Restricting Access Using Security Domains and Node Rules

Restricting Access by Domains

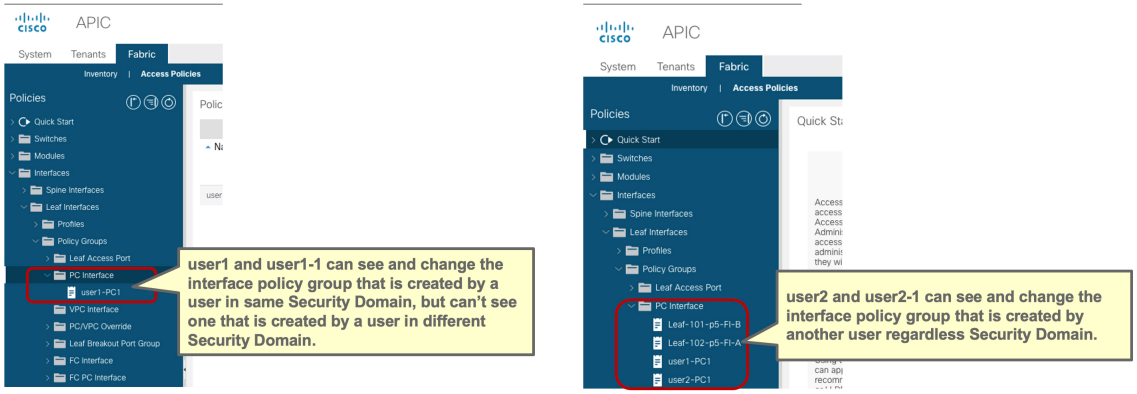
Security domains allow fabric administrators to expose resources selectively to a set of users and provide those users with the required level of permissions to read and modify those resources. By using security domains, multiple set of users can share the underlying infrastructure while having separated management access to their resources.

Starting with Cisco Application Policy Infrastructure Controller (APIC) release 5.0(1), you can configure security domains as "Restricted." A restricted security domain allows a fabric administrator to prevent a group of users from viewing or modifying any objects created by a group of users associated with a different security domain when users in both groups have the same assigned privileges.

For example, a user associated with restricted security domain `domainA` cannot see policies, profiles, or users configured by users associated with security domain `domainB`. Users associated with `domainB` can see policies, profiles, or users configured by users associated with `domainA`, unless `domainB` is also configured as restricted. A user will always have read-only visibility to system-created configurations for which the user has proper privileges. You can give a user associated with a restricted security domain a broad level of privileges within that domain without the concern that the user could inadvertently affect another tenant's physical environment.

The following figure illustrates the concept of restricted security domains:

Figure 1: Restricted Security Domains



Restricted security domains play an important role in providing multi-tenancy capabilities in policies and profiles outside the tenant level, such as in access policies. Even if access policies do not belong to any tenant, by using separated restricted security domains per tenant, users from each tenant can create access policies that are hidden to users in other tenants.

Assigning a Node to a Domain

Using an RBAC node rule, the fabric administrator can assign a physical node, such as a leaf switch, to a security domain. This node assignment allows a user in that security domain to access and perform operations on a node assigned as part of the node rule. Only a user with node management privileges within the security domain can configure nodes assigned to that domain. The user has no access to nodes outside of the security domain, and users in other security domains have no access to the node assigned to the security domain. To create or modify configurations on a node assigned to the security domain, a user in that domain must also be assigned to domain `all` with the `port-mgmt` role that contains the `custom-port-privilege` privilege by default or a custom role that contains the `custom-port-privilege` privilege.

Note When configuring a local user who will manage ports on an assigned node, you must grant the user a role in domain `all`, and the `admin` role in the security domain to which the node is assigned. Both roles must have the **Role Privilege Type** configured as `Write`.

Guidelines and Limitations for Security Domains and Node Rules

When configuring security domains and node rules, follow these guidelines and limitations. In this section, a "restricted node user" is a user in a restricted security domain to which a node has been assigned.

