Provisioning Core ACI Fabric Services

This chapter contains the following sections:

Time Synchronization and NTP

Within the Cisco Application Centric Infrastructure (ACI) fabric, time synchronization is a crucial capability upon which many of the monitoring, operational, and troubleshooting tasks depend. Clock synchronization is important for proper analysis of traffic flows as well as for correlating debug and fault time stamps across multiple fabric nodes.

An offset present on one or more devices can hamper the ability to properly diagnose and resolve many common operational issues. In addition, clock synchronization allows for the full utilization of the atomic counter capability that is built into the ACI upon which the application health scores depend. Nonexistent or improper configuration of time synchronization does not necessarily trigger a fault or a low health score. You should configure time synchronization before deploying a full fabric or applications so as to enable proper usage of these features. The most widely adapted method for synchronizing a device clock is to use Network Time Protocol (NTP).

Prior to configuring NTP, consider what management IP address scheme is in place within the ACI fabric. There are two options for configuring management of all ACI nodes and Application Policy Infrastructure Controllers (APICs), in-band management and/or out-of-band management. Depending upon which management option is chosen for the fabric, configuration of NTP will vary. Another consideration in deploying time synchronization is where the time source is located. The reliability of the source must be carefully considered when determining if you will use a private internal clock or an external public clock.

In-Band and Out-of-Band Management NTP

Note See the Adding Management Access section in this guide for information about in-band management access and out-of-band management access.

- Out-of-band management NTP—When an ACI fabric is deployed with out-of-band management, each node of the fabric, inclusive of spines, leaves, and all members of the APIC cluster, is managed from outside the ACI fabric. This IP reachability will be leveraged so that each node can individually query the same NTP server as a consistent clock source. To configure NTP, a Date and Time policy must be created that references an out-of-band management endpoint group. Date and Time policies are confined to a single pod and must be deployed across all pods provisioned in the ACI fabric.
- In-Band Management NTP—When an ACI fabric is deployed with in-band management, consider the reachability of the NTP server from within the ACI in-band management network. In-band IP addressing used within the ACI fabric is not reachable from anywhere outside the fabric. To leverage an NTP server external to the fabric with in-band management, construct a policy to enable this communication. The steps used to configure in-band management policies are identical to those used to establish an out-of-band management policy. The distinction is around how to allow the fabric to connect to the NTP server.

NTP over IPv6

NTP over IPv6 addresses is supported in hostnames and peer addresses. The gai.conf can also be set up to prefer the IPv6 address of a provider or a peer over an IPv4 address. The user can provide a hostname that can be resolved by providing an IP address (both IPv4 or IPv6, depending on the installation or preference).

Configuring NTP Using the GUI

Procedure

Step 1 On the menu bar, choose **FABRIC** > **Fabric Policies**.

Step 2 In the **Navigation** pane, choose **Pod Policies** > **Policies**.

Step 3 In the **Work** pane, choose **Actions** > **Create Date and Time Policy**.

Step 4 In the **Create Date and Time Policy** dialog box, perform the following actions:

a) Enter a name for the policy to distinguish between the different NTP configurations in your environment..

b) Click **enabled** for the **Authentication State** field and expand the **NTP Client Authentication Keys** table and enter the key information. Click **Update** and **Next**.

c) Click the + sign to specify the NTP server information (provider) to be used.

d) In the **Create Providers** dialog box, enter all relevant information, including the following fields: **Name**, **Description**, **Minimum Polling Intervals**, and **Maximum Polling Intervals**.

- If you are creating multiple providers, check the **Preferred** check box for the most reliable NTP source.

- In the Management EPG drop-down list, if the NTP server is reachable by all nodes on the fabric through out-of-band management, choose Out-of-Band. If you have deployed in-band management, see the details about In-Band Management NTP. Click **OK**.

Repeat the steps for each provider that you want to create.

Step 5 In the **Navigation** pane, choose **Pod Policies** > **Policy Groups**.

Step 6 In the **Work** pane, choose **Actions** > **Create Pod Policy Group**.

Step 7 In the **Create Pod Policy Group** dialog box, perform the following actions:

a) Enter a name for the policy group.

b) In the **Date Time Policy** field, from the drop down list, choose the NTP policy that you created earlier. Click **Submit**.
The pod policy group is created. Alternatively, you can use the default pod policy group.

Step 8 In the **Navigation** pane, choose **Pod Policies** > **Profiles**.

Step 9 In the **Work** pane, double-click the desired pod selector name.

Step 10 In the Properties area, from the **Fabric Policy Group** drop down list, choose the pod policy group you created. Click **Submit**.

Configuring NTP Using the NX-OS Style CLI

When an ACI fabric is deployed with out-of-band management, each node of the fabric is managed from outside the ACI fabric. You can configure an out-of-band management NTP server so that each node can individually query the same NTP server as a consistent clock source.

Procedure

Step 1 **configure**

Enters configuration mode.

Example:

```
apic1# configure
```

Step 2 **template ntp-fabric** *ntp-fabric-template-name*

Specifies the NTP template (policy) for the fabric.

Example:

```
apic1(config)# template ntp-fabric pol1
```

Step 3 **[no] server** *dns-name-or-ipaddress* **[prefer]** [**use-vrf** {**inb-mgmt** | **oob-mgmt**}] [**key** *key-value*]

Configures an NTP server for the active NTP policy. To make this server the preferred server for the active NTP policy, include the **prefer** keyword. If NTP authentication is enabled, specify a reference key ID. To specify the tenant in-band or out-of-band management access VRF, include the **use-vrf** keyword with the **inb-mgmt** or **oob-mgmt** keyword.

Example:

```
apic1(config-template-ntp-fabric)# server 192.0.20.123 prefer use-vrf oob-mgmt
```

Step 4 **[no] authenticate**

Enables (or disables) NTP authentication.

Example:

```
apic1(config-template-ntp-fabric)# no authenticate
```

Step 5 **[no] authentication-key** *key-value*

Configures an authentication NTP authentication. The range is 1 to 65535.

Example:

```
apic1(config-template-ntp-fabric)# authentication-key 12345 md5 "key_value"
```

Step 6 **[no] trusted-key** *key-value*

Configures a trusted NTP authentication. The range is 1 to 65535.

Example:

```
apic1(config-template-ntp-fabric)# trusted-key 54321
```

Step 7 **exit**

Returns to global configuration mode

Example:

```
apic1(config-template-ntp-fabric)# exit
```

Step 8 **template pod-group** *pod-group-template-name*

Configures a pod-group template (policy).

Example:

```
apic1(config)# template pod-group allPods
```

Step 9 **inherit ntp-fabric** *ntp-fabric-template-name*

Configures the NTP fabric pod-group to use the previously configured NTP fabric template (policy).

Example:

```
apic1(config-pod-group)# inherit ntp-fabric pol1
```

Step 10 **exit**

Returns to global configuration mode

Example:

```
apic1(config-template-pod-group)# exit
```

Step 11 **pod-profile** *pod-profile-name*

Configures a pod profile.

Example:

```
apic1(config)# pod-profile all
```

Step 12 **pods** {*pod-range-1-255* | **all**}

Configures a set of pods.

Example:

```
apic1(config-pod-profile)# pods all
```

Step 13 **inherit pod-group** *pod-group-name*

Associates the pod-profile with the previously configured pod group.

Example:

```
apic1(config-pod-profile-pods)# inherit pod-group allPods
```

Step 14 **end**

Returns to EXEC mode.

Example:

```
apic1(config-pod-profile-pods)# end
```

Examples

This example shows how to configure a preferred out-of-band NTP server and how to verify the configuration and deployment.

```
apic1# configure t
apic1(config)# template ntp-fabric pol1
apic1(config-template-ntp-fabric)# server 192.0.20.123 use-vrf oob-default
apic1(config-template-ntp-fabric)# no authenticate
apic1(config-template-ntp-fabric)# authentication-key 12345 md5 abcdef1235
apic1(config-template-ntp-fabric)# trusted-key 12345
apic1(config-template-ntp-fabric)# exit
apic1(config)# template pod-group allPods
apic1(config-pod-group)# inherit ntp-fabric pol1
apic1(config-pod-group)# exit
apic1(config)# pod-profile all
apic1(config-pod-profile)# pods all
apic1(config-pod-profile-pods)# inherit pod-group allPods
apic1(config-pod-profile-pods)# end
apic1#
```

```
apic1# show ntpq
 nodeid     remote         refid   st    t   when   poll   reach  delay    offset   jitter

 ------  -  ------------  ------  ----  --  -----  -----  -----  ------   ------   ------
 1       *  192.0.20.123  .GPS.         u   27     64     377    76.427   0.087    0.067

 2       *  192.0.20.123  .GPS.         u   3      64     377    75.932   0.001    0.021
 3       *  192.0.20.123  .GPS.         u   3      64     377    75.932   0.001    0.021
```

Configuring NTP Using the REST API

Procedure

Step 1 Configure NTP.

