Alternate Procedures for Creating vCenter Domain, Interface, and Switch Profiles

We recommend using the unified configuration wizard for performing configuration tasks before installing Cisco ACI Virtual Edge. However, you may need to configure separate, more detailed policies.

This appendix includes individual procedures for creating a vCenter domain profile and different kinds of interface and switch profiles:

Create Port Channel Switch and Interface Profiles

Before you can install Cisco ACI Virtual Edge, create switch and interface profiles.

Before you begin

In Step 4 d of this procedure, you choose a leaf switch node ID from the drop-down list. It must match the node ID of the leaf switch connected to the ESXi or Layer 2 cloud host. Check the leaf switch node ID in the **Fabric Membership** window by going to **Fabric** > **Inventory** > **Fabric Membership**.

Procedure

Step 1 Log in to the Cisco APIC.

Step 2 Choose **Fabric** > **Access Policies**.

Step 3 In the **Policies** navigation pane, expand the **Switches** folder and the **Leaf Switches** folder.

Step 4 Right-click the **Profiles** folder, and then choose **Create Leaf Profile**.

Step 5 In the **Create Leaf Profile (STEP 1 > Profile)** dialog box, complete the following steps:

a) In the **Name** field, enter a name.

b) In the **Leaf Selectors** field, click the + icon to create a new switch selector.

c) In the **Name** field, enter a name.

Alternate Procedures for Creating vCenter Domain, Interface, and Switch Profiles

d) In the **Blocks** field, choose a leaf switch node ID from the drop-down list.

e) Click **Update**.

f) Click **Next**.

Step 6 In the **Create Leaf Profile (STEP 2 > Associations)** dialog box, in the **Interface Selectors Profiles** area, click the + icon to create a new interface selector profile.

Step 7 In the **Create Interface Profile** dialog box, complete the following steps:

a) In the **Name** field, enter the vLeaf name.

b) In the **Interface Selectors** area, click the + icon to create a new interface selector.

Step 8 In the **Create Access Port Selector** dialog box, complete the following steps:

a) Enter a name for the selector in the **Name** field.

b) In the **Interface IDs** field, enter the access port interface IDs for the physical interfaces connected to the ESXi host.

c) In the **Interface Policy Group** drop-down list, choose **Create PC Interface Policy Group**.

Step 9 In the **Create PC Interface Policy Group** dialog box, enter the policy group name in the **Name** field.

Step 10 In the **Port Channel Policy** field, choose **Create Port Channel Policy** from the drop-down list.

Step 11 In the **Create Port Channel Policy** dialog box, complete the following steps:

a) Enter the policy name in the **Name** field.

b) In the **Mode** field, choose one of the following values:

- **Static Channel - Mode On**
- **LACP Active**
- **LACP Passive**
- **MAC Pinning**
- **MAC Pinning-Physical-NIC-load**

Note Do not use MAC pinning with a direct connection to a VPC leaf pair. Instead, use Link Aggregation Control Protocol (LACP) or enhanced LACP to provide redundancy and reliability. Using MAC pinning with a direct connection leads to traffic loss when peer leaf switches are rebooted. Use MAC Pinning only where virtual port channel (VPC) cannot be supported, such as for Cisco UCS Fabric Interconnects with southbound interfaces.

c) Click **Submit**.

Step 12 In the **Create PC Interface Policy Group** dialog box, complete the following steps:

a) In the **Attached Entity Profile** field, choose a profile you created earlier or create one from the drop-down list.

b) Click **Submit**.

Step 13 In the **Create Access Port Selector** dialog box, click **OK**.

Step 14 In the **Create Leaf Interface Profile** dialog box, click **Submit**.

Step 15 In the **Create Leaf Profile** dialog box, choose the new interface profile and then click **Finish**.

Create VPC Interface and Switch Profiles Using the GUI

Procedure

Step 1 Log in to the Cisco APIC.

Step 2 Choose **Fabric** > **Access Policies**.