- When upgrading from an earlier Cisco Application Policy Infrastructure Controller (APIC) release to a 5.0 release, you must reconfigure any rules, policies, or roles that use the more granular earlier privileges.
- When downgrading from a Cisco APIC 5.0 release to an earlier release, you must manually edit and retain default roles. Roles modified under a Cisco APIC 5.0 release are retained.
- A spine switch cannot be assigned using RBAC node rules.

- When creating RBAC node rules, you should not assign a node to more than one security domain.
- A restricted node user can configure only policies. An admin user should perform node configuration and troubleshooting.
- A restricted node user can access default system-created managed objects.
- A restricted node user can view fabric-level fault counts in the Fault Dashboard.
- A restricted node user can view node-level faults, such as those from AAA servers, NTP servers, and DNS servers.
- If an admin or nonrestricted domain user associates a relationship policy to an access policy created by a restricted node user, that policy will be visible to the restricted node user.
- You cannot configure a restricted node user using the CLI.
- By default, the `port-mgmt` role has the `custom-port-privilege` privilege that contains predefined access policy managed objects. You can add more managed objects using the procedure in Configuring a Custom Privilege, on page 5.

Creating a Security Domain

Use this procedure to create a security domain.

Step 1 On the menu bar, choose **Admin** > **AAA**.

Step 2 In the **Navigation** pane, click **Security**.

Step 3 In the **Work** pane, select the **Security Domains** tab > **Actions**.> **Create Security Domain**.

Step 4 In the **Create Security Domain** dialog box, perform the following actions:

a) In the **Name** field, type a name for the security domain.

b) Enter a **Description**.

c) To set the security domain as a **Restricted RBAC Domain**, put a check in the **Enabled** check box.

If you configured the security domain as a restricted domain, users who are assigned to this domain cannot see policies, profiles, or users configured by users associated with other security domains.

d) Click **Save**.

Creating a Node Rule to Assign Access to a Node

Use this procedure to configure an RBAC node rule that assigns a physical node, such as a leaf switch, to a security domain.

Before you begin

Create a security domain to which the node will be assigned.

Step 1 On the menu bar, choose **Admin** > **AAA**.

Step 2 In the **Navigation** pane, click **Security**.

Step 3 In the **Work** pane, select the **RBAC Rules** tab > **Node Rules** subtab > **Actions** > **Create RBAC Node Rule**.

The screen is displayed.

Step 4 In the **Create RBAC Rule for Node** screen that is displayed, enter the following details:

a) Click **Select Node ID** to select a node from the drop down list.

b) To assign an **RBAC Rule for Port** , click **Add RBAC Rule for Port**, and enter a name and associate a domain to the rule by clicking **Select Domain** . Click the tick-mark after choosing the domain.

You can assign more than one RBAC rule for the selected port by clicking **Add RBAC Rule for Port** again.

c) Click **Save**.

What to do next

Assign users who will manage the node assigned to the security domain.

Custom Roles and Privileges

Creating a Custom Role with Custom Privileges

Use this procedure to create a role and choose a set of privileges.

Before you begin

Refer to the set of predefined roles and privileges listed in AAA RBAC Roles and Privileges to determine which privileges should be available in the custom role. If you need read or write access to a managed object (MO) that is not exposed in a predefined privilege, you can configure a custom privilege, as described in in Configuring a Custom Privilege, on page 5.

Step 1 On the menu bar, choose **Admin** > **AAA**.

Step 2 In the **Navigation** pane, click **Security**.

Step 3 In the **Work** pane, select the **Roles** tab.

Step 4 In the **Work** pane, click on the Actions icon drop-down list and select **Create Role**.

Step 5 In the **Create Role** screen, perform the following actions:

a) In the **Name** field, type a name for the role.

b) In the **Description** field, type a description.

c) Click **Add Privileges**. In the **Select Privileges** window that is displayed, select one or more privileges for the role, by selecting the required check-box(es).

d) Click **Select** (on the Select Privileges window).

Step 6 Click **Save**.

What to do next

If you selected a custom privilege, such as `custom-privilege-1`, follow the steps in Configuring a Custom Privilege, on page 5 to choose the managed objects (MOs) that will be exposed with this custom privilege.