Example:

```
POST url: https://APIC-IP/api/node/mo/uni/fabric/time-test.xml

<imdata totalCount="1">
    <datetimePol adminSt="enabled" authSt="disabled" descr="" dn="uni/fabric/time-CiscoNTPPol"
 name="CiscoNTPPol" ownerKey="" ownerTag="">
        <datetimeNtpProv descr="" keyId="0" maxPoll="6" minPoll="4" name="10.10.10.11"
preferred="yes">
            <datetimeRsNtpProvToEpg tDn="uni/tn-mgmt/mgmtp-default/inb-default"/>
        </datetimeNtpProv>
    </datetimePol>
</imdata>
```

Step 2 Add the default Date Time Policy to the pod policy group.

Example:

```
POST url: https://APIC-IP/api/node/mo/uni/fabric/funcprof/podpgrp-calo1/rsTimePol.xml

POST payload: <imdata totalCount="1">
<fabricRsTimePol tnDatetimePolName="CiscoNTPPol">
</fabricRsTimePol>
</imdata>
```

Step 3 Add the pod policy group to the default pod profile.

Example:

```
POST url:
https://APIC-IP/api/node/mo/uni/fabric/podprof-default/pods-default-typ-ALL/rspodPGrp.xml

payload: <imdata totalCount="1">
<fabricRsPodPGrp tDn="uni/fabric/funcprof/podpgrp-calo1" status="created">
</fabricRsPodPGrp>
</imdata>
```

Verifying NTP Operation Using the GUI

Procedure

Step 1 On the menu bar, choose **FABRIC** > **Fabric Policies**.

Step 2 In the **Navigation** pane, choose **Pod Policies** > **Policies** > **Date and Time** > ***ntp_policy*** > ***server_name***.

The *ntp_policy* is the previously created policy. An IPv6 address is supported in the Host Name/IP address field. If you enter a hostname and it has an IPv6 address set, you must implement the priority of IPv6 address over IPv4 address.

Step 3 In the **Work** pane, verify the details of the server.

Verifying NTP Policy Deployed to Each Node Using the NX-OS Style CLI

Procedure

Step 1 Log onto an APIC controller in the fabric using the SSH protocol.

Step 2 Attach to a node and check the NTP peer status, shown as follows:

```
apic1# fabric  node_name show ntp peer-status
```

Step 3 Repeat step 2 for different nodes in the fabric.

NTP Server

The NTP server enables client switches to also act as NTP servers to provide NTP time information to downstream clients. When the NTP server is enabled, the NTP daemon on the switch responds with time information to all unicast (IPv4/IPv6) requests from NTP clients. NTP server implementation is complaint to NTP RFCv3. As per NTP RFC, server will not maintain any state related to clients.

- NTP Server enables the in-band/out-of-band management IP of the switches to serve NTP client requests.
- NTP Server, like existing NTP Client functionality works only with In-band & Out-of-band Management VRFs.
- NTP Server responds to incoming NTP requests on both Management VRFs, and responds back using the same VRF.
- NTP Server supports both IPv4/IPv6.
- Switches can sync as IPv4 Client and serve as IPv6 server and vice versa.
- Switches can sync as NTP client via out-of-band management VRF and serve through in-band management VRF and vice versa.
- No additional Contracts or IP Table Configurations are required.
- If the switch is synced to the upstream server, then the server will send time info with stratum number, an increment to its system peer's stratum.
- If the switch clock is undisciplined (not synced to upstream server), then the server will send time information with stratum 16. Clients will not be able to sync to this server.

By default, NTP server functionality is disabled. It needs to be enabled explicitly by config policy.

Note Clients can use the in-band, out-of-band IP of the leaf as the NTP server IP. Clients can also use the BD SVI of the EPG which they are part of, also as NTP server IP.

Note Fabric switches should not sync to other switches of the same fabric. The Fabric switches should always sync to external NTP servers.

Enabling the NTP Server Using the GUI

This section explains how to enable an NTP server when configuring NTP in the APIC GUI.

Procedure

Step 1 On the menu bar, choose **FABRIC** > **Fabric Policies**.

Step 2 In the **Navigation** pane, choose **Pod Policies** > **Policies** .

The **Date and Time** option appears in the **Navigation** pane.

Step 3 From the **Navigation** pane, right-click on **Date and Time** and choose **Create Date and Time Policy**.

The **Create Date and Time Policy** dialog appears in the **Work** pane.

Step 4 In the **Create Date and Time Policy** dialog box, perform the following actions:

a) Enter a name for the policy to distinguish between the different NTP configurations in your environment.

b) For the **Server State** option, click **enabled**.

Server State enables switches to act as NTP servers to provide NTP time information to downstream clients.

Note To support the server functionality, it is always recommended to have a peer setup for the server. This enables the server to have a consistent time to provide to the clients.

When **Server State** is enabled:

- The NTP server sends time info with a stratum number, an increment to the system peer's stratum number, to switches that are synched to the upstream server.
- The server sends time info with stratum 16 if the switch clock is not synched to the upstream server. Clients are not able to sync to this server.

Note To support the server functionality, it is always recommended to have a peer setup for the server. The peer setup allows for a consistent time to provide to the clients.

c) For the **Master Mode** option, click **enabled**.

Master Mode enables the designated NTP server to provide undisciplined local clock time to downstream clients with a configured stratum number. For example, a leaf switch that is acting as the NTP server can provide undisciplined local clock time to leaf switches acting as clients.

Note
- **Master Mode** is only applicable when the server clock is undisciplined.
- The default master mode **Stratum Value** is 8.

d) For the **Stratum Value** field, specify the stratum level from which NTP clients will get their time synchronized. The range is from 1 to 14.

e) Click **Next**.
f) Click the + sign to specify the NTP server information (provider) to be used.
g) In the **Create Providers** dialog box, enter all relevant information, including the following fields: **Name**, **Description**, **Minimum Polling Intervals**, and **Maximum Polling Intervals**.

- If you are creating multiple providers, check the **Preferred** check box for the most reliable NTP source.
- In the Management EPG drop-down list, if the NTP server is reachable by all nodes on the fabric through out-of-band management, choose Out-of-Band. If you have deployed in-band management, see the details about In-Band Management NTP. Click **OK**.

Repeat the steps for each provider that you want to create.

Step 5 In the **Navigation** pane, choose **Pod Policies** then right-click on **Policy Groups**.

The **Create Pod Policy Group** dialog appears.

Step 6 In the **Work** pane, choose **Actions** > **Create Pod Policy Group**.

Step 7 In the **Create Pod Policy Group** dialog box, perform the following actions:

a) Enter a name for the policy group.
b) In the **Date Time Policy** field, from the drop down list, choose the NTP policy that you created earlier. Click **Submit**.
The pod policy group is created. Alternatively, you can use the default pod policy group.

Step 8 In the **Navigation** pane, choose **Pod Policies** > **Profiles**.

Step 9 In the **Work** pane, double-click the desired pod selector name.

Step 10 In the Properties area, from the **Fabric Policy Group** drop down list, choose the pod policy group you created.

Step 11 Click **Submit**.

Enabling the NTP Server Using the CLI

This section explains how to enable the NTP server feature using CLI commands.

Before you begin

Procedure

Step 1 Enter the global configure mode:

Example:

```
apic1#configure t
```

Step 2 Configure an NTP server for the active NTP policy.

Example:

```
apic1(config)#template ntp-fabric default
```

Step 3 Specify the NTP server.

Example:

```
apic1(config-template-ntp-fabric)#server 10.81.254.201 prefer use-vrf oob-default
```

Step 4 Enable the switches to act as NTP servers.

Example:

```
apic1(config-template-ntp-fabric)#server-mode
```

Step 5 Enable the switches to act in NTP mastermode with a stratum value of 10.

Example:

```
apic1(config-template-ntp-fabric)#master stratum 10
```

Step 6 Return to global configuration

Example:

```
aic1(config-template-ntp-fabric)#exit
```

Enabling the NTP Server Using the REST API

This example demonstrates how to configure the NTP server using the REST API.

Procedure

Enable `serverState` and `masterMode` and specify the `StratumValue` (the `StratumValue` can be from 1-14.

