LCI workshop
on high performance clustered computing

Linux Clusters Institute: OpenStack Keystone

Yale, August 13th – 17th 2018

John Michael Lowe | Senior Cloud Engineer
Indiana University
jomlowe@iu.edu

Jetstream

Keystone

- Tokens
- Domains
- Backends
- Performance
- Deployment considerations

Tokens

Tokens grant time limited access and contain a users identity including the project, role, and domain.

All user and interservice interactions require a valid token which is checked against policy for authorization.

Tokens are included in the X-Auth-Token header for the OpenStack RESTful apis.

```
curl -s \ -H "X-Auth-Token: $OS_TOKEN" \
"http://localhost:5000/v3/domains" | python -mjson.tool
```

Issuing Tokens

The RESTful api can be use directly in this way:

```
curl -i \ -H "Content-Type: application/json" \
-d ' { "auth":
  { "identity": { "methods": ["password"],
          "password": { "user": { "name": "admin",
           "domain": { "id": "default" },
             "password": "adminpwd" } } } } }' \
http://localhost:5000/v3/auth/tokens
```

Issuing Tokens

The openstack cli is used in this way:

```
openstack token issue
```

```
+------------+----------------------------------------------------------------------------+
| Field      | Value                                                                      |
+------------+----------------------------------------------------------------------------+
| expires    | 2018-08-01T19:13:58+0000                                                   |
| id         | gAAAAABbYfhm7DwnUFjDLBszajDvoZeSg9iESY0fxjKSMo3KZxSrh_n6Xh93EOJYGkXjDmdtL4pg1Sp5wGeKQxzobr-
4VumGGv1Gy_ditorUvTZUnb8qE8FM5uncT1RGXgUtaxK-05hXoz661Xvwh5ZW7emzjZcDEj7_lGJ8a6sO39eRp2UyEE |
| project_id | e0c43302e9a740a480d05381d20aa66e
|
| user_id    | eea2fdcc10ee42d0a26ec74caf9a45ad
|
+------------+----------------------------------------------------------------------------+
```

Tokens

UUID

- Generate short unique id
- Keep list of active tokens
- Revocation is easy
- Does not scale well

Tokens

PKI

- Sign a UUID token with expiration
- Token size swells
- Only the signing key and certificate is stored

Tokens

Fernet

- Symmetric encryption of UUID with epiration
- Avoids token bloat
- No PKI infrastructure
- Set of past present and future signing keys must be distributed to all keystone servers

Domains

- Domains are logical buckets to put users, two users can have the same username if they are in different domains
- Authentication methods and backends can be set by domain
- Some higher order services use domains to segregate the trusted service accounts they create

Backends

SQL

- Usernames, groups, and passwords are kept in sql database
- Default domain goes here
- Simple and self contained

LDAP

- Usernames, groups, and password hashes are kept in ldap
- Should use a separate domain
- Read only

External Auth

- Trust Apache to pass an identity validated by simple http auth
- Some restrictions on use with federated identity
- Can support any type of identity that Apache has modules for

Users, Groups, Projects, and Roles

- Projects are first class owning all resources, users cannot own a resource
- Users and groups are assigned roles to allow them to create/read/update/delete resources belonging to a project
- WARNING: Admin role is special, admin on one project is admin over all projects

Performance Considerations

- Fernet tokens are now default, no disk access to validate tokens
- A token is required to ask Keystone if some other token is valid, a service validating a user token takes two validations
- Memcached is an in memory key value store and can be used to cache a token after validation so only a match is required, all services can use the same memcache

Deployment Considerations

- This is the one service that absolutely positively must have over the wire encryption
- Always deployed as a WSGI application behind Apache or Nginx for throughput and TLS

EC2 Credentials

- Keystone can generate and validate AWS style credentials
- A access key and secret key identify a user/domain/project and cannot be used to generate other credentials
- Allows use of stock S3 clients and EC2 clients with appropriately configured OpenStack deployments

Service Catalog

- Keystone keeps the authoritative list of service endpoints for an OpenStack Custer
- Most Clients are configured with only the keystone endpoint and query for other needed endpoints

Resources

- Docs https://docs.openstack.org/keystone/latest/
- Installation Guide https://docs.openstack.org/keystone/latest/install/index.html

Questions