Cisco ACI Virtual Pod Installation Guide, Release 5.1(x)

First Published: 2021-02-24

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

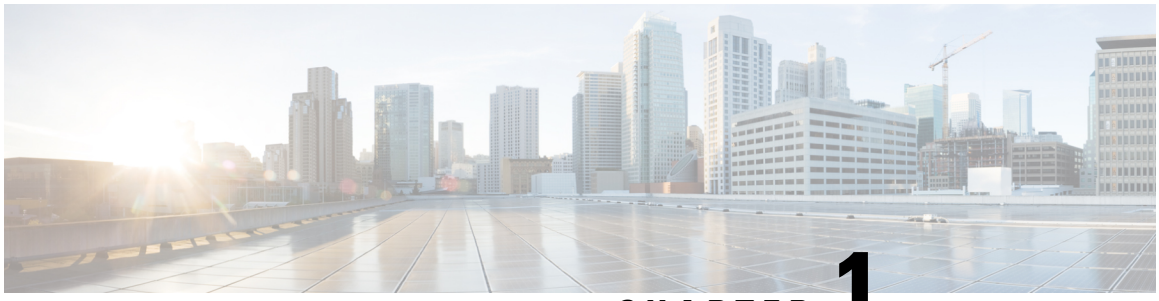
All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.

CONTENTS



CHAPTER 1

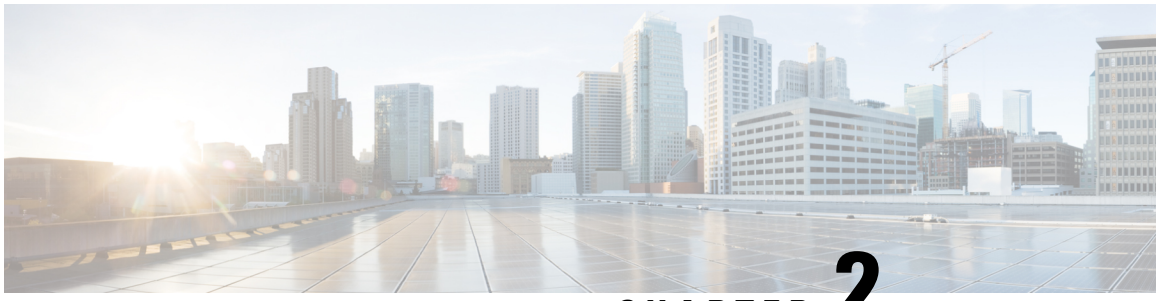
New and Changed

New and Changed Information

The following table provides an overview of the significant changes to this guide up to this current release. The table does not provide an exhaustive list of all changes in the guide or of the new features up to this release.

Table 1: New Features and Changed Behavior in the Cisco ACI Virtual Pod Installation Guide

Cisco APIC Release Version	Feature	Description	Where Documented
5.1(x)	N/A	There is no new installation-related content for Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) in this release.	For information about limitations and bugs, see the *Cisco ACI Virtual Pod Release Notes*.



CHAPTER 2

Cisco ACI vPod Overview

Cisco ACI vPod: Extending the Cisco ACI Fabric

Organizations increasingly adopt hybrid data center models to meet infrastructure demands, flexibility, and reduce costs. They combine various technologies—including virtual private clouds and other internal IT resources—with remote locations. The remote locations can be hosted data centers, satellite data centers, or multicloud environments.

However, hybrid deployments require consistent management and policy for workloads regardless of their location. They also require support for disaster recovery and the ability to migrate workloads between data centers. Meanwhile, they can lack compatible hardware or space to add new equipment.

By deploying Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod), you can overcome these challenges and virtually extend the Cisco ACI fabric into various remote locations.

What Cisco ACI vPod Is

Cisco ACI vPod was introduced with general availability in Cisco APIC Release 4.0(2). It is a software-only solution that you can deploy wherever you have at least two servers on which you can run the VMware ESXi hypervisor. Cisco ACI vPod and its components—a virtual spine (vSpine), virtual leaf (vLeaf), and Cisco ACI Virtual Edge, run on the ESXi hypervisor.

Cisco ACI vPod allows you to use Cisco ACI Virtual Edge where you do not have a physical leaf. You can use up to eight instances of Cisco ACI Virtual Edge in each Cisco ACI vPod in the remote location as you would in your on-premises data center.

Cisco ACI vPod communicates with a physical, on-premises pod or multipod over an interpod network (IPN). You configure the physical pod or multipod, the IPN connection, and Cisco ACI vPod in Cisco Application Policy Infrastructure Controller (APIC). You then use the Cisco ACI vCenter plug-in, a Python script, or PowerCLI to deploy Cisco ACI vPod components.

Benefits of Cisco ACI vPod

Once Cisco ACI vPod is installed, you can use it with Cisco APIC to enforce Cisco ACI fabric policy in the remote location.

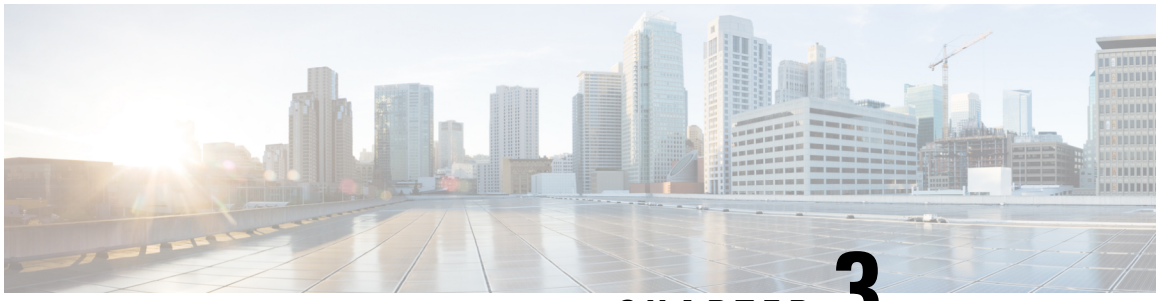
Cisco APIC provides central management of workloads in the on-premises data center and the remote location. It enables you to enforce policy easily and consistently in both on-premises and remote locations.

