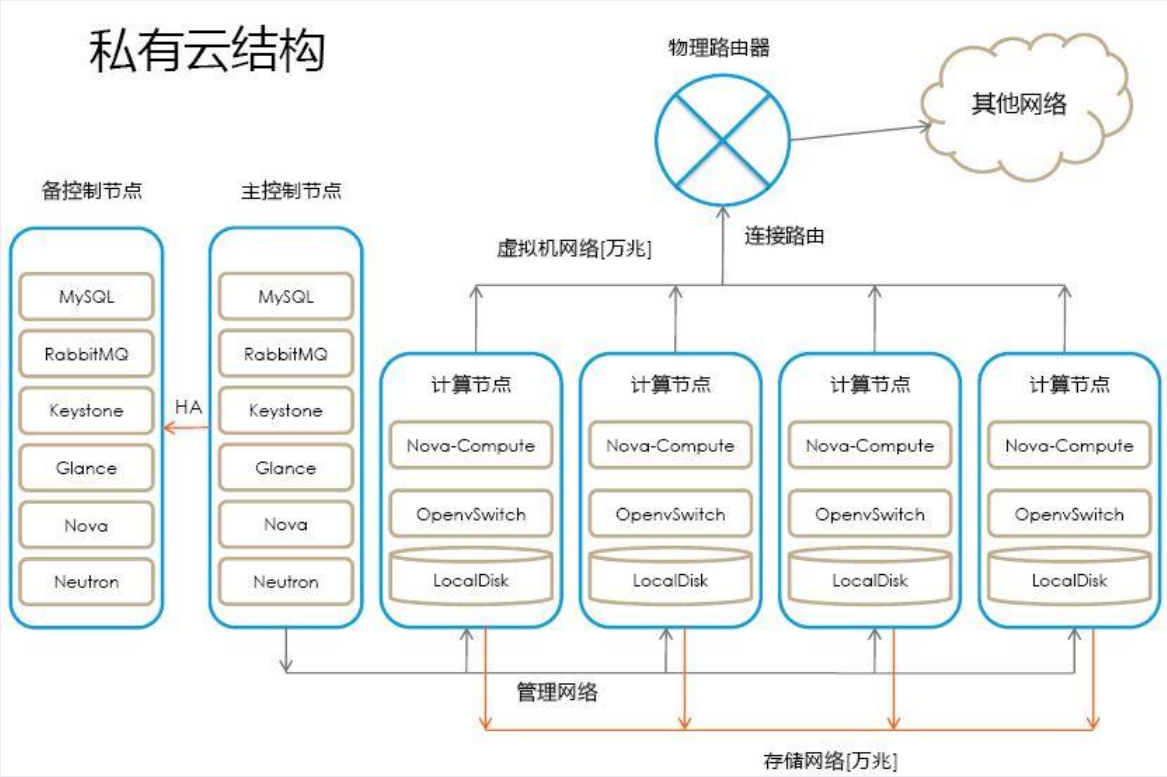
OpenStack

云计算基础

回顾



- 主控节点由哪些组件组成？备控节点的用途是什么？
- 计算节点\存储节点由哪些组件组成？
- SDN采用什么组件？

1

云平台系统构建基础工作

按云平台的网络拓扑结构图进行设备准备与网络连接，完成云平台系统安装基础工作：

- 准备OpenStack搭建云计算平台项目所需的软件资源
- 确定各节点的名称
- 配置各节点的IP网络地址
- 按要求安装各节点的操作系统
- 配置系统环境变量
- 在控制节点、网络节点、实例节点和存储节点分别修改，完成各节点的配置安装
- 验证安装基础工作

云计算平台的系统架构

任务实现

节点部署服务示意图

- 控制节点 组件

  MySQL

  RabbitMQ，Memcache

  Keystone

  Glance；Nova；Neutron

- 实例节点 组件

  Nova；Neutron

- 实例节点 组件

  Swift；Cinder

2

云平台系统安装基础工作

与Linux相关的操作知识—yum

01 可以同时配置多个资源库(Repository)

02 简洁的配置文件(/etc/yum.conf，/etc/yum.repos.d 下的文件)

