Managing Tenants

- Tenants, on page 1
- Virtual Routing and Forwarding (VRF), on page 5
- Bridge Domains, on page 7
- Application Profiles, on page 10
- End Point Groups, on page 12
- Contracts, on page 17
- Adding Contracts to EPGs, on page 20
- Contract Labels, on page 23
- Fabric Extender (FEX), on page 25

Tenants

A tenant is a logical container for application policies that enables you to exercise domain-based access control by isolating the resources such as applications, databases, web servers, network-attached storage, virtual machines, firewalls, Layer 4 to Layer 7 services, and so on. Tenants can represent a customer in a service provider setting, an organization or domain in an enterprise setting, or just a convenient grouping of policies.

A fabric can contain anywhere from one tenant, which may be useful for a small commercial environment, to 64,000+ tenants, for a cloud service provider in which case you assign each company their own tenant. Another use case would be to have a Dev tenant and a Production tenant. In this case, you create network constructs, EPGs, and policies in Dev tenant first and then simply copy it to the Production tenant. It ensures that the dev and prod are the exact same and takes away the human error that comes along with manual copying of these objects.

Note Configure a tenant before you can deploy any Layer 4 to Layer 7 services.

Tenant Types

The system provides the following four kinds of tenants:

- User tenant—Defined by the administrator according to the needs of users. It contains policies that govern the operation of resources such as applications, databases, web servers, network-attached storage, virtual machines, and so on.

- Common tenant—Provided by the system but can be configured by the fabric administrator. It contains policies that govern the operation of resources accessible to all tenants, such as firewalls, load balancers, Layer 4 to Layer 7 services, intrusion detection appliances, and so on.
- Infrastructure tenant—It contains policies that govern the operation of infrastructure resources such as the fabric VXLAN overlay.
- Management tenant—It contains policies that govern the operation of fabric management functions used for in-band and out-of-band configuration of fabric nodes.

Tenant Features

- Tenants can be isolated from one another or can share resources.
- Tenants do not represent a private network.
- Entities in the tenant inherit its policies.
- The primary elements that the tenant contains are filters, contracts, outside networks, bridge domains, Virtual Routing and Forwarding (VRF) instances, and application profiles that contain endpoint groups (EPGs).

Note In the APIC GUI under the tenant navigation path, a VRF (context) is called a private network.

Setting up a Tenant

This procedure provides an overview of how to set up a tenant for an APIC account in Cisco UCS Director.You can also use the workflows provided in Cisco UCS Director Orchestration to complete a guided setup of tenants for various use cases. For more information, see Cisco UCS Director Orchestration Guide.

This procedure assumes that you have already completed the following prior to creating tenants:

- The Day 0 setup of ACI fabric.
- The nodes in ACI fabric are connected and discovered.
- The APIC controller cluster has been configured.
- Cisco UCS Director is configured and the ACI pod has been set up.

Step 1 Create a Tenant.

See Creating a Tenant, on page 3.

Step 2 Create a Virtual Routing and Forwarding (VRF) (also known as Private Network).

See Creating a VRF, on page 6.

Step 3 Add Bridge Domain to the VRF.

See Adding a Bridge Domain to VRF, on page 7.

Step 4 Create Application Profiles.

See Creating an Application Profile for the Tenant, on page 11.

Step 5 Create EPGs.

See Adding an EPG, on page 12.

Step 6 Add domain to EPGs.

See Adding a Domain to an EPG, on page 13.

Step 7 Add Static path to EPGs.

See Adding a Static Path to EPG, on page 14.

Step 8 Create Contracts.

See Creating Contracts, on page 18.

Step 9 Add contracts to EPGs.

See Adding a Consumed Contract to an EPG, on page 21.

See Adding a Provided Contract to an EPG, on page 20.

Creating a Tenant

Before you begin

Verify that Tags, monitoring policy, and security domains for the objects in the APIC account are configured before adding a tenant.

Create users in ACI and assign a security domain to the users or user groups. See User Access, Authentication, and Accounting chapter in Cisco APIC Basic Configuration Guide.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click **Add**.

Step 6 On the **Add APIC Tenant** screen, complete the fields, including the following:

a) Add a unique name and description for the Tenant.

b) (Optional) Click **Select** and check the tag you want to use.

Tags are used to assign a descriptive name to a group of objects. For example, to enable easy searchable access to all web server EPGs, assign a web server tag to all such EPGs. Web server EPGs throughout the fabric can be located by referencing the web server tag.

c) (Optional) Click **Select** and check the monitoring policy that you want to use.

When you apply a monitoring policy, it overrides the default monitoring policy.

d) Click **Select** and check the security domain that you want to use.

It is necessary to also assign the user to one or more security domains. By default, the ACI fabric includes two special pre-created domains:

- **All**—Allows access to the entire management information tree (MIT).
- **Infra**—Allows access to fabric infrastructure objects/subtrees, such as fabric access policies.

For example, if you have created a security domain for Production, given users roles, and attached them to that security domain, then choose the Production security domain instead of **All**.

e) Click **Submit**.

What to do next

After creating a tenant, create a VRF (also known as a private network) for the tenant.

Viewing Tenants

You can view a list of tenants that are onboarded in Cisco UCS Director and its details.

Step 1 Choose **Policies** > **Resource Groups**.

