# Keystone

KEYSTONE

*an OpenStack Community Project*

# 概述

- Keystone原理
  - 什么是Keystone?
  - Keystone的主要功能
  - Keystone的概念
  - 示例：Keystone与其它服务交互的流程
- 实验：
  - 启用启动服务器后，DevStack的启动
  - 通过图形界面的Horizon访问Openstack
  - 通过命令行访问OpenStack
  - 通过REST API访问OpenStack
  - 管理项目、用户、角色

# Keystone原理

- 什么是Keystone?
- Keystone的主要功能
- Keystone的概念
- 示例：Keystone与其它服务交互的流程

# 什么是Keystone?

- Keystone is an OpenStack service that provides API client authentication, service discovery, and distributed multi-tenant authorization by implementing OpenStack's Identity API.
- 主要功能：
  - 身份验证 Authentication
  - 授权 Authorization
  - 服务目录 Catalog of services

# Keystone的主要概念

- 用户 User

- 凭证 Credentials


- 验证 Authentication


- 令牌 Token

- 项目/租户 Project/Tenant

- 服务 Service

- 端点 Endpoint

- 角色 Role

# Keystone的主要概念

用户
User

项目/租户
Project/Tenant

策略
Policy


凭证
Credentials

服务
Service

域
Domain


验证
Authentication

端点
ndpoint

组
Group

令牌
Token

角色
Role

区域
Region

# 策略 Policy

```
$ cat /etc/keystone/policy.json
{
    "admin_required": "role:admin or is_admin:1",
    "service_role": "role:service",
    "service_or_admin": "rule:admin_required or rule:service_role",
    "owner" : "user_id:%(user_id)s",
    "admin_or_owner": "rule:admin_required or rule:owner",
    "token_subject": "user_id:%(target.token.user_id)s",
    "admin_or_token_subject": "rule:admin_required or rule:token_subject",

    "default": "rule:admin_required",

    "identity:get_service": "rule:admin_required",
    "identity:list_services": "rule:admin_required",
    "identity:create_service": "rule:admin_required",
    "identity:update_service": "rule:admin_required",
    "identity:delete_service": "rule:admin_required",

    "identity:get_user": "rule:admin_or_owner",
    "identity:list_users": "rule:admin_required",
    "identity:create_user": "rule:admin_required",
    "identity:update_user": "rule:admin_required",
    "identity:delete_user": "rule:admin_required",
    "identity:change_password": "rule:admin_or_owner"

.....略.....
```