03 自动解决增加或删除rpm包时遇到的倚赖性问题

04 使用方便

05 保持与RPM数据库的一致性

OpenStack程序化配置

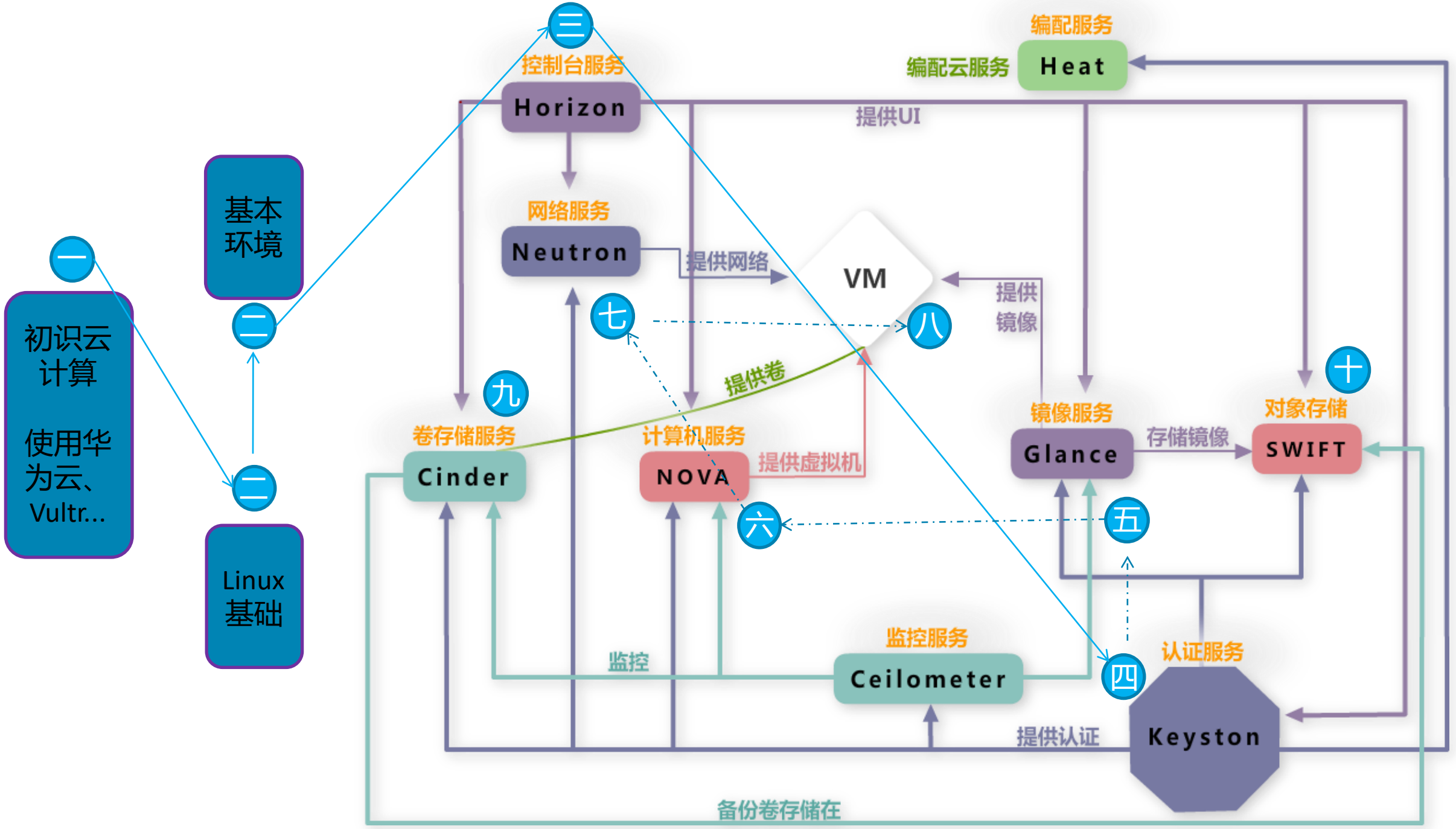
```
#!/bin/bash

##### 用户配置区 开始 #####################
# 将此脚本放在/root目录; chmod +x install_basic.sh; ./install_basic.sh
##### 用户配置区 结束  #####################

#--------------------------------------------
# 安装OpenStack基本环境
#--------------------------------------------
hostipaddress=127.0.0.1

#) 设定主机名字
hostnamectl set-hostname controller
cat >> /etc/hosts <<EOF
#127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
#::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
$hostipaddress controller
EOF

#--------------------------------------------
# 安装OpenStack基本环境
# 禁用防火墙；关闭Selinux
#--------------------------------------------
systemctl stop firewalld.service
systemctl disable firewalld.service
systemctl status firewalld.service
setenforce 0
......
```

