Restricting Access

Restricting Access by Domains

A restricted security domain allows a fabric administrator to prevent a group of users, such as Tenant A, from viewing or modifying any objects created by a group of users in a different security domain, such as Tenant B, when users in both groups have the same assigned privileges. For example, a tenant administrator in Tenant A's restricted security domain will not be able to see policies, profiles, or users configured in Tenant B's security domain. Unless Tenant B's security domain is also restricted, Tenant B will be able to see policies, profiles, or users configured in Tenant A. Note that a user will always have read-only visibility to system-created configurations for which the user has proper privileges.

For example, consider a user in a restricted security domain is associated to Tenant A. Tenant A includes two application profiles, application profile 1 created by the user and application profile 2 created by an administrator. The user can view only application profile 1 although application profile 2 is also with the same tenant. When a user is in a restricted security domain, even profiles created by administrators are not visible.

In the above example, an unrestricted user (user not in a restricted security domain), can view both, application profile 1 and application profile 2, although application profile 2 was created by another user (administrator).

RBAC Roles

The Cloud Application Policy Infrastructure Controller (cAPIC) provides access according to a user's role through role-based access control (RBAC). A fabric user is associated with the following:

- A set of roles
- For each role, a privilege type: no access, read-only, or read-write
- One or more security domain tags that identify the portions of the management information tree (MIT) that a user can access

The Cloud APIC manages access privileges at the managed object (MO) level. A privilege is an MO that enables or restricts access to a particular function within the system. For example, fabric-equipment is a privilege bit. This bit is set by the cAPIC on all objects that correspond to equipment in the physical fabric.

A role is a collection of privilege bits. For example, because an “admin” role is configured with privilege bits for “fabric-equipment” and “tenant-security,” the “admin” role has access to all objects that correspond to equipment of the fabric and tenant security.

A security domain is a tag associated with a certain subtree in the cAPIC object hierarchy. For example, the default tenant “common” has a domain tag `common`. Similarly, the special domain tag `all` includes the entire MIT object tree. An administrator can assign custom domain tags to the MIT object hierarchy.

Creating a user and assigning a role to that user does not enable access rights. It is necessary to also assign the user to one or more security domains. By default, the cAPIC fabric includes two special pre-created domains:

- All—allows access to the entire MIT
- Infra—allows access to fabric infrastructure objects/subtrees, such as fabric access policies

Cisco Cloud APIC supports the following AAA roles and privileges:

Privilege	Description
Role: admin	
admin	Provides full access to all of the features of the fabric. The admin privilege can be considered to be a union of all other privileges.
Role: aaa	
aaa	Used for configuring authentication, authorization, accounting, and import/export policies.
Role: access-admin	
access-connectivity	Used for Layer 1-3 configuration under infra, static route configurations under a tenant's L3Out, management infra policies, and tenant ERSPAN policies.
access-equipment	Used for access port configuration.
access-protocol	Used for Layer 1-3 protocol configurations under infra, fabric-wide policies for NTP, SNMP, DNS, and image management, and operations-related access policies such as cluster policy and firmware policies.
access-qos	Used for changing CoPP and QoS-related policies.
Role: fabric-admin	

Privilege	Description
fabric-connectivity	Used for Layer 1-3 configuration under the fabric, firmware and deployment policies for raising warnings for estimating policy deployment impact, and atomic counter, diagnostic, and image management policies on leaf switches and spine switches.
fabric-equipment	Used for atomic counter, diagnostic, and image management policies on leaf switches and spine switches.
fabric-protocol	Used for Layer 1-3 protocol configurations under the fabric, fabric-wide policies for NTP, SNMP, DNS, and image management, ERSPAN and health score policies, and firmware management traceroute and endpoint tracking policies.
Role: nw-svc-admin	
nw-svc-policy	Used for managing Layer 4 to Layer 7 service devices and network service orchestration.
Role: nw-svc-params	
nw-svc-params	Used for managing Layer 4 to Layer 7 service policies.
Role: ops	
ops	Used for viewing the policies configured including troubleshooting policies.
Role: port-mgmt	
port-mgmt	Used for assigning a node to a security domain. A user in a security domain with a Node Rule must also be assigned to domain `all` with the role of `port-mgmt`.
Role: tenant-admin	
aaa	Used for configuring authentication, authorization, accouting and import/export policies.
access-connectivity	Used for Layer 1-3 configuration under infra, static route configurations under a tenant's L3Out, management infra policies, and tenant ERSPAN policies.
access-equipment	Used for access port configuration.
access-protocol	Used for Layer 1-3 protocol configurations under infra, fabric-wide policies for NTP, SNMP, DNS, and image management, and operations-related access policies such as cluster policy and firmware policies.

