Open Source MANO

by ETSI

OSM Multi-tenancy: users, projects and RBAC

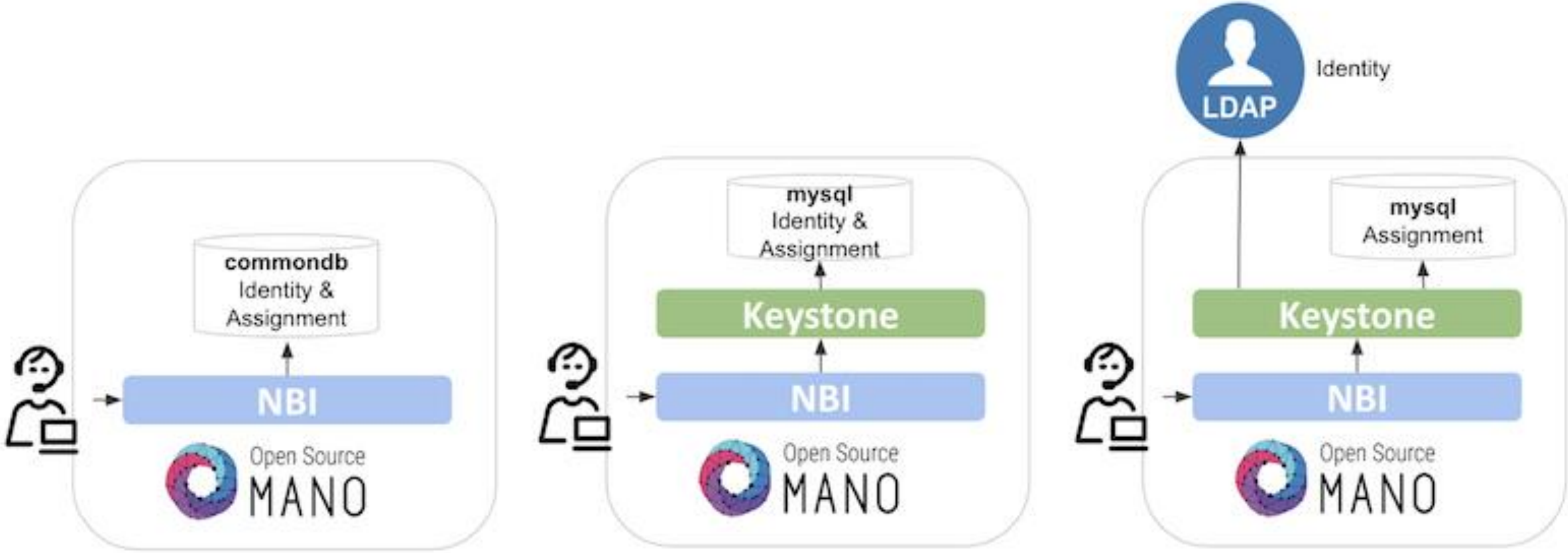
Gerardo García (Telefónica, OSM TSC Chair)

OSM Training Seminar - SLICES

13/02/2024

Role-Based Access Control (RBAC) in OSM

- Role-Based Access Control (RBAC) in OSM provides different users and projects a controlled access to different resources. Authorization is granted if a user has the necessary role to perform an action



Authentication backends

- Two backends
  - Internal: handles identity and assignment resources locally by NBI.
  - Keystone (default): external component to handle identity and assignment resources, together with out-of-the-box integrations (i.e. LDAP).
- LDAP integration
  - When using the Keystone back-end, an external LDAP server may be used for user authentication, whereas the assignment information (RBAC roles/projects) is always stored in the local Keystone mysql database. In this working model, two user and project domains are used.
    - The default domain, in which the external LDAP is not checked, mainly intended for administrative users (e.g. the admin user).
    - The ldap domain, in which the validation of credentials is delegated to the LDAP server. User creation and deletion is also done in the external LDAP, and the GUI and osm client are used for assigning users to projects, and for assigning roles.

Key concepts

- Users can belong to one or more projects
  - Users have a password to authenticate
- Projects can have one or more users
- Projects have quotas, which limit the number of elements that can be added to the project
- Each user in a project has a role, which grants permissions to do certain operations
- Each role consists of a list of NorthBound operations that can be either granted or denied.

User management

- CLI Commands for user management

```
osm user-create                creates a new user
osm user-delete                deletes a user
osm user-list                  list all users
osm user-show                  shows the details of a user
osm user-update                updates user information
```

Project management

- CLI Commands for project management:

```
osm project-create             creates a new project
osm project-delete             deletes a project
osm project-list               list all projects
osm project-show               shows the details of a project
osm project-update             updates a project (only the name can be updated)
```

- Quotas limit the number of elements that can be added on each project.
- Quotas apply to the following elements: vnfds, nsds, slice_templates, pduds, ns_instances, slice_instances, vim_accounts, wim_accounts, sdn_controllers, k8sclusters, k8srepos, osmrepos, ns_subscriptions
- Default value: 500 for each element type

Role management

- CLI Commands for role management:

```
osm role-create                 creates a new role
osm role-delete                 deletes a role
osm role-list                   list all roles
osm role-show                   show specific role
osm role-update                 updates a role
```

- Roles contains permissions with a boolean value of True (granted) or False (denied). If missing it applies the parent permission.
- Global administrative permissions: default, admin
- Per-element permissions

```
nsds: True # grant all operations over nspkgs
nsds:get: True # grant listing nspkgs
nsds:id:get: True # grant showing a concrete nspkg
nsds:id:delete: False # deny deleting a nspkg
```

Role management

```
role-create                creates a new role
role-delete                deletes a role
role-list                  list all roles
role-show                  show specific role
role-update                updates a role
```

By default, OSM is installed with the following pre-created users, projects and roles

- Users: admin, assigned to project admin with role system_admin (system-wide privileges).
- Projects: admin
- Roles:
  - *system_admin.* All operations are allowed. This role cannot be deleted.
  - *account_manager*. Only administrative operations, such as management of users, projects and roles are allowed. End user operations such as onboarding packages or instantiation are not allowed.
  - *project_admin*: allows operations inside the project, but not outside the scope of the project. Administrative operations are not allowed either.
  - *project_user*: allows onboarding packages and instantiation inside the project, but not creation of VIMs, WIMs, etc.

Exercise

- Check the users, roles and projects that you can see in OSM with your user
- Check the role of your user and what you can do
- Try to create a user
- Try to create a project
- Try to create a role

Open Source MANO by ETSI

Thank You!