项目3

身份认证服务

任务01 keystone管理认证用户

任务02 创建租户、用户并绑定用户权限


一
初识云计算
使用华为云、Vultr...
二
基本环境
二
Linux基础
三
控制台服务
Horizon
编配服务
编配云服务
Heat
提供UI
网络服务
Neutron
提供网络
VM
七
八
提供镜像
九
提供卷
卷存储服务
Cinder
计算机服务
NOVA
提供虚拟机
六
镜像服务
Glance
存储镜像
对象存储
SWIFT
十
五
监控
监控服务
Ceilometer
四
认证服务
Keyston
提供认证
备份卷存储在

学习目标

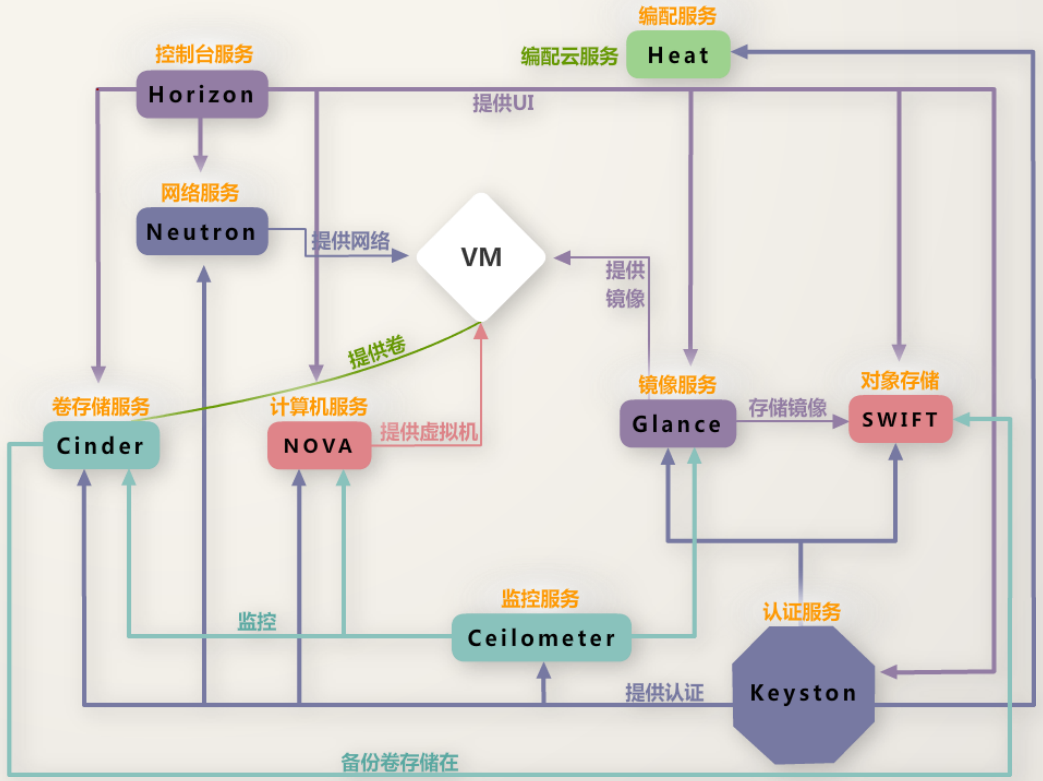
- 了解Keystone的基本概念
- 理解Keystone的服务流程
- 掌握项目、用户的不同创建方法
- 掌握Keystone基本使用方法

Keystone管理认证用户

1

KeyStone是OpenStack基础支持服务，keystone有如下作用:

- 管理用户和权限
- 维护OpenStack Services的Endpoint
- 认证（Authentication）和鉴权（Authorization）



1

keystone管理认证用户

相关概念

```
[root@controller ~]# more admin-openrc
export OS_USERNAME=admin
export OS_PASSWORD=123456
export OS_PROJECT_NAME=admin
export OS_USER_DOMAIN_NAME=Default
export OS_PROJECT_DOMAIN_NAME=Default
export OS_AUTH_URL=http://controller:5000/v3
export OS_IDENTITY_API_VERSION=3
export OS_IMAGE_API_VERSION=2
[root@controller ~]# openstack user list
+----------------------------------+-----------+
| ID                               | Name      |
+----------------------------------+-----------+
| 3160471e8dfd42ce86cb2841ec008cf3 | myuser    |
| 66485da943284391b1d766141401f67a | placement |
| 8fa781f0a3f949bea5eef3f0c34d448a | glance    |
| c05c25620aa14b6891f03679cbe9b3fe | nova      |
| ee4ba4cfff6a42aea67cef4463efe376 | admin     |
| f39c4bd536594a52bd726d575009420a | neutron   |
+----------------------------------+-----------+
```