Step 3 In the **Policies** navigation pane, expand the **Policies** and **Switch** folders.

Step 4 Right-click the **VPC Domain** folder and choose **Create VPC Domain Policy**.

Step 5 In the **Create VPC Domain Policy** dialog box, complete the following steps:

a) In the **Name** field, enter a name for the policy.

b) In the **Peer Dead Interval** field, enter a value.

The range is from 3 seconds to 300 seconds.

c) Click **Submit** to save the policy.

Step 6 In the **Policies** navigation pane, expand the **Switches** and **Leaf Switches**folders, right-click the **Profiles** folder and choose **Create Leaf Profile**.

Step 7 In the **Create Leaf Profile** dialog box, complete the following steps:

a) In the **Name** field, enter a name for the profile.

b) In the **Leaf Selectors** area, click the + icon.

c) In the **Name** field, enter a switch selector name.

d) From the **Blocks** drop-down list, choose a leaf to be associated with a policy group.

e) Click **Update**.

f) Click **Next**.

Step 8 In the **Create Leaf Profile** dialog box, in the **Interface Selector Profiles** area, click the + icon.

Step 9 In the **Create Leaf Interface Profile** dialog box, complete the following steps:

a) In the **Name** field, enter a name for the profile.

b) In the **Interface Selectors** area, click the + icon.

Step 10 In the **Create Access Port Selector** dialog box, complete the following actions:

a) In the **Name** field, enter a selector name.

b) In the **Interface IDs** field, enter a range value.

c) From the **Interface Policy Group** drop-down list, choose **Create VPC Interface Policy Group** from the drop-down list.

Step 11 In the **Create VPC Interface Policy Group** dialog box, complete the following steps:

a) In the **Name** field, enter a name for the policy group.

b) From the **Port Channel Policy** drop-down list, choose **Create Port Channel Policy** from the drop-down list.

Step 12 In the **Create Port Channel Policy** dialog box, complete the following actions:

a) In the **Name** field, enter a name for the policy.

b) In the **Mode** field, choose one of the following options appropriate to your setup:

- **Static Channel - Mode On**

Alternate Procedures for Creating vCenter Domain, Interface, and Switch Profiles

- **LACP Active**
- **LACP Passive**
- **MAC Pinning**
- **MAC Pinning-Physical-load**

Note Do not use MAC pinning with a direct connection to a VPC leaf pair. Instead, use Link Aggregation Control Protocol (LACP) or enhanced LACP to provide redundancy and reliability. Using MAC pinning with a direct connection leads to traffic loss when peer leaf switches are rebooted. Use MAC Pinning only where virtual port channel (VPC) cannot be supported, such as for Cisco UCS Fabric Interconnects with southbound interfaces.

c) Click **Submit**.

Step 13 In the **Create VPC Interface Policy Group** dialog box, complete the following actions:

a) In the **Attached Entity Profile** field, choose **default** from the drop-down list.

You can create a new attachable entity profile to override policy after you create the node policy. You may need to do so if you have intermediate Layer 2 devices between the leaf and ESXi hosts that are running the Cisco ACI Virtual Edge and if you want to use LACP with the top of rack (TOR) switch/leafs on the fabric side but use another policy, such as MAC pinning, on the Cisco ACI Virtual Edge side.

b) Click **Submit**.

Step 14 In the **Create Access Port Selector** dialog box, click **OK**.

Step 15 In the **Create Leaf Interface Profile** dialog box, click **Submit**.

Step 16 In the **Create Leaf Profile** dialog box, complete the following steps:

a) In the **Interface Selector Profiles** area, check the check box for the interface selector profile that you created in Step 9 a.
b) Click **Finish**.

Step 17 To add a second leaf to the VPC, complete the following steps:

a) Repeat Step 1 through Step 10 b; however at Step 7 b, enter the node ID of the other leaf.
b) In the **Create Access Port Selector** dialog box, choose the name of the policy group that you created in Step 11 a.
c) Click **OK**.
d) Repeat Step 15 and Step 16.

