Modeling an Application with Cisco ACI Multi-Site Policy Manager

Introduction

Cisco® Application Centric Infrastructure (Cisco ACI™) Multi-Site is the policy manager component used to define intersite policies that need to be deployed across separate Cisco ACI fabrics that are part of the same multisite architecture.

The goal of this document is to describe how to use the Cisco ACI Multi-Site policy manager to deploy the specific use case shown in Figure 1.
In this use case, three separate Cisco ACI fabrics are interconnected and part of the same multisite architecture. The first two fabrics represent tightly coupled sites, characterized by having common stretched objects (tenant, Virtual Routing and Forwarding [VRF], Bridge Domain [BD], and Endpoint Group [EPG] objects). The third fabric represents a separate site offering shared services to the first two sites. The networking view for this use case is shown in Figure 2.
The following are the characteristics of the objects defined in the three fabrics:

- Tenant A and VRF A are stretched between Sites 1 and 2.
- EPG1, EPG2, and BD1 are also stretched between those sites.
- BD2 and BD3 are not stretched and have unique IP subnets assigned to them.
- Tenant-Shared and all the corresponding objects (VRF, BD, and EPG) are defined only locally at Site 3.
- EPG1 is consuming the contract C1 provided by EPG2 at Sites 1 and 2.
- EPG1 is also consuming the contract C2 provided by EPG-Shared, which is hence offering shared services to Tenant A.

**Note:** Multiple tenants may be accessing the shared service at Site 3. For simplicity, this example shows only one.

The rest of this document describes the specific configuration steps required to satisfy the specific requirements listed here.

The document assumes that the initial configuration steps to set up a Cisco ACI Multi-Site architecture have been completed already. It also assumes that the different Cisco ACI fabrics are managed by the Cisco ACI Multi-Site policy manager and have successfully established Multiprotocol Border Gateway Protocol (MP-BGP) Ethernet VPN (EVPN) peering with each other.

The proposed approach consists of defining a schema with two separate templates. The first template will be used to push the configuration for the stretched objects at Sites 1 and 2. The second template will be used for the local configuration of Site 3.

**Note:** It is possible to use two separate schemas: each one with associated the corresponding template described here. Schemas are just logical grouping of policies, so functionally both models would behave similarly. As a best practice, closely related applications should belong to the same schema, and larger applications and more complex shared services (where more than two or three consumer applications exist) should use separate schemas.

**Creating the template for Cisco ACI Sites 1 and 2**

After connecting to the Cisco ACI Multi-Site GUI, the first step is to define the first Tenant A, as shown in Figure 3.

**Figure 3. Adding Tenant A**
The created Tenant A should then be associated (hence created) at Sites 1 and 2 (in this specific example they are called San Jose and San Francisco, as shown in Figure 4).

Figure 4. Associating Tenant A with Sites 1 and 2

Notice the Tenant A can also be associated with one or more security domains, which must have been previously created inside each specific Cisco Application Policy Infrastructure Controller (APIC) domain. The use of security domains allows you to define the portions of the Management Information Tree (MIT) that a user can access (hence, the specific set of objects with which the user will be able to interact). For more information about APIC security domains, refer to the following document: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/aci-fundamentals/b_ACI-Fundamentals/b_ACI-Fundamentals_chapter_01010.html.
The next step consists of adding a schema (which in this example will be named ACI Multi-Site Use Case, as shown in Figure 5).

Figure 5. Adding a new schema

The newly created schema will by default have a template associated with it. Rename the template Sites 1-2 Template and associate it with Tenant A, as shown in Figure 6. This is the template used to push the configuration to the first two sites.

Figure 6. Associating the first template with Tenant A

Note: In the first Cisco ACI Multi-Site implementation, the template represents the atomic unit for change of scope. Therefore, any policy change made to the template will always be applied and pushed at one time to all the sites associated with that template.

The template can be associated with the sites to which it should be deployed (Sites 1 and 2) by clicking the + sign on the left next to the keyword Sites (Figure 7).
As shown in Figure 7, you must make sure that the correct template—Sites 1-2 Template—and only that one template, gets associated with the sites. After you click Save, the GUI shows that the template has been indeed associated with the sites (Figure 8).