JSON-- JavaScript Object Notation

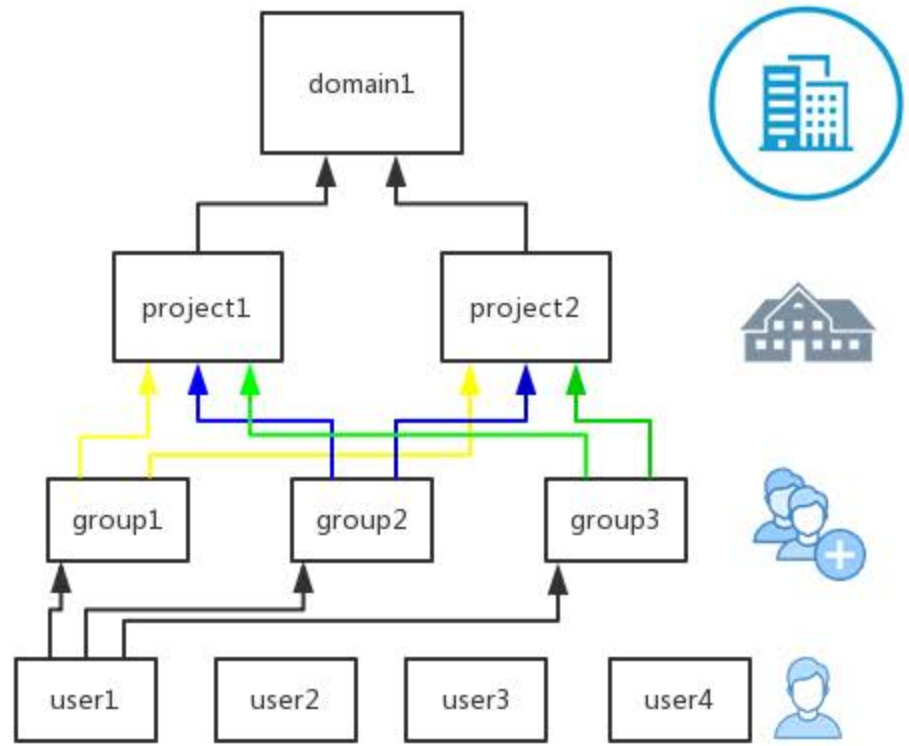
- 轻量级的数据交换格式
- 独立于编程语言
- 文本格式

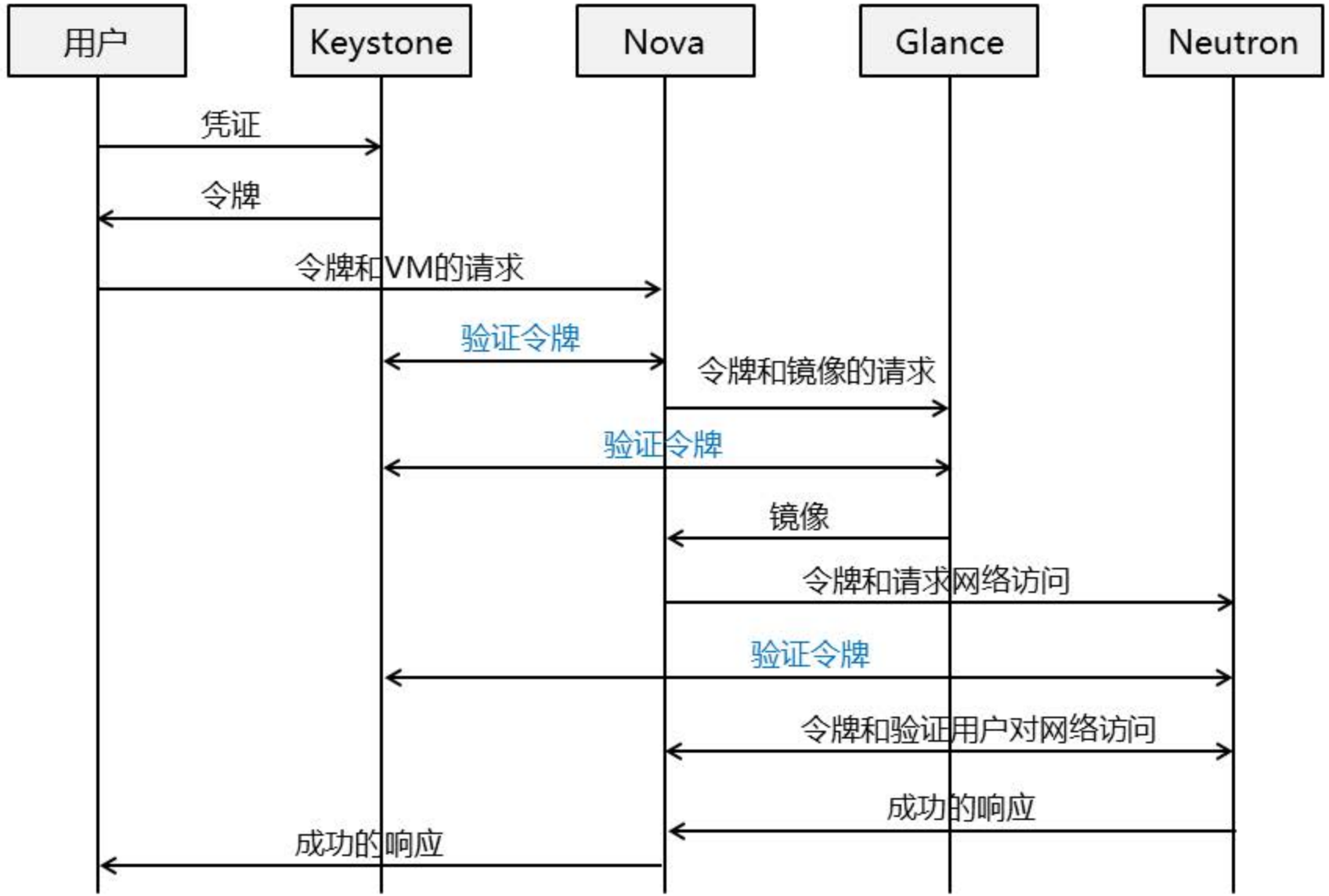
示例：

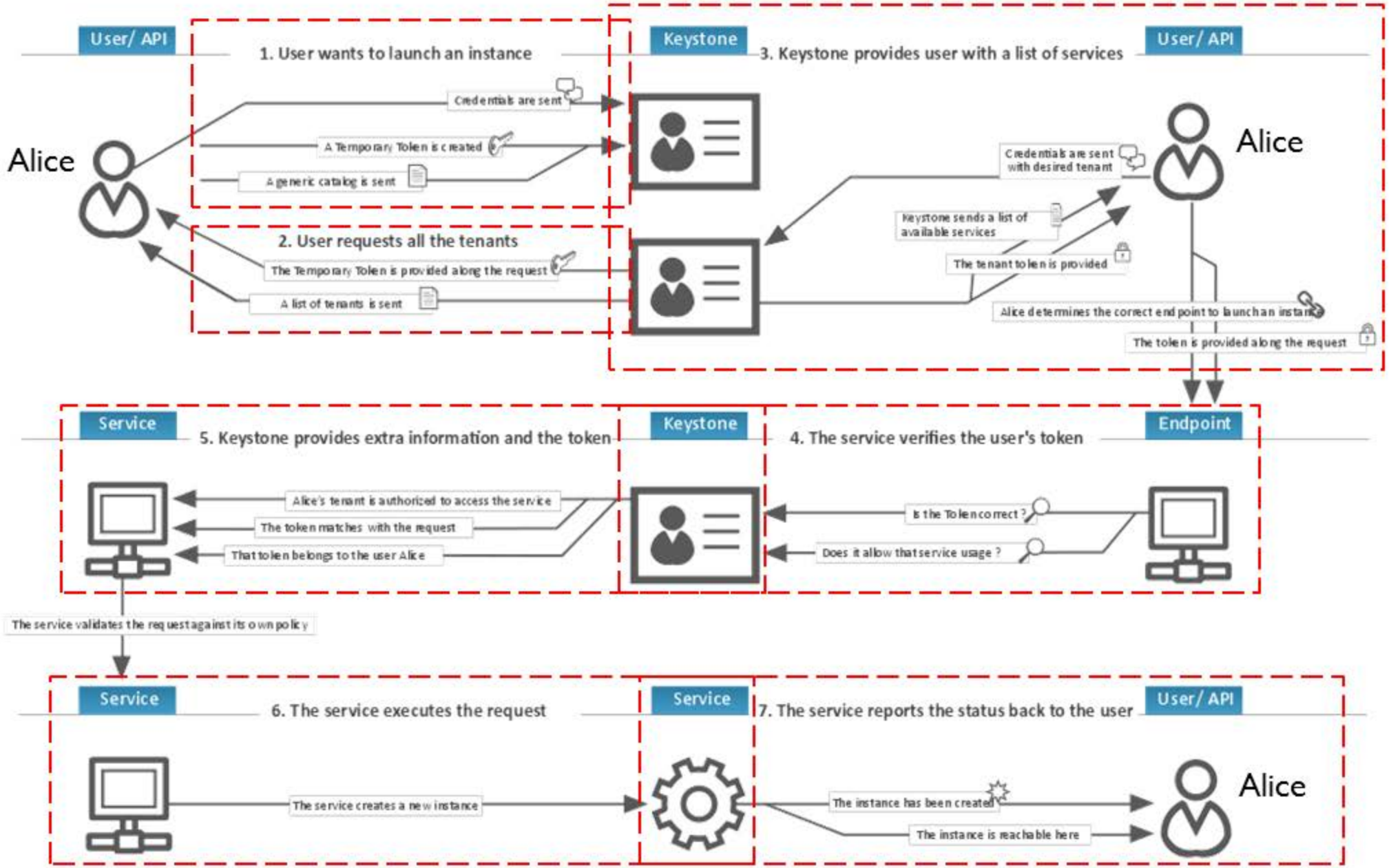
```
{
"FirstName": "Tom",
"LastName": "Chen"
}
```

# Keystone V3中的新概念

- Keystone V3 做出了许多变化和改进：
  - 将 Tenant 改称为 Project
  - 引入 Group 的概念
  - 引入 Domain 的概念
  - 引入 Region 的概念
  - ……




