



云操作系统应用

CONTENTS

目 录

第4章

认证服务 Keystone

Keystone 是 OpenStack 的身份认证服务，当安装 OpenStack 身份认证服务时，必须将之注册到其 OpenStack 安装环境的每个服务，身份认证服务才可以追踪那些已经安装的 OpenStack 服务，以及在网络中定位它们。Keystone 组成主要分为以下部分。

域 (Domain)：Domain 实现真正的多租户 (multi-tenancy) 架构，Domain 担任 Project 的高层容器。云服务的客户是 Domain 的所有者，他们可以在自己的 Domain 中创建多个 Projects、Users、Groups 和 Roles。通过引入 Domain，云服务客户可以对其拥有的多个 Project 进行统一管理，而不必再像过去那样对每一个 Project 进行单独管理。

用户 (User)：那些使用 OpenStack 云服务的人、系统、服务的数字表示。身份认证服务会验证那些生成调用的用户发过来的请求，用户登录且被赋予令牌以访问资源，用户可以直接被分配到特别的租户和行为，如果他们是被包含在租户中的。

凭证 (Credential)：用户身份的确认数据，例如，用户名和密码、用户名和 API 密钥，或者是一个由身份服务提供的授权令牌。认证 (Authentication)：确认用户身份的流程，OpenStack 身份认证服务确认发过来的请求，即验证由用户提供的凭证。

令牌 (Token)：一个字母数字混合的文本字符串，用户访问 OpenStack API 和资源，令牌可以随时撤销，以及有一定的时间期限。

租户 (Project)：用于组成或隔离资源的容器，租户会组成或隔离身份对象，一个租户会映射到一个客户、一个账户、一个组织或一个项目。

服务 (Service)：一个 OpenStack 服务，如计算服务 (Nova)，对象服务 (Swift)，或镜像服务 (glance)。它提供一个或多个端点来让用户可以访问资源和执行操作。

角色 (Role)：定义了一组用户权限的用户，可赋予其执行某些特定的操作。在身份服务认证服务 Keystone 第4章 45 中，一个令牌所携带用户信息包含角色列表。服务在被调用时会看用户是什么样的角色，这个角色赋予的权限能够操作什么资源。

Keystone 客户端：为 OpenStack 身份 API 提供的一组命令行接口。例如，用户可以运行 `keystone service-create` 和 `keystone endpoint-create` 命令在其 OpenStack 环境中去注册服务。

策略 (Policy)：OpenStack 对用户的验证除了 OpenStack 的身份验证以外，还需要鉴别用户对某个服务是否有访问权限。Policy 机制就是用来控制某一个 User 在某个 Tenant 中某个操作的权限。这个 User 能执行什么操作，不能执行什么操作，就是通过 Policy 机制来实现的。对于 Keystone 服务来说，Policy 就是一个 json 文件，通过配置这个文件 (`/etc/keystone/policy.json`)，Keystone Service 实现了对 User 的基于用户角色的权限管理。

端点 (Endpoint)：一个网络可访问的服务地址，通过它可以访问一个服务，通常是个 URL 地址。不同 Region 有不同的 Service Endpoint。Endpoint 告诉 OpenStack Service 去哪里访问特定的 Service。比如，当 Nova 需要访问 Glance 服务去获取 Image 时，Nova 通过访问 Keystone 拿到 Glance 的 Endpoint，然后通过访问该 Endpoint 去获取 Glance 服务。我们可以通过 Endpoint 的 Region 属性去定义多个 Region。

Endpoint 的使用对象分为以下三类。

Adminurl：给 admin 用户使用。

Internalurl：供 OpenStack 内部服务使用，以便与其他服务进行通信。

Publicurl：其他用户可以访问的地址。

4.2 Keystone 数据库操作

控制节点数据库操作:

登录 MySQL 并创建 Keystone 数据库

```
# mysql -uroot -p000000
```

```
[root@controller ~]# mysql -uroot -p000000
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 15
Server version: 10.1.12-MariaDB MariaDB Server
```

```
Copyright (c) 2000, 2016, Oracle, MariaDB Corporation Ab and others.
```

```
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

```
MariaDB [(none)]>
```

创建 Keystone 数据库:

```
# CREATE DATABASE keystone;
```

```
MariaDB [(none)] CREATE DATABASE keystone;
Query OK, 1 row affected (0.01 sec)
```

4.2 Keystone 数据库操作

设置授权用户和密码:

```
GRANT ALL PRIVILEGES ON keystone.* TO 'keystone'@'%' IDENTIFIED BY '000000';
```

```
GRANT ALL PRIVILEGES ON keystone.* TO 'keystone'@'localhost' IDENTIFIED BY '000000';
```

```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON keystone.* TO 'keystone'@'%' IDENTIFIED BY '000000';
```