Step 2 On the **Resource Groups** page, click **Tenant**.

Step 3 Click the row with the tenant for which you want to view details.

Step 4 Click **View Details** to view the service offerings of the tenant.

Step 5 Click the row with the service offering and click **View details** to view the resource groups of a tenant.

Note If the disaster recovery support is enabled for the tenant, the resource groups of the primary site and the disaster recovery site are displayed.

Step 6 Click the row with the resource group and click **View details** to view the following information:

- **Resource Entity**—Displays a list of available resources, such as, VMWare cluster, resource pool, and data store, in a vPOD. During tenant onboarding, the resources matching the capacity, capability and tag of the tenant requirement are filtered from resource group and matched resources are added to the vPOD. With the capacity expansion support, the vPOD can store more than one resources for each resource type such as VMware cluster, resource pool, and storage pool. As multiple resources of same resource type is available in vPOD, the tenant expansion is possible after consumption of allocated resources.

  The tenant-specific and container-specific resource limits assist in provisioning VMs and BMs. During provisioning, all the available resources in vPOD are referred to find out the matching resources for resource allocation. After the resource filtration and selection, the matching resources from the same account are allocated for VM deployment.

  When a resource is no longer consumed by the container, you can delete the resource. To delete the resource, click the row with the resource and click **Delete**.

- **Tenant Details**—Displays more details of the tenant.
- **Tenant Resource Limits**—Displays availability of both virtual and physical resources in a tenant. The resources reserved during tenant onboarding are displayed along with the used and available resource values. The VDCs Limit

column specifies the maximum number of containers that are reserved for the tenant. The Available Number of VDCs column represents the number of containers that are available for provisioning. The physical resource limits display the blades that are reserved as part of tenant onboarding, along with the number of blades used for bare metal provisioning.

- **Container Resource Limits**—Displays availability of both virtual and physical resources in a container. The resource limits that are set during container creation are displayed along with the used and available resources.

  Note If a container is created without a resource limit, the value of the virtual resources is displayed as Not Set.

- **Private Network**—Displays the private networks created for the tenant. Click the row of a private network and click **View Details** to view the supernet and subnet pools of the private network. The **Supernets** screen lists the supernets available for the tiers. The **Subnets** screen displays the sub-network pool that is used for load balancer configuration during the container deployment.

Virtual Routing and Forwarding (VRF)

A Virtual Routing and Forwarding (VRF) is similar to a virtual router that defines a Layer 3 address domain. It is an IP technology that allows multiple instances of a routing table to coexist on the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflict. For example, a production VRF could be on the same network as the development VRF but the two have different default gateways.

A tenant can have multiple VRFs (also known as private network). One or more bridge domains are associated with a VRF. There are several policies you can associate with a private network, including OSPF and BGP timers, as well as how long end points should be retained.

Virtual Routing and Forwarding (VRF) Guidelines

The following guidelines and limitations apply for virtual routing and forwarding (VRF) instances:

- Within a single VRF instance, IP addresses must be unique. Between different VRF instances, you can have overlapping IP addresses.
- If shared services are used between VRF instances or tenants, make sure that there are no overlapping IP addresses.
- Any VRF instances that are created in common tenant is seen in other user-configured tenants.
- VRF supports enforced mode or unenforced mode. By default, a VRF instance is in enforced mode, which means all endpoint groups within the same VRF instance cannot communicate to each other unless there is a contract in place.
- Switching from enforced to unenforced mode (or the opposite way) is disruptive.

For more in-depth information, see the Cisco Application Centric Infrastructure Fundamentals Guide.

Creating a VRF

A Virtual Routing and Forwarding (VRF) object (also known as private layer 3 network in ACI) contains the Layer 2 and Layer 3 forwarding configuration, and IP address space isolation for tenants. Each tenant can have one or more VRFs, or share one default VRF with other tenants as long as there is no overlapping IP addressing being used in the ACI fabric.

Before you begin

Verify that you have configured the BGP Timers Policies and OSPF Timers

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Private Networks**.

Step 7 Click **Add**.

Step 8 On the **Add Tenant Private Network** screen, complete the following fields:

a) Add a unique name for the private network.

b) From the **Policy Enforcement** drop-down list, choose from the following options:

- **Enforced**—Security rules (contracts) are enforced.
- **Unenforced**—Security rules (contracts) are not enforced.

The default is **enforced**.

c) Enter the description for the private network.

d) Click **Select** and check the BGP timer that you want to use.

The Border Gateway Protocol (BGP) timer policy enables you to specify the intervals for the periodic activities and supplies two options for graceful restart control.

e) Click **Select** and check the OSPF timer that you want to use.

The context-level OSPF timer policy provides the Hello timer and Dead timer intervals configuration. OSPF timers control the behavior of protocol messages and shortest path first (SPF) calculations.

f) Click **Select** and check the monitoring policy that you want to associate with the tenant.

When you apply a monitoring policy, it overrides the default monitoring policy.

g) Click **Submit**.

What to do next

After creating a private network, you create a bridge domain and link it to this VRF.

Bridge Domains

A bridge domain represents a Layer 2 forwarding construct within the fabric. It helps you to constrain broadcast and multicast traffic. It is a logical container for subnets.

