TFF-16 RBAC Support for Fabric Object - Virtual Port Group

1. Introduction

Purpose of the document

- Blueprint/Feature Lead: sajeesh mathew / Nagendra Prasath Maynattamai Prem Chandran
- Core team: contacts to the core team members
- JIRA EPIC: Unable to locate Jira server for this macro. It may be due to Application Link configuration.

2. Problem statement

There are some use case where multiple customers/tenants sharing the same fabric. Different overlay resources have to be bound to tenants including Virtual Port-Group.

By default a subtending tenant has no fabrics, devices, nor ports visibility. It must be assigned by the super admin (user that on-boarded the fabrics).

Following are the three use cases are addressed in this story
Use case 1 : Cloud admin shares on-boarded physical ports with tenant and tenant creates VPG .
Use case 2 : Cloud admin shares physical router and tenant creates logical router.

3. Proposed solution

- All fabric objects will be owned by the Cloud admin.
- Cloud admin can share objects with other tenants including fabric objects.
- Sharing can be done using UI workflow.
- If a tenant admin is creating an object, that object will be shared with that tenant. Automatic Sharing based on RBAC AUTH_TOKEN of the user will take care of by the API server.
- To support UI workflow, required fabric objects can be shared to tenant admins with “Read” permission .

3.1 Affected Modules

None

3.2 Alternatives considered

3.3 API schema changes

None

3.4 User workflow impact

3.5 UI changes

None

3.6 Operations and Notification impact

None

4. Implementation

Use case 1 : Cloud admin shares on-boarded physical ports with tenant and tenant creates VPG .

1. Cloud admin shares physical port(s) with a specific tenant.
2. Tenant admin creates their own VPG using these physical ports.
3. Tenant admin applies tenant's security policies and other features on this VPG.
4. Tenant admin creates his VLANs (virtual networks) on this VPG.
5. Only the tenant creating the VPG can see the port(s) and the VPG.

Workflow with proposed design

Creation of fabric an onboarding physical routers

- Cloud admin will create the fabric and onboard physical routers and physical ports.
- Cloud admin will be the owner of fabric objects (fabric, physical routers ,physical ports) under global system configuration.

Object Sharing

- Cloud admin will share physical ports with tenant1.
- Cloud admin will share fabric/physical-router with 'R' permission and
physical-port with 'RX' permissions.

VPG creation

- Tenant1 admin will create VPG1 using the physical ports shared with it.
- VPG1 will be owned Cloud admin and automatically shared with tenant1 based on RBAC AUTH_TOKEN of the user .

VLAN association

- Tenant admin for tenant1 will create VMI and VN within the project.
- Tenant admins for tenant1 will associate VMI (VPG1-10) and VN1 with VPG1(which result in VLAN association).
- VN’s or VMI’s shared to tenant1 also can be associated with VPG1.

Port and VPG visibility

- VPG1 will be visible cloud admin and tenant1 admin.
- VPG1 won’t be visible to other tenant admins.(no sharing)
- To support UI workflow we can share Physical port/physical router to tenant1 admin with “Read” permission

Use case 2 : Cloud admin shares physical router and tenant creates logical router.

1. Cloud admin shares a physical router (PR) with other tenants.
2. Tenants create logical routers (LR) on this PR.
3. PR is visible to all tenants. A tenant can see only their LR’s on this PR.

Workflow with proposed design

Creation of fabric an onboarding physical routers
- Cloud admin will create the fabric and onboard physical routers and physical ports.
- Cloud admin will be the owner of fabric objects (fabric, physical routers ,physical ports) under global system configuration.

Object Sharing

- Cloud admin will share physical routers with tenant1. Cloud admin will share fabric with 'R' permission and
physical-router with 'RX' permissions.
- Sharing can be done using UI workflow or using VNC API’s .

LR creation

- Tenant1 admin will create LR R1. R1 will be owned by cloud administrator and shared with tenant1 .
- Public LR and NAT attributes can only be updated by cloud admin . RBAC ACL’s will be added to enforce this restriction.

LR visibility

- Physical Routers will visible to Cloud admin and tenants to which these ports are being shared.
- R1 will be visible cloud admin and tenant admin .

4.1 Assignee(s)

4.2 Work items

5. Performance and scaling impact

5.1 API and control plane

n/a

5.2 Forwarding performance

n/a

6. Upgrade

n/a

7. Deprecations

n/a

8. Dependencies

n/a

9. Testing

9.1 Unit tests

9.2 Dev tests

9.3 System tests

10. Documentation Impact

It will be documented as part of release documentation by the doc team.

11. References

⚠ Unable to locate Jira server for this macro. It may be due to Application Link configuration.