```
Query OK, 0 rows affected (0.18 sec)
```

```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON keystone.* TO 'keystone'@'localhost' IDENTIFIED BY '000000';
```

```
Query OK, 0 rows affected (0.00 sec)
```

```
MariaDB [(none)]> exit
```

4.3 安装并配置 Keystone

控制节点安装 Keystone 所需软件包

```
yum install openstack-keystone httpd mod_wsgi -y
```

```
[root@controller ~]# yum install openstack-keystone httpd mod_wsgi -y
```

生成一个随机值作为初始配置期间的管理令牌:

```
# openssl rand -hex 10
```

```
[root@controller ~]# openssl rand -hex 10  
d8ee7dcf815952129818
```

使用vi命令编辑/etc/keystone/keystone.conf 文件, 做如下配置与修改, 使用刚刚生成的随机值替换:

```
# vi /etc/keystone/keystone.conf
```

```
[root@controller ~]# vi /etc/keystone/keystone.conf
```

```
[DEFAULT]
```

```
admin_token = d8ee7dcf815952129818
```

```
[DEFAULT]
```

```
admin_token = d8ee7dcf815952129818
```

4.3 安装并配置 Keystone

配置数据库链接：

```
[database]
```

```
connection = mysql+pymysql://keystone:000000@controller (报错改localhost) /keystone
```

```
[database]
```

```
connection = mysql+pymysql://keystone:000000@controller/keystone
```

配置 provider，配置完成后保存文件并退出：

```
[token]
```

```
provider = fernet
```

```
[token]
```

```
provider = fernet
```

同步数据库：

```
su -s /bin/sh -c "keystone-manage db_sync" keystone
```

```
[su -s /bin/sh -c "keystone-manage db_sync" keystone
```

注： 进入 Keystone 数据库查看是否有数据表，验证是否同步成功。



4.3 安装并配置 Keystone

初始化密钥:

```
# keystone-manage fernet_setup --keystone-user keystone --keystone-group keystone
```

```
[root@controller ~]# keystone-manage fernet_setup --keystone-user keystone --keystone-group keystone
```

4.4 配置 Apache 服务

使用vi命令编辑/etc/httpd/conf/httpd.conf 文件。

添加:

```
ServerName controller
```

```
[root@controller ~]# vi /etc/httpd/conf/httpd.conf
```

```
ServerName controller
```

创建/etc/httpd/conf.d/wsgi-keystone.conf 文件。

添加:

```
Listen 5000
Listen 35357
<VirtualHost *:5000>
WSGIDaemonProcess keystone-public processes=5 threads=1 user=keystone group=keystone displayname=%{GROUP}
WSGIProcessGroup keystone-public
WSGIScriptAlias / /usr/bin/keystone-wsgi-public
WSGIApplicationGroup %{GLOBAL}
WSGIPassAuthorization On
ErrorLogFormat "%{cu}t %M"
ErrorLog /var/log/httpd/keystone-error.log
CustomLog /var/log/httpd/keystone-access.log combined
<Directory /usr/bin>
Require all granted
</Directory>
</VirtualHost>
<VirtualHost *:35357>
```

4.4 配置 Apache 服务

```
WSGIDaemonProcess keystone-admin processes=5 threads=1 user=keystone group=keystone displayname=%{GROUP}
WSGIProcessGroup keystone-admin
WSGIScriptAlias / /usr/bin/keystone-wsgi-admin
WSGIApplicationGroup %{GLOBAL}
WSGIPassAuthorization On
ErrorLogFormat "%{cu}t %M"
ErrorLog /var/log/httpd/keystone-error.log
CustomLog /var/log/httpd/keystone-access.log combined
<Directory /usr/bin>
Require all granted
</Directory>
</VirtualHost>
```

启动并设置 Apache HTTP 服务开机自启：

```
# systemctl enable httpd.service
# systemctl start httpd.service
```

4.5 创建 Service 和 API Endpoints

1. 配置身份认证令牌

```
# export OS_TOKEN=自己生成的随机
```

```
[root@controller ~]# export OS_TOKEN=d8ee7dcf815952129818
```

2. 配置端点 URL

```
# export OS_URL=http://controller:35357/v3
```

```
[root@controller ~]# export OS_URL=http://controller:35357/v3
```

3. 配置 API 版本

```
# export OS_IDENTITY_API_VERSION=3
```

```
[root@controller ~]# export OS_IDENTITY_API_VERSION=3
```

4. 为 Keystone 本身创建服务

```
# openstack service create --name keystone --description "OpenStack Identity" identity
```