Configuring a Custom Privilege

Use this procedure to configure a custom privilege, providing read or read/write access to one or more managed objects (MOs) that are not exposed in a predefined privilege.

Managed object classes are described in the Cisco APIC Management Information Model Reference. For each MO class, the reference lists the predefined roles that have read or read/write privileges for that class.

For each predefined privilege, you can see a list of MO classes and the read/write permission by using the Cisco APIC Roles and Privileges Matrix.

To configure a custom privilege with read or write access permission to an MO class, you must use the APIC REST API. For instructions on using the API, see the *Cisco APIC REST API Configuration Guide*.

Compose and send an APIC REST API POST in the format below to create an object of class `aaa:RbacClassPriv`.

Example:

```
POST https://<APIC-IP>/api/node/mo/uni/rbacdb/rbacclpriv-<moClassName>.json

{
    "aaaRbacClassPriv":
    {
        "attributes":
        {
            "name": "<moClasssName>",
            "wPriv": "<privilege>",
            "rPriv": "<privilege>"
        }
    }
}
```

In the *moClassName* value of the URI, include the name of the object class for which you are configuring access.

In the payload, provide the following attributes:

- `name`: Name of the object class for which you are configuring access.
- `wPriv`: Name of the custom privilege that will include write access to objects of the class.
- `rPriv`: Name of the custom privilege that will include read access to objects of the class.

To assign read and write access to a custom privilege, enter the name of the custom privilege in both `wPriv` and `rPriv`.

Example

This example shows how to configure the custom privilege `custom-privilege-1` with both read and write access to objects of the class `fabric:Pod`.

```
POST https://apic-aci.cisco.com/api/node/mo/uni/rbacdb/rbacclpriv-fabricPod.json

{
    "aaaRbacClassPriv":
    {
        "attributes":
        {
            "name": "fabricPod",
            "wPriv": "custom-privilege-1",
            "rPriv": "custom-privilege-1"
        }
    }
}
```

What to do next

Add the custom privilege to a custom role, using the procedure described in Creating a Custom Role with Custom Privileges, on page 4.

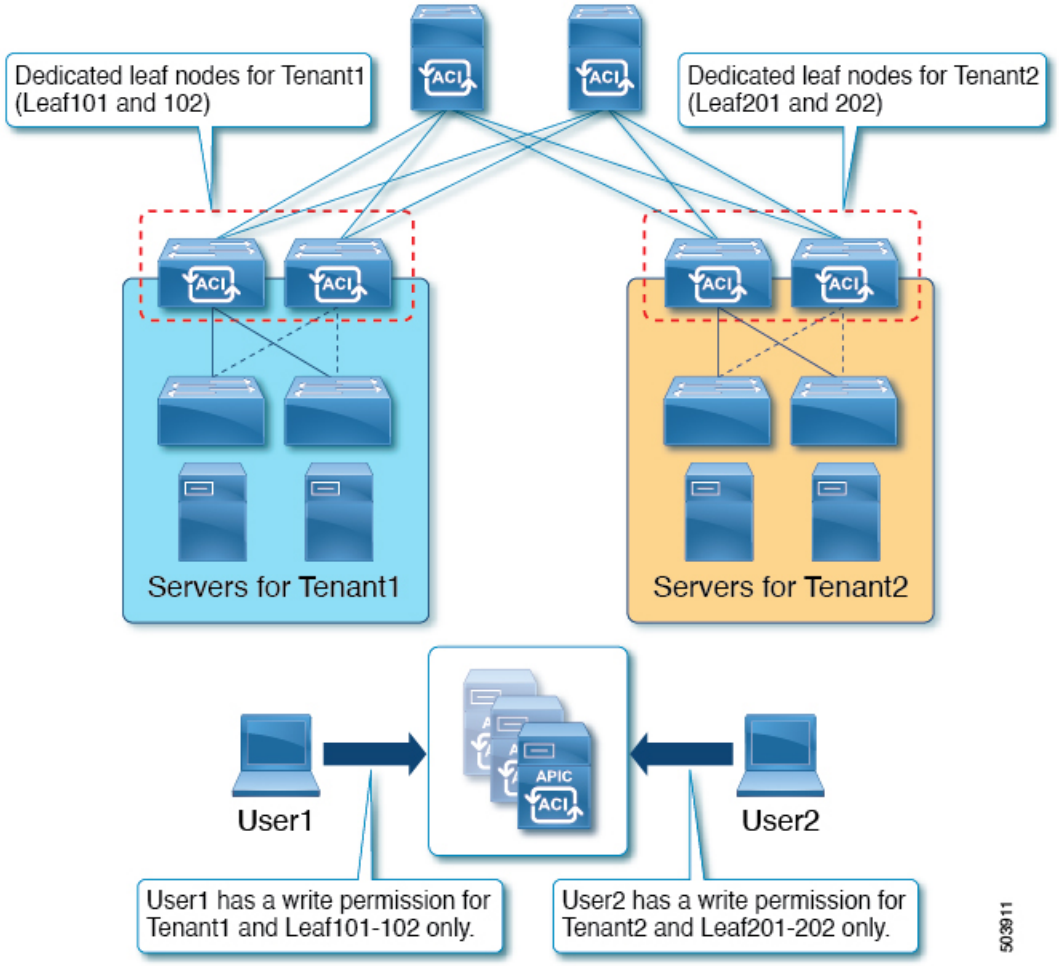
Use Case Example of Configuring an RBAC Node Rule