显示 13 项

用户名	描述
stu	-
glance	-
ceilometer	-
nova	-
cinder	-
demo	-

用户（User）

User是使用OpenStack服务的实体，可以是人，也可以是其他系统或者服务。

如 除admin和demo用户外，OpenStack为nova、cinder、glance、neutron等服务创建相应的User。

OpenStack通过注册相关服务用户来管理服务，如Nova服务注册nova用户来管理相应的服务。

1

keystone管理认证用户

相关概念

角色（Role）

安全中
认证：解决“你是谁？”的问题；
鉴权：解决“你能干什么？”的问题，
Keystone借助Role来实现“鉴权”。

角色代表一组用户可以访问的资源权限：
1. User可分配一个或多个Role；
2. Service决定每个Role能做什么；
3. Service通过policy.json文件对Role进行访问控制。

```
[root@controller ~]# openstack role list
+----------------------------------+--------+
| ID                               | Name   |
+----------------------------------+--------+
| 392a0b02818a41c6aa46d410071bb7d2 | member |
| 5a720f30c567440395a33cf266a924c6 | admin  |
| b2b0147f4b524eb09d614cc922bd8eaf | reader |
| e315fcfe907f4cb0b691c4bad1f46234 | myrole |
+----------------------------------+--------+
```

1

keystone管理认证用户

相关概念

认证（Authentication）

认证（Authentication）是 KeyStone验证User身份的过程。

User访问OpenStack 需要提供用户名和密码，Keystone验证通过后会给User签发一个Token作为后续访问的凭证。

用户在随后的请求中使用这个令牌去访问资源中其他应用，此时非使用用户名/密码（安全；效率）。

1

keystone管理认证用户

相关概念

证书（Credentials）

Credentials是User用来证明自己的身份信息，可以是：
1 .用户名、密码;
2. API key ;
3. 其他认证方式。

令牌（Token）

Token通常数字和字母组成的字符串；用来作为访问资源的记号。
User 成功通过 Keystone 认证后， Token 由 Keystone分配给用户。
1. 令牌的有效期是有限的，可以随时被撤回（默认Token有效期为24小时）；
2. Token用作访问Service的认证信息;
3. Service会通过Keystone验证Token。

1

Keystone管理认证用户

相关概念

服务（Service）

OpenStack的Service包括Compute(Nova)、Block Storeage(Cinder)、Object Storage（Swift）...等；Service提供特定功能，通过端点（Endpoint）访问。

端点（Endpoint）

端点（Endpoint）是一个网络访问地址，通常是URL。服务Service通过Endpoint暴露自己的API。
Service的Endpoint由Keystone维护。

```
[root@controller ~]# openstack service list
+----------------------------------+-----------+-----------+
| ID                               | Name      | Type      |
+----------------------------------+-----------+-----------+
| 35f684d7db2c44ca9b65691f9054ba07 | placement | placement |
| 9508fd7b0de942438323ed539794d741 | glance    | image     |
| 99e6156fed73476e8d16ebbc92be6a3f | keystone  | identity  |
| b3268d566159495e83ade2a249619958 | nova      | compute   |
| b43292f21ed94f9998624afbaee12d00 | neutron   | network   |
+----------------------------------+-----------+-----------+
```

```
[root@controller ~]# openstack endpoint list
+----------------------------------+----------+--------------+--------------+---------+-----------+----------------------------+
| ID                               | Region   | Service Name | Service Type | Enabled | Interface | URL                        |
+----------------------------------+----------+--------------+--------------+---------+-----------+----------------------------+
| 134f60a3d10443579f1c210a13d97d96 | RegionOne | keystone     | identity     | True    | admin     | http://controller:5000/v3/ |
| 25081232269142d2a1b393f386f96700 | RegionOne | glance       | image        | True    | public    | http://127.0.0.1:9292      |
| 2b7721972cb24849b3a8a7684559f9bf | RegionOne | glance       | image        | True    | admin     | http://127.0.0.1:9292      |
| 32d6fd9627da4fb1b5df11206f7df6d2 | RegionOne | placement    | placement    | True    | public    | http://controller:8778     |
| 44d3731948f84b8b88066d12eed44b47 | RegionOne | glance       | image        | True    | internal  | http://127.0.0.1:9292      |
| 5e664076ec8e4ee6a33943db7183eee0 | RegionOne | neutron      | network      | True    | public    | http://controller:9696     |
| 661cdf4519684cf2b8fa484961e834ac | RegionOne | placement    | placement    | True    | admin     | http://controller:8778     |
| 686192ec7ed94480b14b96eb2aa06580 | RegionOne | keystone     | identity     | True    | public    | http://controller:5000/v3/ |
| 6bc365392ba04aab8c5ea167ea446041 | RegionOne | keystone     | identity     | True    | internal  | http://controller:5000/v3/ |
| a994c05892f94f91afe27eb497ae23d0 | RegionOne | placement    | placement    | True    | internal  | http://controller:8778     |
| b4b042afb7724f53b35fc7f8737d5687 | RegionOne | nova         | compute      | True    | admin     | http://controller:8774/v2.1 |
| bce19c2c536f43ceb43f75dd3c5c9937 | RegionOne | nova         | compute      | True    | public    | http://controller:8774/v2.1 |
| bf310507f3c045719af9c923cfb07c09 | RegionOne | neutron      | network      | True    | admin     | http://controller:9696     |
| f53e9d6f62e140ca934967fd47473b51 | RegionOne | nova         | compute      | True    | internal  | http://controller:8774/v2.1 |
| ff018daa13dd4183872d7492df7a7e6a | RegionOne | neutron      | network      | True    | internal  | http://controller:9696     |
+----------------------------------+----------+--------------+--------------+---------+-----------+----------------------------+
```

