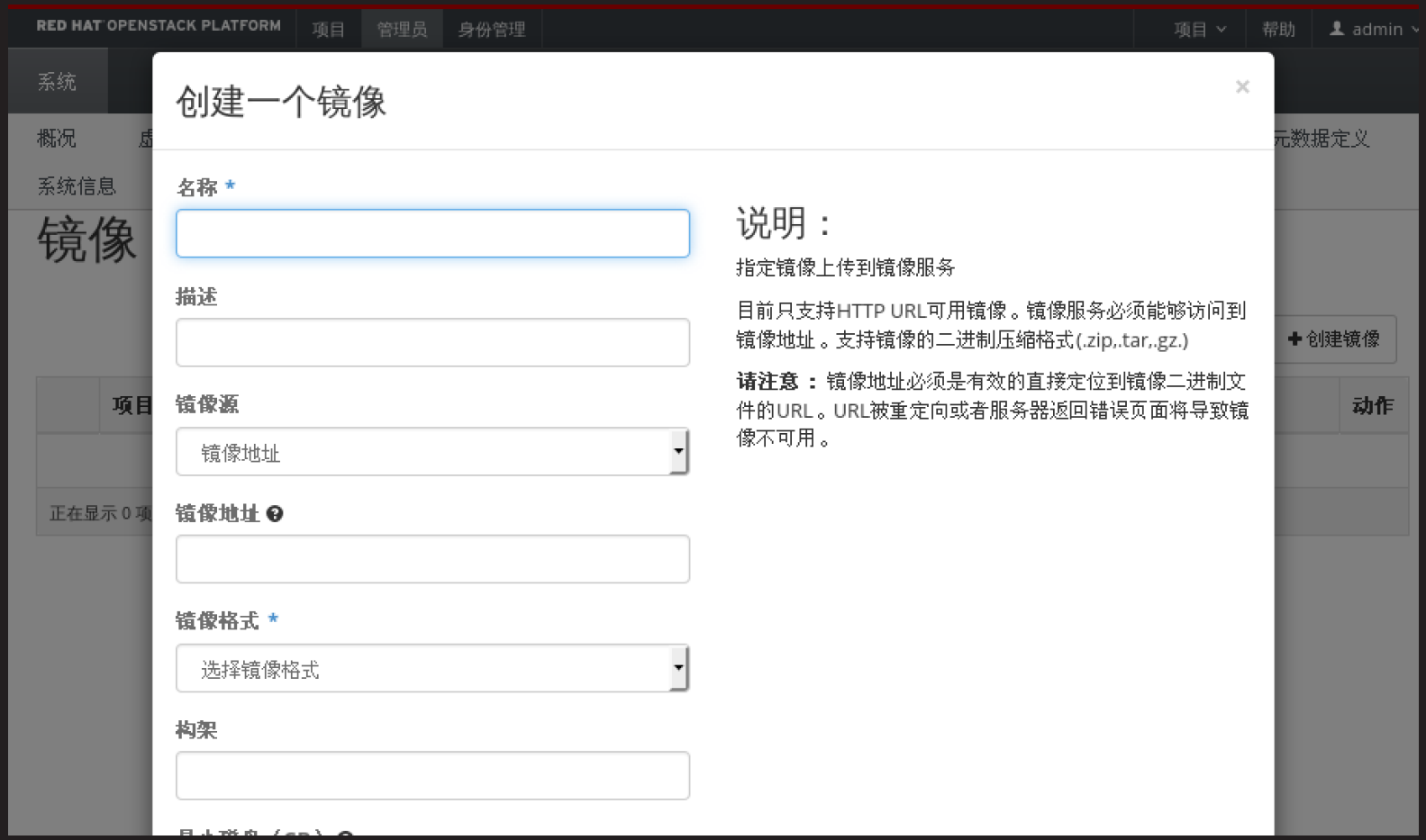
知识讲解

Tedu.cn
达内教育

镜像应用

通过Horizon管理镜像

知识讲解



通过命令行管理镜像

知识讲解

- 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）

知识讲解

