# Keystone的意义

## （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。主要的功能是：实现用户的身份认证，基于角色的权限管理，以及Openstack其他组件的访问地址的管理与安全策略的管理。

## （二）使用Keystone的意义

Keystone的意义就是为整个Openstack的各个组件提供一个统一的验证方式。

# Keystone的功能

## （一）用户管理

账户管理，身份认证管理，授权管理。

## （二）服务目录管理

登记了Openstack中所有服务的访问url地址，如Nova, Glance等。

# 认证服务中的关键词

## （一）User（用户）

一个访问者，系统或服务在OpenStack中的数字表示，已经登录的用户会被分配一个令牌环来访问资源。

## （二）Credentials（凭证）

用来确认用户身份的数据，如用户名和密码，用户名和API Key，或是认证服务提供的身份验证令牌。

## （三）Authentication（验证）

确认用户身份的过程。

## （四）Token（令牌）

一个用于访问OpenStack API和资源的字母数字字符串，一个临时的令牌有时间限制的，可以随时撤销。

## （五）Tenant（租户）

一个组织或孤立资源的容器，如一个租户中包含着Nova服务，根据服务运行的要求，一个租户可以映射到客户，账户，组织或项目中。

## （六）Service（服务）

Openstack中众多服务，如计算服务（Nova），对象存储服务（swift），镜像服务（glance），每个服务提供了多个端点，可以供用户访问资源。

## （七）Endpoint（端点）

一个用于访问某个服务的url地址。

## （八）Role（角色）

定制化的包含特定用户权限和特权的权限集合。

## （九）Keystone Client（Keystone命令行工具）

命令行工具，通过该工具可以创建用户，角色，服务和端点。

# Keystone组件之间的沟通方式

## （一）用户认证过程

### 1. 令牌生成

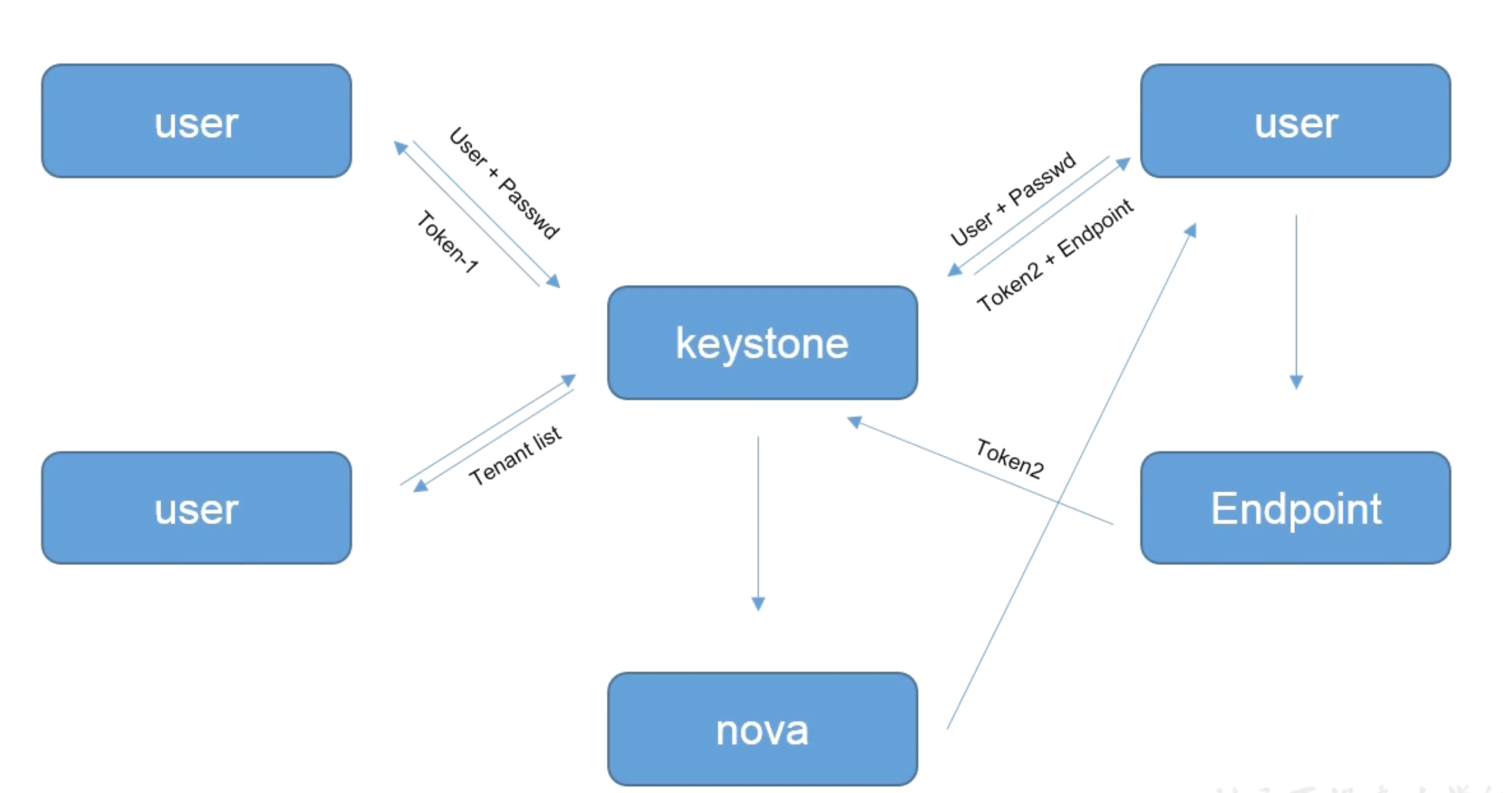
用户首先通过用户名和密码验证身份后，Keystone组件就会返还一个Token令牌给用户，同时该组件也会记录下Token的信息。