The yellow symbol corresponding to each site indicates that the defined template has not been deployed yet to the sites (this information can also be seen by moving the mouse over the symbol).

Note: The same symbol will appear every time configuration drift occurs between the template and the policies that are actually implemented in an APIC domain. Drift would occur, for instance, if a user were to locally modify on the APIC an object originally pushed from the Cisco ACI Multi-Site policy manager.
The next configuration step consists of creating the application profile Sites 1-2 AP and defining the two EPGs: EPG1 and EPG2 (Figure 9).

Figure 9. Defining the application profile and associated EPGs

The boxes for the defined EPGs are shown in red because they have not yet been associated with their corresponding bridge domains (this association will be performed in a subsequent step). When defining the EPGs, you must also associate a domain (virtual, physical, etc.) with them, so that you can specify the type of endpoints that can be deployed as part of those security groups. In the example in Figure 2, virtual machines are associated with the bridge domains and EPGs deployed at Sites 1 and 2, so you can assign the desired Virtual Machine Manager (VMM) domain with the EPGs, as shown in Figure 10.

Note: This association is performed at the site level by selecting the specific site first. This approach is needed because the desired VMM domain must first be configured in the site-specific APIC. It can then be used by the Cisco ACI Multi-Site policy manager.

Figure 10. Associating a VMM domain with the EPG
You can now define the bridge domains, starting with BD1, which is to be stretched across Sites 1 and 2 (Figure 11).

Figure 11. Defining bridge domain BD1

Notice that by default three flags are enabled for the newly created bridge domain:

- **L2STRETCH**: This flag indicates that the bridge domain should be stretched across both sites, which implies that the associated IP subnet 10.10.1.0/24 will also be available in the two sites.

- **INTERSITEBUMTRAFFICALLOW**: This flag indicates that flooding is enabled across the sites for Layer 2 broadcast, unknown unicast, and multicast frames. This capability is required, for example, to allow live migration of endpoints and to deploy intersite application clusters. If this flag was not set, the same bridge domain and associated IP subnet would still be deployed at the two sites (because the bridge domain is stretched), but the deployment could handle only intersite “cold” IP mobility scenarios (for example, for disaster-recovery use cases).

- **OPTIMIZEWANBANDWIDTH**: This flag helps ensure association of a unique multicast group with this bridge domain. This feature optimizes the utilization of WAN bandwidth because it prevents flooding across a site’s broadcast, unknown unicast, and multicast frames that are associated with different bridge domains that, even if they are not configured as stretched, may have been assigned the same multicast group.

**Note**: The flooding of broadcast, unknown unicast, and multicast frames associated with a given bridge domain across sites is implemented by one spine elected as the designated forwarder and performing head-end replication (that is, multicast is not required in the Layer 3 infrastructure that interconnects the sites).

The recommended approach is to keep the default Proxy option to help ensure that Layer 2 unknown unicast traffic is sent across sites from the spine nodes, but only if the destination endpoint has been discovered and advertised from a specific remote site through an MP-BGP EVPN update. If the endpoint is not known by the local spine nodes, the traffic will be dropped without being flooded across sites (which is the desired behavior).

Notice that at this point BD1 has not been associated with a VRF instance (hence its box is also shown as red). This association will occur in a subsequent step. Before creating this association, create bridge domain BD2, which is not to be stretched across sites (Figure 12).
Because the bridge domain is not stretched, you cannot assign an IP subnet to it in this step. The IP subnet becomes a site local value that can be configured after you select the site (in the left panel) and click the specific bridge domain, as shown in Figure 13.

Figure 13. Configuring the site-local IP subnet associated with BD2
Now configure the gateway IP addresses 10.10.2.254/24 for San Jose (Site 1) and 10.10.3.254/24 for San Francisco (Site 2).

At this point, you can return to the template level, define a new VRF instance (VRF A), associate BD1 and BD2 with VRF A, and associate EPG1 with BD1 and EPG2 with BD2. If all those steps are completed correctly, selecting BD1 will show that it is associated with VRF A and also with EPG1, as shown in Figure 14 (the same will be true for BD2).

