Multi Cloud IaaS with Domain Trust in Openstack

Navid Pustchi, Farhan Patwa, Ravi Sandhu

Quick Summary

Keystone Background:

- ✓Identity service from OpenStack cloud platform.
- ✓Users and resources can be federated within trusted clouds.
- ✓Keystone, Federation internal service can generate and consume SAML assertions to federate users and groups.
- ✓Keystone to Keystone Federation forms a homogenous multi-cloud IaaS platform.

Motivation:

- ✓ Users and resources in federation can only administered by *cloud-admin* which results in inflexible federation administration.
- ✓Federation relation administration is not specified.

Proposed Solution:

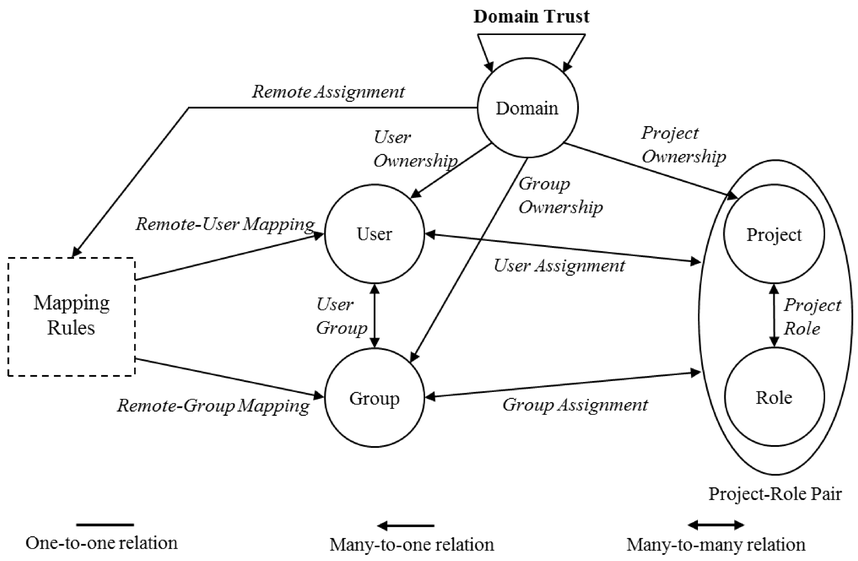
- ✓We present a cross-cloud domain trust model.
- ✓We extend current Keystone model to support domain-trust.
- ✓Domain-trust relation and remote mapping characterizes a fine-grained Federation of domain resources.

Our Scope:

- ✓The solution applies to homogenous federation of Cloud IaaS such as OpenStack.

Technical Details

Multi Cloud OpenStack Access Control (MC-OSAC)



Remote Assignment:

- ✓ CRUD operations in order to create, update and delete mapping rules by *domain-admin*.

Mapping rules:

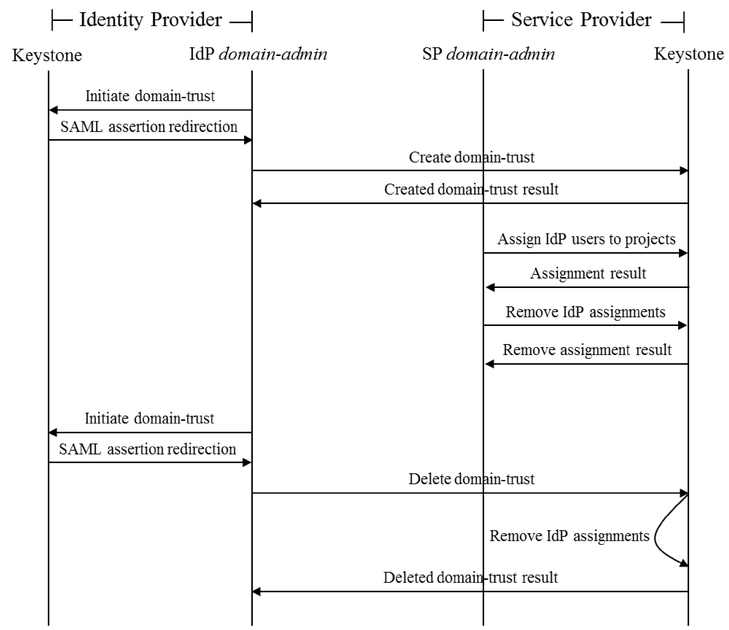
- ✓ Specify federated user to local group or user in json format .

```
{
   "group" {
      "name": "developers",
      "domain": {
         "name": "clients"
      }
   }
},
{
   "group": {
      "id": "89678b"
   }
}
```

Remote mapping:

- ✓ Process of federated user assignment to local users or groups.

Implementation:




```
+--------------------+-----------------+-------------+
| remote_domain | local_domain | trust_type |
+--------------------+-----------------+-------------+
| Default            | default         | beta        |
| domain1            | default         | beta        |
+--------------------+-----------------+-------------+
```

Required Changes:

- ✓Policy file and service is modified to enable *domain-admin* perform CRUD operations on mapping rules.
- ✓*Federated-domain-trust* table stores trust relation in trsustee cloud federation backend.
- ✓Methods are added to assignment service to restrict cross-domain assignments.
- ✓To enable remote assignments for *domain-admin* in federation, we added methods to enable and restrict remote mappings.