- 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

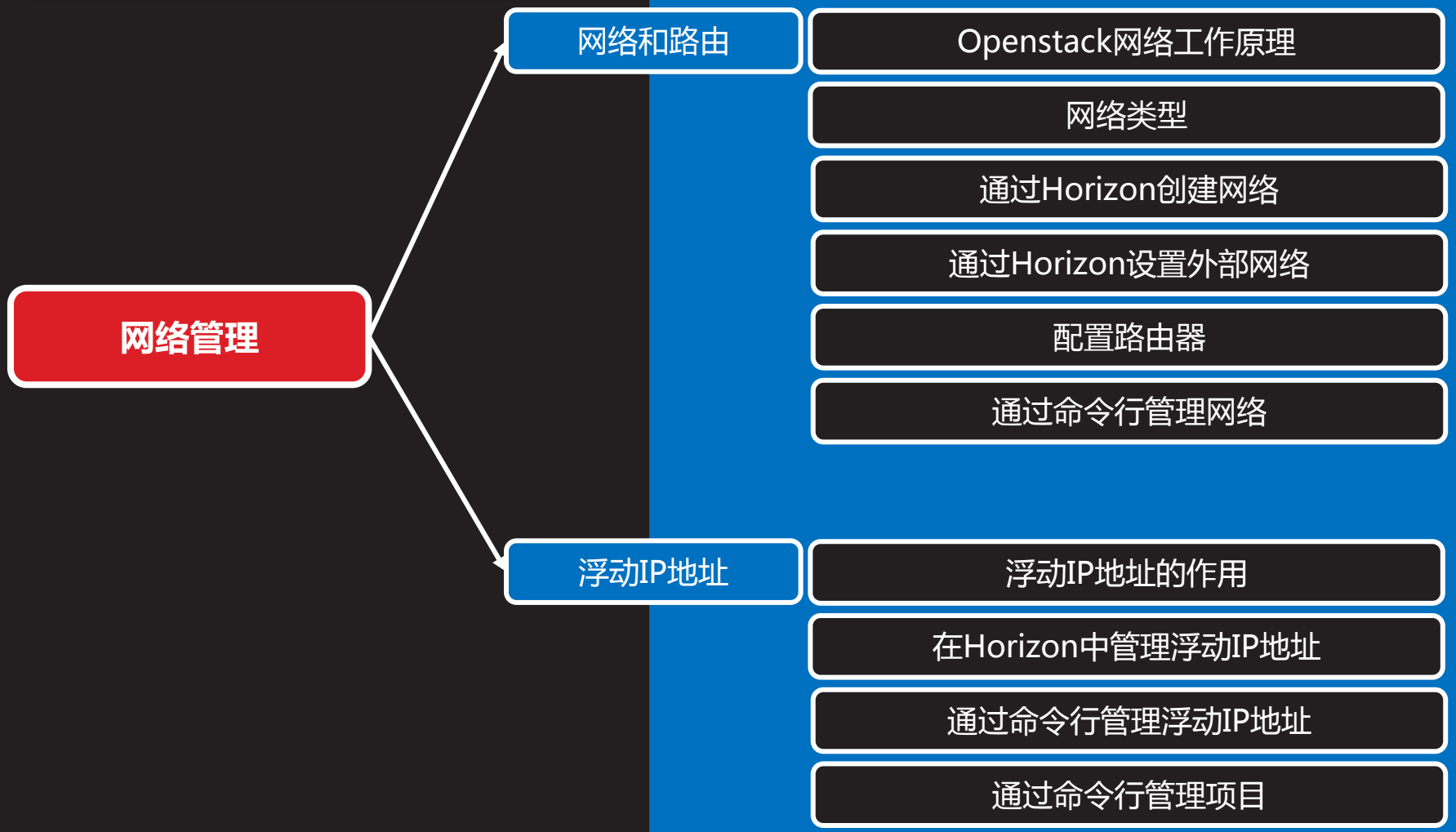
  [root@vh02 ~(keystone_admin)]# openstack image delete small_rhel6