### 2. 端点信息获取

用户需要从Keystone组件中获取各种服务的端点信息，需要向Keystone组件发送请求，此次携带的就是Token令牌了，Keystone组件检查令牌的有效性，之后返回端点信息给用户。

### 3. 访问端点

用户获取到端点信息后，携带着令牌直接访问端点的url，端点将令牌发送给Keystone组件进行验证，验证成功后，端点开始执行操作。



## （二）用户创建虚拟机的组件交互过程

### 1. 用户凭证验证

用户发送凭证给Keystone组件进行验证，Keystone验证成功后，返回令牌给用户。

### 2. 用户发送请求给Nova

用户携带着令牌发送请求给Nova，请求创建虚拟机，Nova向Keystone验证令牌的有效性，验证成功后，继续操作。

### 3. Nova发送请求给Glance

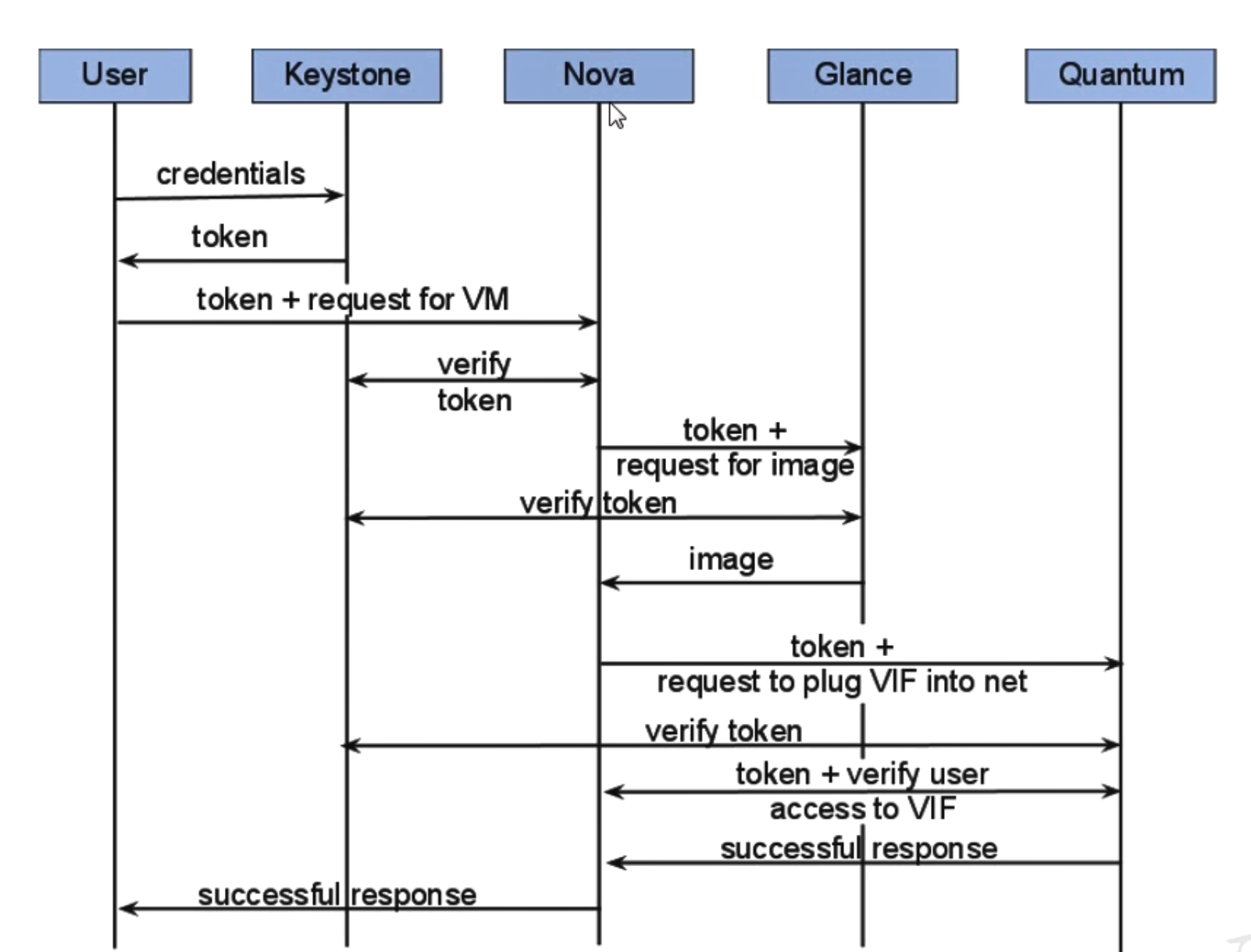
Nova服务携带令牌给Glance服务，请求镜像，Glance服务向Keystone服务验证令牌的有效性，验证成功后，将镜像返回给Nova服务，继续操作。

### 4. Nova发送请求给Neutron服务

生成镜像后，需要IP地址，Nova服务携带令牌发送请求给Neutron服务，Neutron服务向Keystone服务验证令牌，验证成功后，返回网络信息给Nova服务，以及成功响应信息。

### 5. Nova返回成功响应信息给用户

Nova服务接受到Neutron发送的成功响应后，返回给用户成功响应信息。



## （三）用户-角色-服务的交互

一个用户可以放置在多个租户中；

一个用户可以绑定到不同的角色；

一个角色可以绑定到不同的服务；