A bridge domain must have at least one subnet associated with it but can contain multiple subnets. When you configure a bridge domain with multiple subnets, the first subnet added becomes the primary IP address on the SVI interface. Subsequent subnets are configured as secondary IP addresses. When the switch reloads, the primary IP address can change unless it is marked explicitly.

One or more EPGs can be associated with each bridge domain. EPGs within the same bridge domain may be configured to talk to each other, but they do not have layer 2 adjacency enabled by default.

Bridge domains in Cisco Application Centric Infrastructure (ACI) have several configuration options to allow the administrator to tune the operation in various ways. To learn more about the various options, see Cisco Application Centric Infrastructure Fundamentals Guide.

Note Once a bridge domain is configured, its mode cannot be switched.

A bridge domain must be linked to a Virtual Routing and Forwarding (VRF).

Subnets

A subnet defines the IP address range that can be used within the bridge domain. A bridge domain can contain multiple subnets, but a subnet is contained within a single bridge domain. The scope of a subnet can be public, private, or shared under a bridge domain or an EPG. See Adding a Subnet to a Bridge Domain, on page 9.

DHCP Relay Labels

DHCP Relay is required only when the DHCP server is in a different EPG or private network than the clients. DHCP label associates the provider DHCP server with the bridge domain. The DHCP label object also specifies the owner. If your infrastructure requires DHCP relay labels, see Adding a DHCP Relay Label to a Bridge Domain, on page 10.

Note The bridge domain DHCP label must match the DHCP Relay name. Label matching enables the bridge domain to consume the DHCP Relay.

Adding a Bridge Domain to VRF

A bridge domain is a unique Layer 2 forwarding domain that contains one or more subnets. Each bridge domain must be linked to a VRF.

Before you begin

Create a Tenant for your customer, organization, or domain and configure your private network.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Bridge Domains**.

Step 7 Click **Add**.

Step 8 On the **Add Tenant Bridge Domain** screen, complete the following fields:

a) Add a unique name and description for the Bridge Domain.

b) Click **Select** and check the network you want to use for the account.

This is the virtual routing and forwarding (VRF) object associated with the tenant for which this bridge domain is created. It is also known as context or private network.

c) From the **Forwarding** drop-down list, choose the forwarding parameter from the following options:

This sets the forwarding capacity between Layer 2 and Layer 3 networks. The values can be:

- **Optimize**—Automatically sets the Unicast and ARP parameters. Selects options: Hardware Proxy for L2 Unknown Unicast and Flood for Unknown Multicast Flooding with Unicast Routing enabled.
- **Custom**—Reveals the Unicast and ARP selections for custom configuration. If you choose custom forwarding, then complete the following additional parameters:

  1. From the **L2 Unknown Unicast** drop-down list, select the unicast parameter. The values can be **Flood** or **Hardware Proxy**.

     The default is Hardware Proxy. If enabled, unicast traffic flooding is blocked at a specific port, only permitting egress traffic with MAC addresses that are known to exist on the port. If you chose Flood, it floods the unicast traffic to all Layer 2 ports.

  2. From the **Unknown Multicast Flooding** drop-down list, select the multicast parameter. The values can be **Flood** or **Optimized Flood**.

  3. Check **ARP Flooding** to configure the flooding for the bridge domain.

     This enables ARP flooding, so that the Layer 2 broadcast domain maps IP addresses to the MAC addresses. If flooding is disabled, unicast routing is performed on the target IP address.

  4. Check **Unicast Routing** to configure the bridge domain routing. This forwarding method is based on predefined forwarding criteria (IP or MAC address). The default is layer 3 forwarding (IP address).

d) Check **Custom Mac Address** to configure the bridge domain Mac address and enter the address in **Mac Address** field.

By default, a bridge domain takes the fabric wide default MAC address of 00:22:BD:F8:19:FF. Configure this property to override the default address.

e) By default, the **Endpoint Dataplane Learning** drop-down list is set to true to enable data-plane IP learning on remote and local leaf switches.

f) The **Limit IP Learning to Subnet** drop-down list appears only when the **Endpoint Dataplane Learning** drop-down list is set to true. By default, the value of the **Limit IP Learning to Subnet** drop-down list is set to true. If this option is set to true, the fabric will learn only IP addresses for subnets configured on the bridge domain.

g) Click **Select** and check the IGMP snoop policy you want to use for this tenant.

This policy inspects the IGMP membership report messages from interested hosts. It limits the multicast traffic to the subset of VLAN interfaces on which the hosts reside.

h) Click **Select** and check the L3 out interface that you want to assign to this tenant.

This is the name of the Layer 3 outside interface associated with this object.

i) Click **Select** and check the route profile of L3 out network.

L3 Out is the network outside the fabric, configured for the tenant consuming this bridge domain, that is reachable by a specific route to external networks of a tenant application. The route profile specifies policies for external networks.

j) Click **Select** and check the monitoring policy associated with the tenant.

Step 9 Click **Submit**.

Adding a Subnet to a Bridge Domain

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Bridge Domains**.

Step 7 On the **Bridge Domains** page, choose the row with the domain to which you want to add the subnet and click **View Details**.

Step 8 Click **Subnet**.

Step 9 On the **Subnet** page, click **Add**.