Step 18 In the **Policies** navigation pane, expand the **Policies** and **Switch** folders.

Step 19 Right-click **Virtual Port Channel default**, and then choose **Create VPC Explicit Protection Group**.

Step 20 In the **Create VPC Explicit Protection Group** dialog box, enter a name, ID, and switch values for the protection group. Click **Submit** to save the protection group.

Note Each pair of leaf switches has one VPC Explicit Protection Group with a unique ID.

Note The same virtual port channel policy can contain multiple VPC explicit protection groups.

Create FEX Node Interface and Switch Profiles Using the GUI

Note If you have a FEX directly connected to a leaf, see the section "Cisco Fabric Extender" in the Topology appendix of this guide for information about limitations.

Before you begin

In Step 4 d of this procedure, you choose a leaf switch node ID that is connected with the FEX from the drop-down list. It must match the node ID of the leaf switch connected to the ESXi or Layer 2 cloud host. Check the leaf switch node ID in the **Fabric Membership** window by going to **Fabric** > **Inventory** > **Fabric Membership**.

Procedure

Step 1 Log in to the Cisco Application Policy Infrastructure Controller (APIC).

Step 2 Choose **Fabric** > **Access Policies**.

Step 3 In the **Policies** navigation pane, expand the **Switches** and **Leaf Switches** folders.

Step 4 Right-click the **Profiles** folder, and then choose **Create Leaf Profile**.

Step 5 In the **Create Leaf Profile STEP 1 > Profile** dialog box, complete the following steps:

a) In the **Name** field, enter a profile name.
b) In the **Leaf Selectors** field, click the + icon.
c) In the **Name** field, enter a name.
d) In the **Blocks** field, choose a leaf switch node ID that is connected with the FEX from the drop-down list.
e) Click on the **Blocks** drop-down arrow or anywhere on the **Create Switch Profile** dialog box so you can see the **Update** button.
f) Click **Update**.
g) Click **Next**.

Step 6 In the **Create Leaf Profile STEP 2 > Associations** dialog box, in the **Interface Selectors Profiles** area, click the + icon to create a new interface selector profile.

Step 7 In the **Create Leaf Interface Profile** dialog box, complete the following steps:

a) In the **Name** field, enter the vLeaf name.
b) In the **Interface Selectors** area, click the + icon to create a new interface selector.

Step 8 In the **Create Access Port Selector** dialog box, complete the following steps:

a) Enter a name for the selector in the **Name** field .
b) In the **Interface IDs** field, enter the access port interface IDs on the leaf that is connected to the FEX.
c) Check the **Connected To Fex** check box.
d) From the **FEX Profile** drop-down list, choose **Create FEX profile**.

Step 9 In the **Create FEX Profile** dialog box, complete the following steps:

a) In the **Name** field, enter an FEX profile name.
b) In the **FEX Access Interface Selectors** area, click the + icon to specify the FEX access ports.

Alternate Procedures for Creating vCenter Domain, Interface, and Switch Profiles

Step 10 In the **Create Access Port Selector** dialog box, complete the following steps:

a) In the **Name** field, enter a selector name.
b) In the **Interface IDs** area, specify the access ports on the FEX that are connected to the ESXi server hosting the Cisco ACI Virtual Edge.
c) In the **Interface Policy Group** area, choose an option from the drop-down list.

You can choose **Create PC Interface Policy Group**, **Create VPC Interface Policy Group**, or **Create Leaf Access Port Policy Group**.

Step 11 In the dialog box for the option that you chose in Step 10c, complete the following steps:

a) In the **Name** field, enter an access policy group name.
b) In the **Attached Entity Profile** area, choose the appropriate attached entity profile.
c) Click **Submit**.

Step 12 In the **Create Access Port Selector** dialog box, verify that the newly created access port policy group appears in the **Interface Policy Group** area, and then click **OK**.

Step 13 In the **Create FEX Profile** dialog box, verify that the newly created FEX access interface selector profile appears in the **FEX Access Interface Selectors** area, and then click **Submit**.

