2.4.3 Keyston – 认证服务

讲师：汪洋

目录

1 组件说明

一、什么是 Keystone

Keystone 是 OpenStack Identity Service 的项目名称，是一个负责身份管理与授权的组件

主要功能：实现用户的身份认证，基于角色的权限管理，及openstack其他组件的访问地址和安全策略管理

二、为什么需要 Keystone

Keystone项目的主要目的是给整个openstack的各个组件（nova，cinder,glance...）提供一个统一的验证方式

- 用户管理
  - Account 账户
  - Authentication 身份认证
  - Authorization 授权
- 服务目录管理

User（用户） 一个人、系统或服务在OpenStack中的数字表示。已经登录的用户分配令牌环以访问资源。用户可以直接分配给特定的租户，就像隶属于每个组。

Credentials（凭证） 用于确认用户身份的数据。例如：用户名和密码，用户名和API key，或由认证服务提供的身份验证令牌

Authentication（验证） 确认用户身份的过程。

Token（令牌） 一个用于访问OpenStack API和资源的字母数字字符串。一个临牌可以随时撤销，并且持续一段时间有效

Tenant（租户） 一个组织或孤立资源的容器。租户和可以组织或隔离认证对象。根据服务运营的要求，一个租户可以映射到客户、账户、组织或项目。

Service（服务） **OpenStack**服务，例如计算服务（**nova**），对象存储服务（**swift**）,或镜像服务（**glance**）。它提供了一个或多个端点，供用户访问资源和执行操作。