The flexibility, scalability, and central management of the Cisco ACI vPod solution enable you to take advantage of the following use case scenarios:

- Extension of the Cisco ACI fabric to the bare-metal cloud
- Extension of the Cisco ACI fabric to brownfield deployments
- Extension of the Cisco ACI fabric to colocation data centers
- Migration of workloads from non-Cisco hardware to the Cisco ACI fabric

Where to Find More Information

For general information, see the *Cisco ACI Virtual Pod Release Notes* on Cisco.com.



CHAPTER 3

Cisco ACI vPod Installation

About Cisco ACI vPod Installation

To install Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod), you perform a series of tasks on the Cisco Application Policy Infrastructure Controller (APIC) and in VMware vCenter. You then use one of three methods to deploy Cisco ACI vPod on ESXi hosts:

- Cisco ACI vCenter plug-in
- VMware PowerCLI (for Windows platforms)
- Python script

You need a client to install the Cisco ACI vPod components: the Cisco ACI vPod virtual spine (vSpine) virtual machine (VM), the virtual leaf (vLeaf) VM, and the Cisco Application Centric Infrastructure (ACI) Virtual Edge.

Note Use only the Cisco ACI vCenter plug-in, the VMware Power CLI, or a Python script for installation. Use only the vSphere Web Client to modify vApp properties.

Note When you deploy the Cisco ACI Virtual Edge VM on the ESXi hosts, OpFlex automatically comes online. Do not attach VMkernel ports to the Infra port group.

The following sections provide information about prerequisites and installation methods.

Cisco ACI vPod Installation Workflow

This section provides a high-level description of the tasks that are required to install and deploy Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) in the remote site.

1. Fulfill all prerequisites, which include tasks in the Cisco Application Policy Infrastructure Controller (APIC) and VMware vCenter.

   See the section Prerequisites for Installing Cisco ACI vPod, on page 7 in this guide.

2. Using Cisco Application Policy Infrastructure Controller (APIC), prepare a physical pod in the on-premises data center to communicate with the Cisco ACI vPod in the remote site over an interpod network (IPN). Preparation includes defining a tunnel endpoint (TEP) and Open Shortest Path First (OSPF). Also make sure that the physical pod or all the physical pods in a multipod setup have external TEP pools configured.

   See the section Preparing the Physical Pod IPN Connectivity Using the Cisco APIC GUI, on page 8 in this guide.

3. Using Cisco APIC, create a Cisco ACI Virtual Edge VMM domain.

   See the section "vCenter Domain, Interface, and Switch Profile Creation" in the Installation chapter of the *Cisco ACI Virtual Edge Installation Guide*.

4. Using Cisco APIC, add the Cisco ACI vPod. This task includes defining the virtual spine (vSpine) and virtual leaf (vLeaf) virtual machines (VMs)—one vSpine VM and one vLeaf VM for each node where you will deploy Cisco ACI vPod.

   See the section Adding the Cisco ACI vPod Using the Cisco APIC GUI, on page 14 in this guide.

5. Download the Cisco ACI vPod and Cisco ACI Virtual Edge OVF files from Cisco.com and then upload them to the VMware vCenter content library. The Cisco ACI vPod OVF file contains the vSpine and vLeaf, and Cisco ACI Virtual Edge OVF file contains the Cisco ACI Virtual Edge image.

   See the section Uploading the OVF Files to the VMware vCenter Content Library, on page 19 in this guide.

6. In VMware vCenter, deploy the Cisco ACI vPod vSpine and vLeaf VMs on the ESXi hosts.

   See the section Deploying Cisco ACI vPod VMs on the ESXi Hosts Using the Cisco ACI vCenter Plug-In, on page 20 in this guide. See the chapter "

   See the chapter "Cisco ACI vCenter Plug-in" in the *Cisco ACI Virtualization Guide* for information about installing, using, and upgrading the Cisco ACI vCenter plug-in.

7. Install the Cisco ACI Virtual Edge, making sure to enable it in vPod mode and choose the Cisco ACI vPod that you want it to be part of.

   See the chapter "Cisco ACI Virtual Edge Installation" chapter in the *Cisco ACI Virtual Edge Installation Guide*.

Prerequisites for Installing Cisco ACI vPod

Perform the following tasks before you install Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod):

- Deploy the Cisco ACI fabric on the on-premises data center; this includes setting up Cisco Application Policy Infrastructure Controller (APIC).

  See *Cisco Application Centric Infrastructure Fundamentals*, *Cisco APIC Getting Started Guide* and*Cisco APIC Basic Configuration Guide* on Cisco.com.

- Deploy VMware vCenter on the on-premises data center or the remote site.

  See VMware documentation.

- Install the latest version of the Cisco ACI vCenter Plug-in and connect it to the Cisco ACI fabric.

  See the chapter "Cisco ACI vCenter Plug-in" in the *Cisco ACI Virtualization Guide*.

  Note To use the Cisco ACI vPod management tools (the Cisco ACI vCenter plug-in, the VMware PowerCLI, and Python scripts), use vCenter 6.0 Update 3 or later.

- Configure interpod network (IPN) connectivity between the on-premises data center and the remote site.