用户
Keystone
Nova
Glance
Neutron
凭证
令牌
令牌和VM的请求
验证令牌
令牌和镜像的请求
验证令牌
镜像
令牌和请求网络访问
验证令牌
令牌和验证用户对网络访问
成功的响应
成功的响应


User/ API
1. User wants to launch an instance
Keystone
3. Keystone provides user with a list of services
User/ API
Alice
Credentials are sent
A Temporary Token is created
A generic catalog is sent
Credentials are sent with desired tenant
Alice
Keystone sends a list of available services
2. User requests all the tenants
The Temporary Token is provided along the request
The tenant token is provided
A list of tenants is sent
Alice determines the correct end point to launch an instance
The token is provided along the request
Service
5. Keystone provides extra information and the token
Keystone
4. The service verifies the user's token
Endpoint
Alice's tenant is authorized to access the service
The token matches with the request
That token belongs to the user Alice
Is the Token correct ?
Does it allow that service usage ?
The service validates the request against its own policy
Service
6. The service executes the request
Service
7. The service reports the status back to the user
User/ API
The service creates a new instance
The instance has been created
The instance is reachable here
Alice

# 实验

- 考察OpenStack数据库
- 重新启动服务器后，DevStack的启动
- 通过图形界面的Horizon访问Openstack
- 通过命令行访问Openstack
- 通过REST API访问OpenStack
- 管理项目、用户、角色

# 重新启动服务器后，DevStack的启动


```
$ sudo su - stack

$ sudo losetup -f /opt/stack/data/stack-volumes-default-backing-file
$ sudo losetup -f /opt/stack/data/stack-volumes-lvmdriver-1-backing-file

$ script /dev/null
$ screen -c /opt/stack/devstack/stack-screenrc
  Ctrl + A, 然后D退出
```

# 访问OpenStack的方法

- 与OpenStack交互，主要有以下3种方式
  - Dashboard：基于网页的用户界面(GUI)
  - CLI：组件专用的命令行接口
  - API：RESTful(Web)服务
- 无论哪种方式，所以的交互最后还是会回到OpenStack API
- 小工具：
  - `curl`