This section explains a use case that has a mix of configuration options described in this document. See the other parts of this document for information about each option. The use case is based on the following scenario:

Imagine that you have multiple tenants and multiple leaf nodes in your Cisco Application Centric Infrastructure (ACI) fabric. For multi-tenancy, you want to allow a user to manage a specific tenant and a specific set of leaf nodes only. For example:

- User1 can manage only Tenant1, leaf node 101 and 102.
- User2 can manage only Tenant2, leaf node 201 and 202.

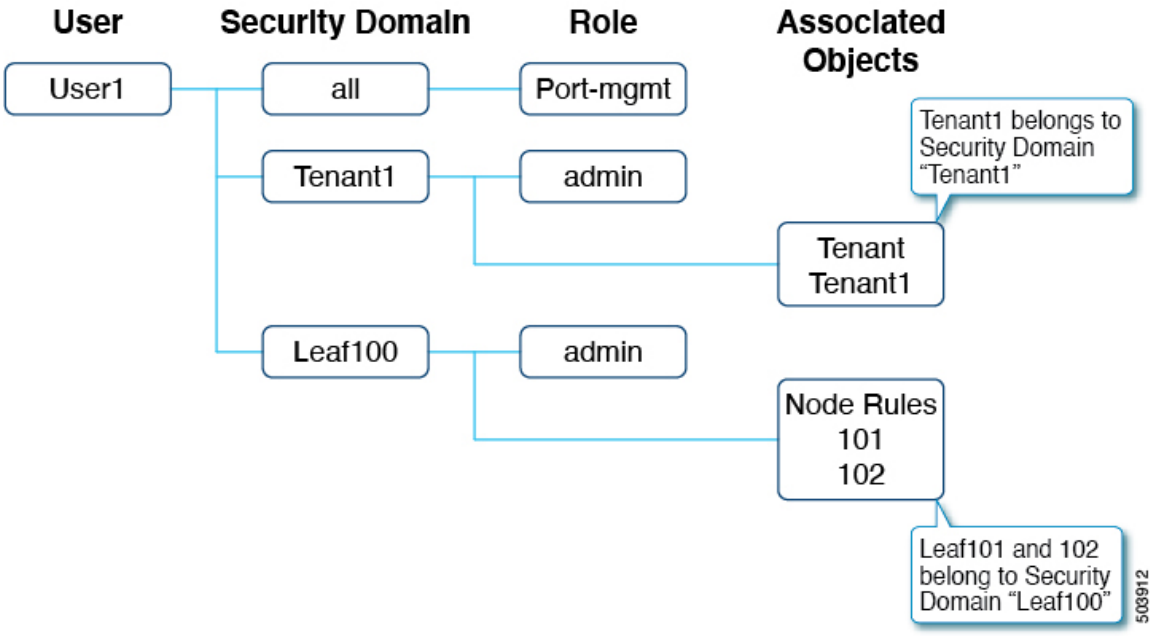
The following figure illustrates the requirements:



This can be achieved by using security domains and RBAC node rules. At a high level, the configuration steps are as follows:

1. Create security domains
2. Create RBAC node rules
3. Create users

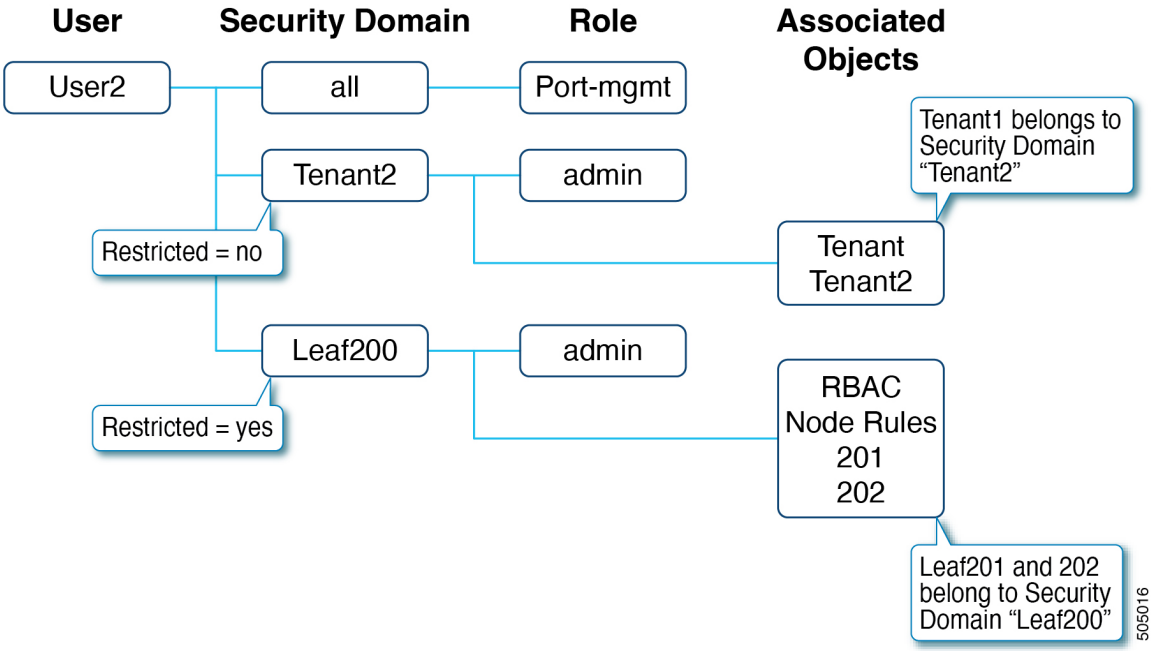
The following figure illustrates the relationship between the configurations for User1 in this example:



User1 has three security domains:

- Domain `all` with `port-mgmt` role: Enables User1 to manage ports related configuration on the assigned leaf nodes.
- Domain `Tenant1` with `admin` role: Enables User1 to manage Tenant1.
- Domain `Leaf100` with `admin` role: Enables User1 to manage Leaf101 and 102.

The following figure illustrates the relationship between the configurations for User2 in this example:



User2 has three security domains as well:

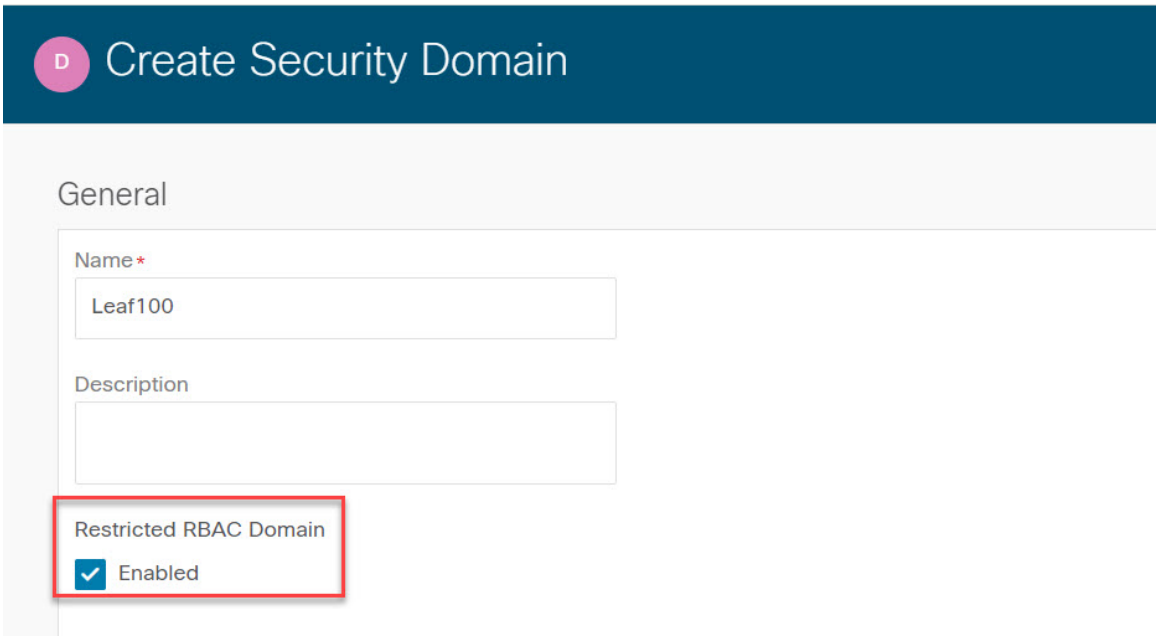
- Domain `all` with `port-mgmt` role: Enables User2 to manage ports related configuration on the assigned leaf nodes.
- Domain `Tenant2` with `admin` role: Enables User2 to manage Tenant2.
- Domain `Leaf200` with `admin` role: Enables User2 to manage Leaf201 and 202.

The following subsections explain the configuration steps in greater detail. The sections describe only the configurations for User1 and Tenant1. The configurations for User2 and Tenant2 follow the same process.

Step 1: Create Security Domains

The first step is to create the security domains: Tenant1 and Leaf100. Although you can combine these security domains, this example uses separate security domains.

To create the domains, in the GUI, go to **Admin** > **AAA** > **Security** > **Security Domains** > **Actions** > **Create Security Domain**.



In this example, **Restricted RBAC Domain** is enabled for security domain Leaf100, which prevents that User1 from seeing the interface policy group, VLAN pool, and other access policies created by other users in different security domains. Exceptions are the default interface policies. Regardless of the **Restricted RBAC Domain** configuration, default interface policies are visible to the leaf RBAC user. That said, if **Restricted RBAC Domain** is enabled, the user cannot make a change to the configuration of the default policies.

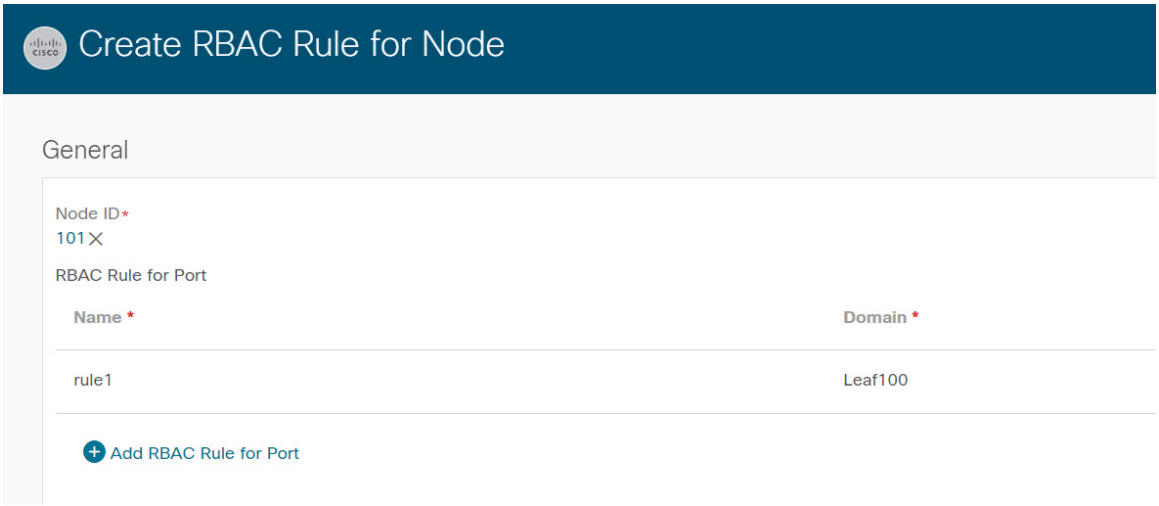
The **Restricted RBAC Domain** is not enabled for security domain Tenant1. For tenant policies, the tenant itself provides enough management isolation, hence it is not required. If you use the same security domain for both tenant RBAC and node RBAC, then enabling the **Restricted RBAC Domain** may be required.