Example:

```
POST url: https://APIC-IP/api/node/mo/uni/fabric/time-test.xml
<datetimePol name="testdatetime" adminSt="enabled" authSt="enabled" serverState="enabled"
masterMode="enabled" StratumValue="10" >
```

Configuring a DHCP Relay Policy

A DHCP relay policy may be used when the DHCP client and server are in different subnets. If the client is on an ESX hypervisor with a deployed vShield Domain profile, then the use of a DHCP relay policy configuration is mandatory.

When a vShield controller deploys a Virtual Extensible Local Area Network (VXLAN), the hypervisor hosts create a kernel (vmkN, virtual tunnel end-point [VTEP]) interface. These interfaces need an IP address in the infrastructure tenant that uses DHCP. Therefore, you must configure a DHCP relay policy so that the APIC can act as the DHCP server and provide these IP addresses.

When an ACI fabric acts as a DHCP relay, it inserts the DHCP Option 82 (the DHCP Relay Agent Information Option) in DHCP requests that it proxies on behalf of clients. If a response (DHCP offer) comes back from a DHCP server without Option 82, it is silently dropped by the fabric. Therefore, when the ACI fabric acts as a DHCP relay, DHCP servers providing IP addresses to compute nodes attached to the ACI fabric must support Option 82.

Configuring a DHCP Server Policy for the APIC Infrastructure Using the GUI

- The port and the encapsulation used by the application Endpoint Group must belong to a physical or VM Manager (VMM) domain. If no such association with a domain is established, the APIC continues to deploy the EPG but raises a fault.
- Cisco APIC supports DHCP relay for both IPv4 and IPv6 tenant subnets. DHCP server addresses can be IPv4 or IPv6. DHCPv6 relay will occur only if IPv6 is enabled on the fabric interface and one or more DHCPv6 relay servers are configured.

Deploying DHCP Relay Policy for an Endpoint Group

Before you begin

Make sure that Layer 2 or Layer 3 management connectivity is configured.

Procedure

Step 1 On the menu bar, choose **TENANTS** > **infra**. In the **Navigation** pane, under **Tenant infra**, expand **Networking** > **Protocol Policies** > **DHCP** > **Relay Policies**.

Step 2 Right-click **Relay Policies** and click **Create DHCP Relay Policy**.

Step 3 In the **Create DHCP Relay Policy** dialog box, perform the following actions:

a) In the **Name** field, enter the DHCP relay profile name (DhcpRelayP).

b) Expand **Providers**. In the **Create DHCP Provider** dialog box, in the **EPG Type** field, click the appropriate radio button depending upon where the DHCP server is connected.

c) In the **Application EPG** area, in the **Tenant** field, from the drop-down list, choose the tenant. (infra)

d) In the **Application Profile** field, from the drop-down list, choose the application. (access)

e) In the **EPG** field, from the drop-down list, choose the EPG. (default)

f) In the **DHCP Server Address** field, enter the IP address for the infra DHCP server. Click **Update**.

Note The infra DHCP IP address is the infra IP address of APIC1. You must enter the default IP address of 10.0.0.1 if deploying for vShield controller configuration.

g) Click **Submit**.

The DHCP relay policy is created.

Step 4 In the **Navigation** pane, expand **Networking** > **Bridge Domains** > **default** > **DHCP Relay Labels**.

Step 5 Right-click **DHCP Relay Labels**, and click **Create DHCP Relay Label**.

Step 6 In the **Create DHCP Relay Label** dialog box, perform the following actions:

a) In the **Scope** field, click the tenant radio button.
This action displays, in the **Name** field drop-down list, the DHCP relay policy created earlier.

b) In the **Name** field, from the drop-down list, choose the name of the DHCP policy created (DhcpRelayP) or create a new relay policy by choosing **Create DHCP Relay Policy**.

c) In the **DHCP Option Policy**, select an existing option policy, or create a new one by choosing **Create DHCP Option Policy**.

d) Click **Submit**.

The DHCP server is associated with the bridge domain.

Step 7 In the **Navigation** pane, expand **Networking** > **Bridge Domains** > **default** > **DHCP Relay Labels** to view the DHCP server created.

Configuring a DHCP Server Policy for the APIC Infrastructure Using the NX-OS Style CLI

- The port and the encapsulation used by the application Endpoint Group must belong to a physical or VM Manager (VMM) domain. If no such association with a domain is established, the APIC continues to deploy the EPG but raises a fault.
- Cisco APIC supports DHCP relay for both IPv4 and IPv6 tenant subnets. DHCP server addresses can be IPv4 or IPv6. DHCPv6 relay will occur only if IPv6 is enabled on the fabric interface and one or more DHCPv6 relay servers are configured.

Before you begin

Ensure that Layer 2 or Layer 3 connectivity is configured to reach the DHCP server address.

Procedure

Configure DHCP server policy settings for the APIC infrastructure traffic.

Example:

DHCP Relay Policy for an Endpoint Group

```
apic1(config)# tenant infra
apic1(config-tenant)# template dhcp relay policy DhcpRelayP
apic1(config-tenant-template-dhcp-relay)# ip address 10.0.0.1 tenant infra application access epg default
apic1(config-tenant-template-dhcp-relay)# exit
apic1(config-tenant)# interface bridge-domain default
apic1(config-tenant-interface)# dhcp relay policy tenant DhcpRelayP
apic1(config-tenant-interface)# exit
```

Example:

DHCP Relay Policy for Layer 3 Outside

```
ifav28-ifc2(config)# tenant dhcpTn
ifav28-ifc2(config-tenant)# template dhcp relay policy DhcpRelayPol
ifav28-ifc2(config-tenant-template-dhcp-relay)# ip address 11.1.1.11 tenant dhcpTn application ap epg serverEpg
ifav28-ifc2(config-tenant-template-dhcp-relay)# exit
ifav28-ifc2(config-tenant)# exit
ifav28-ifc2(config)# leaf 2001
ifav28-ifc2(config-leaf)# interface ethernet 1/4
ifav28-ifc2(config-leaf-if)# no switchport
ifav28-ifc2(config-leaf-if)# vrf member tenant dhcpTn vrf v1
ifav28-ifc2(config-leaf-if)# dhcp relay policy tenant DhcpRelayPol
ifav28-ifc2(config-leaf-if)# exit
```

Configuring a DHCP Server Policy for the APIC Infrastructure Using the REST API

- This task is a prerequisite for users who want to create a vShield Domain Profile.
- The port and the encapsulation used by the application Endpoint Group must belong to a physical or VM Manager (VMM) domain. If no such association with a domain is established, the APIC continues to deploy the EPG but raises a fault.
- Cisco APIC supports DHCP relay for both IPv4 and IPv6 tenant subnets. DHCP server addresses can be IPv4 or IPv6. DHCPv6 relay will occur only if IPv6 is enabled on the fabric interface and one or more DHCPv6 relay servers are configured.

Before you begin

Make sure that Layer 2 or Layer 3 management connectivity is configured.

Procedure

Configure the APIC as the DHCP server policy for the infrastructure tenant.

Note This relay policy will be pushed to all the leaf ports that are connected hypervisors using the attach entity profile configuration. For details about configuring with attach entity profile, see the examples related to creating VMM domain profiles.

Example:

DHCP Relay Policy for EPG

```
<!-- api/policymgr/mo/.xml -->
<polUni>

POST https://apic-ip-address/api/mo/uni.xml


  <fvTenant name="infra">

    <dhcpRelayP name="DhcpRelayP"  owner="tenant">
      <dhcpRsProv tDn="uni/tn-infra/ap-access/epg-default" addr="10.0.0.1" />
    </dhcpRelayP>

    <fvBD name="default">
      <dhcpLbl name="DhcpRelayP" owner="tenant"/>
    </fvBD>

  </fvTenant>
</polUni>
```

Example:

DHCP Relay Policy for Layer 3 Outside

Note You must specify DHCP Relay label under **l3extLIfP** with an appropriate name and owner.

```
<polUni>
  <fvTenant name="dhcpTn">
    <l3extOut name="Out1" >
```

```
      <l3extLNodeP name="NodeP" >
        <l3extLIfP name="Intf1">
           <dhcpLbl name="DhcpRelayPol" owner="tenant" />
        </l3extLIfP>
      </l3extLNodeP>
    </l3extOut>
  </fvTenant>
<polUni>

POST https://apic-ip-address/api/mo/uni.xml
```

Configuring a DNS Service Policy

A DNS policy is required to connect to external servers, for example AAA, RADIUS, vCenter, and services by hostname. A DNS service policy is a shared policy, so any tenant and VRF that uses this service must be configured with the specific DNS profile label. To configure a DNS policy for the ACI fabric, you must complete the following tasks:

- Ensure that the management EPG is configured for the DNS policy, otherwise this policy will not take into effect on the switches.