  See the section Preparing the Physical Pod IPN Connectivity Using the Cisco APIC GUI, on page 8 in this guide for instructions.

- Configure a subnet and, on the VMware side, a port group for the Cisco ACI vPod elements to communicate.

  You need a subnet, a Layer 3 interface for that subnet, and a VLAN on the IPN to communicate with Cisco ACI vPod.

- On a remote site router, configure a gateway for the Cisco ACI vPod tunnel endpoint (TEP) pool subnet configured with DHCP relay to reach Cisco APIC.

  The DHCP relay should be configured for the Cisco APIC IP addresses obtained from the external tunnel endpoint (TEP) pool (routable subnet). The Cisco APIC IP addresses that are assigned from the external TEP pool can be found on the summary screen that appears after you add the Cisco ACI vPod or by using the REST API query for `infraWiNode MO`.

  If you want to change the gateway IP address, you must perform a clean reboot of the virtual spine (vSpine) and virtual leaf (vLeaf) nodes and reboot all the Cisco ACI Virtual Edge virtual machines (VMs) on the Cisco ACI vPod. See the procedure Changing the Gateway IP Address for Cisco ACI vPod, on page 41 in this guide.

- Configure an out-of-band management network and port group for Cisco ACI vPod components and VMware vCenter on the remote site.

  You can have an external DHCP server or VMware vCenter-based IP address pool to assign management IP addresses for vSpines and vLeafs.

- Configure a management cluster for the vSpine and vLeaf.

Note Requirements are 2 vCPU, 8 GB or RAM, and 100 GB of storage for each vSpine and vLeaf.

Note Cisco ACI vPod management should be in a separate management cluster than any instances of Cisco ACI Virtual Edge.

- Create a new Cisco ACI Virtual Edge VMware vCenter VMM domain.

  You can use an existing Cisco ACI Virtual Edge VMM domain with Cisco ACI vPod. However, if you want to create a new one, we recommend that you do so before you add the Cisco ACI vPod.

  See the section "vCenter Domain, Interface, and Switch Profile Creation" in the *Cisco ACI Virtual Edge Installation Guide* on Cisco.com.

  Note Cisco ACI Virtual Edge requirements are 2 vCPU, 4 GB of RAM, and 24 GB of storage.

Preparing the Physical Pod IPN Connectivity Using the Cisco APIC GUI

The physical spines in the on-premises data center communicate with the Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) virtual spine (vSpines) in the remote site over a Layer 3 interpod network (IPN). Before you create the Cisco ACI vPod on the remote site, you first must ensure that a physical pod can communicate with it.

Cisco ACI vPod requires a configuration similar to a multipod environment for IPN connectivity. Configuration of an external tunnel endpoint (TEP) pool on each physical pod is also required for communication between the physical pod or pods and the Cisco ACI vPod.

If an IPN network is not configured, when you try to add a Cisco ACI vPod, you are prompted to do so in a series of **Configure Interpod Connectivity** panels. However, if an IPN network is configured, you do not see the series of panels and can proceed to adding the Cisco ACI vPod.

If the physical pod or any of the physical pods in a multipod setup lacks an external TEP pool, you will be prompted to create one.

Before you begin

You must have at least one physical pod configured.

Note Only spines of EX or later generations are supported for IPN connectivity with Cisco ACI vPod. Although earlier-generation spines can still exist in the physical pod, they cannot connect to the IPN.

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

Step 2 Choose **Fabric** > **Inventory**.

Step 3 Expand **Quick Start** and click **Add Pod**.

Step 4 In the work pane, click **Add Virtual Pod**.

Step 5 In the **Configure Interpod Connectivity STEP 1 > Overview** panel, review the description of the tasks that are required to configure the IPN, and then click **Get Started**.

Step 6 In the **Configure Interpod Connectivity STEP 2 > IP Connectivity** dialog box, complete the following steps:

a) From the **Spine ID** selector, enter the spine node ID.

You can click the + (plus) icon to add more spines.

b) In the **Interface** field, enter the spine switch interface (port and slot) used to connect to the IPN.

You can click the + (plus) icon to add more interfaces.

c) In the **IPv4 Address** field, enter the IPv4 address and network mask for the interface.

Note If you add more than one interface for the same spine ID in the **Configure Interpod Connectivity STEP 2 > IP Connectivity** dialog box, ensure that the IP addresses assigned to each interface are from different subnets.

d) Using the **MTU (bytes)** selector, choose a value for the maximum transmit unit (MTU) of the external network, or type a value into the field.

The range is 1550 to 9216.

e) Click **Next**.

Step 7 **Configure Interpod Connectivity STEP 3 > Routing Protocols** dialog box, in the **OSPF** area, complete the following steps:

a) Leave the **Use Defaults** checked or uncheck it.

When the **Use Defaults** check box is checked, the GUI conceals the optional fields for configuring Open Shortest Path (OSPF). When it is unchecked, it displays all the fields. The check box is checked by default.

b) In the **Area ID** field, enter the OSPF area ID.

c) In the **Area Type** area, choose an OSPF area type.

You can choose **NSSA area** (the default), **Regular area**, or **Stub area**.

d) (Optional) With the **Area Cost** selector list, choose an appropriate OSPF area cost value.

e) (Optional) With the **Authentication Type** selector, choose the OSPF authentication type.

f) (Optional) In the **Authentication Key** field, enter the OSPF authentication key.

g) (Optional) In the **Confirm Key** area, reenter the OSPF authentication key.

h) From the **Interface Policy** drop-down list, choose or configure an OSPF interface policy.

You can choose an existing policy, or you can create one with the **Create OSPF Interface Policy** dialog box.