For the tenant RBAC, a tenant must be associated to a security domain. This example associates Tenant1 to security domain "Tenant1." To associate the domains, in the GUI, go to **Tenant** > **Policy** > **Security Domains**.

Step 2: Create RBAC Node Rules

The next step is to create RBAC node rules to add Leaf101 and Leaf102 to security domain Leaf100. To create the RBAC node rules, in the GUI, go to **Admin** > **AAA** > > **Security** > **RBAC Rules** > **Node Rules** > **Actions** > **Create RBAC Node Rule**.

The following figure shows the RBAC rule for node 101:



Repeat the same configuration for node 102.

Step 3: Create Users

The last step is to create a user: User1. To create the user, in the GUI, go to **Admin** > **AAA** > **Users** > **Actions** > **Create Local User**.

At the **Security** and **Roles** configuration steps, choose the following security domains and roles:

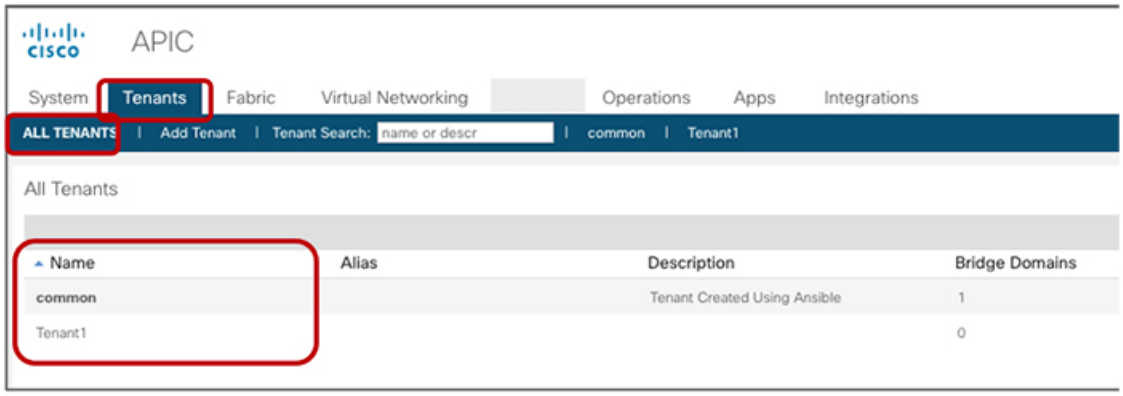
- all: Role `port-mgmt` with the `Write` privilege
- Leaf100: Role `admin` with the `Write` privilege
- Tenant1: Role `admin` with the `Write` privilege