1

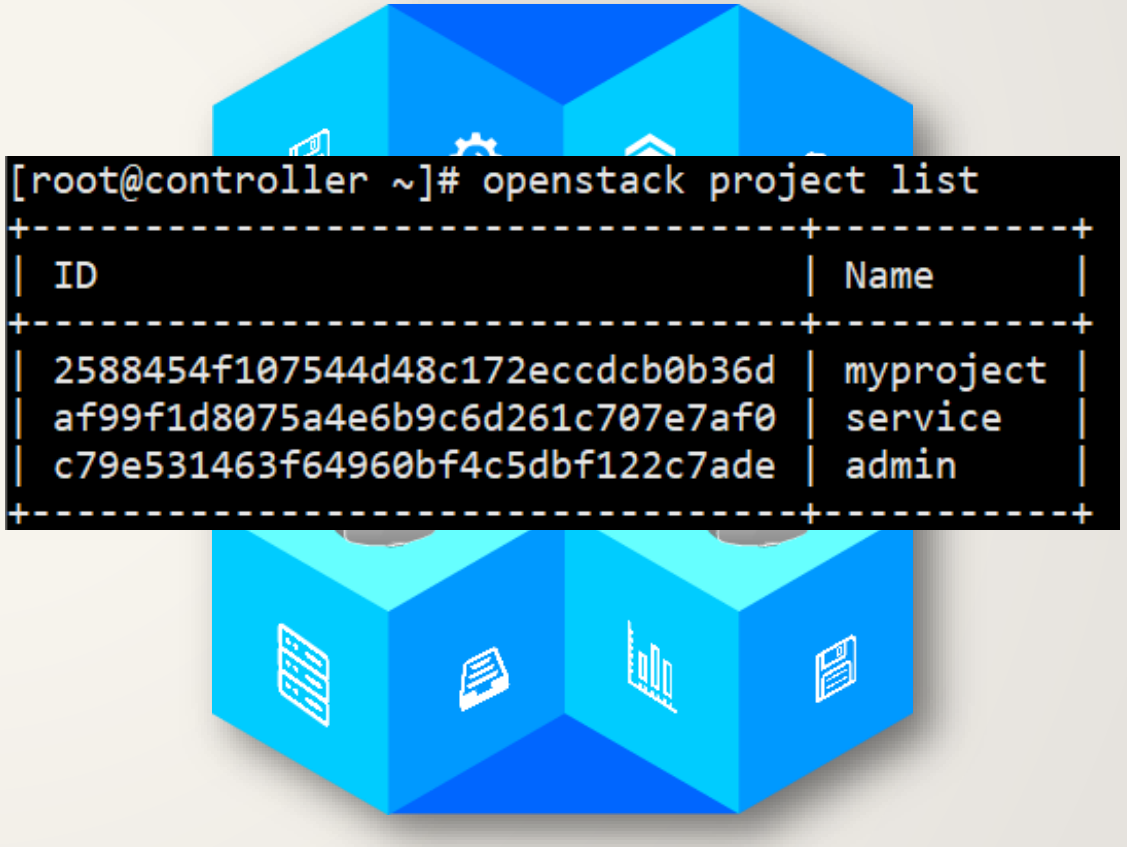
Keystone管理认证用户

相关概念

租户（Project）

项目用于将OpenStack的资源（计算、存储、网络）进行分组和隔离。

1. 资源属于租户，而不是User；
2. OpenStack中， Tenant/Project/Account是通用的；
3. 必须为User指定Project，User才能访问资源。一个User可以有多个项目。