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

课堂练习

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

Tedu.cn
达内教育

网络和路由

Openstack网络工作原理

知识讲解

- 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

知识讲解

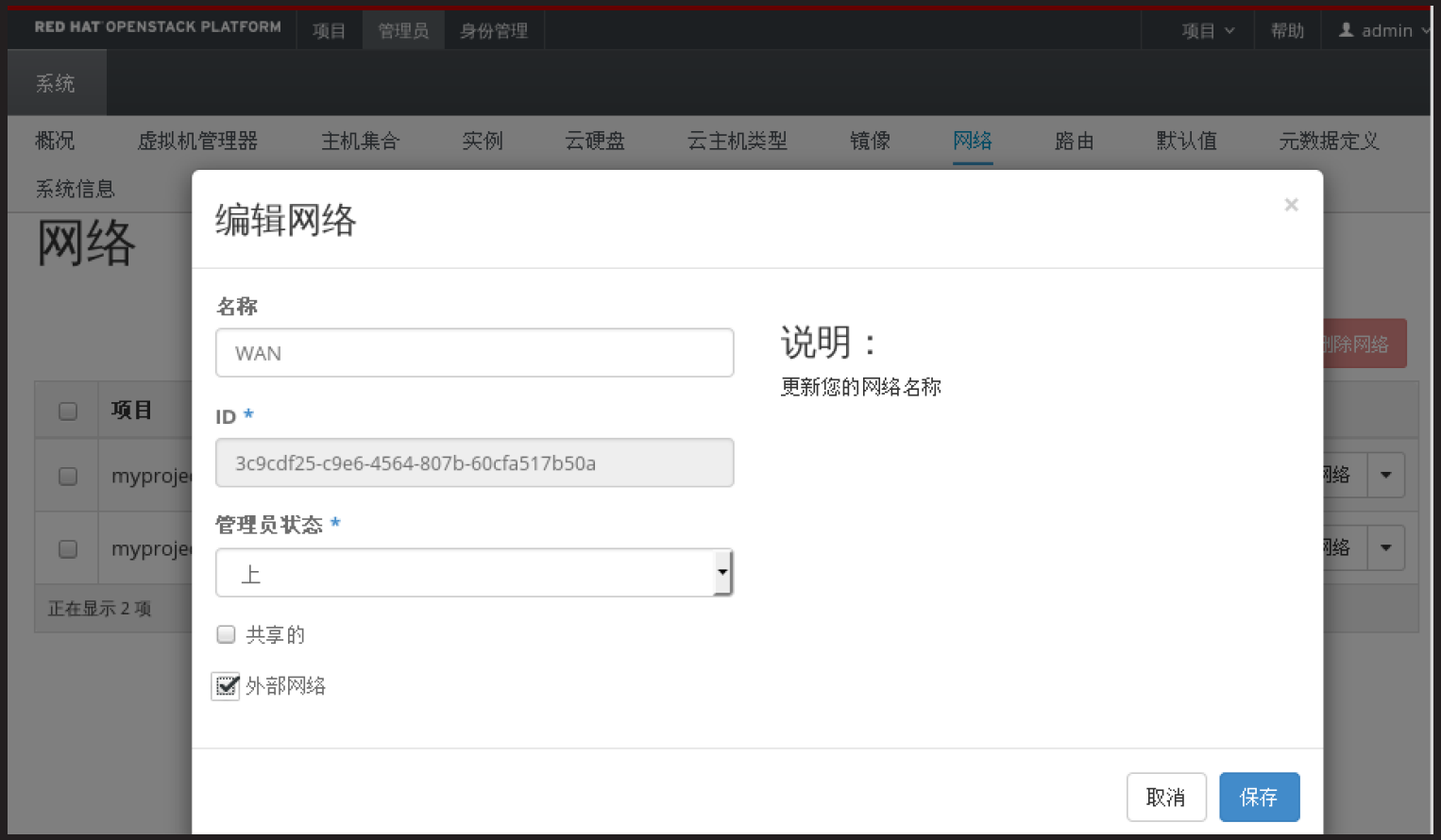
通过Horizon创建网络

- 项目网络由租户在自己的项目中创建

知识讲解

通过Horizon设置外部网络

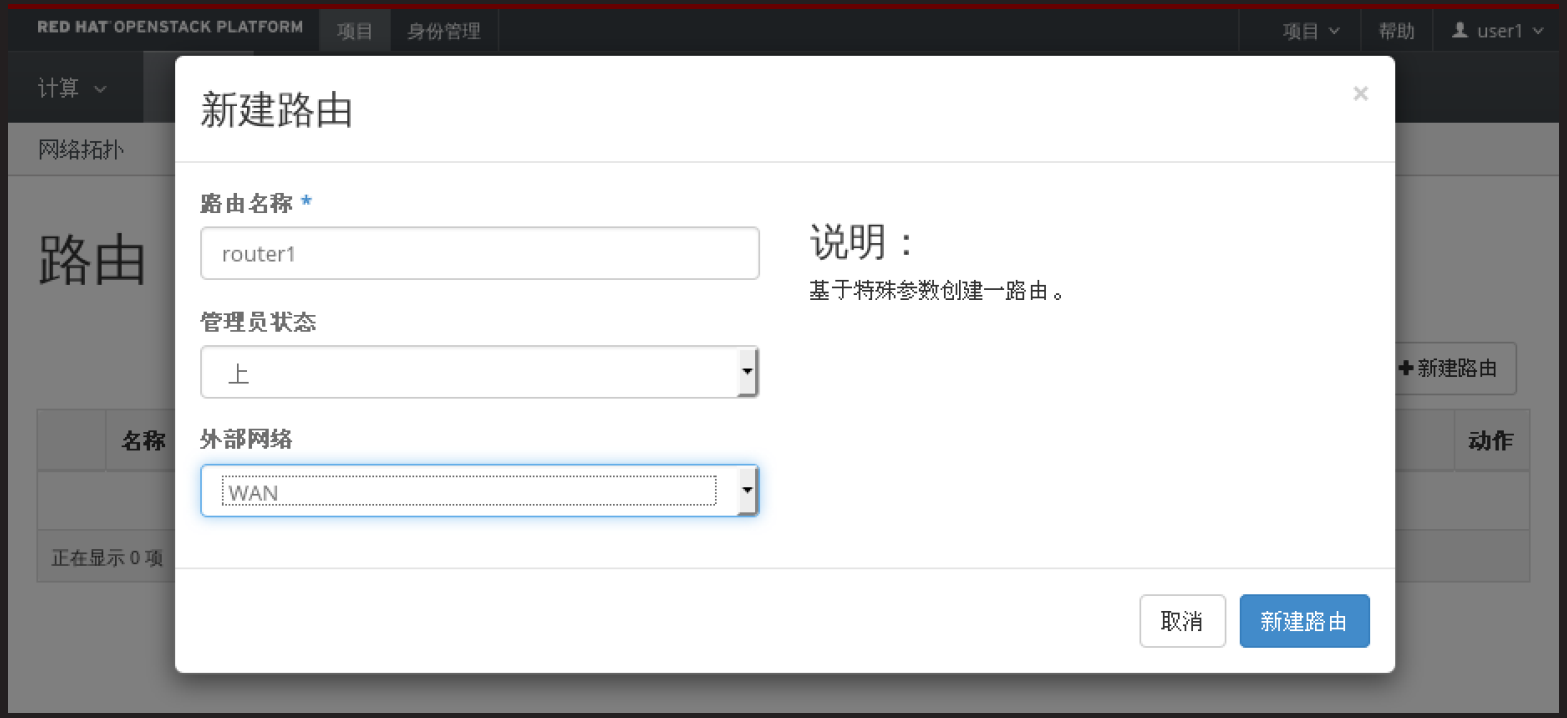
- 外部网络只有管理员有权限设置



知识讲解

配置路由器

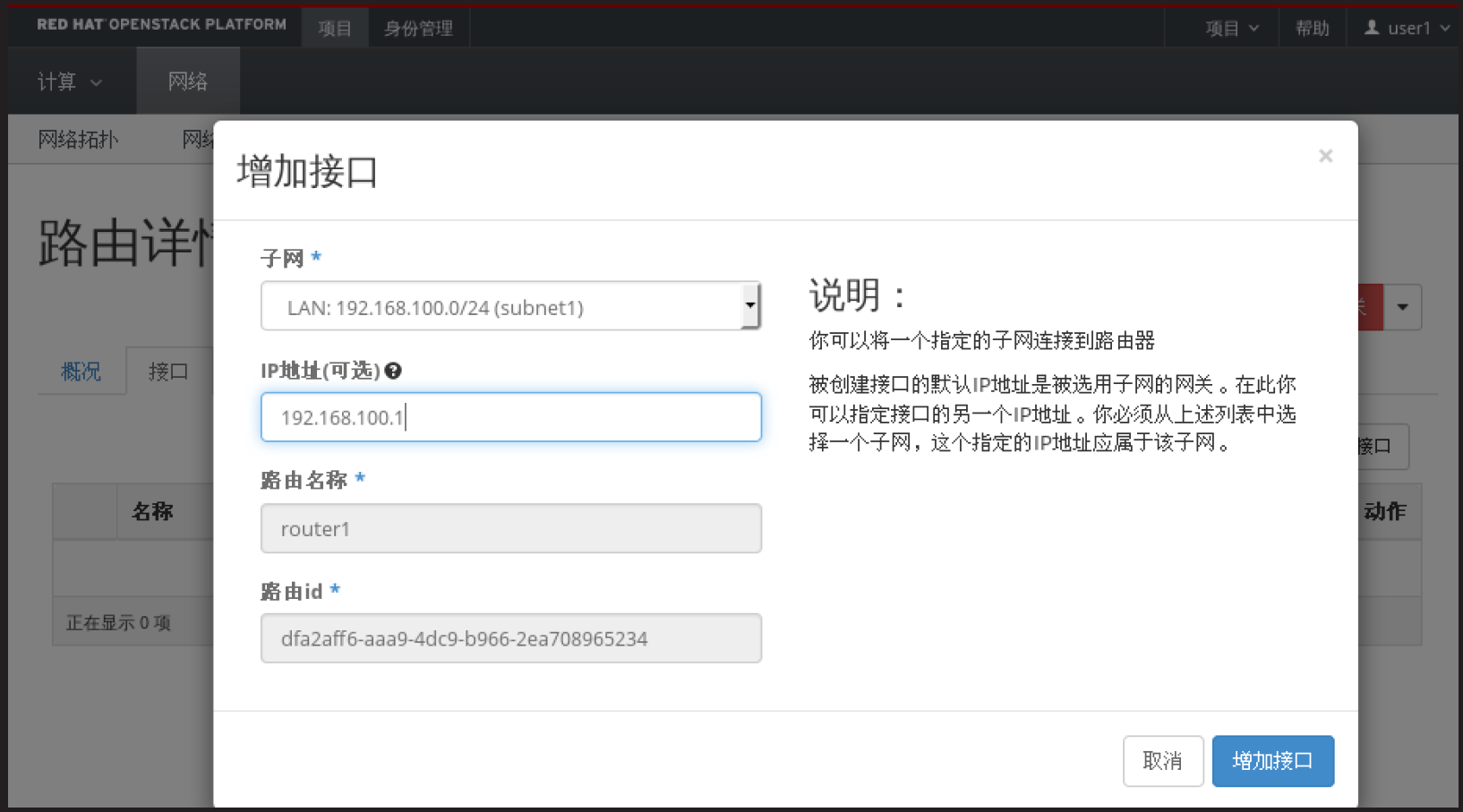