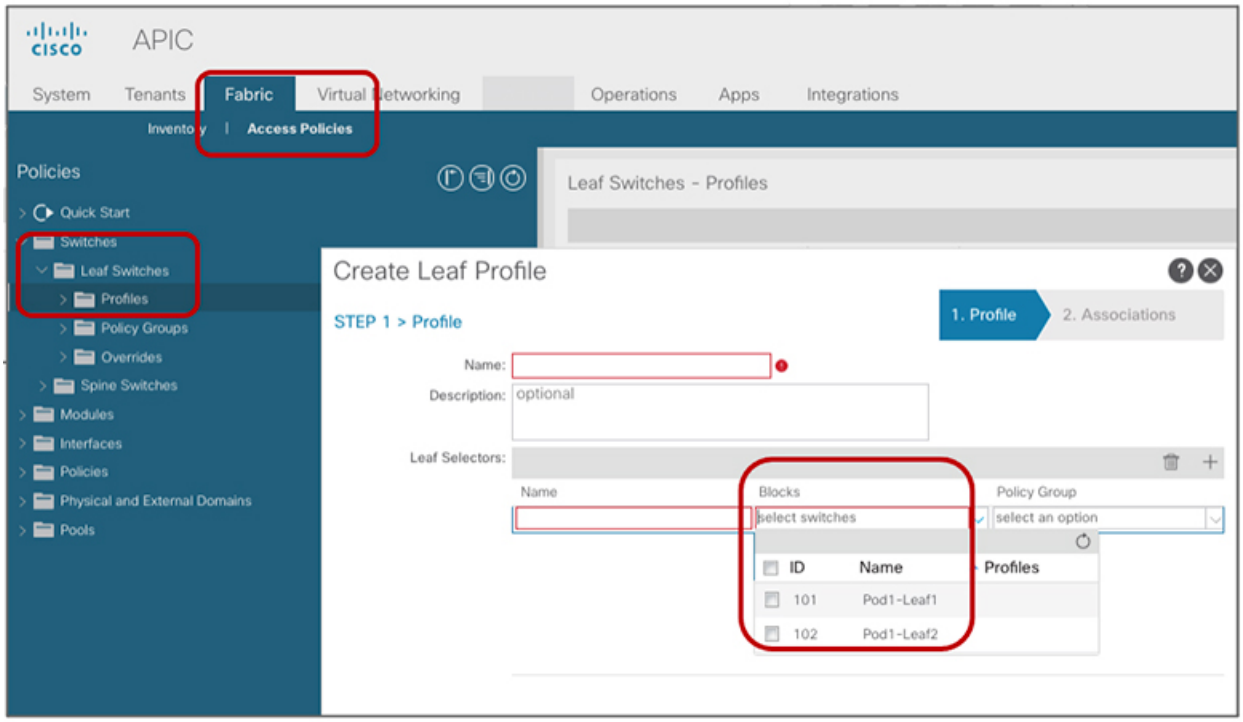
You can use the same configuration for remote users, using either Cisco AVPairs or LDAP group maps, using the procedure described in the "RADIUS, TACACS+, LDAP, RSA, SAML, OAuth 2, and DUO" chapter.

Verifying the RBAC Node Rule

User1 can manage only Tenant1, Leaf 101 and 102. For example:

- User1 cannot see other tenants other than Tenant1 with write privilege and the common tenant with read privilege.
- User1 cannot see other leaf nodes other than Leaf101 and 102 in **Leaf Selectors**.
- User1 cannot see access policies other than those created by users associated with the same security domain, or system-created policies (read-only).


APIC
System
Tenants
Fabric
Virtual Networking
Operations
Apps
Integrations
ALL TENANTS
Add Tenant
Tenant Search:
name or descr
common
Tenant1
All Tenants
Name
Alias
Description
Bridge Domains
common
Tenant Created Using Ansible
1
Tenant1
0


APIC
System
Tenants
Fabric
Virtual Networking
Operations
Apps
Integrations
Inventory
Access Policies
Policies
Quick Start
Switches
Leaf Switches
Profiles
Policy Groups
Overrides
Spine Switches
Modules
Interfaces
Policies
Physical and External Domains
Pools
Leaf Switches - Profiles
Create Leaf Profile
STEP 1 > Profile
1. Profile
2. Associations
Name:
Description:
optional
Leaf Selectors:
Name
Blocks
Policy Group
select switches
select an option
ID
Name
Profiles
101
Pod1-Leaf1
102
Pod1-Leaf2