Step 8 In the **Configure Interpod Connectivity STEP 3 > Routing Protocols** dialog box, in the **BGP** area, complete the following steps:

a) Leave the **Use Defaults** checked or uncheck it.

When the **Use Defaults** check box is checked, the GUI conceals the fields for configuring Border Gateway Protocol (BGP). When it is unchecked, it displays all the fields. The check box is checked by default.

b) In the **Community** field, enter the community name.

We recommend that you use the default community name. If you use a different name, follow the same format as the default.

c) In the **Peering Type** field, choose either **Full Mesh** or **Route Reflector** for the route peering type.

If you choose **Route Reflector** in the **Peering Type** field and you want to remove the spine switch from the controller in the future, you must disable **Route Reflector** in the *BGP Route Reflector* page before removing the spine switch from the controller. Not doing so results in an error.

To disable a route reflector, right-click on the appropriate route reflector in the **Route Reflector Nodes** area in the **BGP Route Reflector** page and select **Delete**. See the section "Configuring an MP-BGP Route Reflector Using the GUI" in the chapter "MP-BGP Route Reflectors" in the *Cisco APIC Layer 3 Networking Configuration Guide*.

d) In the **Peer Password**, field, enter the BGP peer password.

e) In the **Confirm Password** field, reenter the BGP peer password.

f) In the **External Route Reflector Nodes** area, click the + (plus) icon to add nodes.

For redundancy purposes, more than one spine is configured as a route reflector node: one primary reflector and one secondary reflector.

The **External Route Reflector Nodes** fields appear only if you chose **Route Reflector** as the peering type.

Step 9 Click **Next**.

Step 10 In the **Configure Interpod Connectivity STEP 4 > External TEP** dialog box, complete the following steps:

a) Leave the **Use Defaults** checked or uncheck it.

When the **Use Defaults** check box is checked, the GUI conceals some fields that are automatically configured. When it is unchecked, it displays all the fields, and you can enter different values. The check box is checked by default.

b) Note the non-configurable values in the **Pod** and **Internal TEP Pool** fields.

c) In the **External TEP Pool** field, enter the external TEP pool for the physical pod.

The external TEP pool must not overlap the internal TEP pool or external TEP pools belonging to other pods.

d) In the **Dataplane TEP Pool IP** field, accept the default, which is generated when you configure the **External TEP Pool**, or enter a different address.

If you enter a different address, it must be outside of the external TEP pool.

e) In the **Unicast TEP IP** field, accept the default or enter a different unicast TEP IP address.

If you enter a different unicast TEP IP address, it must be outside of the external TEP pool.

f) In the **Router ID** field, accept the default or enter a different IPN router IP address.

If you enter a different IPN router IP address, it must be outside of the external TEP pool.

g) (Optional) In the **Loopback Address** field, enter the IPN router loopback IP address.

The IPN router loopback IP address must be outside of the external TEP pool.

h) Click **Finish**.
The **Summary** panel appears, displaying details of the IPN configuration. You can also click **View JSON** to view the REST API for the configuration. You can save the REST API for later use.

What to do next

Take one of the following actions:

- Click **Add Virtual Pod** to proceed directly with creating a Cisco ACI vPod. See the procedure Adding the Cisco ACI vPod Using the Cisco APIC GUI, on page 14 in this guide.
- Close **OK** to close the **Summary** panel. You can add the Cisco ACI vPod later, returning to the procedure Adding the Cisco ACI vPod Using the Cisco APIC GUI, on page 14 in this guide.

Preparing the Physical Pod IPN Connectivity Using REST API

The physical spines in the on-premises data center communicate with the Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) virtual spine (vSpines) in the remote site over a Layer 3 interpod network (IPN). Before you create the Cisco ACI vPod on the remote site, you first ensure that a physical pod can communicate with it. You also configure a unique unicast IP address and a routable subnet for each physical pod.

Note The procedures using the Cisco Application Policy Infrastructure Controller (APIC) refer to routable subnets as external tunnel endpoint (TEP) pools.

Step 1 Log in to Cisco APIC:

Example:

```
http://<apic-name/ip>:80/api/aaaLogin.xml

data: <aaaUser name="admin" pwd="password”/>
```

Step 2 Configure the TEP pool:

Example:

```
http://<apic-name/ip>:80/api/policymgr/mo/uni/controller.xml

<fabricSetupPol status=''>
    <fabricSetupP podId="1" tepPool="10.0.0.0/16" />
    <fabricSetupP podId="2" tepPool="10.1.0.0/16" status='' />
</fabricSetupPol>
```

Step 3 Configure the node ID policy:

Example:

```
http://<apic-name/ip>:80/api/node/mo/uni/controller.xml

<fabricNodeIdentPol>
<fabricNodeIdentP serial="XXXXXXXXXXX" name="leaf1" nodeId="101" podId="1"/>
<fabricNodeIdentP serial="XXXXXXXXXXX" name="leaf2" nodeId="102" podId="1"/>
<fabricNodeIdentP serial="XXXXXXXXXXX" name="leaf3" nodeId="103" podId="1"/>
<fabricNodeIdentP serial="XXXXXXXXXXX" name="leaf4" nodeId="104" podId="1"/>
<fabricNodeIdentP serial="XXXXXXXXXXX" name="spine1" nodeId="201" podId="1"/>
<fabricNodeIdentP serial="XXXXXXXXXXX" name="spine3" nodeId="202" podId="1"/>
<fabricNodeIdentP serial="XXXXXXXXXXX" name="leaf5" nodeId="105" podId="2"/>
<fabricNodeIdentP serial="XXXXXXXXXXX" name="leaf6" nodeId="106" podId="2"/>
<fabricNodeIdentP serial="XXXXXXXXXXX" name="spine2" nodeId="203" podId="2"/>
```

```
<fabricNodeIdentP serial="XXXXXXXXXXX" name="spine4" nodeId="204" podId="2"/>
</fabricNodeIdentPol>
```