Note For the management EPG, only the default DNS policy is supported.

- Create a DNS profile (default) that contains the information about DNS providers and DNS domains.
- Associate the DNS profile (default or another DNS profile) name to a DNS label under the required tenant.

It is possible to configure a per-tenant, per-VRF DNS profile configuration. Additional DNS profiles can be created and applied to specific VRFs of specific tenants using the appropriate DNS label. For example, if you create a DNS profile with a name of acme, you can add a DNS label of acme to the appropriate **Networking** > **VRF** policy configuration in the tenants configuration.

Configuring External Destinations with an In-Band DNS Service Policy

Configure the external destinations for the services as follows:

Source	In-Band Management	Out-of-Band Management	External Server Location
APIC	IP address or Fully Qualified domain name (FQDN)	IP address or FQDN	Anywhere

Source	In-Band Management	Out-of-Band Management	External Server Location
Leaf switches	IP address	IP address or FQDN **Note** The DNS policy must specify the out-of-band management EPG for reachability of the DNS server.	Anywhere
Spine switches	IP address	IP address or FQDN **Note** The DNS policy must specify the out-of-band management EPG for reachability of the DNS server.	Directly connected to a leaf switch

The following is a list of external servers:

- Call Home SMTP server
- Syslog server
- SNMP Trap destination
- Statistics Export destination
- Configuration Export destination
- Techsupport Export destination
- Core Export destination

The recommended guidelines are as follows:

- The external servers must be atatched to the leaf access ports.
- Use in-band connectivity for the leaf switches to avoid extra cabling for the management port.
- Use out-of-band management connectivity for the spine switches. Connect this out-of-band network for spine switches to one of the leaf ports with in-band management virtual routing and forwarding (VRF) so that the spine switches and the leaf switches can reach the same set of external servers.
- Use IP addresses for the external servers.

Dual Stack IPv4 and IPv6 DNS Servers

DNS servers have primary DNS records which can be A records (IPV4) or AAAA records (IPV6). Both A and AAAA records associate domain name with a specific IP address (IPv4 or IPv6).

The ACI fabric can be configured to use reputable public DNS servers that run on IPv4. These servers are able to resolve and respond with A record (IPv4) or AAAA record (IPv6).

In a pure IPv6 environment, the system administrators must use IPv6 DNS servers. The IPv6 DNS servers are enabled by adding them to /etc/resolv.conf.

A more common environment is to have dual-stack IPv4 and IPv6 DNS servers. In the dual-stack case, both IPv4 and IPv6 name servers are listed in /etc/resolv.conf. However, in a dual-stack environment, simply appending the IPv6 DNS servers to the list may cause a large delay in DNS resolutions. This is because the IPv6 protocol takes precedence by default, and it is unable to connect to the IPv4 DNS servers (if they are listed first in /etc/resolv.conf). The solution is to list IPv6 DNS servers ahead of IPv4 DNS servers. Also add “options single-request-reopen” to enable the same socket to be used for both IPv4 and IPv6 lookups.

Here is an example of resolv.conf in dual-stack IPv4 and IPv6 DNS servers where the IPv6 DNS servers are listed first. Also note the “single-request-reopen” option:

```
options single-request-reopen
nameserver 2001:4860:4680::8888
nameserver 2001:4860:4680::8844
nameserver 8.8.8.8
nameserver 8.8.4.4
```

Dual-Stack IPv4 and IPv6 Environment

If the management network in the ACI fabric supports both IPv4 and IPv6, the Linux system application (glibc) will use the IPv6 network by default because getaddrinfo() will return IPv6 first.

Under certain conditions however, an IPv4 address may be preferred over an IPv6 address. The Linux IPv6 stack has a feature which allows an IPv4 address mapped as an IPv6 address using IPv6 mapped IPv4 address (::ffff/96). This allows an IPv6 capable application to use only a single socket to accept or connect both IPv4 and IPv6. This is controlled by the glibc IPv6 selection preference for getaddrinfo() in /etc/gai.conf.

In order to allow glibc to return multiple addresses when using /etc/hosts, “multi on” should be added to the /etc/hosts file. Otherwise, it may return only the first match.

If an application is not aware whether both IPv4 and IPv6 exist, it may not perform fallback attempts using different address families. Such applications may require a fallback implementation.

Policy for Priority of IPv4 or IPv6 in a DNS Profile

The DNS profile supports version preference choices between IPv4 and IPv6. Using the user interface, you can enable your preference. IPv4 is the default.

The following is an example of a policy based configuration using Postman REST API:

```
<?xml version="1.0" encoding="UTF-8”?>
<!— api/node/mo/uni/fabric/dnsp-default.xml —>
<dnsProfile dn="uni/fabric/dnsp-default" IPVerPreference="IPv6" childAction="" descr="" >
</dnsProfile>
```

The gai.conf settings control destination address selection. The file has a label table, precedence table, and an IPv4 scopes table. The changes for prioritizing IPv4 or IPv6 over the other need to go into the precedence

table entries. Given below are sample contents of the standard file as it is used in Linux systems for many flavors. A single line of precedence label in the file overrides any default settings.

The following is an example of a gai.conf to prioritize IPv4 over IPv6:

```
# Generated by APIC
label ::1/128       0
label ::/0          1
label 2002::/16     2
label ::/96         3
label ::ffff:0:0/96 4
precedence  ::1/128       50
precedence ::/0           40
precedence 2002::/16      30
precedence ::/96          20
# For APICs prefering IPv4 connections, change the value to 100.
precedence ::ffff:0:0/96  10
```

Configuring a DNS Service Policy to Connect with DNS Providers Using the GUI

Before you begin

Make sure that Layer 2 or Layer 3 management connectivity is configured.

Procedure

Step 1 On the menu bar, choose **FABRIC** > **Fabric Policies**. In the **Navigation** pane, expand **Global Policies** > **DNS Profiles**, and click the default DNS profile.

Step 2 In the **Work** pane, in the **Management EPG** field, from the drop-down list, choose the appropriate management EPG (default (Out-of-Band)).

Step 3 Expand **DNS Providers**, and perform the following actions:

a) In the **Address** field, enter the provider address.

b) In the **Preferred** column, check the check box if you want to have this address as the preferred provider.

You can have only one preferred provider.

c) Click **Update**.

d) (Optional) To add a secondary DNS provider, expand **DNS Providers**, and in the **Address** field, type the provider address. Click **Update**.

Step 4 Expand **DNS Domains**, and perform the following actions:

a) In the **Name** field, enter the domain name (cisco.com).

b) In the **Default** column, check the check box to make this domain the default domain.

You can have only one domain name as the default.

c) Click **Update**.

d) (Optional) To add a secondary DNS domain, expand **DNS Domains**. In the **Address** field, enter the secondary domain name. Click **Update**.

Step 5 Click **Submit**.
The DNS server is configured.

Step 6 On the menu bar, click **TENANTS** > **mgmt**.

Step 7 In the **Navigation** pane, expand **Networking** > **VRF** > **oob**, and click **oob**.

Step 8 In the **Work** pane, under **Properties**, in the **DNS labels** field, enter the appropriate DNS label (default). Click **Submit**.
The DNS profile label is now configured on the tenant and VRF.

Configuring a DNS Service Policy to Connect with DNS Providers Using the NX-OS Style CLI

Procedure

Step 1 In the NX-OS CLI, get into configuration mode, shown as follows:

Example:

```
apic1# configure
apic1(config)#
```

Step 2 Configure a DNS server policy.

Example:

```
apic1(config)# dns
apic1(config-dns)# address 172.21.157.5 preferred
apic1(config-dns)# address 172.21.157.6
apic1(config-dns)# domain company.local default
apic1(config-dns)# use-vrf oob-default
```

Step 3 Configure a DNS profile label on any VRF where you want to use the DNS profile.

Example:

```
apic1(config)# tenant mgmt
apic1(config-tenant)# vrf context oob
apic1(config-tenant-vrf)# dns label default
```

Configuring a DNS Service Policy to Connect with DNS Providers Using the REST API

Before you begin

Make sure that Layer 2 or Layer 3 management connectivity is configured.

Procedure

Step 1 Configure the DNS service policy.

Example:

```
POST URL :
https://apic-IP-address/api/node/mo/uni/fabric.xml

<dnsProfile name="default">

    <dnsProv addr="172.21.157.5" preferred="yes"/>
    <dnsProv addr="172.21.157.6"/>

    <dnsDomain name="cisco.com" isDefault="yes"/>

    <dnsRsProfileToEpg tDn="uni/tn-mgmt/mgmtp-default/oob-default"/>

</dnsProfile>
```

Step 2 Configure the DNS label under the out-of-band management tenant.

