Schema Management

Schema Management

To create schemas in the Cisco ACI Multi-Siteenvironment, you must have the following:

- An administrative user account (with complete read/write privileges).
- A APICtenant user accounts (with read/write tenant policy privileges).

  For more information, see *User Access, Authentication, and Accounting* in the *Cisco APIC Basic Configuration Guide, Release 3.x*.
- An available tenant that contains the policies you want to incorporate into your site.

  For more information, refer to Adding Tenants Using the Multi-Site GUI.

The Multi Site GUI provides complete schema management utilities for your Multi Site implementation.

Using your existing tenant policy information in a provided template you can create schemas for your select APIC sites. The following sections describe creating a template and other schema configuration details what you can configure in your schema template:

Creating a Schema Template

Before you begin

- You must have at least one tenant configured, as described in Adding Tenants Using the Multi-Site GUI.

- You must have the tenant policies imported from Cisco APIC that contains the tenant's VRF, bridge domain, and the Application Profile containing the EPGs to associate with a domain.

Procedure

Step 1 On the **Schema** page, click the **Add Schema** button.

Step 2 On the **Untitled Schema** page, enter a name for the schema you intend to create.

Step 3 Access the **Select A Tenant** dialog box and select a tenant from the drop-down menu.

Note Keep in mind, the user account you're using to create a new schema must be associated with the tenant you are trying to add to it, otherwise the tenant will not be available in the drop-down menu. Associating a user account with a tenant is described in Adding Tenants Using the Multi-Site GUI.

What to do next

After you have selected a tenant, all of the tenant's existing policies are imported into your template.

Click **Import** to push the template to your site.

Configuring an Application Profile

Describes how to configure an Application Profile with EPGs.

Procedure

Step 1 In the AP field, click + **Application Profile**.

Step 2 Enter the AP name.

Step 3 Click + **Add EPG** and enter the EPG name in the Display Name field.

Step 4 Optional. Click + **Subnet** to add a subnet to your EPG, if appropriate.

a) On the **Add Subnet** dialog, enter the **Gateway IP** address and a description for the subnet you plan to add.
b) In the **Scope** field select either **Private to VRF** or **Advertised Externally**.
c) Click the check box for **Shared Between VRFs** if appropriate.
d) Click the check box for **No Default SVI Gateway** if appropriate.
e) Click **OK.**

Step 5 Optional. Select **USEG EPG** if appropriate.

a) Enter the **Name** and **Type** for the **USEG ATTR**.
b) Click + **USEG ATTRIBUTE** to add USeg attributes if appropriate.
c) On the **Add uSeg Attributes** dialog, enter a **Display Name**, **Description**, and **Attribute Type**.
d) Click **SAVE**.

Step 6 Select either **Enforced** or **Unenforced** for the Intra EPG Isolation field.

Step 7 Choose a bridge domain in the **Bridge Domain** field.

Step 8 Click + **Contract** to add a contract if appropriate.

a) On the **Add Contract** dialog, enter the contract name and type.
b) Click **SAVE**.

Configuring a Contract

Provides the procedure for configuring contracts to control EPG communications.

Procedure

Step 1 Click + in the box in the **Contract** pane.

Step 2 Enter a name for the contract in the **Contract** dialog in the **Display Name** field under **Display Name**.

Step 3 Choose a value for **Scope** using the drop-down menu.

Step 4 Click **Apply Both Directions** toggle button to apply the filter specified in the contract to either one direction or both directions.

The default setting is **ON**.

Step 5 Click + **Filter**.

a) On the **Add Filter Chain** dialog, click the **Name** field to choose or find a filter.
b) Optional. Select the available directives in the **Directives** field.
c) Click **SAVE**.

What to do next

After you have configured the contract to your specifications, click **Deploy to Sites**.

Configuring a Bridge Domain

Procedure

Step 1 Click + in the **Bridge Domain** pane to add a new bridge domain.

Step 2 Enter a display name for the bridge domain in the **Bridge Domain** field.

Step 3 Select a VRF in the **Virtual Routing and Forwarding** field if appropriate.

Step 4 Select **L2 Stretch**, if appropriate.

Step 5 If you enabled L2 Stretch, you can choose **INTERSITEBUMTRAFFICALLOW**, if appropriate.

Step 6 If you did not enable L2 Stretch, you can choose either **proxy** or **flood** for the **L2UNKNOWNUNICAST.** field

Step 7 Optional. Click + **Subnet** to add a subnet to your Bridge Domain if appropriate.

a) On the **Add Subnet** display, enter the **Gateway IP** address and a description for the subnet you intend to add.
b) In the **Scope** field, select either **Private to VRF** or **Advertised Externally**.
c) Click the check box for **Shared Between VRFs** if appropriate.
d) Click the check box for **No Default SVI Gateway** if appropriate.
e) Click the check box for **Querier** if appropriate.
f) Click **OK**.