Step 10 On the **Add Subnet to Tenant Bridge Domain** screen, complete the following fields:

a) In the **Gateway IP (Address)** field, enter the IP address of the default gateway.

b) In the **Gateway IP (Prefix)** field, enter a prefix in the range of 1-30 that starts with "/x"

c) Check the **Shared Subnet** check box to share the subnet with multiple contexts (VRFs) in the same tenant or across tenants as part of a shared service.

Shared subnets must be unique across the contexts (VRF) involved in the communication. When a subnet under an EPG provides a Layer 3 external network shared service, such a subnet must be globally unique within the entire ACI fabric.

d) Check the **Public Subnet** check box to export it to a routed connection.

e) Check the **Private Subnet** check box to apply the subnet only within its tenant.

f) Check the **Subnet Control (Querier IP)** check box to apply specific protocol to the subnet. Querier IP enables IGMP Snooping on the subnet.

g) Click **Select** and check the L3 out for route profile that you want to use for the bridge domain.

This is the Layer 3 Outside Network (L3extOut) configured for the tenant consuming this bridge domain.

h) Click **Select** and check the route profile that you want to use for this bridge domain.

The route profile specifies policies for external networks.

i) Click **Submit**.

Adding a DHCP Relay Label to a Bridge Domain

DHCP Relay is required when the DHCP server is in a different EPG or private network than the clients. A DHCP relay label contains a name for the label, the scope, and a DHCP option policy. The scope is the owner of the relay server and the DHCP option policy supplies DHCP clients with configuration parameters such as domain, nameserver, and subnet router addresses.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Bridge Domains**.

Step 7 Click the row with the domain to which you want to add the DHCP label and click **View Details**.

Step 8 Click **DHCP Relay Label**.

Step 9 On the **DHCP Relay Label** page, click **Add**.

Step 10 On the **Add DHCP Label To Tenant Bridge Domain** screen, complete the following fields:

a) From the **Scope** drop-down list, choose the scope. Options are:

- **Infra**—The owner is the infrastructure.
- **Tenant**—The owner is the tenant.

The default is **Infra**.

b) Click **Select** and check the DHCP relay policy that you want to use for the tenant bridge domain.

c) Click **Select** and check the DHCP option policy that you want to use.

d) Click **Submit**.

Application Profiles

Application profiles are logical containers that define the policies, services, and relationships between End Point Groups (EPGs). Each application profile contains one or more EPG that can communicate with the other EPGs in the same application profile, and with EPGs in other application profiles according to the contract rules. At minimum, associate one application profile with one EPG.

Modern applications contain multiple components. An application profile models the requirements of an application. For example, an e-commerce application could require a web server, a database server, data

located in a storage area network, and access to outside resources that enable financial transactions. The application profile contains as many (or as few) EPGs as necessary that are logically related for the e-commerce application.

EPGs can be organized according to one of the following:

- The application they provide (such as sap in the example in Appendix A).
- The function they provide (such as infrastructure).
- Where they are in the structure of the data center (such as DMZ).
- Whatever organizing principle that a fabric or tenant administrator chooses to use.

Creating an Application Profile for the Tenant

The application profile is a set of requirements that an application instance has on the virtualized fabric. The policy regulates connectivity and visibility among endpoints within the scope of the policy.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Application Profile**.

Step 7 Click **Add**.

Step 8 On the **Add Tenant Application Profile** screen, complete the following fields:

a) Add a unique name, description, and an alias for the Application Profile.

b) Click **Select** and check the tag name that you want to use for the APIC account.

c) From the **QoS Class** drop-down list, choose from the following options for the priority class:

- **Unspecified**—This is the default value.
- **Level1**—Class 1 Differentiated Services Code Point (DSCP) value
- **Level2**—Class 2 DSCP value
- **Level3**—Class 3 DSCP value

d) Click **Select** and check the monitoring policy associated with the tenant.

When you apply a monitoring policy, it overrides the default monitoring policy.

Step 9 Click **Submit**.

End Point Groups

An End Point Group (EPG) is a logical container of endpoints that have common policy requirements such as security, virtual machine mobility (VMM), QoS, or Layer 4 to Layer 7 services. They have an address (identity), a location, attributes (such as version or patch level), and can be physical or virtual. Knowing the address of an endpoint enables access to all its other identity details. Rather than configure and manage endpoints individually, they are placed in an EPG and are managed as a group.

The ACI fabric can contain the following types of EPGs:

- Application endpoint group
- Layer 2 external outside network instance
- Layer 3 external outside network instance
- Management endpoint groups for out-of-band or in-band access

By default, all endpoints in the same endpoint group can talk to each other without requiring a contract. Intra-endpoint group (intra-EPG) isolation prevents all endpoints in an EPG from talking to each other but inter-EPG communication is still permitted if there is a contract. This is similar to a private VLAN. For example, assume that you have three endpoints: two are in the client endpoint group, while the other endpoint is in the Web endpoint group. If there is a contract between endpoint groups, they can talk to each other.

Regardless of how an EPG is configured, EPG policies are applied only to the endpoints they contain. For example, to configure a WAN router connectivity to the fabric, you configure an EPG that includes any endpoints within the associated WAN subnet. The fabric learns of the endpoints through a discovery process and applies the policies accordingly.

After creating an EPG, add a static path to the EPG to determine the port and leaf/node for the traffic. See Adding a Static Path to EPG, on page 14.