1

Keystone管理认证用户

相关概念

使用云服务的用户不局限于是人，也可以是系统或者服务。
用户可以通过指定的令牌登陆系统并调用资源。
用户可以被分配到特定项目并执行项目相关操作。

在平台构建完毕之后系统会创建_member_、admin两个用户权限，在系统中_member_表示系统的普通用户的权限，拥有系统的正常使用和对当前租户的管理权限。
admin角色是代表系统的管理员身份，对系统有绝对的管理权限。

1 keystone管理认证用户

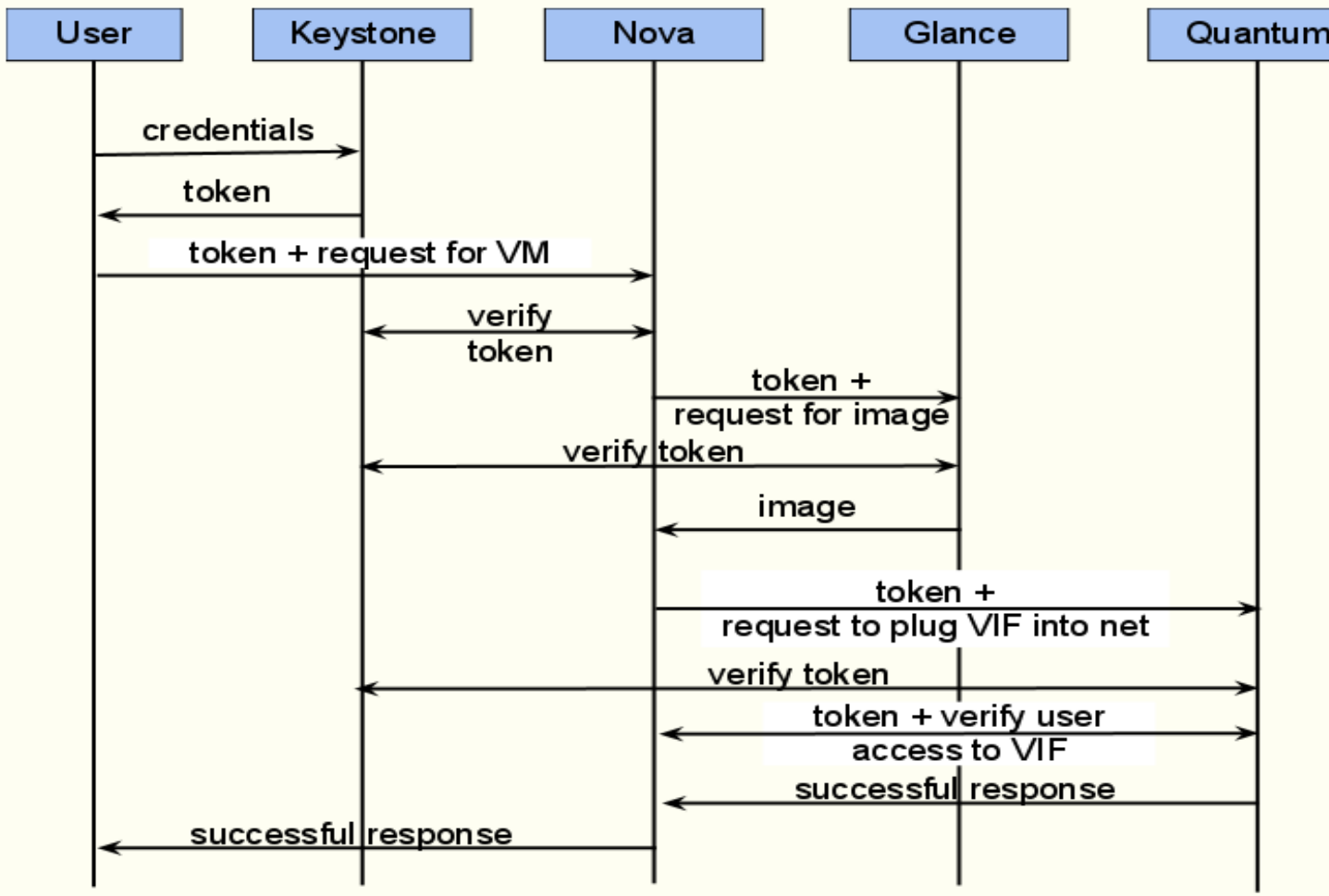
认证服务流程

1. User提供用户名密码请求登录；Keystone验证成功返回token给User；

2. User使用token请求Nova提供服务，Nova会去Keystone查询User Token的有效性；

3. Nova确认token有效后，
   3.1 Nova使用该token请求Glance服务；同前，Glance会向Keystone验证令牌有效性；确认有效后返回image给Nova；
   3.2 Nova使用该token请求Neutron服务；Nuetron向Keystone验证token有效性，确认后提供网络服务；