Example:

```
POST URL: https://apic-IP-address/api/node/mo/uni/tn-mgmt/ctx-oob.xml
<dnsLbl name="default" tag="yellow-green"/>
```

Verifying that the DNS Profile is Configured and Applied to the Fabric Controller Switches Using the NX-OS Style CLI

Procedure

Step 1 Verify the configuration for the default DNS profile.

Example:

```
apic1# show running-config dns

# Command: show running-config dns
# Time: Sat Oct  3 00:23:52 2015
  dns
    address 172.21.157.5 preferred
    address 172.21.157.6
    domain company.local default
    use-vrf oob-default
    exit
```

Step 2 Verify the configurations for the DNS labels.

Example:

```
apic1# show running-config tenant mgmt vrf context oob

# Command: show running-config tenant mgmt vrf context oob
# Time: Sat Oct  3 00:24:36 2015
  tenant mgmt
    vrf context oob
      dns label default
      exit
    exit
```

Step 3 Verify that the applied configuration is operating on the fabric controllers.

Example:

```
apic1# cat /etc/resolv.conf
# Generated by IFC

nameserver 172.21.157.5
nameserver 172.21.157.6
```

Configuring Custom Certificates

Configuring Custom Certificate Guidelines

- Wildcard certificates (such as *.cisco.com, which is used across multiple devices) and its associated private key generated elsewhere are not supported on the APIC as there is no support to input the private key or password in the APIC. Also, exporting private keys for any certificates, including wildcard certificates, is not supported.
- You must download and install the public intermediate and root CA certificates before generating a Certificate Signing Request (CSR). Although a root CA Certificate is not technically required to generate a CSR, Cisco requires the root CA certificate before generating the CSR to prevent mismatches between the intended CA authority and the actual one used to sign the CSR. The APIC verifies that the certificate submitted is signed by the configured CA.
- To use the same public and private keys for a renewed certificate generation, you must satisfy the following guidelines:
  - You must preserve the originating CSR as it contains the public key that pairs with the private key in the key ring.
  - The same CSR used for the originating certificate must be resubmitted for the renewed certificate if you want to re-use the public and private keys on the APIC.
  - Do not delete the original key ring when using the same public and private keys for the renewed certificate. Deleting the key ring will automatically delete the associated private key used with CSRs.

Configuring a Custom Certificate for Cisco ACI HTTPS Access Using the GUI

CAUTION: PERFORM THIS TASK ONLY DURING A MAINTENANCE WINDOW AS THERE IS A POTENTIAL FOR DOWNTIME. The downtime affects access to the APIC cluster and switches from external users or systems and not the APIC to switch connectivity. The NGINX process on the switches will also be impacted but that will be only for external connectivity and not for the fabric data plane. Access to the APIC, configuration, management, troubleshooting and such will be impacted. Expect a restart of all web servers in the fabric during this operation.

Before you begin

Determine from which authority you will obtain the trusted certification so that you can create the appropriate Certificate Authority.

Procedure

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

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

Step 3 In the **Work** pane, choose **Public Key Management** > **Certificate Authorities** > **Create Certificate Authority**.

Step 4 In the **Create Certificate Authority** dialog box, in the **Name** field, enter a name for the certificate authority.

Step 5 In the **Certificate Chain** field, copy the intermediate and root certificates for the certificate authority that will sign the Certificate Signing Request (CSR) for the Application Policy Infrastructure Controller (APIC).

The certificate should be in Base64 encoded X.509 (CER) format. The intermediate certificate is placed before the root CA certificate. It should look similar to the following example:

```
-----BEGIN CERTIFICATE-----
<Intermediate Certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root CA Certificate>
-----END CERTIFICATE-----
```

Step 6 Click **Submit**.

Step 7 In the **Navigation** pane, choose **Public Key Management** > **Key Rings**.

Step 8 In the **Work** pane, choose **Actions** > **Create Key Ring**.

Step 9 In the **Create Key Ring** dialog box, in the **Name** field, enter a name.

Step 10 In the **Certificate** field, do not add any content.

Step 11 In the **Modulus** field, click the radio button for the desired key strength.

Step 12 In the **Certificate Authority** field, from the drop-down list, choose the certificate authority that you created earlier. Click **Submit**.

Note Do not delete the key ring. Deleting the key ring will automatically delete the associated private key used with CSRs.

In the **Work** pane, in the **Key Rings** area, the **Admin State** for the key ring created displays **Started**.

Step 13 In the **Navigation** pane, choose **Public Key Management** > **Key Rings** > ***key_ring_name***.

Step 14 In the **Work** pane, choose **Actions** > **Create Certificate Request**.

Step 15 In the **Subject** field, enter the fully qualified domain name (FQDN) of the APIC.

Step 16 Fill in the remaining fields as appropriate.

Note Check the online help information available in the **Create Certificate Request** dialog box for a description of the available parameters.

Step 17 Click **Submit**.
The object is created and displayed in the **Navigation** pane under the key ring you created earlier. In the **Navigation** pane, click the object and in the **Work** pane, in the **Properties** area, in the **Request** field the CSR is displayed. Copy the contents from the field to submit to the **Certificate Authority**.

Step 18 In the **Navigation** pane, choose **Public Key Management** > **Key Rings** > ***key_ring_name***.

Step 19 In the **Work** pane, in the **Certificate** field, paste the signed certificate that you received from the certificate authority.

Step 20 Click **Submit**.

Note If the CSR was not signed by the Certificate Authority indicated in the key ring, or if the certificate has MS-DOS line endings, an error message is displayed and the certificate is not accepted. Remove the MS-DOS line endings.

The key is verified, and in the **Work** pane, the **Admin State** changes to **Completed** and is now ready for use in the HTTP policy.

Step 21 On the menu bar, choose **Fabric** > **Fabric Policies**.

Step 22 In the Navigation pane, choose **Pod Policies** > **Policies** > **Management Access** > **default**.

Step 23 In the **Work** pane, in the **Admin Key Ring** drop-down list, choose the desired key ring.

Step 24 (Optional) For Client-based authentication, in the **Client Certificate TP** drop-down list, choose the previously created Local User policy and click **Enabled** for **Client Certificate Authentication state**.

Step 25 Click **Submit**.
All web servers restart. The certificate is activated, and the non-default key ring is associated with HTTPS access.

What to do next

You must remain aware of the expiration date of the certificate and take action before it expires. To preserve the same key pair for the renewed certificate, you must preserve the CSR as it contains the public key that pairs with the private key in the key ring. Before the certificate expires, the same CSR must be resubmitted. Do not delete or create a new key ring as deleting the key ring will delete the private key stored internally on the APIC.

Provisioning Fabric Wide System Settings

Configuring APIC In-Band or Out-of-Band Connectivity Preferences

This topic describes how to toggle between in-band and out-of-band connectivity on the APIC server for management access to devices such as authentication servers or SNMP servers external to the ACI fabric. Enabling **inband** executes in-band management connectivity between the APIC server to external devices through leaf switches on the ACI fabric. Enabling **ooband** executes out-of-band management connectivity between the APIC server to external devices through connections external to the ACI fabric.

Before you begin

Configure in-band and out-of-band management networks. For more information, see *Management* in the *Cisco APIC Basic Configuration Guide, Release 3.x*.

Procedure

Step 1 On the menu bar, click **System** > **System Settings**.
Step 2 On the Navigation bar, click **APIC Connectivity Preferences**.
Step 3 To enable the policy, click **inband** or **ooband**.
Step 4 Click **Submit**.

Configure Quota Management Policies

Starting in the Cisco Application Policy Infrastructure Controller (APIC) Release 2.3(1), there are limits on number of objects a tenant admin can configure. This enables the admin to limit the number of managed objects that can be added globally across tenants.

This feature is useful when you want to limit any tenant or group of tenants from exceeding ACI maximums per leaf or per fabric or unfairly consuming a majority of available resources, potentially affecting other tenants on the same fabric.

Procedure

Step 1 On the menu bar, click **System** > **System Settings**.
Step 2 Right-click **Quota** and choose **Create Quota Configuration**..
Step 3 In the **Class** field, choose the object type to limit with the quota.
Step 4 In the **Container Dn** field, enter the distinguished name (DN) that describes the class.
Step 5 In the **Exceed Action** field, choose either **Fail Transaction Action** or **Raise Fault Action**.
Step 6 In the **Max Number** field, enter the maximum number of the managed objects that can be created after which the exceed action will be applied.
Step 7 Click **Submit**.