You can also add static nodes (leaf, spine, or APIC), and domains (physical, VMM, L3, or L3 external - see examples) to EPGs and define how and when they are deployed. See Adding a Static Node to EPG, on page 16 and Adding a Domain to an EPG, on page 13.

Adding an EPG

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Application Profile**.

Step 7 Click the row with the profile that you want to update and click **View Details**.

Step 8 Click **EPG**.

Step 9 Click **Add**.

Step 10 On the **Add Tenant EPG** screen, complete the required fields including the following:

a) Add a unique name, description, and alias for the EPG.

b) (Optional) Click **Select** and check the tag you want to use.
c) From the **QoS Class** drop-down list, choose from the following options for the priority class:

- **Unspecified**—This is the default value.
- **Level1**—Class 1 Differentiated Services Code Point (DSCP) value
- **Level2**—Class 2 DSCP value
- **Level3**—Class 3 DSCP value
- **Custom**—Complete the additional parameter

d) If you chose custom QoS, click **Select** and check the customized quality of service (QoS) class that you want to use for the EPG.
e) Click **Select** and check the bridge domain for the EPG.
f) Click **Select** and check the monitoring policy associated with the tenant.

When you apply a monitoring policy, it overrides the default monitoring policy.

g) Click **Submit**.

Adding a Domain to an EPG

An EPG is associated with domains by being linked to a domain profile, which can be a VMM, physical, Layer 2 external, or Layer 3 external domain.

Before you begin

Create a physical, VMM, Layer 3, or Layer 2 domain for the APIC account.

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **Tenant(s)**.
Step 5 Click the row with the tenant that you want to update and click **View Details**.
Step 6 Click **Application Profile**.
Step 7 Click the row with the profile that you want to update and click **View Details**.
Step 8 Click **EPG**.
Step 9 Click the row with the EPG that you want to update and click **View Details**.
Step 10 Click **Domain**.
Step 11 Click **Add**.
Step 12 On the **Add Domain To EPG** screen, complete the required fields, including the following:
a) Click **Select** and check the domain profile that you want to add to the EPG.
b) From the **Deploy Immediacy** drop-down list, choose a path from the following options:

- **Immediate**—Specifies that the policy is programmed in the hardware policy CAM as soon as it is downloaded in the leaf software.

- **On Demand**—Specifies that the policy is programmed in the hardware policy CAM only when the first packet is received through the data path. This process helps to optimize the hardware space.

c) From the **Resolution Immediacy** drop-down list, choose a path from the following options:

It specifies whether policies are resolved immediately or when needed.

- **Immediate**—Specifies that EPG policies (including contracts and filters) are downloaded to the associated leaf switch software upon hypervisor attachment to VDS. LLDP or OpFlex permissions are used to resolve the hypervisor to leaf node attachments.
- **On Demand**—Specifies that a policy (for example, VLAN, VXLAN bindings, contracts, or filters) is pushed to the leaf node only when a hypervisor is attached to VDS and a VM is placed in the port group (EPG).
- **Pre-provision**—Specifies that a policy (for example, VLAN, VXLAN binding, contracts, or filters) is downloaded to a leaf switch even before a hypervisor is attached to the VDS. Therefore, this option pre-provisions the configuration on the switch.

d) From the **Allow Promiscuous** drop-down list, choose from the following options:

It enables all packets to pass to the VMM domain, which is often used to monitor network activity.

- **Reject**—Packets that do not include the network address are dropped.
- **Accept**—All traffic is received within the VMM domain.

e) From the **Forged Transmits** drop-down list, choose from the following options:

- **Reject**—All non-matching frames are dropped.
- **Accept**—Non-matching frames are received.

It specifies whether to allow forged transmits. A forged transmit occurs when a network adapter starts sending out traffic that identifies itself as something else. This security policy compares the effective address of the virtual network adapter and the source address inside an 802.3 Ethernet frame generated by the virtual machine to ensure that they match.

f) From the **MAC Changes** drop-down list, choose from the following options:

- **Reject**—Does not allow new MAC addresses.
- **Accept**—Allows new MAC addresses.

It enables you to define new MAC addresses for the network adapter within the virtual machine (VM).

g) Click **Submit**.

Adding a Static Path to EPG

Static path policies provide a summary of the configured properties of the policy, fault counts, and history for the static path. Configure the static path to the destination EPG.

Note When an EPG uses a static binding path, the encapsulation VLAN associated with this EPG must be part of a static VLAN pool.

Before you begin

Contracts must be configured.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Application Profile**.

Step 7 Click the row with the profile that you want to update and click **View Details**.

Step 8 Click **EPG**.

Step 9 Click the row with the EPG that you want to update and click **View Details**.

Step 10 Click **Static Path**.

Step 11 Click **Add**.

Step 12 On the **Add Static Path To EPG** screen, complete the following fields:

a) From the **Path Type** drop-down list, choose from the following options:

- **Port**—Is the default value
- **Direct Port Channel**—Class 1 Differentiated Services Code Point (DSCP) value
- **Virtual Port Channel**—Class 2 DSCP value

b) Click **Select** and check the static path that you want to add to the EPG.

c) In the **Encapsulation** field, enter a VLAN value that is part of one of the static VLAN blocks associated with the domain.

d) From the **Deployment Immediacy** drop-down list, choose from the following options:

- **Immediate**—Specifies that the policy is programmed in the hardware policy CAM as soon as it is downloaded in the leaf software.
- **On Demand**—Specifies that the policy is programmed in the hardware policy CAM only when the first packet is received through the data path. This process helps to optimize the hardware space.

