CHINA OpenInfra Days

CHINA OpenInfra Days | IT大咖说 知识共享平台

Keystone在企业级生产环境中的最佳实践

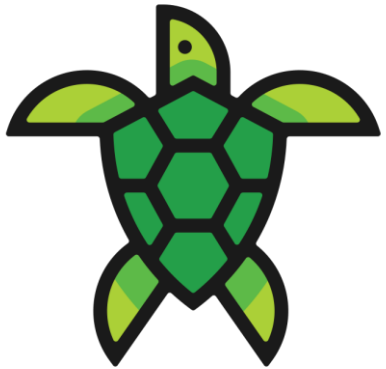
张晓阳

目录：

OpenStack Identity（Keystone）

定义：

- 一个用于认证和授权的共享服务
- 为最终用户和服务提供身份信息
- 介于OpenStack和其他身份服务之间的“经纪人”



功能：

- 组织权限管理、身份认证、服务注册

Token

keystone使用token认证机制，代替用户名密码进行认证。

类型：

- UUID 32字节
- ~~PKI & PKIZ~~ 大约1600+字节，压缩减少14.86%
- FERNET 200字节左右

目录：

LDAP对接

LDAP（Lightweight Directory Access Protocol）是轻量级目录访问协议，广泛应用于企业统一用户管理。有存量大、关系复杂等特点。

社区提供方案

- 修改keystone配置文件
- [ldap]
- url = ldap://localhost
- user = dc=Manager,dc=example,dc=org
- password = samplepassword
- suffix = dc=example,dc=org
- user_tree_dn = ou=Users,dc=example,dc=org
- user_objectclass = inetOrgPerson
- [identity]
- driver = ldap
- domain_specific_drivers_enabled = True
- domain_config_dir = /etc/keystone/domains

- 重启keystone服务

LDAP对接最佳实践

- 界面选择对接LDAP信息
- 使用domain_config存储配置，不需要重启keystone服务

与大规模的集中认证集成

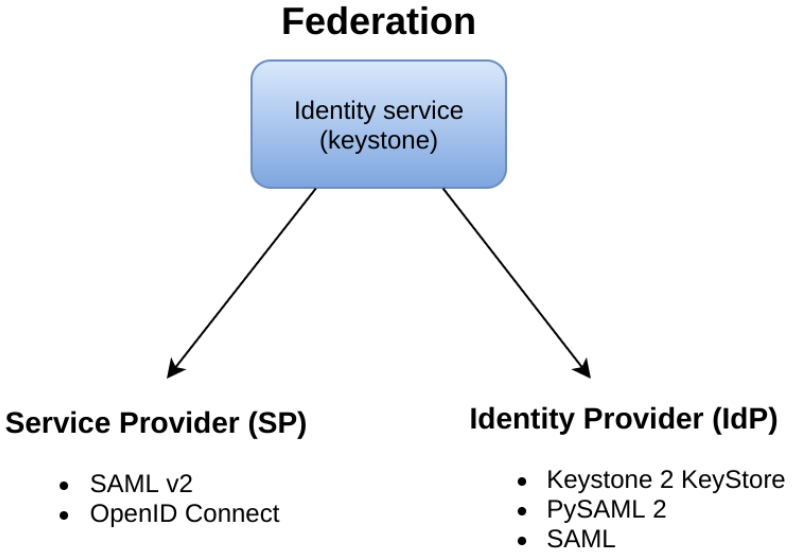
- 使用Fernet Token
- 配置memcache
- 多套OpenStack环境之间同步user、project、domain、role等资源id

目录：

- Openstack Identity简介
- 实践一：LDAP对接
- **实践二：Federation**
- 实践三：Quota运用
- 实践四：Application Credentials
- 社区展望