Endpoint（端点） 一个用于访问某个服务的可以通过网络进行访问的地址，通常是一个**URL**地址。

Role（角色） 定制化的包含特定用户权限和特权的权限集合

Keystone Client（keystone命令行工具） **Keystone**的命令行工具。通过该工具可以创建用户，角色，服务和端点等。。。

用户：张三

凭证：身份证

验证：验证身份证

令牌：房卡

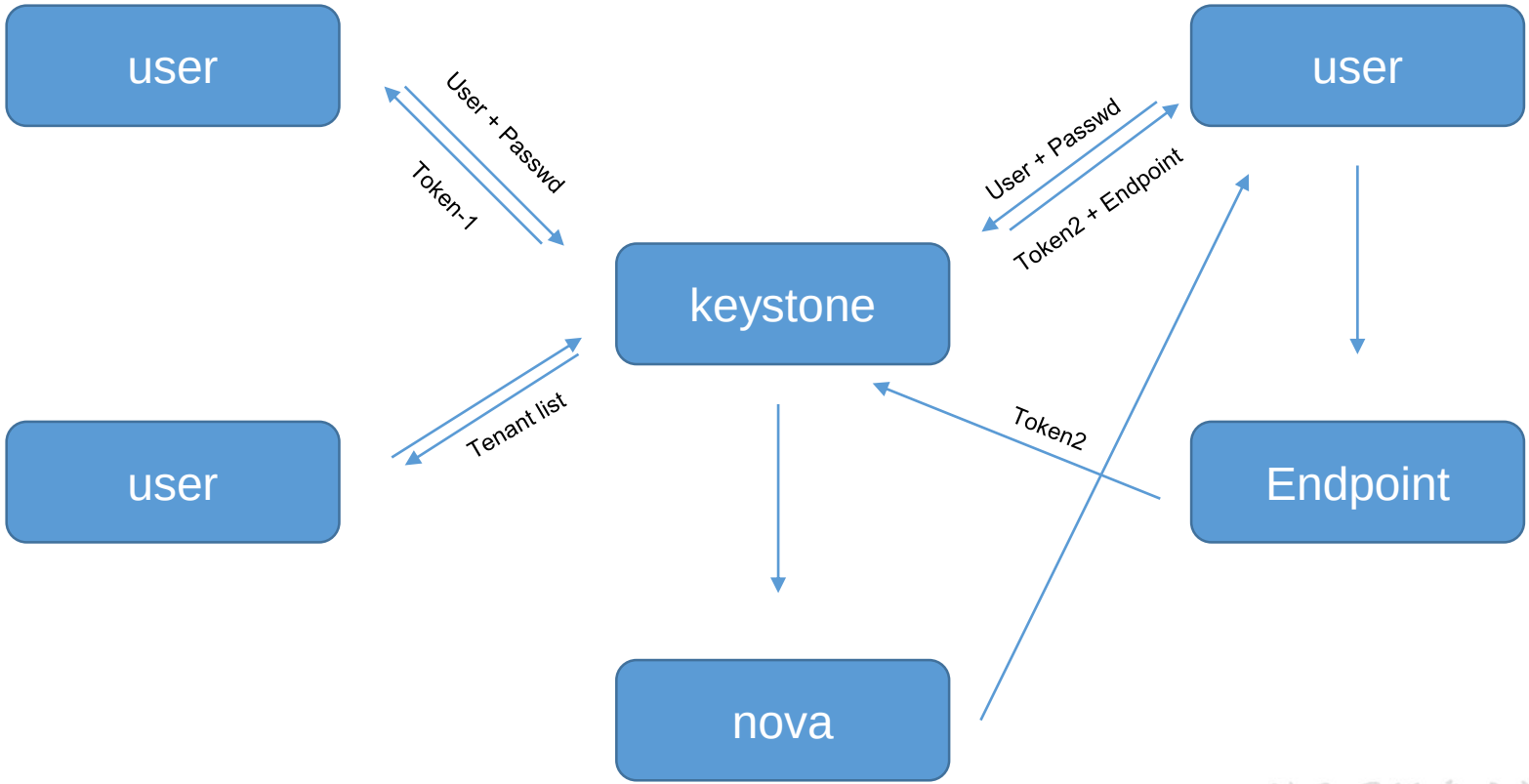
租户：宾馆

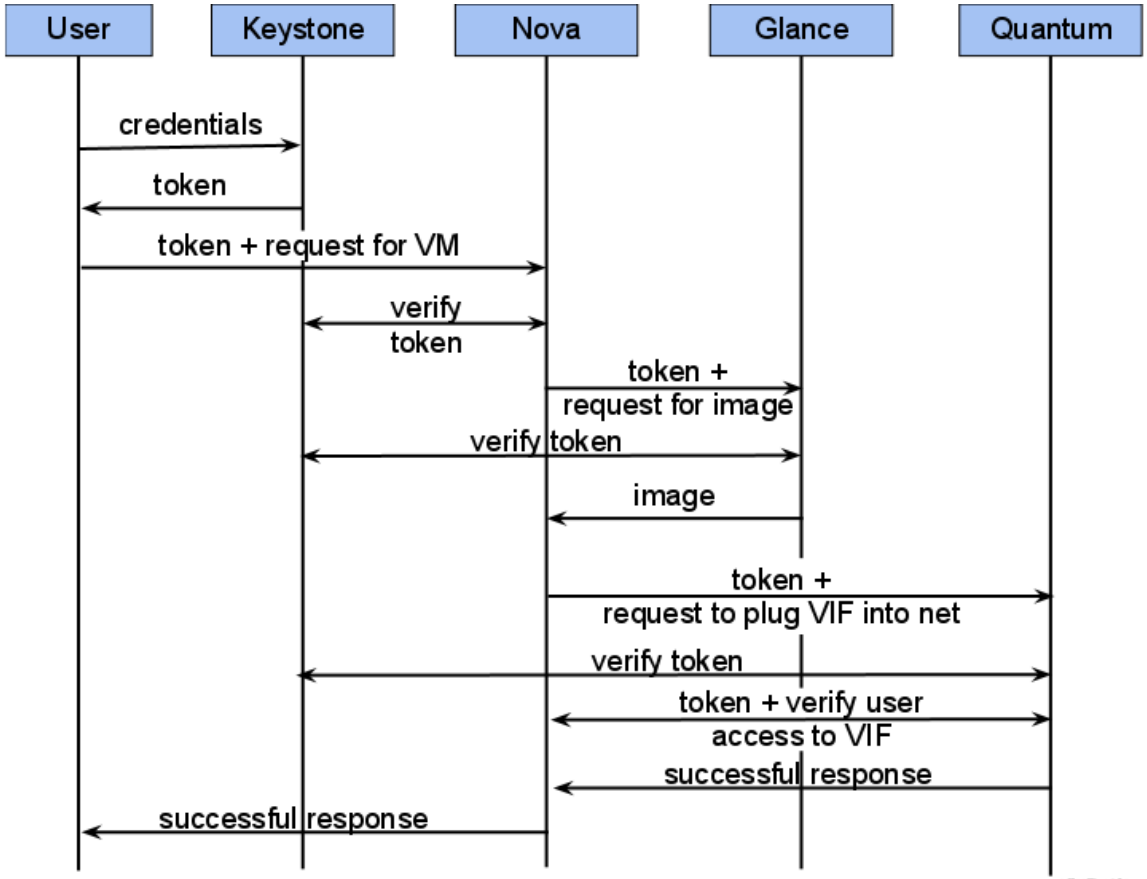
服务：住宿、餐饮

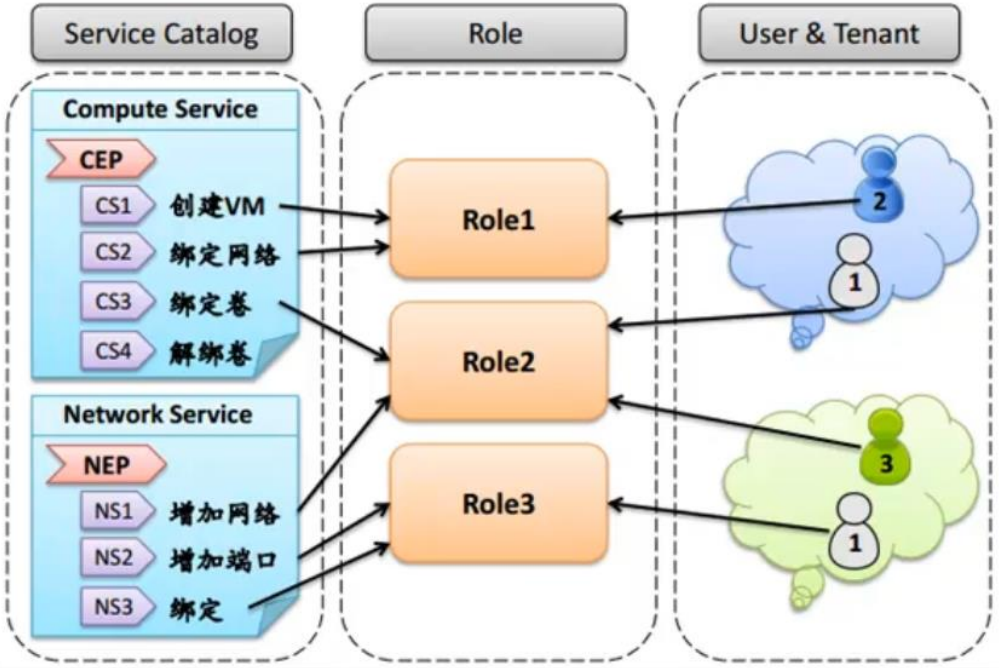
端点：路径

角色：VIP等级

2 组件之间沟通方式


user
User + Passwd
Token-1
user
User + Passwd
Token2 + Endpoint
keystone
user
Tenant list
Token2
Endpoint
nova


User
Keystone
Nova
Glance
Quantum
credentials
token
token + request for VM
verify token
token + request for image
verify token
image
token + request to plug VIF into net
verify token
token + verify user access to VIF
successful response
successful response


Service Catalog
Role
User & Tenant
Compute Service
CEP
CS1
创建VM
CS2
绑定网络
CS3
绑定卷
CS4
解绑卷
Network Service
NEP
NS1
增加网络
NS2
增加端口
NS3
绑定
Role1
Role2
Role3
2
1
3
1

3 构建实验

基本环境确定

构建文档