Step 14 In the **Create Access Port Selector** dialog box, complete the following steps:

a) Verify that the newly created FEX profile appears in the **FEX Profile** area.
b) Enter an ID in the**FEX ID** field.
c) Click **OK**.

Step 15 In the **Create Leaf Interface Profile** dialog box, verify that the leaf-side interface port selector profile is present, and then click **Submit**.

Step 16 In the **Create Leaf Profile STEP 2 > Associations** dialog box, in the **Interface Selector Profiles** area, check the check box for the interface selector profile that you created for the FEX, and then click **Finish**.

What to do next

You should verify that the FEX node policy configuration was successful. However, you need to wait about 10 minutes to give the Cisco APIC time to complete the configuration.

To verify the FEX node policy configuration, complete the following steps in the Cisco APIC GUI:

1. Choose **Fabric** > **Inventory**.
2. In the **Inventory** navigation pane, expand the folder for the pod containing the leaf node for which the FEX node profile was created.
3. Expand the folder for the leaf node.
4. Choose the **Fabric Extenders** folder.
5. In the **Fabric Extenders** work pane, ensure that the FEX is present.

Modify the Interface Policy Group to Override vSwitch-Side Policies

After you create a node policy, you may need to create your own attachable entity profile. This may be necessary if you have intermediate Layer 2 devices between the leaf and ESXi hosts that are running the Cisco ACI Virtual Edge. Such devices include the Cisco Nexus 5000/7000 series switches or blade servers (Unified Computing System [UCS].

The override allows a separate link policy to be configured for the intermediate devices and for the Cisco ACI Virtual Edge host uplinks. For example, if you have UCS Fabric Interconnects connected to ACI, and your Cisco ACI Virtual Edge hosts are running on UCS blades, you may want the UCS Fabric Interconnect uplinks for each FI channeled using Port Channel policy, but the host vNICs for the UCS blades are configured separately using MAC pinning.

Note You may need to choose a vSwitch policy if both of the following are true:

- The ESXi servers hosting vSwitches are connected to the leaf through a Layer 2 switch or blade server.
- The network requires that the interface group policies between the Layer 2 device and the vSwitch hosted by the ESXi server be different from the interface group policies between the Layer 2 switch and leafs. The policies include Port Channel, Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), Spanning Tree Protocol (STP), and Firewall.

Before you begin

- Before you create a custom attachable entity profile, you must create a VMware vCenter domain. See the section Create a VMM Domain Profile for Cisco ACI Virtual Edge , on page 8 in this guide for more information.

  Note When you create a vCenter domain, you must select an attachable entity profile. However, because you do not have one yet, leave the **Attachable Entity Profile** field blank, or choose default. After you create the custom profile, you can associate it with the vCenter domain.

- Ensure that under **Fabric** > **Access Policies** > **Interfaces** > **Leaf Interfaces** > **Profiles**, the desired interface profiles with port selectors have been created. You associate the ports with the override polices later.
- You must have a vSwitch policy configured for your vCenter domain.

Procedure

Step 1 Log in to the Cisco APIC.

Step 2 Choose **Fabric** > **Access Policies**.

Step 3 In the **Policies** navigation pane, expand the **Policies** and **Global** folders, right-click the **Attachable Access Entity Profiles** folder, and then choose **Create Attachable Access Entity Profile**.

Step 4 In the **Create Attachable Access Entity Profile, Step 1 > Profiles** dialog box, complete the following actions:

a) In the **Name** field, enter a name for the profile.
b) Check the **Enable Infrastructure VLAN** check box.
c) Click the **+** icon to expand **Domains**, and add the VMM domain to be associated with the attachable entity profile.
d) Click **Update**.
e) Click **Next**.

Step 5 In the **Create Attachable Access Entity Profile, Step 2> Association to Interfaces** dialog box, choose the interface policy groups that you want to associate with the attachable entity profile.