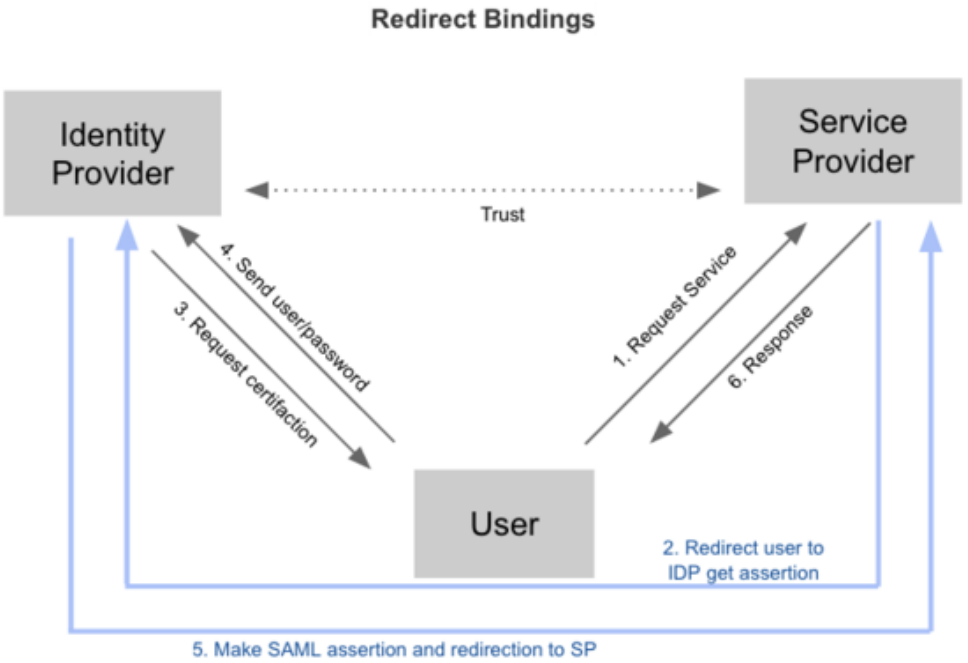
Federation

federation即联邦认证，为最终用户提供一种安全使用现有认证服务的机制。



Federation最佳实践

- OpenStack Multi-Region
- Web SSO



目录：

Quota

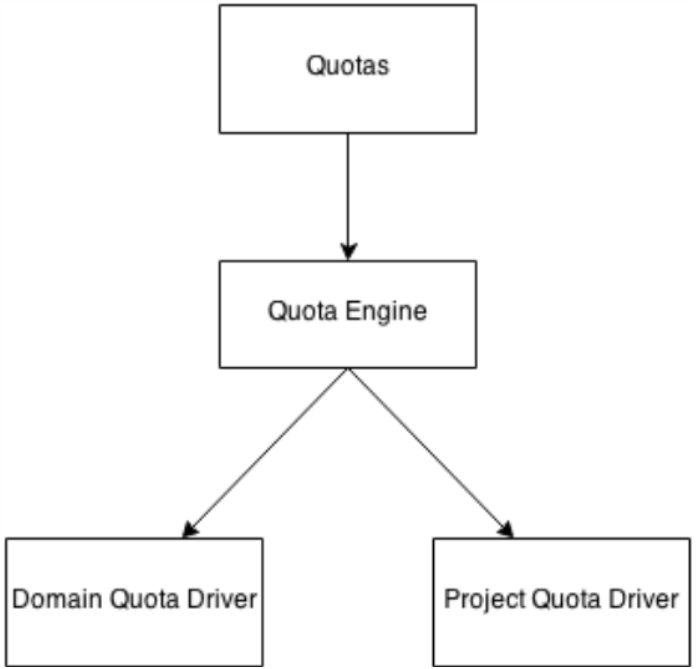
通过配额管理，限制项目资源的使用，防止系统容量在没有通知的情况下消耗殆尽。

项目quota限制的优先级：

- quota > quota_class > conf

Quota最佳实践

- Domain Quota
- Multi-level



目录：

- Openstack Identity简介
- 实践一：LDAP对接
- 实践二：Federation
- 实践三：Quota运用
- **实践四：Application Credentials**
- 社区展望

Application Credentials

应用程序凭证是用户创建的单个项目作用域内的认证方法，用于将其单个项目上的权限子集委托给其他人使用。

- 用户可以拥有自己的secret
- 灵活的权限委托机制
- 以最少的停机时间或无需停机的方式进行适当的rotating

Application Credentials最佳实践

- keystonemiddleware
- 多云管理
- 云应用

```
[keystone_authtoken]
auth_url = https://keystone.server/identity/v3
auth_type = v3applicationcredential
application_credential_id = 6cb5fa6a13184e6fab65ba2108adf50c
application_credential_secret= glance_secret
```

目录：

Queens版本新功能

- application credentials
- system scope & system role assignment
- oslo.policy improvements
- unified limits & flat enforcement
- project tags
- v2.0 API removal

Rocky版本正在实现的功能

- default roles
- unified limits API stabilization
- strict hierarchial enforcement model
- application credentials capability lists
- improved multi-factor authentication

Stein版本展望

- default roles across services
- oslo.limit adoption
- strict hierarchial enforcement model
- federated identity improvements

CHINA
OpenInfra Days

IT大咖说
知识共享平台

Thank You