Configuring a VRF for the Tenant

Procedure

Step 1 Click the + in the VRF field.
Step 2 Enter a display name for the VRF in the **Display Name** field.

Configuring a Filter for Contracts

Provides a method to create a filter. A filter is similar to an Access Control List (ACL), used to filter traffic through contracts associated to EPGs.

Procedure

Step 1 Click the + on the Filter object under in the Filter pane.
Step 2 Enter a display name in the **Display Name** field.
Step 3 Click + **Entry** to provide information for your schema filter on the **Add Entry** display:
a) Enter a name for the schema filter entry in the **Name** field on the **Add Entry** dialog.
b) Optional. Enter a description for the filter in the **Description** field.
c) Enter the details as appropriate to filter EPG communication.

For example, to add an entry allowing HTTPS traffic through a filter, choose **TYPE**: **IP**, **IP PROTOCOL**: **TCP**, and **DESTINATION PORT RANGE FROM** and **DESTINATION PORT RANGE TO**: **https**.

d) Click **SAVE**.

Configuring an External EPG

In this schema field, you configure an **EXTERNAL EPG** for each site, to enable the sites to connect. To configure an external EPG for each site, in a site-specific template perform the following steps:

Before you begin

- Create an L3Out in Cisco APIC on all sites where the tenant and VRF are stretched.
- The VRF for each L3Out must be the same for all sites. Changing the VRF in APIC, after the external EPGs are deployed, resets the L3Out and requires reconfiguring and redeploying the external EPG for the site.

Procedure

Step 1 Click + to create an **EXTERNAL EPG**.

Step 2 Enter the external EPG name.

Step 3 Add the contracts required for the external EPGs to communicate.

Note If you are associating a contract with the external EPG, as provider, choose contracts only from the tenant associated with the external EPG. Do not choose contracts from other tenants.

If you are associating the contract to the external EPG, as consumer, you can choose any available contract.

Step 4 Click the site-specific template.

Step 5 Click the external EPG.

Step 6 In the external EPG details pane, **L3OUT** field, choose the L3Out on the site to be used for the external EPG.

What to do next

Optional. You can also add a subnet under the external EPG.

Repeat these steps to create an external EPG for each site.

List of Schemas

After you have create your schema, it displays both on the Dashboard and the Schemas page.

You can use the functionality available on these two pages to monitor the usage and the health of your schema when it is deployed. Also, you can access and edit specific areas of the implemented schema policies using the Multi-Site GUI.

For more information about the functionality of these Multi-Site pages, refer to Overview of the Cisco ACI Multi-Site GUI.

Managing Shared Services Shadow EPGs and BDs

When the EPGs in the Shared Services use case provider site group and consumer site group are in different VRFs and communicate through global contracts, the EPGs and bridge domains (BDs) deployed to one group of sites are mirrored in the other group of sites, so that in all these APIC sites they appear to be deployed,

when they were actually deployed in only one of the site groups. These mirrored objects are known as "shadow EPGs or BDs".

For example, if the provider site group tenant and VRF are stretched across Site 1 and Site 2, and the consumer site group tenant and VRF are stretched across Site 3 and Site 4, in the APIC GUI at Site 1, Site 2, Site 3, and Site 4, you can see both tenants and their policies. They appear with the same names as the ones that were deployed directly to each site. Perform the following steps in the APIC GUI to distinguish the "shadow" EPG or BD from the other one. This is expected behavior and the shadow objects should not be removed.

Before you begin

In Cisco ACI Multi-Site, deploy the Shared Services with Stretched Provider EPG use case, including:

- A schema and template for a provider site group with a stretched tenant and VRF, and an EPG providing a global contract
- A schema and template for a consumer site group with a different tenant and VRF, and EPGs that consume the global contract

Procedure

Step 1 To identify a shadow EPG in a pair of EPGs with the same name, in the APIC GUI, navigate to **Tenants** > ***tenant-name*** > **Application Profiles** > ***ap-name*** > **Application EPGs** > ***epg-name*** > **Static Ports**.

A shadow EPG has no path to the static port.

Step 2 To identify a shadow BD from a pair of BDs with the same name, in the APIC GUI, navigate to **Tenants** > ***tenant-name*** > **Networking** > **Bridge Domains** > ***bd-name*** > **Subnets** > ***subnet-name***.

The subnet for a shadow BD has **No Default SVI Gateway** enabled.