Note For each interface policy group, you can choose either the **All** or the **Specific** radio button. The **All** radio button associates all the interfaces from that interface policy group with the attachable entity profile. The **Specific** radio button associates specific interfaces from a specific node. If you choose a **Specific** radio button for an interface policy group, you will be asked to specify the switch IDs and Interfaces and then click an **Update** button.

Step 6 Click **Finish**.

Step 7 Go to **Virtual Networking** > **Inventory**

Step 8 In the left navigation pane, expand the **VMM Domains** and **VMware** folders, and then choose the relevant VMM domain.

Step 9 In the work pane, click the **VSwitch Policy** tab.

Step 10 From the appropriate vSwitch policy drop-down list, choose the policy that you want to apply as an override policy.

Step 11 Click **Submit**.

Create a VMM Domain Profile for Cisco ACI Virtual Edge

Before you can install Cisco Application Centric Infrastructure (ACI) Virtual Edge, you must create a VMM domain for it in Cisco Application Policy Infrastructure Controller (APIC).

Note Use this procedure to configure uplinks for the Cisco ACI Virtual Edge endpoint groups. You cannot configure the uplinks when you create the Cisco ACI Virtual Edge VMM domain using the configuration wizard under the **Fabric** tab. However, if you have already created the Cisco ACI Virtual Edge, you can still add uplinks. See the procedure "Edit the VMM Domain and Modify the Uplinks" in the *Cisco ACI Virtualization Guide, Release 4.2(x)*.

Before you begin

- Ensure that the multicast IP address pool has enough multicast IP addresses to accommodate the number of EPGs to be published to the VMware vCenter domain. You can add more IP addresses to a multicast address pool that is already associated with a VMware vCenter domain at any time.

Alternate Procedures for Creating vCenter Domain, Interface, and Switch Profiles

- Ensure that you have enough VLAN IDs. If you do not, ports EPGs might report that no encapsulation is available.
- Ensure that VMware vCenter is installed, configured, and reachable through the in-band/out-of-band management network.
- Ensure that you have the administrator/root credentials to the VMware vCenter.
- Create interface and switch profiles. See the section "Creating Port Channel Switch and Interface Profiles" in this guide for instructions.
- (Optional) Create an attachable entity profile (AEP).

  During the procedure to create a vCenter domain profile, you are asked to choose or create an AEP. If you want to create one ahead of time, follow the procedure "Configuring an Attachable Entity Profile Using the GUI" in the Cisco ACI Virtual Edge Configuration Guide.

Note Enable the infrastructure VLAN within the AEP assigned to the Cisco ACI Virtual Edge VMM domain. Do this regardless of whether you create the AEP before or during VMware vCenter domain profile creation. In the **Create Attachable Access Entity Profile** dialog box, check the **Enable Infrastructure VLAN** check box.

Procedure

Step 1 Log in to Cisco APIC.

Step 2 Go to **Virtual Networking** > **Inventory**.

Step 3 In the Inventory navigation pane, expand **VMM Domains**, right-click **VMware**, and then choose **Create vCenter Domain**.

Step 4 In the **Create vCenter Domain** dialog box, complete the following steps:

a) In the **Virtual Switch Name** field, enter a name.

b) In the **Virtual Switch Area**, choose **Cisco AVE**.

Choosing **Cisco AVE** creates the VMM domain for Cisco ACI Virtual Edge.

Note Perform the following two substeps if you want to use VMware vSphere Proactive HA. Cisco APIC tells VMware vCenter to quarantine a host with a nonworking Cisco ACI Virtual Edge and move the VMs to a host with a working Cisco ACI Virtual Edge. The feature is not available for Cisco ACI Virtual Edge when it is part of Cisco ACI vPod.

You also must enable Proactive HA in VMware vCenter. See the appendix Improving Cisco ACI Virtual Edge Availability with VMware vSphere Proactive HA in this guide.

c) With the **AVE Time Out Time (seconds)** selector, choose the time period to trigger VMware vCenter to quarantine a host with a nonworking Cisco ACI Virtual Edge and move VMs from the host.