Create an Enforced BD Exception List

This topic describes how to create a global exception list of subnets which are not subject to an enforced bridge domain. With the Enforced BD feature configured, the endpoints in a subject endpoint group (EPG) can only ping subnet gateways within the associated bridge domain.

The exception IP addresses can ping all of the BD gateways across all of your VRFs.

A loopback interface configured for an L3Out does not enforce reachability to the IP address that is configured for the subject loopback interface.

When an eBGP peer IP address exists in a different subnet than the subnet of the L3Out interface, the peer subnet must be added to the allowed exception subnets. Otherwise, eBGP traffic is blocked because the source IP address exists in a different subnet than the L3Out interface subnet.

Before you begin

Create an enforced bridge domain (BD).

Procedure

Step 1 On the menu bar, click **System** > **System Settings**.

Step 2 Click **BD Enforced Exception List**.

Step 3 Click the + on **Exception List**.

Step 4 Add the IP address and network mask for the subnet that can ping any subnet gateway.

Step 5 Repeat to add more subnets that are exceptions to the enforced bridge domain.

Step 6 Click **Submit**.

Create a BGP Route Reflector Policy and Route Reflector Node Endpoints

This topic describes how to create ACI fabric route reflectors, which use multiprotocol BGP (MP-BGP) to distribute external routes within the fabric. To enable route reflectors in the ACI fabric, the fabric administrator must select the spine switches that will be the route reflectors, and provide the autonomous system (AS) number. Once route reflectors are enabled in the ACI fabric, administrators can configure connectivity to external networks.

Before you begin

Required:

- To connect external routers to the ACI fabric, the fabric infrastructure administrator must configure spine nodes as Border Gateway Protocol (BGP) route reflectors.
- For redundancy purposes, more than one spine is configured as a router reflector node (one primary and one secondary reflector).

Procedure

Step 1 To create a BGP Route Reflector policy, perform the following steps:

a) On the menu bar, click **System** > **System Settings**.
b) Click **BGP Route Reflector**.
c) Enter the Autonomous System Number.
d) Click the + on **Route Reflector Nodes**.
e) Enter the spine route reflector node ID endpoint, and click **Submit**.,

Step 2 To create external route reflector node endpoints, perform the following steps:

a) Click the + on **External Route Reflector Nodes**.
b) Choose the spine to serve as external route reflector node endpoint.
c) If this is a site managed by Multi-Site, you can also specify an intersite spine route reflector.

d) Click **Submit**.

Configure a Fabric Wide Control Plane MTU Policy

This topic describes how to create a fabric-wide Control Plane (CP) MTU policy, that sets the global MTU size for control plane packets sent by the nodes (APIC and the switches) in the fabric.

In a multipod topology, the MTU setting for the fabric external ports must be greater than or equal to the CP MTU value set. Otherwise, the fabric external ports might drop the CP MTU packets.

Note If you set the L3Out Interface Profile to inherit the MTU from the IPN, it will be 9150. If you want the MTU to be used across the IPN to be 9216, you must explicitly configure it in the L3Out Interface Profile (at **Tenants** > ***tenant-name*** > **Networking** > **External Routed Networks** > **Create Routed Outside** > **Nodes and Interface Protocol Profiles** > **Create Node Profile** > **Create Interface Profile**).

If you change the IPN or CP MTU, Cisco recommends changing the CP MTU value first, then changing the MTU value on the spine of the remote pod. This reduces the risk of losing connectivity between the pods due to MTU mismatch.

Procedure

Step 1 On the menu bar, click **System** > **System Settings**.

Step 2 Click **Control Plane MTU**.

Step 3 Enter the MTU for fabric ports.

Step 4 Click **Submit**.

Create a COOP Group Policy

This topic describes how to create a Council of Oracle Protocol (COOP) Group Policy, which is used to communicate the mapping information (location and identity) to the spine proxy. A leaf switch forwards endpoint address information to the spine switch 'Oracle' using Zero Message Queue (ZMQ). COOP running on the spine nodes will ensure all spine nodes maintain a consistent copy of endpoint address and location information and additionally maintain the distributed hash table (DHT) repository of endpoint identity to location mapping database.

Procedure

Step 1 On the menu bar, click **System** > **System Settings**.

Step 2 Click **COOP Group**.

Step 3 Choose the policy property type. The type can be **Compatible Type** or **Strict Type**.

The Oracle Nodes are the spines in the fabric, automatically populated by the system.

Step 4 Click **Submit**

Configure Endpoint Loop Protection

The endpoint loop protection policy specifies how loops detected by frequent MAC moves are handled. To configure EP loop protection perform the following steps:

Procedure

Step 1 On the menu bar, click **System** > **System Settings**.

Step 2 Click **Endpoint Controls**.

Step 3 Click the **Ep Loop Protection** tab.

Step 4 To enable the policy, click **Enabled** in the **Administrative State** field.

Step 5 Optional. Set the loop detection interval, which specifies the time to detect a loop. The interval range is from 30 to 300 seconds. The default setting is 60 seconds.

Step 6 Set the loop detection multiplication factor, which is the number of times a single EP moves between ports within the loop detection interval. The range is from 1 to 255. The default is 4.

Step 7 Choose the action to take when detecting a loop.

The action can be:

- **BD Learn Disable**
- **Port Disable**

The default is **Port Disable**.

Step 8 Click **Submit**.

About the Rogue Endpoint Control Policy

A rogue endpoint attacks top of rack (ToR) switches through frequently, repeatedly injecting packets on different ToR ports and changing 802.1Q tags (thus, emulating endpoint moves) causing learned class and EPG port changes. Misconfigurations can also cause frequent IP and MAC address changes (moves).

Such rapid movement in the fabric causes significant network instability, high CPU usage, and in rare instances, endpoint mapper (EPM) and EPM client (EPMC) crashes due to significant and prolonged messaging and transaction service (MTS) buffer consumption. Also, such frequent moves may result in the EPM and EPMC logs rolling over very quickly, hampering debugging for unrelated endpoints.

The rogue endpoint control feature addresses this vulnerability by quickly:

- Identifying such rapidly moving MAC and IP endpoints
- Stopping the movement by temporarily making endpoints static (thus, quarantining the endpoint)
- Keeping the endpoint static for the **Rogue EP Detection Interval** and dropping the traffic to and from the rogue endpoint. After this time expires, deleting the unauthorized MAC or IP address

- Generating a host tracking packet to enable the system to re-learn the impacted MAC or IP address
- Raising a fault, to enable corrective action

The rogue endpoint control policy is configured globally and, unlike other loop prevention methods, functions at the level of individual endpoints (IP and MAC addresses). It does not distinguish between local or remote moves; any type of interface change is considered a move in determining if an endpoint should be quarantined.

The rogue endpoint control feature is disabled by default.

Limitations of the Rogue Endpoint Control Policy

The following limitations apply when using a rogue endpoint control policy:

- Changing rogue endpoint control policy parameters will not affect existing rogue endpoints.
- If a rogue endpoint is enabled, loop detection and bridge domain move frequency will not take effect.
- Disabling the rogue endpoint feature clears all rogue endpoints.
- You must disable the rogue endpoint feature prior to upgrading or downgrading the Cisco Application Policy Infrastructure Controller (Cisco APIC).
- The endpoint mapper (EPM) has value limits for rogue endpoint parameters. If you set the parameter values outside of this range, the Cisco APIC raises a fault for each mismatched parameter.
- The rogue endpoint feature is not supported on remote leaf switches or Cisco ACI Multi-Site.

Configure the Rogue Endpoint Control Policy Using the GUI

You can configure the **Rogue EP Control** policy for the fabric, to detect and delete unauthorized endpoints, using the Cisco Application Policy Infrastructure Controller (Cisco APIC) GUI. This topic also includes the steps to clear rogue endpoints on a TOR switch, ad-hoc.

The policy options have the following valid and supported values:

- **Rogue EP Detection Interval**—Sets the rogue endpoint detection interval, which specifies the time to detect rogue endpoints. Valid values are from 0 to 65535 seconds. The default is 60.
- **Hold Interval (sec)**—Interval in seconds after the endpoint is declared rogue, where it is kept static so learning is prevented and the traffic to and from the Rogue endpoint is dropped. After this interval, the endpoint is deleted. Valid values are from 1800 to 3600. The default is 1800.
- **Rogue EP Detection Multiplication Factor**—Sets the rogue endpoint detection multiplication factor for determining if an endpoint is unauthorized. If the endpoint moves more times than this number, within the EP detection interval, the endpoint is declared rogue. Valid values are from 2 to 10. The default is 6.