4. Nova反馈操作结果至用户。



服务申请认证机制流程

keystone管理认证用户

配置keystone应用环境

安装Keystone服务需要以下步骤：

1. 创建Keystone数据库；
2. 安装Apache HTTP服务器来服务认证请求；
3. 创建Keystone服务实体和API端点；
4. 创建域、项目、用户和角色。

Keystone服务主配置文件存放在/etc/keystone，名为keystone.conf，在配置文件中需要配置初始的token值和数据库的连接地址等。

keystone管理认证用户

配置keystone应用环境

1. 创建keystone数据库并授权

Keystone后台数据库采用MySQL数据库

具体命令如下：

```
mysql -p123456
------------------------------
CREATE DATABASE keystone;  -- 创建数据库，名为keystone
GRANT ALL PRIVILEGES ON keystone.* TO 'keystone'@'localhost' IDENTIFIED BY 'keystone';  -- keystone授权
GRANT ALL PRIVILEGES ON keystone.* TO 'keystone'@'%' IDENTIFIED BY 'keystone';

flush privileges;
show databases;
select user,host from mysql.user;
exit
------------------------------
```

keystone管理认证用户

配置keystone应用环境

2. 安装keystone相关软件包

具体命令如下：

yum install openstack-keystone httpd mod_wsgi -y --- 安装Apache及wsgi
yum install openstack-keystone python-keystoneclient openstack-utils -y -- 提供CLI及openstack-config，方便配置

修改keystone配置 （注意以下方式和Vi区别）

openstack-config --set /etc/keystone/keystone.conf database connection mysql+pymysql://keystone:keystone@contro
openstack-config --set /etc/keystone/keystone.conf token provider fernet --- 令牌提供方式 uuid\ pki \ fernet

uuid 随机生成16进制序列

vi /etc/keystone/keystone.conf 手工设定上述值

3. 初始化keystone认证服务

具体命令如下：

```
keystone-manage bootstrap --bootstrap-password 123456 \
  --bootstrap-admin-url http://controller:5000/v3/ \
  --bootstrap-internal-url http://controller:5000/v3/ \
  --bootstrap-public-url http://controller:5000/v3/ \
  --bootstrap-region-id RegionOne
```

1）在endpoint表增加3个服务实体的API端点

2）在local_user表中创建admin用户

3）在project表中创建admin和Default项目（默认域）

4）在role表创建3种角色，admin，member和reader

5）在service表中创建identity服务

keystone管理认证用户

配置keystone应用环境

4. keystone认证服务端点（Endpoint）

云环境下每个服务运行在特定的URL和端口上，Keystone负责管理这些端点：

```
[root@controller ~(keystone_admin)]# openstack endpoint list
+----------------------------------+-----------+--------------+--------------+---------+-----------+----------
-------------------------------------+
| ID                               | Region    | Service Name | Service Type | Enabled | Interface | URL
                                     |
+----------------------------------+-----------+--------------+--------------+---------+-----------+----------
-------------------------------------+
| 0b4d0e3808fa4d48aecc0308d137e21e | RegionOne | gnocchi      | metric       | True    | admin     | http://19
2.168.0.32:8041                      |
| 0c557a51d6db497085b82cf27003c991 | RegionOne | cinderv3     | volumev3     | True    | public    | http://19
2.168.0.32:8776/v3/%(tenant_id)s     |
| 166d6701b1884ed0b297b1f8489ec326 | RegionOne | swift        | object-store | True    | admin     | http://19
2.168.0.32:8080/v1/AUTH_%(tenant_id)s |
| 16e6d1271132412bbcf36337749c07ac | RegionOne | glance       | image        | True    | internal  | http://19
2.168.0.32:9292                      |
| 1ae2ad0c2e0a496d9c2f65cc40767a9d | RegionOne | gnocchi      | metric       | True    | internal  | http://19
2.168.0.32:8041                      |
| 201bbd4aa90c43bb9fa28d70294fb3e3 | RegionOne | neutron      | network      | True    | public    | http://19
2.168.0.32:9696                      |
```