Once EPG policies are downloaded to the leaf software, you can choose the deployment preferences to specify when a policy is pushed into leaf switches.

e) From the **Mode** drop-down list, choose the static association from the following options:

EPG tagging refers to configuring a static path under an EPG.

- **Tagged**—Select this mode if the traffic from the host is tagged with a VLAN ID.
- **Untagged**—Select this mode if the traffic from the host is untagged (without VLAN ID).

When a leaf switch is configured for an EPG to be untagged, for every port this EPG uses, the packets exit the switch untagged.

Note When an EPG is deployed as untagged, do not deploy that EPG as tagged on other ports of the same switch.

- **802.1P Untagged**—Select this mode if the traffic from the host is tagged with a 802.1P tag. When an access port is configured with a single EPG in native 802.1p mode, its packets exit that port untagged. When an access port is configured with multiple EPGs, one in native 802.1p mode, and some with VLAN tags, all packets exiting that access port are tagged VLAN 0 for EPG configured in native 802.1p mode and for all other EPGs packets exit with their respective VLAN tags.

  Note Only one native 802.1p EPG is allowed per access port.

f) Click **Submit**.

Adding a Static Node to EPG

Before you begin

Create nodes in the APIC system.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Application Profile**.

Step 7 Click the row with the profile that you want to update and click **View Details**.

Step 8 Click **EPG**.

Step 9 Click the row with the EPG that you want to update and click **View Details**.

Step 10 Click **Static Node**.

Step 11 Click **Add**.

Step 12 On the **Add Static Node To EPG** screen, complete the following fields:

a) Click **Select** and check the node that you want to add to the EPG.

b) In the **Encapsulation** field, enter a VLAN value that is part of one of the static VLAN blocks associated with the domain.

c) From the **Mode**drop-down list, choose the static association from the following options:

- **Native**
- **Regular**

d) From the **Deployment Immediacy** drop-down list, choose the policy from the following options:.

- **Immediate**—Specifies that the policy is programmed in the hardware policy CAM as soon as the policy is downloaded in the leaf software.
- **Lazy**—Specifies that the policy is programmed in the hardware policy CAM only when the first packet is received through the data path. This process helps to optimize the hardware space.

Once EPG policies are downloaded to the leaf software, you can choose the deployment preferences to specify when a policy is pushed into leaf switches.

e) Click **Submit**.

Contracts

EPGs can only communicate with other EPGs according to contract rules. Contracts determine the type of traffic that can pass between EPGs, including the protocols and ports allowed. If there is no contract, inter-EPG communication is disabled by default. There is no contract required for intra-EPG communication. A contract contains one or more subjects.

An EPG can both provide and consume the same contract. An EPG can also provide and consume multiple contracts simultaneously.

Contract Subjects

A subject is a sub-application running behind an endpoint group. A contract can encapsulate multiple subjects. An EPG associates with a subject and defines rules under the association for consuming, providing, or for peer-to-peer communications to that subject. Subjects contain filters and optional labels.

Export Contract feature enables you to export the XML or JSON code for later use with the REST API.

Provider and Consumer Contracts

Contracts can contain multiple communication rules and multiple endpoint groups. The relationship between an EPG and a contract can be either a provider or consumer. When an EPG provides a contract, communication with that EPG can be initiated from other EPGs as long as the communication complies with the provided contract. When an EPG consumes a contract, the endpoints in the consuming EPG may initiate communication with any endpoint in an EPG that is providing that contract.

Filters

Filters enable you to specify the protocols you want to permit for traffic management between two EPGs. For example, you may want to permit only `https` traffic. There are several types of filters.

- Permit—It allows traffic.
- Deny (Taboo)—For specific use cases. You may specify to allow all traffic in a contract, but set up taboos to deny certain traffic.
- Redirect—Useful to send traffic from an EPG to a layer 4-7 device such as a firewall, load balancer, or IPS/IDS.
- Mark—To mark traffic for Quality of Service reasons.

You can add filters to a contract by adding filter chains (consumer or provider) to contract subjects.

Contract Labels

Labels are optional advanced identifiers. When you use labels, you can specify more complex relationships between EPGs. Labels allow for control over which subjects and filters to apply when communicating between a specific pair of endpoint groups. Without labels, a contract applies every subject and filter between consumer and provider endpoint groups. You can use labels to represent a complex communication scenario, within the scope of a single contract, then reuse this contract while specifying only a subset of its policies across multiple endpoint groups.

Taboo Contracts

A Taboo contract provides a way for an EPG to specify the subjects on which communication is not allowed.

Creating Contracts

Without a contract, the default forwarding policy is to not allow any communication between EPGs but all communication within an EPG is allowed.

Note If two tenants are participating in same contract, ensure that they are not able to see each other and that their endpoint groups are not able to communicate.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Contracts**.

Step 7 Click **Add**.

Step 8 On the **Add Tenant Contract** page, complete the following fields:

a) Add a unique name and description for the contract.