Procedure

Step 1 On the menu bar, click **System** > **System Settings**.

Step 2 On the navigation bar, click **Endpoint Controls** and click the **Rogue EP Control** tab.

Step 3 Set the **Administrative State** to **Enabled**.

Step 4 Optional. Reset the **Rogue EP Detection Interval (sec)**, **Rogue EP Detection Multiplication Factor**, or the **Hold Interval (sec)**.

Step 5 (Optional) To clear rogue endpoints on a TOR switch, perform the following steps:

a) On the Cisco APIC menu bar, click **Fabric** > **Inventory**.
b) On the Navigation bar, expand the Pod and click the leaf switch where you want to clear rogue endpoints.
c) When the leaf switch summary appears in the work pane, right-click the leaf switch name in the Navigation bar, and choose **Clear Rogue Endpoints**.
d) Click **Yes**.

Configure Rogue Endpoint Control Using the NX-OS Style CLI

You can configure the **Rogue EP Control** policy for the fabric, to detect and delete unauthorized endpoints, using the NX-OS style CLI.

Procedure

Step 1 **configure**

Enters global configuration mode.

Example:

```
apic1# configure
```

Step 2 **endpoint rogue-detect enable**

Enables the global Rogue Endpoint Control policy.

Example:

```
apic1(config)# endpoint rogue-detect enable
```

Step 3 **endpoint rogue-detect hold-interval** *hold_interval*

Sets the hold interval in seconds after the endpoint is declared rogue, where it is kept static so learning is prevented, and the traffic to and from the rogue endpoint is dropped. After this interval, the endpoint is deleted. Valid values are from 1800 to 3600 seconds. The default is 1800.

Example:

```
apic1(config)# endpoint rogue-detect hold-interval 1800
```

Step 4 **endpoint rogue-detect interval** *interval*

Sets the rogue detection interval in seconds, which specifies the time to detect rogue endpoints. Valid values are from 0 to 65535 seconds. The default is 60.

Example:

```
apic1(config)# endpoint rogue-detect interval 60
```

Step 5 **endpoint rogue-detect factor** *factor*

Specifies the multiplication factor for determining if an endpoint is unauthorized. If the endpoint moves more times during the interval, the EP is declared rogue. Valid values are from 2 to 10. The default is 6.

Example:

```
apic1# endpoint rogue-detect factor 6
```

Step 6 This example configures a Rogue Endpoint Control policy.

Example:

```
apic1# cconfigure
apic1(config)# endpoint rogue-detect enable
apic1(config)# endpoint rogue-detect hold-interval 1800
apic1(config)# endpoint rogue-detect interval 60
apic1(config)# endpoint rogue-detect factor 6
```

Configure the Rogue Endpoint Control Policy Using the REST API

You can configure the **Rogue EP Control** policy for the fabric, to detect and delete unauthorized endpoints, using the REST API.

Procedure

To configure the Rogue EP Control policy, send a post with XML similar to the following:

Example:

```
<polUni>
    <infraInfra>
        <epControlP name="default" adminSt="enabled"  holdIntvl="1800"
rogueEpDetectIntvl="60" rogueEpDetectMult="6"/>
    </infraInfra>
</polUni>
```

Configure IP Aging

This topic describes how to enable an IP Aging policy. When enabled, the IP aging policy ages unused IPs on an endpoint.

When the Administrative State is enabled, the IP aging policy sends ARP requests (for IPv4) and neighbor solicitations (for IPv6) to track IPs on endpoints. If no response is given, the policy ages the unused IPs.

Procedure

Step 1 On the menu bar, click **System** > **System Settings**.

Step 2 Click **Endpoint Controls**.

Step 3 Click the **Ip Aging** tab.

Step 4 To enable the policy, click **Enabled** in the **Administrative State** field.

What to do next

Create an End Point Retention policy, which is required, to specify the timer used for tracking IPs on endpoints. Navigate to **Tenants** > *tenant-name* > > **Policies** > **Protocol** > **End Point Retention**.

Disable Remote Endpoint Learning

This topic describes how to enable or disable IP end point learning.

The scope of this policy is fabric-wide. After configuration, a policy is pushed to each leaf switch as it comes up.

You should enable this policy in fabrics which include the Cisco Nexus 9000 series switches, 93128 TX, 9396 PX, or 9396 TX switches with the N9K-M12PQ uplink module, after all the nodes have been successfully upgraded to APIC Release 2.2(2x) or higher.

After any of the following configuration changes, you may need to manually flush previously learned IP endpoints:

- Remote IP endpoint learning is disabled
- The VRF is configured for ingress policy enforcement
- At least one Layer 3 interface exists in the VRF

To manually flush previously learned IP endpoints, enter the following command on both VPC peers: `vsh -c "clear system internal epm endpoint vrf <vrf-name> remote"`

To enable or disable IP end point learning, perform the following steps:

Procedure

Step 1 On the menu bar, click **System** > **System Settings**.
Step 2 Click **Fabric Wide Setting**.
Step 3 Click the check box on **Disable Remote EP Learn**.
Step 4 Click **Submit**.

Globally Enforce Subnet Checks

This topic describes how to enable or disable subnet checking. When enabled, IP address learning is disabled outside of subnets configured in a VRF, for all other VRFs.

The scope of this policy is fabric-wide. After configuration, a policy is pushed to each leaf switch as it comes up.

Procedure

Step 1 On the menu bar, click **System** > **System Settings**.
Step 2 Click **Fabric Wide Setting**.
Step 3 Click the check box on **Enforce Subnet Check**.
Step 4 Click **Submit**.

Reallocate a GIPo

This topic describes how to enable reallocating GIPos on non-stretched BDs to make room for stretched BDs.

The scope of this policy is fabric-wide. After configuration, a policy is pushed to each leaf switch as it comes up.

Procedure

Step 1 On the menu bar, click **System** > **System Settings**.
Step 2 Click **Fabric Wide Setting**.
Step 3 Click the check box on **Reallocate Gipo**.
Step 4 Click **Submit**.

Globally Enforce Domain Validation

This topic describes how to enforce domain validation. When enabled, a validation check is performed when a static path is added, to determine if no domain is associated with an EPG.

The scope of this policy is fabric-wide. After configuration, a policy is pushed to each leaf switch as it comes up.

Procedure

Step 1 On the menu bar, click **System** > **System Settings**.
Step 2 Click **Fabric Wide Setting**.
Step 3 Click the check box on **Enforce Domain Validation**.
Step 4 Click **Submit**.

Enable OpFlex Client Authentication

This topic describes how to enable OpFlex client authentication for GOLF and Linux.

To deploy GOLF or Linux Opflex clients in an environment where the identity of the client cannot be guaranteed by the network, you can dynamically validate the client's identity based on a client certificate.

Note When you enable certificate enforcement, connectivity with any GOLF or Linux Opflex client that does not support client authentication is disabled.

The scope of this policy is fabric-wide. After configuration, a policy is pushed to each leaf switch as it comes up.

Procedure

Step 1 On the menu bar, click **System** > **System Settings**.

Step 2 Click **Fabric Wide Setting**.

Step 3 Click the check box on **OpFlex Client Authentication** to enable or disable enforcing client certificate authentication for GOLF and Linux Opflex clients.

Step 4 Click **Submit**.

Create a Load Balancer Policy

This topic describes how to configure the default Load Balancer policy.

The load balancing policy options balance traffic among the available uplink ports. Static hash load balancing is the traditional load balancing mechanism used in networks where each flow is allocated to an uplink based on a hash of its 5-tuple. This load balancing gives a distribution of flows across the available links that is roughly even. Usually, with a large number of flows, the even distribution of flows results in an even distribution of bandwidth as well. However, if a few flows are much larger than the rest, static load balancing might give suboptimal results.

Procedure

Step 1 On the menu bar, click **System** > **System Settings**.

Step 2 Click **Load Balancer**.

Step 3 Choose the **Dynamic Load Balancing Mode**.

The dynamic load balancer (DLB) mode adjusts the traffic allocations according to congestion levels. It measures the congestion across the available paths and places the flows on the least congested paths, which results in an optimal or near optimal placement of the data. DLB can be configured to place traffic on the available uplinks using the granularity of flows or of flowlets. Flowlets are bursts of packets from a flow that are separated by intervals. The mode can be **Aggressive**, **Conservative**, or **Off** (the default).

Step 4 Enable or disable **Dynamic Packet Prioritization** by choosing **On** or **Off** (the default.