2 创建租户、用户并绑定用户权限

管理认证服务

为了方便用户调用这些服务，openstack为每一个服务提供一个用于访问的端点（endpoint）

如果需要访问服务，则必须知道他的端点

端点一般为url，我们知道服务的url，就可以访问它

端点的url具有public、private和admin三种权限

Public url可以被全局访问

private url只能被局域网访问

admin url被从常规的访问中分离出来。

4. 配置管理员账户的相关变量

具体命令如下：

vi admin-openrc -- 命名方式 任意
添加如下内容：

```
export OS_USERNAME=admin              --- 用户名
export OS_PASSWORD=123456             --- 密码
export OS_PROJECT_NAME=admin      --- 项目名称
export OS_USER_DOMAIN_NAME=Default   --- 用户所在域名称
export OS_PROJECT_DOMAIN_NAME=Default
export OS_AUTH_URL=http://controller:5000/v3   --- 认证URL
export OS_IDENTITY_API_VERSION=3          --- 认证版本号
export OS_IMAGE_API_VERSION=2             --- Image的认证版本号
```

3 keystone管理认证用户

Keystone环境使用

验证服务

Keystone服务安装完毕之后，可以通过请求身份令牌来验证服务。

具体命令如下（注意不同OpenStack版本区别）：

旧版

```
$keystone --os-username=admin --os-password=123456
--os-auth-url=http://172.24.0.10:35357/v2.0  token-get
//以admin用户访问http://172.24.0.10:35357/v2.0地址获取token值
```

新版

[root@openstack01 ~]# openstack --os-auth-url http://controller:5000/v3 --os-username=admin token issue

3 keystone管理认证用户

管理认证用户

创建用户

创建一个名称为“alice”账户，密码为“123456”、邮箱为“alice@example.com”。命令如下（注意不同OpenStack版本区别）：

旧版

```
$keystone user-create --name=alice --pass=123456 --email=alice@example.com
```

新版

```
openstack user create --domain default --password=12345 --email=alice@example.com alice
```

keystone管理认证用户

管理认证用户

创建租户

创建一个名为example的keystone域：

```
$openstack domain create --description "An Example Domain" example
```

为keystone系统环境创建名为service的项目提供服务：

```
$openstack project create --domain default --description "Service Project" service
```

keystone管理认证用户

管理认证用户

创建租户

创建myproject项目和对应的用户及角色：

```
$openstack project create --domain default --description "Demo Project" myproject
```

在默认域创建myuser用户：

```
$openstack user create --domain default --password=myuser myuser
```

keystone管理认证用户

管理认证用户

创建租户

在role表创建myrole角色：

```
$openstack role create myrole
```

将myrole角色添加到myproject项目中和myuser用户组中：

```
$openstack role add --project myproject --user myuser myrole
```

keystone管理认证用户

管理认证用户

作为管理员用户去请求一个认证的token：

```
$openstack --os-auth-url http://controller:5000/v3 \
  --os-project-domain-name Default --os-user-domain-name Default \
  --os-project-name admin --os-username admin token issue
```

keystone管理认证用户

例题

例题1：配置租户和用户

创建以下OpenStack项目：

myproject

testproj

创建以下OpenStack用户：

Robert应该是myproject的成员，并且应该是管理员。罗伯特的电子邮件地址应该是Robert@domain0.example.com。

George应该是myproject的一员。George的电子邮件地址应该是George@domain0.example.com。

William应该是testproj的成员，并且应该是管理员。威廉的电子邮件地址应该是 William@domain0.example.com。

John 应该是testproj的成员。John的电子邮件地址应为John@domain0.example.com。

所有用户帐户的密码是redhat。

keystone管理认证用户

例题

答案:

source admin-openrc

openstack project create myproject
openstack project create testproj

openstack user create --project myproject --password redhat --email Robert@domain0.example.com Robert
openstack user create --project myproject --password redhat --email George@domain0.example.com George
openstack role add --project myproject --user Robert admin

openstack user create --project testproj --password redhat --email William@domain0.example.com William
openstack user create --project testproj --password redhat --email John@domain0.example.com John
openstack role add --project testproj --user William admin

3 创建租户、用户并绑定用户权限

管理认证服务

- 查询服务目录

Service Catalog（服务目录）是Keystone为OpenStack提供的一个REST API端点列表，并以此作为决策参考。

```
openstack catalog list                    # 可以显示所有已有的service


openstack endpoint list
openstack project list
openstack user list
```

Thank YOU!