- 内外网通过路由器连接起来



知识讲解

配置路由器（续1）

- 创建路由接口，与内网相连



知识讲解

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

知识讲解

通过命令行管理网络（续1）

知识讲解

- 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

课堂练习

Tedu.cn
达内教育

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

知识讲解

在Horizon中管理浮动IP地址

知识讲解

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

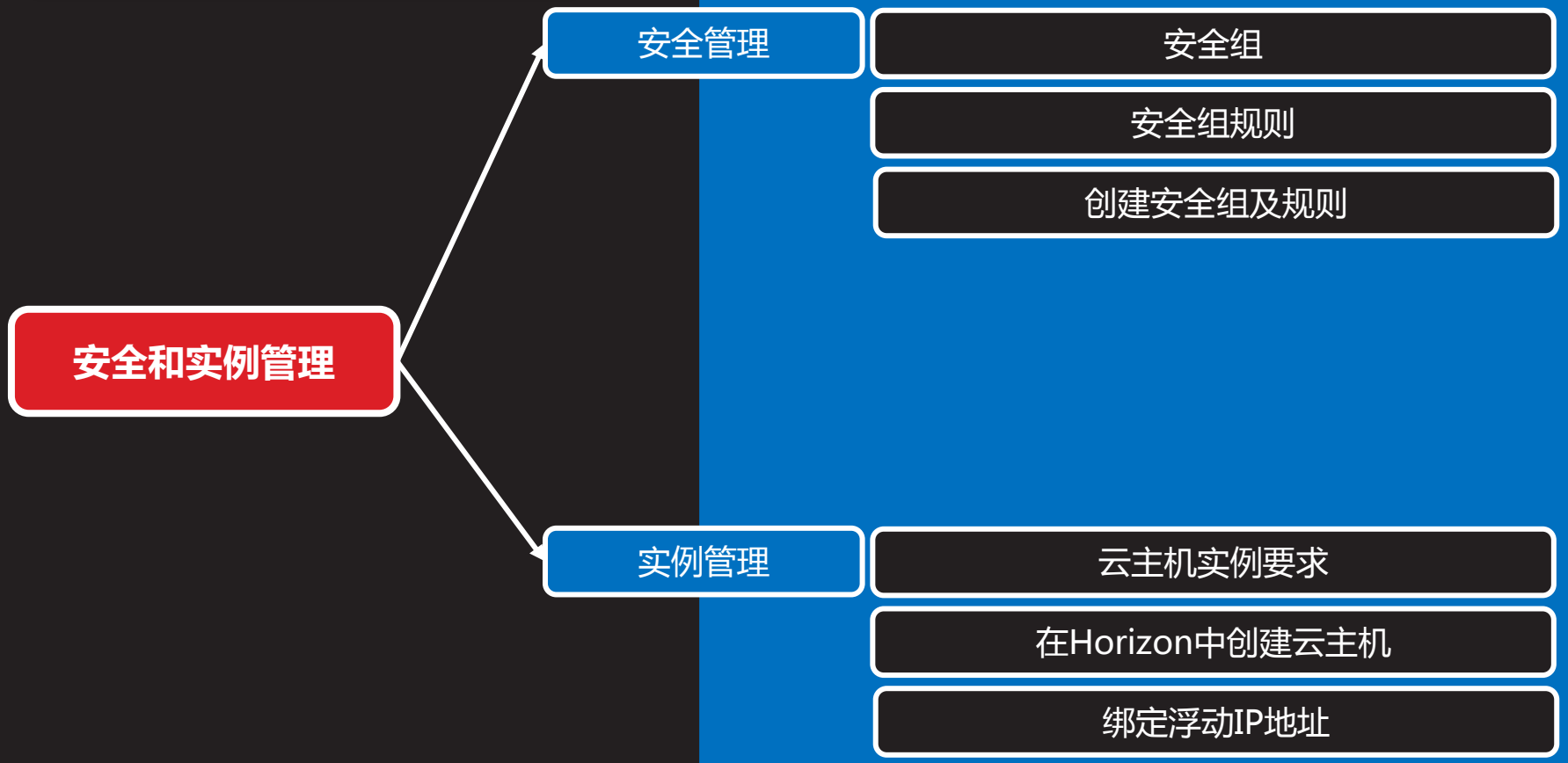
知识讲解