Dynamic Packet Prioritization (DPP) prioritizes short flows higher than long flows; a short flow is less than approximately 15 packets. Short flows are more sensitive to latency than long ones. DPP can improve overall application performance.

Step 5 Choose the Load Balancing Mode. The mode can be **Link Failure** or **Traditional** (the default).

The load balancer administrative state. In all modes of load balancing, static or dynamic, the traffic is sent only on those uplinks or paths that meet the criteria for equal cost multipath (ECMP); these paths are equal and the lowest cost from a routing perspective.

Step 6 Click **Submit**.

Enable a Time Precision Policy

This topic describes how to enable Precision Time Protocol (PTP), a time synchronization protocol for nodes distributed across a network. Its hardware timestamp feature provides greater accuracy than other time synchronization protocols such as Network Time Protocol (NTP).

PTP is a distributed protocol that specifies how real-time PTP clocks in the system synchronize with each other. These clocks are organized into a master-member synchronization hierarchy with the grandmaster clock, the clock at the top of the hierarchy, determining the reference time for the entire system. Synchronization is achieved by exchanging PTP timing messages, with the members using the timing information to adjust their clocks to the time of their master in the hierarchy. PTP operates within a logical scope called a PTP domain.

Procedure

Step 1 On the menu bar, click **System** > **System Settings**.

Step 2 Click **Precision Time Protocol**.

Step 3 Choose **Enabled** or **Disabled**.

If you choose disable PTP, NTP time is used to sync the fabric. If you enable PTP, a spine is automatically chosen as a master to which the entire site gets synced.

Step 4 Click **Submit**.

Enable a Global System GIPo Policy

This topic describes how to use the infra tenant GIPo as the system GIPo.

An ACI multipod deployment requires the 239.255.255.240 system Global IP Outside (GIPo) to be configured on the inter-pod network (IPN) as a PIM BIDIR range. This 239.255.255.240 PIM BIDIR range configuration on the IPN devices can be avoided by using the infra GIPo as System GIPo.

Before you begin

Upgrade all of the switches in the ACI fabric, including the leaf switches and spine switches, to the latest APIC release.

Procedure

Step 1 On the menu bar, click **System** > **System Settings**.

Step 2 Choose **Enabled** or **Disabled** (the default) on **Use Infra GIPo as System GIPo**

Step 3 Click **Submit**.

Provisioning Global Fabric Access Policies

Create a Global Attachable Access Entity Profile

An Attachable Entity Profile (AEP) represents a group of external entities with similar infrastructure policy requirements. The infrastructure policies consist of physical interface policies that configure various protocol options, such as Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), or Link Aggregation Control Protocol (LACP).

An AEP is required to deploy VLAN pools on leaf switches. Encapsulation blocks (and associated VLANs) are reusable across leaf switches. An AEP implicitly provides the scope of the VLAN pool to the physical infrastructure.

The following AEP requirements and dependencies must be accounted for in various configuration scenarios, including network connectivity, VMM domains, and multipod configuration:

- The AEP defines the range of allowed VLANS but it does not provision them. No traffic flows unless an EPG is deployed on the port. Without defining a VLAN pool in an AEP, a VLAN is not enabled on the leaf port even if an EPG is provisioned.
- A particular VLAN is provisioned or enabled on the leaf port that is based on EPG events either statically binding on a leaf port or based on VM events from external controllers such as VMware vCenter or Microsoft Azure Service Center Virtual Machine Manager (SCVMM).
- Attached entity profiles can be associated directly with application EPGs, which deploy the associated application EPGs to all those ports associated with the attached entity profile. The AEP has a configurable generic function (infraGeneric), which contains a relation to an EPG (infraRsFuncToEpg) that is deployed on all interfaces that are part of the selectors that are associated with the attachable entity profile.

A virtual machine manager (VMM) domain automatically derives physical interface policies from the interface policy groups of an AEP.

Before you begin

Create the tenant, VRF, application profiles, and EPGs to associate to the attached entity profile.

Procedure

Step 1 On the menu bar, click **Fabric** > **External Access Policies**.

Step 2 On the navigation bar, expand **Policies** and **Global**.

Step 3 Right-click **Attachable Access Entity Profile** and choose **Create Attachable Access Entity Profile**.

Step 4 Enter a name for the policy.

Step 5 Click the + icon on **Domains** table.

Step 6 Enter a physical domain, a previously created physical, Layer 2, Layer 3, or Fibre Channel domain, or create one.

Step 7 Enter the encapsulation for the domain and click **Update**.

Step 8 Click the + icon on the **EPG DEPLOYMENT** table.

Step 9 Enter the tenant, application profile, EPG, encapsulation (such as vlan-1), primary encapsulation (primary encapsulation number) and interface mode (trunk, Access (802.1P, or Access (Untagged).

Step 10 Click **Update**.

Step 11 Click **Next**.

Step 12 Choose the interfaces to associate to the attachable entity profile.

Step 13 Click **Finish**.

Configure the Global QoS Class Policy

The global QoS Class policy can be used to:

- Preserve the CoS priority level, to guarantee that the CoS value in 802.1P packets which enter and transit the ACI fabric is preserved. 802.1P CoS preservation is supported in single pod and multipod topologies. In multipod topologies, CoS Preservation can be used where you want to preserve the QoS priority settings of 802.1P traffic entering POD 1 and egressing out of POD 2, but you are not concerned with preserving the CoS/DSCP settings in interpod network (IPN) traffic between the pods. To preserve CoS/DSCP settings when multipod traffic is transitting an IPN, use a DSCP policy (configured at **Tenants** > **infra** > > **Policies** > **Protocol** > **DSCP class-cos translation policy for L3 traffic**)
- Reset the properties for the default QoS class levels, such as the **MTU**, **Queue Limit**, or **Scheduling Algorithm**.

Procedure

Step 1 On the menu bar, click **Fabric** > **External Access Policies**.

Step 2 On the navigation bar, expand **Policies** and **Global**.

Step 3 Click **QOS Class**.

Step 4 To enable 802.1P CoS preservation, click the **Preserve COS** check box.

Step 5 To change the default settings for a QoS class, double-click on it. Enter the new settings and click **Submit**.

Create a Global DHCP Relay Policy

The global DHCP Relay policy identifies the DHCP Server for the fabric.

Procedure

Step 1 On the menu bar, click **Fabric** > **External Access Policies**.

Step 2 On the navigation bar, expand **Policies** and **Global**.

Step 3 Right-click **DHCP Relay** and choose **Create DHCP Relay Policy**.

Step 4 Enter a name for the policy.

Step 5 Click the + icon on **Providers**.

Step 6 Choose the EPG type, and for an application EPG, choose the tenant, application profile, and the EPG to be the provider.

Step 7 In the **DHCP Server Address** field, enter the IP address for the server.

Step 8 Click **OK**.

Enable a Global MCP Instance Policy

Enable a global Mis-Cabling Protocol (MCP) instance policy. In the current implementation, only one instance of MCP runs in the system.

Procedure

Step 1 On the menu bar, click **Fabric** > **External Access Policies**.

Step 2 On the navigation bar, expand **Policies** and **Global**.

Step 3 Click **MCP Instance Policy default**.

Step 4 Change the **Admin State** to **Enabled**.

Step 5 Set other properties as needed for your fabric.

Step 6 Click **Submit**.

What to do next

Create an Error Disabled Recovery Policy

The error disabled recovery policy specifies the policy for re-enabling a port that was disabled due to one or more pre-defined error conditions.

Procedure

Step 1 On the menu bar, click **Fabric** > **External Access Policies**.

Step 2 On the navigation bar, expand **Policies** and **Global**.

Step 3 Click **Error Disabled Recovery Policy**..

Step 4 Double-click on an event to enable it for the recovery policy.

Step 5 Click the check box and click **Update**.

Step 6 Optional. Repeat steps 4 and 5 for more events.

Step 7 Optional. Reset the **Error disable recovery interval (sec)**.

Step 8 Click **Submit.**

Configure a Global Port Tracking Policy

Uplink failure detection can be enabled in the fabric access global port tracking policy. The port tracking policy monitors the status of links between leaf switches and spine switches. When an enabled port tracking policy is triggered, the leaf switches take down all access interfaces on the switch that have EPGs deployed on them.

Procedure

Step 1 On the menu bar, click **Fabric** > **External Access Policies**.

Step 2 On the navigation bar, expand **Policies** and **Global**.

Step 3 Click **Port Tracking**.

Step 4 Enable port tracking by setting the **Port tracking state** to **on**.

Step 5 Optional. Change the **Daily restore timer**.

Step 6 Enter the **Number of active spine links that triggers port tracking**

Step 7 Click **Submit**