```
[root@controller ~]# openstack service create --name keystone --description "OpenStack Identity" identity
```

Field	Value
description	OpenStack Identity
enabled	True
id	c92ab555dc1343e88c681c0bd9d7073b
name	keystone
type	identity

4.5 创建 Service 和 API Endpoints

然后，创建 Keystone 身份认证服务的端点：

身份认证服务管理了一个与环境相关的 API 端点目录。使用这个目录来决定如何与创建环境中的其他服务进行通信。

OpenStack 使用三个 API 端点代表每种服务：**admin**、**internal** 和 **public**。默认情况下，管理 API 端点允许修改用户和租户，而公共和内部 API 不允许这些操作。此次安装为所有端点和默认 “RegionOne” 区域都使用管理网络。

1. 创建公共端点

```
# openstack endpoint create --region RegionOne identity public http://controller:5000/v3
```

2. 创建外部端点

```
# openstack endpoint create --region RegionOne identity internal http://controller:5000/v3
```

3. 创建管理端点

```
# openstack endpoint create --region RegionOne identity admin http://controller:35357/v3
```

4.5 创建 Service 和 API Endpoints

```
[root@controller ~]# openstack endpoint create --region RegionOne identity admin  
http://controller:35357/v3
```

Field	Value
enabled	True
id	f71e9892343d4f46858abcd1d66f28cc
interface	admin
region	RegionOne
region_id	RegionOne
service_id	c92ab555dc1343e88c681c0bd9d7073b
service_name	keystone
service_type	identity
url	http://controller:35357/v3

4.5 创建 Service 和 API Endpoints

```
[root@controller ~]# openstack endpoint create --region RegionOne identity public http://controller:5000/v3
```

Field	Value
enabled	True
id	61d01c55d75e43ecab7a058bffca25c8
interface	public
region	RegionOne
region_id	RegionOne
service_id	c92ab555dc1343e88c681c0bd9d7073b
service_name	keystone
service_type	identity
url	http://controller:5000/v3

```
[root@controller ~]# openstack endpoint create --region RegionOne identity internal http://controller:5000/v3
```

Field	Value
enabled	True
id	c72f985423844546bda6d377af4c88d4
interface	internal
region	RegionOne
region_id	RegionOne
service_id	c92ab555dc1343e88c681c0bd9d7073b
service_name	keystone
service_type	identity
url	http://controller:5000/v3

4.6 创建 domain、project、user、role

1. 创建默认（default）的 domain

```
# openstack domain create --description "Default Domain" default
```

```
[root@controller ~]# openstack domain create --description "Default Domain" default
```

Field	Value
description	Default Domain
enabled	True
id	dafc8ccd6b0a469ea6faeb8a4c3620d3
name	default

2. 创建名字为 admin 的 project

```
# openstack project create --domain default --description "Admin Project" admin
```

3. 创建名字为 admin 的 user

```
# openstack user create --domain default --password-prompt admin （回车之后输入自定义密码）
```


4.6 创建 domain、project、user、role

4. 创建名字为 admin 的 role

```
# openstack role create admin
```

5. 进行关联

```
# openstack role add --project admin --user admin admin
```

6. 创建名为 service 的 project

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

7. 创建名为 demo 的 project

```
# openstack project create --domain default --description "Demo Project" demo
```

8. 创建名为 demo 的 user

```
# openstack user create --domain default --password-prompt demo （回车之后输入自定义密码）
```

9. 创建名为 demo 的 role

```
# openstack role create user
```

10. 进行关联

```
# openstack role add --project demo --user demo user
```

4.6 创建 domain、project、user、role

```
[root@controller ~]# openstack project create --domain default --description "Admin Project" admin
```

Field	Value
description	Admin Project
domain_id	daafc8ccd6b0a469ea6faeb8a4c3620d3
enabled	True
id	b2cfff43e0ba1440ea65a123f968a1e9f
is_domain	False
name	admin
parent_id	daafc8ccd6b0a469ea6faeb8a4c3620d3

```
[root@controller ~]# openstack user create --domain default --password-prompt admin
```

User Password:

Repeat User Password:

Field	Value
domain_id	daafc8ccd6b0a469ea6faeb8a4c3620d3
enabled	True
id	1e23989a3506458d80466b0bc94f221c
name	admin

4.6 创建 domain、project、user、role

```
[root@controller ~]# openstack role create admin
```

Field	Value
domain_id	None
id	c7f3f3593fb0453cafb29a1fe0d940b
name	admin

```
[root@controller ~]# openstack role add --project admin --user admin admin
```

```
[root@controller ~]# openstack project create --domain default --description "Service Project" service
```

Field	Value
description	Service Project
domain_id	dafc8ccd6b0a469ea6faeb8a4c3620d3
enabled	True
id	597f00cc696440ba915ab24ab3382b07
is_domain	False
name	service
parent_id	dafc8ccd6b0a469ea6faeb8a4c3620d3