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

课堂练习

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

Tedu.cn
达内教育

安全管理

安全组

- 安全组用于控制对虚拟机实例的访问
- 安于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

知识讲解

安全组规则

知识讲解

- 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

知识讲解

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

知识讲解

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

课堂练习

Tedu.cn
达内教育

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

知识讲解

在Horizon中创建云主机

知识讲解

绑定浮动IP地址

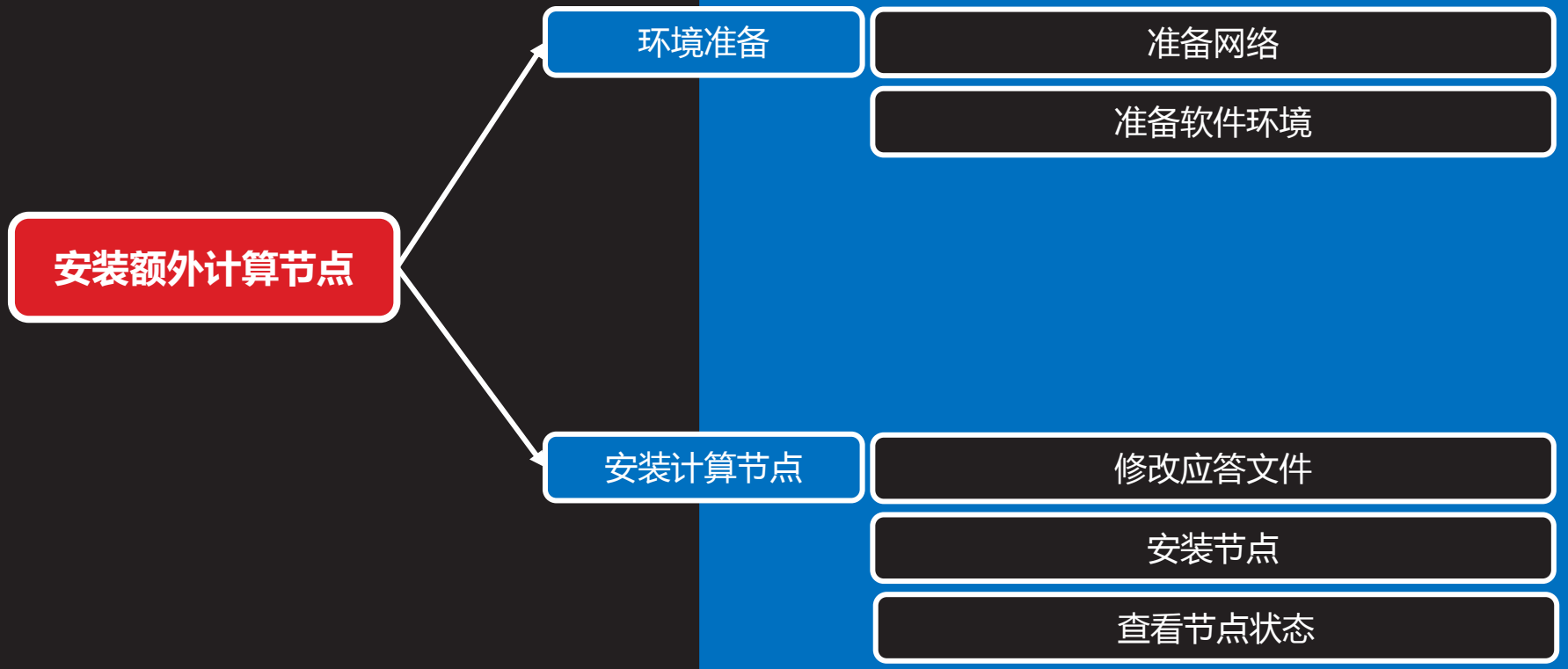
- 远程主机通过访问浮动IP地址来访问云主机

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

课堂练习

安装额外计算节点



Tedu.cn
达内教育

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

知识讲解

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

知识讲解

Tedu.cn
达内教育

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
```

知识讲解

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

知识讲解

查看节点状态

- 安装后的状态如图所示

知识讲解

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

课堂练习

总结和答疑

Tedu.cn
达内教育

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

知识讲解

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

知识讲解

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

知识讲解

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

知识讲解