If you create contracts under the common and user tenants, that are consumed by the same tenant, they must have different names.

b) From the **Scope** drop-down list, choose from the following options:

- **Application Profile**—The contract is applied to endpoint groups in the application profile.
- **Context**—The contract is applied to endpoint groups in the same Virtual Routing and Forwarding (VRF).
- **Global**—This contract is applied to endpoint groups throughout the fabric.
- **Tenant**—This contract is applied to endpoint groups within the same tenant.

c) From the **Priority** drop-down list, choose the priority level of the service contract from the following options:

- **Level1**—Class 1 Differentiated Services Code Point (DSCP) value

- **Level2**—Class 2 DSCP value
- **Level3**—Class 3 DSCP value
- **Unspecified**—This is the default value.

The default option is **Unspecified**.

Step 9 Click **Submit**.

What to do next

Create contract subjects to specify the information that can be communicated and the mechanism of communication.

Creating a Contract Subject

A subject is a sub-application running behind an endpoint group. A contract can encapsulate multiple subjects. An endpoint group always associates with a subject and defines rules under the association for consuming, providing, or for peer-to-peer communications to that subject.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Contracts**.

Step 7 Click the row with the contract that you want to update and click **View Details**.

Step 8 Click **Contract Subjects**.

Step 9 Click **Add**.

Step 10 On the **Add Tenant Contract Subject** page, complete the required fields, including the following:

a) Add a unique name and description for the contract subject.

b) Check **Reverse Filter Ports** to apply the same subject rule to the reverse filter ports when the contract applies in both directions. If you choose this option, enter the following additional parameters:

- **In Term Service Graph**
- **In Term QoS**
- **Out Term Service Graph**
- **Out Term QoS**

c) Check **Apply Both Directions** to apply the contract to both inbound and outbound traffic. If the selected contract does not apply to both, then the filter chain must be configured for consumer to provider and provider to consumer separately.

d) Click **Select** and check the box for the service graph that you want to add to the contract.

The service graph is an image that shows the relationship between contracts and subjects.

e) From the **QoS** drop-down list, choose the traffic priority for the associated EPG from the following options:

Each system class manages one lane of traffic.

- **Level1**—Class 1 Differentiated Services Code Point (DSCP) value
- **Level2**—Class 2 DSCP value
- **Level3**—Class 3 DSCP value
- **Unspecified**—This is the default value.

The default option is **Unspecified**.

Step 11 Click **Submit**.

What to do next

Create consumer and provider contracts.

Adding Contracts to EPGs

Provided Contracts

EPGs can only communicate with other EPGs according to contract rules. Contracts determine the types of traffic that can pass between EPGs, including the protocols and ports allowed.

The relationship between an EPG and a contract can be either a provider or consumer. When an EPG provides a contract, communication with that EPG can be initiated from other EPGs as long as the communication complies with the provided contract. When an EPG consumes a contract, the endpoints in the consuming EPG may initiate communication with any endpoint in an EPG that is providing that contract.

An EPG can both provide and consume the same contract. An EPG can also provide and consume multiple contracts simultaneously.

Adding a Provided Contract to an EPG

You can associate contracts that were created earlier to create policy relationships between the EPGs. A provided contract is a contract for which the EPG is a provider.

Note Verify that both provided and consumed contracts have the same name.

Before you begin

Contracts must be configured.

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **Tenant(s)**.
Step 5 Click the row with the tenant that you want to update and click **View Details**.
Step 6 Click **Application Profile**.
Step 7 Click the row with the profile that you want to update and click **View Details**.
Step 8 Click **EPG**.
Step 9 Click the row with the EPG that you want to update and click **View Details**.
Step 10 Click **Consumed Contract**.
Step 11 Click **Add**.
Step 12 On the **Add Provided Contract To EPG** screen, complete the fields including the following:

a) Click **Select** and check the contract that you want to add to the EPG.
b) From the **QoS** drop-down list, choose the traffic priority for the associated EPG from the following options:

Each system class manages one lane of traffic.

- **Unspecified**—This is the default value.
- **Level1**—Class 1 Differentiated Services Code Point (DSCP) value
- **Level2**—Class 2 DSCP value
- **Level3**—Class 3 DSCP value

c) Click **Submit**.

Consumed Contracts

Also need to look into Taboo Contract and Filters.

Adding a Consumed Contract to an EPG

You can associate contracts that were created earlier to create policy relationships between the EPGs. A consumed contract is a contract for which the EPG is a consumer.

Note Verify that both provided and consumed contracts have the same name.

Before you begin

Contracts must be configured.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **Tenant(s)**.
Step 5 Click the row with the tenant that you want to update and click **View Details**.
Step 6 Click **Application Profile**.
Step 7 Click the row with the profile that you want to update and click **View Details**.
Step 8 Click **EPG**.
Step 9 Click the row with the EPG that you want to update and click **View Details**.
Step 10 Click **Consumed Contract**.
Step 11 Click **Add**.
Step 12 On the **Add Consumed Contract To EPG** screen, complete the fields including the following:

a) Click **Select** and check the contract that you want to add to the EPG.
b) From the **QoS** drop-down list, choose the traffic priority for the associated EPG from the following options:

Each system class manages one lane of traffic.