You can choose any value between 10 and 300 seconds, inclusive. The default is 30 seconds.

d) Check the **Host Availability Assurance** check box.

Alternate Procedures for Creating vCenter Domain, Interface, and Switch Profiles

Checking the check box creates a VMware Proactive HA object in VMware vCenter. The object enables VMware vCenter to quarantine a host with a nonworking Cisco ACI Virtual Edge and move VMs from the host.

Note Activation of VMware Proactive HA in vCenter is required before a host with nonworking Cisco ACI Virtual Edge can be quarantined.

e) In the **Switching Preference** area, choose **No Local Switching** or **Local Switching**.

For information about switching preferences, see the section What Cisco ACI Virtual Edge Is in the *Overview* chapter of this guide.

Note If you choose **No Local Switching**, you can use only VXLAN encapsulation.

f) If you chose **Local Switching** in Step 4f, in the **Default Encap Mode** area, choose a mode.

You can choose **VLAN mode** or **VXLAN mode**. You can use both encapsulation methods within the same VMM domain. See the section "Mixed-Mode Encapsulation Configuration" in the Cisco ACI Virtual Edge Configuration Guide.

g) From the **Associated Attachable Entity Profile** drop-down list, create or choose a profile that you created earlier.

See "Configuring an Attachable Entity Profile Using the GUI" in the Cisco ACI Virtual Edge Configuration Guide for instructions.

h) From the VLAN Pool drop-down list, choose or create a VLAN pool.

If Cisco ACI Virtual Edge will be deployed in mixed-mode or VLAN mode, create two VLAN pools: one for primary encapsulation and one for private VLAN implementation. The role for the private VLAN pool must be internal. If Cisco ACI Virtual Edge will be deployed in VXLAN mode, only a private VLAN pool is necessary.

i) In the **AVE Fabric-Wide Multicast Address** field, enter an address.

j) From the **Pool of Multicast Addresses (one per-EPG)** drop-down list, choose or create a pool.

k) In the **vCenter Credentials** area, click the **+** (plus) icon, and in the **Create vCenter credential** dialog box, do the following: Enter the VMware vCenter account profile name in the **Name** field, the VMware vCenter username in the **Username** field, enter and confirm the VMware vCenter password, and then click **OK**.

l) In the **vCenter** area, click the **+** (plus) icon, and in the **Create vCenter Controller** dialog box, do the following: Enter the VMware vCenter controller name, the VMware vCenter host name or IP address, the DVS version, data center name (which must match the data center name configured in VMware vCenter), select the credentials created in the previous step, and then click **OK**.

You can choose a DVS version 5.5 or later.

Note You can create multiple vCenter controllers in the same domain. If you want to create more vCenter controllers, repeat this substep for each new vCenter controller.

m) In the **Create vCenter Domain** dialog box, click **Submit**.

In the VMware work pane, you should see the newly created VMM domain, which will be pushed to VMware vCenter.

n) From the **Number of Uplinks** drop-down list, choose the umber of uplinks to the virtual switch uplink port group.

You can choose to associate up to 32 uplinks to the virtual switch uplink port group. This step is optional; if you do not choose a value, eight uplinks are associated with the port group by default. You can name

Alternate Procedures for Creating vCenter Domain, Interface, and Switch Profiles

the uplinks after you finish creating the VMM domain. You can also configure failover for the uplinks when you create or edit the VMM domain association for an EPG.

o) Configure the **Port Channel Mode**, **vSwitch Policy**, and other features as appropriate to your setup.

The port channel policy inside the vSwitch policy should be configured correctly, matching the supported topology requirement.

What to do next

- Add one or more ESXi hosts and their PNICs to the newly created Cisco ACI Virtual Edge DVS using the vSphere Web Client on the VMware vCenter.
- Enable vSphere Proactive HA in VMware vCenter if you have not done so already.
- Rename the uplinks or configure failover for them.

Alternate Procedures for Creating vCenter Domain, Interface, and Switch Profiles