```
[root@controller ~]# openstack project create --domain default --description "Demo Project" demo
```

Field	Value
description	Demo Project
domain_id	dafc8ccd6b0a469ea6faeb8a4c3620d3
enabled	True
id	5d2f3650e89346239b5fcb07e3ae92ff
is_domain	False
name	demo
parent_id	dafc8ccd6b0a469ea6faeb8a4c3620d3

4.7 验证 Keystone 服务

1. 不生效临时的环境变量

```
# unset OS_TOKEN OS_URL
```

2. 查看 admin 用户，请求身份验证令牌

```
# openstack --os-auth-url http://controller:35357/v3 --os-project-domain-name default --os-user-domain-name default --os-project-name admin --os-username admin token issue
```

3. 查看 demo 用户，请求身份验证令牌

```
# openstack --os-auth-url http://controller:35357/v3 --os-project-domain-name default --os-user-domain-name default --os-project-name demo --os-username demo token issue
```

```
[root@controller ~]# openstack --os-auth-url http://controller:35357/v3 --os-project-domain-name default --os-user-domain-name default --os-project-name admin --os-username admin token issue
```

Field	Value
expires	2017-11-27T09:02:01.362149Z
id	gAAAAABaG8Z6ga7sg6Gias85U7FQDYf4Ou9Fi1EPcmYUMIvrSfXNwnzzefx57UetejfQikr6WLkmvts_qFit8bID-10ZttemIrkGGeSuer1I-FgJu5kcgqNv2DPD4-1RuPO68ZyELwzXITXYLrLXGHfZcdDXTjjMjhG4CH3BTf0LRgjYOZdT9k
project_id	b2cff43e0ba1440ea65a123f968a1e9f
user_id	1e23989a3506458d80466b0bc94f221c

4.6 创建 domain、project、user、role

```
[root@controller ~]# openstack user create --domain default --password-prompt demo
```

User Password:

Repeat User Password:

Field	Value
domain_id	dafc8ccd6b0a469ea6faeb8a4c3620d3
enabled	True
id	6002d09d700c4ddc99536b87b073b5d5
name	demo

```
[root@controller ~]# openstack role create user
```

Field	Value
domain_id	None
id	6bf5f2aec5774a79984870a6c7e77ab0
name	user

```
[root@controller ~]# openstack role add --project demo --user demo user
```

4.7 验证 Keystone 服务

```
[root@controller ~]# openstack --os-auth-url http://controller:35357/v3 --os-project-domain-name default --os-user-domain-name default --os-project-name demo --os-username demo token issue
```

Field	Value
expires	2017-11-27T09:04:05.775507Z
id	gAAAAABaG8b214Lq7Rzu5etmkwktEiNNhPtW4EQin4NVxqmJchHfuFUqxXP5gfVK5WRxy0UL_GsA8qfgBcRmb7cyeSYqwmDFgPGJFgbY69USEhh4Ab41ew2QQCRKBioUHCoe0NxfvbFvBcd99kI-JWu3cOn_EaAN-FS1a7HcDdQ14yeZ7HHzUv0
project_id	5d2f3650e89346239b5fcb07e3ae92ff
user_id	6002d09d700c4ddc99536b87b073b5d5

4. 写入环境变量

创建/root/admin-openrc 文件。

添加：

```
export OS_PROJECT_DOMAIN_NAME=default
export OS_USER_DOMAIN_NAME=default
export OS_PROJECT_NAME=admin
export OS_USERNAME=admin
export OS_PASSWORD=123456
export OS_AUTH_URL=http://controller:35357/v3
export OS_IDENTITY_API_VERSION=3
export OS_IMAGE_API_VERSION=2
```

4.7 验证 Keystone 服务

创建/root/demo-openrc 文件。

添加：

```
export OS_PROJECT_DOMAIN_NAME=default
export OS_USER_DOMAIN_NAME=default
export OS_PROJECT_NAME=demo
export OS_USERNAME=demo
export OS_PASSWORD=000000
export OS_AUTH_URL=http://controller:35357/v3
export OS_IDENTITY_API_VERSION=3
export OS_IMAGE_API_VERSION=2
```

5. 生效并验证

```
# . admin-openrc
# openstack token issue
```

```
[root@controller ~]# . admin-openrc
[root@controller ~]# openstack token issue
```

Field	Value
expires	2017-11-27T09:13:39.705294Z
id	gAAAAABaG8k2qi8fGm7y6oZK3uXKGT2EqUo1GEvsURP93tqdVw9mLOU9t1BTHd9pIx_6Mu2ZFNaWRI7hEeNu5E6sbovmCeXsMgbxwz-SsPB_1UYZUZPKf_81RmDhrTpt7Pi2k8oiA1w8wrv8tLnDnMRgYbP4uaL9pt_aHB6dD_wwaN3t1C870Uk
project_id	b2cff43e0ba1440ea65a123f968a1e9f
user_id	1e23989a3506458d80466b0bc94f221c

谢谢观看