# 通过图形界面的Horizon访问Openstack

# 通过命令行访问Openstack

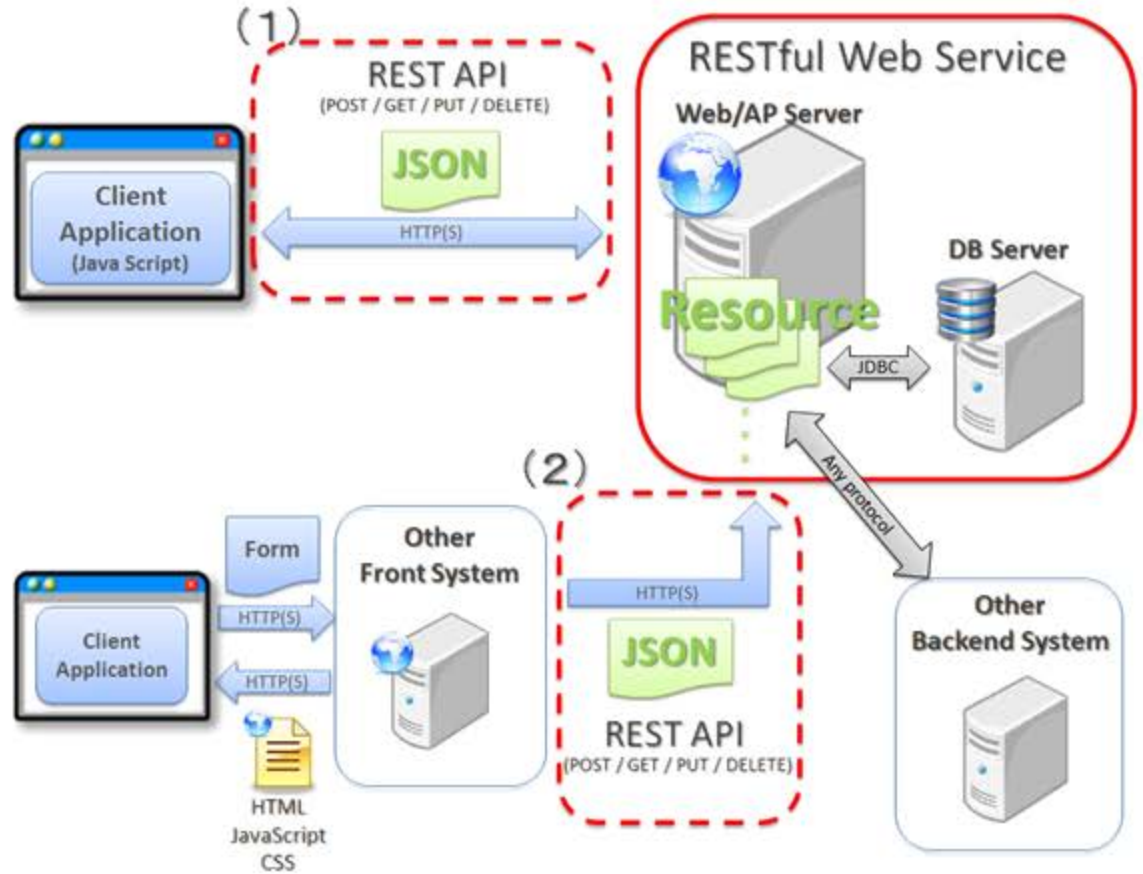
- 分类：
  - 通用： **openstack**（立即模式、交互模式、自动完成…）
  - 专用： **~~keystone~~、nova、glance、cinder…..**
- 为Shell设置环境变量，提高CLI的效率

```
$ source /opt/stack/devstack/openrc admin admin
WARNING: setting legacy OS_TENANT_NAME to support cli
tools.

$ env | grep ^OS

$ openstack user list
```

```
+----------------------------------+-----------+
| ID                               | Name      |
+----------------------------------+-----------+
| 0e82fa106a3e48dc9889e8d498f54e3a | alt_demo  |
| 185b66893de040a1aacfe80263a5d20e | admin     |
| 1a8fdec2e51b4ce6baf28f77673008ee | nova      |
| 4c07c34f87b14aed866c0e050bb0ffa9 | demo      |
| 5e06df10203f46798bf91434366d5f39 | cinder    |
| 7eb65ff570a54af2bc967a505ce3e764 | neutron   |
| dfc5bf898da648038ee0dc06225d2853 | glance    |
| f56b8fff46f0468488c7878d6a053615 | placement |
+----------------------------------+-----------+
```

# 背景知识：REST和RESTful

- REST = REpresentational State Transfer
- “通俗”理解：
  - 用URL定位资源
  - 用HTTP动词描述操作
    - GET、POST、PUT、DELETE
  - 传递数据与状态码