Privilege	Description
access-qos	Used for changing CoPP and QoS-related policies.
fabric-connectivity	Used for Layer 1-3 configuration under the fabric, firmware and deployment policies for raising warnings for estimating policy deployment impact, and atomic counter, diagnostic, and image management policies on leaf switches and spine switches.
fabric-equipment	Used for atomic counter, diagnostic, and image management policies on leaf switches and spine switches.
fabric-protocol	Used for Layer 1-3 protocol configurations under the fabric, fabric-wide policies for NTP, SNMP, DNS, and image management, ERSPAN and health score policies, and firmware management traceroute and endpoint tracking policies.
nw-svc-policy	Used for managing Layer 4 to Layer 7 service devices and network service orchestration.
tenant-network-profile	Used for managing tenant configurations, such as deleting and creating network profiles, and deleting and creating endpoint groups.
tenant-protocol	Used for managing configurations for Layer 1-3 protocols under a tenant, for tenant traceroute policies, and as write access for firmware policies.
tenant-qos	Used for QoS-related configurations for a tenant.
tenant-security	Used for contract-related configurations for a tenant.
Role: tenant-ext-admin	
tenant-connectivity	Used for Layer 1-3 connectivity changes, including bridge domains, subnets, and VRFs; for atomic counter, diagnostic, and image management policies on leaf switches and spine switches; tenant in-band and out-of-band management connectivity configurations; and debugging/monitoring policies such as atomic counters and health score.
tenant-epg	Used for managing tenant configurations such as deleting/creating endpoint groups, VRFs, and bridge domains.
tenant-ext-connectivity	Used for write access firmware policies; managing tenant L2Out and L3Out configurations; and debugging/monitoring/observer policies.

Privilege	Description
tenant-ext-protocol	Used for managing tenant external Layer 1-3 protocols, including BGP, OSPF, PIM, and IGMP, and for debugging/monitoring/observer policies such as traceroute, ping, oam, and eptrk. Generally only used for write access for firmware policies.
tenant-network-profile	Used for managing tenant configurations, such as deleting and creating network profiles, and deleting and creating endpoint groups.
tenant-protocol	Used for managing configurations for Layer 1-3 protocols under a tenant, for tenant traceroute policies, and as write access for firmware policies.
tenant-qos	Used for QoS-related configurations for a tenant.
tenant-security	Used for contract-related configurations for a tenant.

Custom privileges can be assigned to any MO Class. Twenty-two custom privileges are displayed in the Cisco Cloud APIC GUI. If one of these custom privileges is assigned to any class, that MO's access will include the newly added custom privilege. One custom privilege can be associated with one or more MO classes.

Note Although custom privileges are displayed by the Cisco Cloud APIC GUI, they are currently not supported.

A set of predefined managed object classes can be associated with domains. These classes should not have overlapping containment. Examples of classes that support domain association are as follows:

- Layer 2 and Layer 3 network managed objects
- Network profiles (such as physical, Layer 2, Layer 3, management)
- QoS policies

When an object that can be associated with a domain is created, the user must assign domain(s) to the object within the limits of the user's access rights. Domain assignment can be modified at any time.

RBAC Rules

RBAC rules selectively expose resources (such as, application profiles, EPGs, contracts) to users that are otherwise inaccessible because they are in a different security domain. An RBAC rule comprises two parts: the distinguished name (DN) that locates the object to be accessed and the name of the security domain that contains the user who will access the object.

There are two types of RBAC rules:

- Implicit—a user inherits a rule or permission based on RBAC hierarchy
- Explicit—a rule is directly assigned to the user based on certain policies

Both restricted and unrestricted security domains are supported.

Note While an RBAC rule exposes an object to a user in a different part of the management information tree, it is not possible to use the CLI to navigate to such an object by traversing the structure of the tree. However, as long as the user knows the DN of the object included in the RBAC rule, the user can use the CLI to locate it via an MO find command.

Guidelines and Limitations for Restricted Domains

The following are the guidelines and restrictions for the users of restricted domains:

- If a user from one security domain is assigned another security domain, the user gets access to the configurations associated with the new domain.
- A user can be part of one or more security domains which are marked “restricted”.
- Restricted domain users have read-only access to system created configurations.
- For a user with multiple security domains, the combined length of all security domains cannot exceed 1024 characters. If the length exceeds 1024, the user will have policy creation issues.
- Restricted domain on the Cloud APIC is not supported on the cloud resources. This means, a user of one restricted domain will be able to see cloud resources created by a user of another restricted domain.

Creating an RBAC Rule Using the Cisco Cloud APIC GUI

This section explains how to create an RBAC rule using the GUI.

Note You can configure RBAC rules, however the Cloud APIC GUI does not support the configurations. The DN configured using this procedure (step 4) can be queried using API.

Before you begin

Create a security domain. For the detailed task, see Creating a Security Domain.

Step 1 Click the **Intent** icon. The **Intent** menu appears.

Step 2 Click the drop-down arrow below the **Intent** search box and choose **Administrative**.

A list of **Administrative** options appears in the **Intent** menu.

Step 3 From the **Administrative** list in the **Intent** menu, click **Security** > **RBAC Rules** > **Create RBAC Rule**. The **Create RBAC Rule** dialog box appears.

Step 4 In the **DN** field, enter the DN for the rule.

For creating an explicit RBAC rule, locate the DN for the application in ObjectStore. Use that DN value here.

Step 5 Choose a security domain:

a) Click **Select Security Domain**. The **Select Security Domain** dialog box appears.

b) From the **Select Security Domain** dialog box, click to choose a security domain from the column on the left then click **Select**. You return to the **Create RBAC Rule** dialog box.

Step 6 From the **Allow Writes** field, click **Yes** to allow writes or **No** to not allow writes.

Step 7 Click **Save** when finished.

Note After creating an explicit RBAC rule, a user assigned to a security domain will be able to only see the application and its children that were defined earlier (from ObjectStore).