Step 4 Configure infra L3Out and external connectivity profile:

Example:

```
http://<apic-name/ip>:80/api/node/mo/uni.xml

<polUni>

<fvTenant descr="" dn="uni/tn-infra" name="infra" ownerKey="" ownerTag="">

   <l3extOut descr="" enforceRtctrl="export" name="multipod" ownerKey="" ownerTag=""
targetDscp="unspecified" status=''>
      <ospfExtP areaId='0' areaType='regular' status=''/>
      <bgpExtP status='' />
      <l3extRsEctx tnFvCtxName="overlay-1"/>
      <l3extProvLbl descr="" name="prov_mp1" ownerKey="" ownerTag="" tag="yellow-green"/>

      <l3extLNodeP name="bSpine">
        <l3extRsNodeL3OutAtt rtrId="201.201.201.201" rtrIdLoopBack="no" tDn="topology/pod-1/node-201">

            <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
            <l3extLoopBackIfP addr="201::201/128" descr="" name=""/>
            <l3extLoopBackIfP addr="201.201.201.201/32" descr="" name=""/>
         </l3extRsNodeL3OutAtt>

        <l3extRsNodeL3OutAtt rtrId="202.202.202.202" rtrIdLoopBack="no" tDn="topology/pod-1/node-202">

            <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
            <l3extLoopBackIfP addr="202::202/128" descr="" name=""/>
            <l3extLoopBackIfP addr="202.202.202.202/32" descr="" name=""/>
         </l3extRsNodeL3OutAtt>

        <l3extRsNodeL3OutAtt rtrId="203.203.203.203" rtrIdLoopBack="no" tDn="topology/pod-2/node-203">

            <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
            <l3extLoopBackIfP addr="203::203/128" descr="" name=""/>
            <l3extLoopBackIfP addr="203.203.203.203/32" descr="" name=""/>
         </l3extRsNodeL3OutAtt>

        <l3extRsNodeL3OutAtt rtrId="204.204.204.204" rtrIdLoopBack="no" tDn="topology/pod-2/node-204">

            <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
            <l3extLoopBackIfP addr="204::204/128" descr="" name=""/>
            <l3extLoopBackIfP addr="204.204.204.204/32" descr="" name=""/>
         </l3extRsNodeL3OutAtt>

         <l3extLIfP name='portIf'>
            <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-1/paths-201/pathep-[eth1/1]"
encap='vlan-4'  ifInstT='sub-interface' addr="201.1.1.1/30" />
            <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-1/paths-201/pathep-[eth1/2]"
encap='vlan-4'  ifInstT='sub-interface' addr="201.2.1.1/30" />
            <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-1/paths-202/pathep-[eth1/2]"
encap='vlan-4'  ifInstT='sub-interface' addr="202.1.1.1/30" />
            <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-2/paths-203/pathep-[eth1/1]"
encap='vlan-4'  ifInstT='sub-interface' addr="203.1.1.1/30" />
            <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-2/paths-203/pathep-[eth1/2]"
encap='vlan-4'  ifInstT='sub-interface' addr="203.2.1.1/30" />
            <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-2/paths-204/pathep-[eth4/31]"
encap='vlan-4'  ifInstT='sub-interface' addr="204.1.1.1/30" />

           <ospfIfP>
               <ospfRsIfPol tnOspfIfPolName='ospfIfPol'/>
```

```
            </ospfIfP>

          </l3extLIfP>
       </l3extLNodeP>

       <l3extInstP descr="" matchT="AtleastOne" name="instp1" prio="unspecified"
targetDscp="unspecified">
            <fvRsCustQosPol tnQosCustomPolName=""/>
       </l3extInstP>
    </l3extOut>

   <fvFabricExtConnP descr="" id="1" name="Fabric_Ext_Conn_Pol1" rt="extended:as2-nn4:5:16" status=''>

       <fvPodConnP descr="" id="1" name="">
          <fvIp addr="100.11.1.1/32"/>
       </fvPodConnP>
       <fvPodConnP descr="" id="2" name="">
          <fvIp addr="200.11.1.1/32"/>
       </fvPodConnP>
       <fvPeeringP descr="" name="" ownerKey="" ownerTag="" type="automatic_with_full_mesh"/>
       <l3extFabricExtRoutingP descr="" name="ext_routing_prof_1" ownerKey="" ownerTag="">
          <l3extSubnet aggregate="" descr="" ip="100.0.0.0/8" name="" scope="import-security"/>
          <l3extSubnet aggregate="" descr="" ip="200.0.0.0/8" name="" scope="import-security"/>
          <l3extSubnet aggregate="" descr="" ip="201.1.0.0/16" name="" scope="import-security"/>
          <l3extSubnet aggregate="" descr="" ip="201.2.0.0/16" name="" scope="import-security"/>
          <l3extSubnet aggregate="" descr="" ip="202.1.0.0/16" name="" scope="import-security"/>
          <l3extSubnet aggregate="" descr="" ip="203.1.0.0/16" name="" scope="import-security"/>
          <l3extSubnet aggregate="" descr="" ip="203.2.0.0/16" name="" scope="import-security"/>
          <l3extSubnet aggregate="" descr="" ip="204.1.0.0/16" name="" scope="import-security"/>
       </l3extFabricExtRoutingP>
    </fvFabricExtConnP>
</fvTenant>
</polUni>
```

Step 5 Configure a routable subnet for each physical pod.