# 通过REST API访问OpenStack

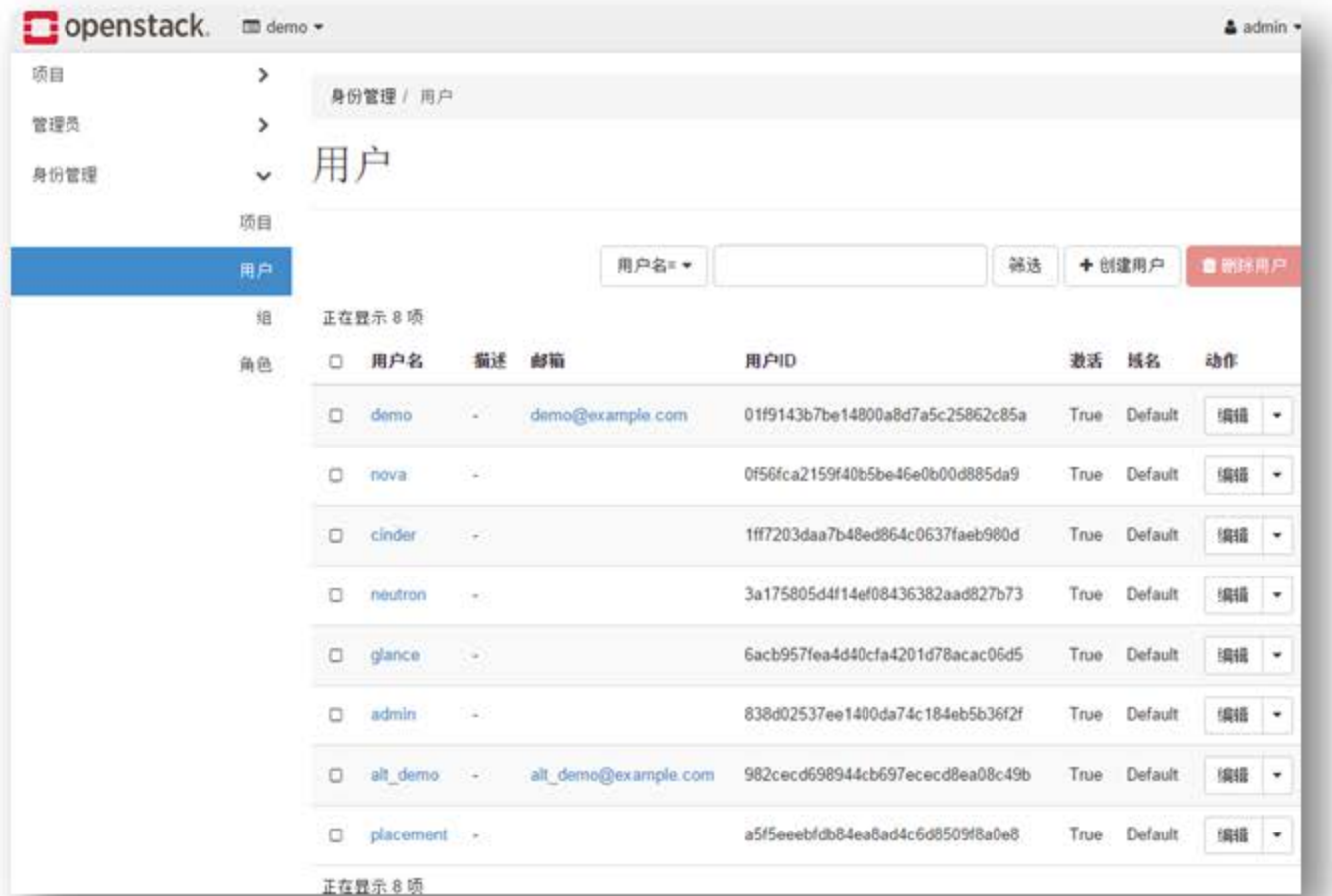
```
# curl -i \
  -H "Content-Type: application/json" \
  -d '
{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "domain": {"id":"default"},
                    "name": "admin",
                    "password": "secret"
                }
            }
        }
    }
}' \
  http://localhost/identity_admin/v3/auth/tokens
```


```
# HTTP/1.1 201 Created
Date: Mon, 14 Aug 2017 07:36:02 GMT

Server: Apache/2.4.18 (Ubuntu)

X-Subject-Token: gAAAAABZkVLidtFXM1H1L2Y3gvmBY8-
bEndUl62NHetB-hA7JJ2Z0dyoshDd6CoAWADYjXUgQ29E-
_Z88dboqzLPQRemsar2VV2fmTn_0tUd9m-
QLpM_TGroDp2cjMT6ZB87uY_U2okMXN4V4CRMLEZom3HmUCpUYg

Vary: X-Auth-Token

x-openstack-request-id: req-5ec8a52e-68fd-4a2a-a77f-
08f5b4f0c5ea

Content-Length: 312
Content-Type: application/json
{"token": {"issued_at": "2017-08-14T07:36:02.000000Z",
"audit_ids": ["gnoary7qTiSjgD-CZjlB_w"], "methods":
["password"], "expires_at": "2017-08-
14T08:36:02.000000Z", "user": {"password_expires_at":
null, "domain": {"id": "default", "name": "Default"},
"id": "838d02537ee1400da74c184eb5b36f2f", "name":
"admin"}}}
```


openstack.

# 实验：管理项目、用户、角色

```
$ openstack help project
  project create
  project delete
  project list
  project set
  project show

$ openstack help user
  user create
  user delete
  user list
  user password set
  user set
  user show

$ openstack help role
  role add
  role assignment list
  role create
  role delete
  role list
  role remove
  role set
  role show
```



# 总结

- Keystone原理
- 实验：
  - 启用启动服务器后，DevStack的启动
  - 通过图形界面的Horizon访问Openstack
  - 通过命令行访问Openstack
  - 通过REST API访问OpenStack
  - 管理项目、用户、角色