- **Unspecified**—This is the default value.
- **Level1**—Class 1 Differentiated Services Code Point (DSCP) value
- **Level2**—Class 2 DSCP value
- **Level3**—Class 3 DSCP value

c) Click **Submit**.

Adding a Consumed Contract Interface

Before you begin

Contracts must be configured.

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **Tenant(s)**.
Step 5 Click the row with the tenant that you want to update and click **View Details**.
Step 6 Click **Application Profile**.
Step 7 Click the row with the profile that you want to update and click **View Details**.
Step 8 Click **EPG**.
Step 9 Click the row with the EPG that you want to update and click **View Details**.
Step 10 Click **Consumed Contract Interface**.
Step 11 Click **Add**.
Step 12 On the **Add Consumed Contract Interface To EPG** screen, complete the fields including the following:

a) Click **Select** and check the contract interface that you want to add to the EPG.
b) From the **Priority** drop-down list, choose a priority for the selected EPG from the following options:
   - **Level1**—Class 1 Differentiated Services Code Point (DSCP) value.
   - **Level2**—Class 2 DSCP value
   - **Level3**—Class 3 DSCP value
   - **Unspecified**—Is the default value
c) Click **Submit**.

Contract Labels

Adding a Consumed Label to a Contract Subject

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **Tenant(s)**.
Step 5 Click the row with the tenant that you want to update and click **View Details**.
Step 6 Click **Contracts**.
Step 7 Click the row with the contract that you want to update and click **View Details**.
Step 8 Click **Contract Subjects**.
Step 9 Click the row with the contract subject that you want to update and click **View Details**.
Step 10 Click **Consumed Label**.
Step 11 Click **Add**.
Step 12 On the **Add Consumed Label to Contract To Contract Subject** screen, complete the following fields:
a) From the **Match Type** drop-down list, choose the subject match criteria across providers, from the following options:
   - **Atleast One**
   - **Atmost One**
   - **None**
   - **All**
b) Enter a **Label Name**.

   A subject label is used as classification criteria for subjects being consumed by the EPGs participating in the contract.
c) From the **Label Tag** drop-down list, choose a tag.

It is the search keyword or term that is assigned to the application profile. A tag allows you to group multiple objects by a descriptive name. You can assign the same tag name to multiple objects and you can assign one or more tag names to an object.

d) Check **Complement** for the contract to take effect if the labels do not match.
e) Click **Submit**.

Adding a Provided Label to a Contract Subject

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **Tenant(s)**.
Step 5 Click the row with the tenant that you want to update and click **View Details**.
Step 6 Click **Contracts**.
Step 7 Click the row with the contract that you want to update and click **View Details**.
Step 8 Click **Contract Subjects**.
Step 9 Click the row with the contract subject that you want to update and click **View Details**.
Step 10 Click **Provided Label**.
Step 11 Click **Add**.
Step 12 On the **Add Provided Label to Contract To Contract Subject** screen, complete the following fields:

a) From the **Match Type** drop-down list, choose the subject match criteria across providers, from the following options:

- **Atleast One**
- **Atmost One**
- **None**
- **All**

b) Enter a **Label Name**.

A subject label is used as classification criteria for subjects being consumed or provided by the EPGs participating in the contract.

c) From the **Label Tag** drop-down list, choose a tag.

It is the search keyword or term that is assigned to the application profile. A tag allows you to group multiple objects by a descriptive name. You can assign the same tag name to multiple objects and you can assign one or more tag names to an object.

d) Check **Complement** for the contract to take effect if the labels do not match.
e) Click **Submit**.

Fabric Extender (FEX)

Fabric Extender (FEX) behave as a remote line card for a parent switch. The FEX is an extension of the parent swicth fabric, with the FEX and the parent switch together form a distributed modular system. This means that the FEXs are completely managed from the parent switch and appear as physical ports on that switch.

Adding a FEX Profile

A FEX profile enables you to define policy for the ports facing hosts on the FEX and configure FEX interfaces.

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **FEX Profile**.
Step 5 Click **Add**.
Step 6 Enter the name and description of the profile used for configuring FEX.
Step 7 Click **Submit**.

What to do next

You have to add the interface port selector to the FEX profile to identify the interfaces between the node and the host.

Adding an Access Port Selector to the FEX Profile

Access port selector is used for identifying the interfaces between the node and the host (such as hypervisor), which consume the policies in the interface policy group.

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **FEX Profile**.
Step 5 Click the row with the FEX profile to which you want to add an access port selector and click **View Details**.
Step 6 In the **FEX Profile Access Port Selectors** tab, click **Add**.
Step 7 On the **Create Fex Profile Access Port Selector** screen, complete the following fields:

- Enter the name and description of the interface selector. We recommend that you include information about where and when the policy must be used, in the description field.
- Enter the ID of the interfaces that consume the policies in the interface policy group. You can enter a single FEX interface, one or more interface ranges, or All.

- Click **Select** to view the list of available interface policy group. Check the interface policy group that you want the interfaces to consume and click **Select**.

Step 8 Click **Submit**.

What to do next

You can add access port blocks and sub-port blocks to the access port selector of the FEX profile. Choose an access port selector and click **View Details** to view the access port blocks and sub port blocks of the access port selector. Click **Add** under respective tabs to add the access port block and sub port block.