Example:

```
URL: https://<controllername>/api/node/mo/uni/controller/setupPol.xml

POST:

<fabricSetupP podId="1">
<fabricExtRoutablePodSubnet pool="197.16.0.0/25"
    reserveAddressCount = 2/>
</fabricSetupP>
```

In the example, `pool` defines the routable subnet or external TEP pool. You can reserve some of the IP addresses from the start of the pool by the `reserveAddressCount`. Cisco APIC does not manage these IP addresses, which you can configure as desired.

Note the following:

- The minimum size of each routable TEP pool is /28, and the maximum size is /22 for each physical pod.
- Addresses from this TEP pool are allocated to border leafs and spines: physical TEP (PTEP) for border leafs and controller-plane TEP (CP-TEP) for spines.
- Each Cisco APIC is allocated one routable IP address.
- One multicast TEP IP address for each site is allocated from the Pod 1 routable subnet.

Step 6 Configure a unique unicast TEP IP address and an IP addressed used as the Border Gateway Protocol (BGP) next hop for each physical pod:

You can configure these addresses from the reserved portion of the external TEP pool (routable subnet).

Example:

```
<fvTenant name="infra">

     <fvFabricExtConnP id="1" rt="extended:as2-nn4:5:16">
     <fvPodConnP id="1">
  <fvIp addr="108.11.1.1/32"/>
     <fvExtRoutableUcastConnP addr="197.16.0.1/32"/>
</fvFabricExtConnP>
</fvTenant>
```

Step 7 Configure a multiprotocol BGP (MP-BGP) route reflector.

Example:

```
https://<apic-name-or-ip>/api/policymgr/mo/uni.xml

<polUni>
  <fabricInst>
    <fabricPodP name="default">
      <fabricPodS name="default" type="ALL">
        <fabricRsPodPGrp tDn="uni/fabric/funcprof/podpgrp-default"/>
      </fabricPodS>
    </fabricPodP>

    <fabricFuncP name="default">
      <fabricPodPGrp name="default">
        <fabricRsPodPGrpBGPRRP tnBgpInstPolName="default"/>
      </fabricPodPGrp>
    </fabricFuncP>

    <bgpInstPol name="default">
      <bgpAsP asn="200"/>
      <bgpRRP>
        <bgpRRNodePEp id="202" status=""/>
      </bgpRRP>
    </bgpInstPol>
  </fabricInst>
</polUni>
```

If you configure a route reflector and want to remove the spine switch from the controller in the future, you must disable **Route Reflector** on the *BGP Route Reflector* Cisco APIC page before removing the spine switch from the controller. Not doing so results in an error.

To disable a route reflector, right-click on the appropriate route reflector in the **Route Reflector Nodes** area in the **BGP Route Reflector** page and select **Delete**. See the section "Configuring an MP-BGP Route Reflector Using the GUI" in the chapter "MP-BGP Route Reflectors" in the *Cisco APIC Layer 3 Networking Configuration Guide*.

Adding the Cisco ACI vPod Using the Cisco APIC GUI

To add a Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod), you define the pod ID and tunnel endpoint (TEP) pool. You also configure the virtual spine (vSpine) and virtual leafs (vLeaf) virtual machines (VMs) on the two required nodes.

Before you begin

- You must have prepared a physical pod in the on-premises data center to communicate with Cisco ACI vPod in the remote site. See Preparing the Physical Pod IPN Connectivity Using the Cisco APIC GUI, on page 8 in this guide.
- We recommend that you create a Cisco Application Centric Infrastructure (ACI) Virtual Edge virtual machine manager (VMM) domain before you create the Cisco ACI vPod.

Note This procedure enables you to create the VMM if you have not done so earlier. Creating a Cisco ACI Virtual Edge VMM domain before you add a Cisco ACI vPod requires more steps than creating the domain in the **Add Virtual Pod** dialog box. However, doing earlier enables you to configure more options. If you create the Cisco ACI Virtual Edge VMM domain here, Cisco APIC creates selectors and attachable entity profiles for the vSpine and vLeaf VMs.

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

Step 2 Take one of the following actions:

- If you completed the previous procedure "Preparing the Physical Pod IPN Connectivity Using the Cisco APIC GUI, on page 8" and have not closed the **Configure Interpod Connectivity** summary panel, skip Step 3 through Step 5, and resume this procedure at Step 6.
- If you have completed the previous "Preparing the Physical Pod IPN Connectivity Using the Cisco APIC GUI, on page 8" procedure and have closed the **Configure Interpod Connectivity** summary panel box, proceed to Step 3 in this procedure.

Step 3 Choose **Fabric** > **Inventory**.

Step 4 Expand **Quick Start** and click **Add Pod**.

Step 5 In the work pane, click **Add Virtual Pod**.

Step 6 In the **Configure Add Virtual STEP 1 > Overview** panel, review the graphics and text that describe the tasks that are required to add the Cisco ACI vPod, and then click **Get Started**.

Step 7 In the **Add Virtual Pod STEP 1 > Virtual Pod** dialog box, in the **Virtual Pod Configuration Area**, complete the following steps:

a) In the **Pod ID** field, choose the Pod ID.

The Pod ID can be any positive integer; however, it must be unique in the Cisco ACI fabric.

b) In the **Pod TEP Pool** field, enter the pool address and subnet.

c) In the **Pool of Reserved IP** field, enter a pool of reserved IP addresses within the pod TEP pool.

The pool consists of IP addresses that are not sent by the DHCP server and which you can reserve for a specific use. The reserved subnet must be at the start or the end of the TEP pool. The subnet must be no larger than a quarter of the TEP pool.

d) In the **Gateway IP Address** field, enter the TEP pool gateway IP address.

e) In the **Dataplane TEP IP** field, accept the automatically generated dataplane TEP IP address or enter a new one.