![Figure 14. BD1 association with VRF A and EPG 1](image)

The last step required to implement the configuration shown for Sites 1 and 2 in Figure 1 consists of creating the contract C1 and verifying that EPG2 is providing it and that EPG1 is consuming it. In this specific example, C1 is used to provide HTTP access (hence it has an associated HTTP filter), and it has VRF scope because it is used only between EPGs that are defined as part of the same VRF A (Figure 15).

![Figure 15. Creating contract C1 with associated filter HTTP](image)
The specific rules associated with the HTTP filter can then be configured by selecting the filter (Figure 16).

**Figure 16.** Creating a specific entry for the HTTP filter

![ACI Multi-Site Use Case](image)

The rule Permit HTTP simply identifies (and implicitly permits) traffic destined for TCP port 80, as shown in Figure 17.

**Figure 17.** Permitting traffic destined for TCP port 80

![Update Permit HTTP](image)

Finally, the defined contract C1 can be associated with EPG2 (the provider of the contract) and EPG1 (the consumer). After performing those steps, select the contract C1 in the GUI to immediately verify the EPGs that are consuming it and providing it (Figure 18).
As shown in Figure 18, C1 has two local relationships, because it is consumed and provided by EPGs that are part of the VRF instance in scope for this contract.

The template can now be pushed to Sites 1 and 2, so that the associated configuration can be implemented in each APIC domain (Figure 19).

If the pushing of the configuration is successful, each APIC will return this information to the Cisco ACI Multi-Site policy manager, which would reflect it as shown in Figure 20.
At this point, virtual machines connected to EPG1 can access virtual machines connected to EPG2 through HTTP, independent of the specific location (Site 1 or 2) at which they are deployed. The Cisco ACI Multi-Site architecture provides the required intersite connectivity and policy enforcement.

Creating the template for Cisco ACI Site 3

The template configuration for Sites 1 and 2 is completed. Now you can create a new template (named Site 3 Template) to push the local-only configuration to that fabric. The template must be associated only with Site 3 (New York in our specific example), which implicitly ensures that no objects will be stretched to other sites. Even so, when BD3 is configured, you should explicitly select the flag not to stretch it.

The configuration steps required to create all the objects for Site 3 are similar to the ones already performed for Sites 1 and 2, and they are hence not detailed here.

After the template is successfully deployed at Site 3, the GUI should show the existence of another template associated only with Site 3 and containing all the objects, as shown in Figure 21.

Figure 21. Template deployed at Site 3 (New York)

Defining and applying policy for shared services access

The only remaining step consists of defining the policy that allows EPG1 at Sites 1 and 2 to consume contract C2 provided by EPG-Shared at Site 3. To achieve this, you define contract C2 as associated with Site 3. As shown in Figure 22, the contract should be defined with global scope, because it needs to be used between EPGs deployed across tenants (EPG1 in Tenant A and EPG-Shared in Tenant-Shared).
Figure 22. Defining contract C2 at Site 3 (with global scope)

Contract C2 has a specific Allow DNS filter associated with it to allow EPG-Shared to provide shared Domain Name System (DNS) services. As a consequence, you then must verify that EPG1 at Sites 1 and 2 consumes contract C2, to provide access to this shared DNS service (Figure 23).

Figure 23. EPG1 consuming contract C2
The information that EPG1 is consuming the C2 contract is displayed at the bottom right of screen shown in Figure 23. The C2 contract is not displayed as part of the central Contract section of Sites 1-2 Template, because it was defined as part of Site 3 Template, which contains the EPG provider of that contract. When selecting contract C2 in this template, you can see that a local relationship is established with EPG1 defined as part of Sites 1-2 Template (Figure 24).

Figure 24. Local relationship for contract C2

Note: An external relationship (and not a local one) would be shown between the EPGs if they were part of templates associated with different schemas.

Conclusion

All the configuration information needed to allow inter-tenant communication (with the correct policy enforcement) is now put in place in each APIC domain as a result of the pushing of the configuration from the Cisco ACI Multi-Site policy manager.

For more information