If you enter a new dataplane TEP IP address, it can be from the reserved subnet but must not conflict with other IPs used in that subnet.

Note If the entered dataplane TEP IP address is not from the Cisco ACI vPod TEP pool, you must configure a route for it on the IPN and the Cisco ACI fabric. Doing so enables them to accept this route. See the appendix Configuring Cisco ACI to Accept More Routes from the IPN, on page 43 in this guide.

Step 8 In the **Add Virtual Pod STEP 1 > Virtual Pod Virtual Leafs** area, use the **vLeaf 1** and **vLeaf 2** selectors to choose the node ID for each of the vLeafs.

Step 9 In the **Virtual Spines** area, complete the following steps:

Note The **Router ID** field is autogenerated.

a) With the **Node ID** selectors, choose the ID for each virtual spine.
b) (Optional) In the **Loopback Address** fields, enter the loopback address for each virtual spine.

Note If the entered router ID and loopback addresses are not from the Cisco ACI vPod TEP pool, you must configure routes for them on the IPN and the Cisco ACI fabric. Doing so enables the IPN and Cisco ACI fabric to accept these routes. See the appendix Configuring Cisco ACI to Accept More Routes from the IPN, on page 43 in this guide.

Step 10 In the **Add Virtual Pod STEP 2 > Virtual Pod BGP** area, leave the **Use Defaults** check box checked or uncheck it to display the fields to configure an optional Border Gateway Protocol (BGP) peer password.

The password is for BGP communication between the vLeaf and vSpine.

a) In the **BGP Password** field, enter the BGP) peer password.
b) In the **Confirmation** field, re-enter the BGP peer password.

Step 11 Click **Next**.

Step 12 In the **Add Virtual Pod STEP 3 > vCenter Domain** dialog box, from the **VMM Domain** drop-down list, complete the following steps:

a) From the **vCenter Domain Name** drop-down list, choose an existing Cisco ACI Virtual Edge vCenter domain or enter the name of a new domain, revealing several configuration fields.
b) In the **AVE VLAN Range** field, enter the encapsulation block range.

The **AVE VLAN Range** is the internal VLAN range that is used for private VLANs (PVLANs).

Cisco APIC creates a VLAN pool with the block that you specify.

c) In the **vCenter Name**, enter the name of the VMware vCenter where you want to create the domain.
d) In the **Datacenter** field, enter the name of the data center where you want to create the domain.
e) In the **vCenter Username** field, enter your VMware vCenter username.
f) In the **vCenter Password** field, enter your VMware vCenter password.
g) In the **Confirm Password** field, reenter your VMware vCenter password.
h) In the **Fabric-Wide Multicast Address** field, enter an address.

The address must be different from the pool of multicast addresses and unique in the Cisco ACI fabric.

i) **Pool of Multicast Addresses (one per EPG)** field, enter a multicast address pool.
j) From the **DVS Version** drop-down list, accept the **vCenter Default** or choose another version.

Step 13 Click **Finish**.

Cisco APIC displays a summary of information about the Cisco ACI vPod and provides a JSON file, which enables you to duplicate the configuration.

Note Be sure to capture the following information that Cisco APIC also displays:

- The administrator passphrase that is required when you deploy Cisco ACI vPod in VMware vCenter.

  The passphrase is good for 60 minutes. If you need more time between adding the Cisco ACI vPod and deploying it, you can capture a new one that Cisco APIC regenerates every 60 minutes. Go to **System** > **System Settings** > **APIC Passphrase**. The work pane displays the passphrase.

- The Cisco APIC external TEP address that is required to configure as the DHCP relay in the IPN.

What to do next

- You can view the vSpine and vLeaf pending node registrations in the Cisco APIC GUI: Go to **Fabric** > **Inventory** > **Fabric Membership** > **Nodes Pending Registration**. The nodes remain in the**Nodes Pending Registration** panel until Cisco ACI vPod is successfully deployed and the discovery process is complete.
- Perform the tasks in the sections Uploading the OVF Files to the VMware vCenter Content Library, on page 19 and Deploying Cisco ACI vPod VMs on the ESXi Hosts Using the Cisco ACI vCenter Plug-In, on page 20 in this guide.

Adding the Cisco ACI vPod Using REST API

To add a Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod), you define the pod ID and tunnel endpoint (TEP) pool. You also configure the virtual spine (vSpine) and virtual leafs (vLeaf) virtual machines (VMs) on the two required nodes.

Before you begin

- You must have prepared a physical pod in the on-premises data center to communicate with Cisco ACI vPod in the remote site. See Preparing the Physical Pod IPN Connectivity Using the Cisco APIC GUI, on page 8 or Preparing the Physical Pod IPN Connectivity Using REST API, on page 11 in this guide.
- We recommend that you create a Cisco Application Centric Infrastructure (ACI) Virtual Edge virtual machine manager (VMM) domain before you create the Cisco ACI vPod.

Step 1 Add the Cisco ACI vPod:

Example:

```
https://<controllername>/api/node/mo/uni/controller/setupPol.xml

<fabricSetupPol>
<fabricSetupP tepPool="196.0.128.0/22" podId="3" podType="virtual">
<fabricSetupAllocP gatewayAddress="196.0.128.1"        reservedAddress="196.0.128.0/27"/>
<fabricAssociatedSetupP pool="20.0.0.0/28" >
<fabricSetupAllocP gatewayAddress="20.0.0.14" reservedAddress="20.0.0.8/29"/>
</fabricAssociatedSetupP>
<fabricPodDhcpServer nodeId="301" serverType="primary”/>
<fabricPodDhcpServer nodeId="303" serverType="secondary”/>
```

```
</fabricSetupP>
</fabricSetupPol>
```

Cisco ACI vPod creation: To create the Cisco ACI vPod, you must post the `fabricSetupP` policy with the primary TEP pool of the pod:

```
<fabricSetupP tepPool="196.0.128.0/22" podId="3" podType="virtual">
```

- IP addresses for virtual leafs (vLeafs) and virtual spines (vSpines) will be allocated from the primary TEP pool.
- The primary TEP pool also can be used for Cisco ACI Virtual Edge and Head-End Replicated (HREP) IP addresses.

The minimum size of each TEP pool subnet is /28, and the maximum size is /22.

Gateway IP address: You must specify the gateway IP address and a subnet for Cisco ACI vPod from start or the end of each reserved TEP pool subnet. The gateway will be programmed automatically (using DHCP) by Cisco Application Policy Infrastructure Controller (APIC) in the vLeaf and vSpine. The reserved part of the subnet is not managed by APIC and typically is used for the gateway, HSRP-related IPs, dataplane TEP, and Router ID.

```
<fabricSetupAllocP gatewayAddress="196.0.128.1" reservedAddress="196.0.128.0/27"/>
```

Secondary TEP pools: You can add secondary TEP pools to the Cisco ACI vPod by posting a `fabricAssociatedSetupP` policy. This optional configuration is used only when you want to configure more than one subnet on the Cisco ACI vPod. Secondary subnets are used only for Cisco ACI Virtual Edge in the Cisco ACI vPod.

```
<fabricAssociatedSetupP pool="20.0.0.0/28" >
<fabricSetupAllocP gatewayAddress="20.0.0.14" reservedAddress="20.0.0.8/29"/>
</fabricAssociatedSetupP>
```

The `gatewayAddress` and `reservedAddress` have the same meaning as for the primary subnet.

DHCP server configuration: You must post a `fabricPodDhcpServer` policy to configure DHCP servers running in primary and secondary modes on vLeafs, for example.

```
<fabricPodDhcpServer nodeId="301" serverType="primary”/>
<fabricPodDhcpServer nodeId="303" serverType="secondary”/>
```

Step 2 Add the IP address for the Border Gateway Protocol (BGP) next hop and the BGP password for the Cisco ACI vPod.

Example:

```
<fvFabricExtConnP descr="" id="1" name="Fabric_Ext_Conn_Pol1" rt="extended:as2-nn4:5:16" status=''>

      <fvPodConnP descr="" id="3">
         <fvIp addr="166.11.1.1/32"/>
         <fvPasswordConfig password="12345"/>
      </fvPodConnP>
</fvFabricExtConnP>
```

Cisco ACI vPod Deployment Using the VMware vCenter

After you fulfill the installation prerequisites, you can use the VMware vCenter to deploy Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod). You use the Cisco ACI vCenter plug-in, which automates the process.

You first upload the Cisco ACI vPod virtual machine (VM) Open Virtualization Format (OVF) file to the VMware vCenter content library. (To get the OVF file, simply extract it from the Cisco ACI vPod Open Virtualization Appliance (OVA) file.)

You also must upload the Cisco Application Centric Infrastructure (ACI) Virtual Edge OVF file to the VMware vCenter content library. You can then deploy the Cisco ACI vPod VMs and the Cisco ACI Virtual Edge VM.

Note After you deploy Cisco ACI vPod, do not remove it from the VMware vCenter inventory and then add it back. Doing so removes all the configuration that you made during deployment. Deploy a new Cisco ACI vPod instead of adding an existing one back to the inventory.

After you deploy Cisco ACI vPod, verify that the interface has a virtual tunnel endpoint (VTEP) address. See the section "Verifying the Cisco ACI vPod Deployment" in this guide.

Uploading the OVF Files to the VMware vCenter Content Library

Before you can deploy the Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) on the ESXi hosts, you upload two Open Virtualization Format (OVF) files to the VMware vCenter Library. They are the Cisco ACI vPod OVF file containing the vSpine and vLeaf, and the Cisco ACI Virtual Edge OVF file containing the Cisco ACI Virtual Edge image.

Note If you use a local data store for content library storage, re-create the content library after you remove a host and then reattach it to the VMware vCenter. Re-creating the content library is necessary because the datastore ID changes after the host is reattached, breaking the association between the content library and the datastore.

Note Complete this procedure twice—once for the Cisco ACI vPod OVF file and once for the Cisco ACI Virtual Edge OVF file.

Before you begin

You must have done the following:

- Downloaded the folder with the Cisco ACI vPod OVF file and the folder with the Cisco ACI Virtual Edge OVF file from Cisco.com to your computer.
- Made sure that the Cisco ACI vPod file and the Cisco ACI Virtual Edge file are compatible with the version of Cisco APIC.
- Created a Cisco ACI Virtual Edge VMM domain on Cisco APIC.
- If you plan to use the Cisco ACI vCenter plug-in to deploy Cisco ACI vPod, ensure that the fabric has been registered with the plug-in.

  See the chapter "Cisco ACI vCenter Plug-in" in the *Cisco ACI Virtualization Guide* for instructions for installing and using the plug-in.

Step 1 Log in to the vSphere Web Client.

Step 2 Choose **Content Libraries**.

You can use an existing content library or create one to receive the upload of the Cisco ACI vPod OVF and Cisco ACI Virtual Edge files. See VMware documentation for instructions.

Step 3 Choose the library and then click **Import item**.

Step 4 In the **Import library item** dialog box, click the **Browse** button.

Step 5 In the pop-up dialog box, choose the OVF file and click **Open**.

Another pop-up dialog box appears, prompting you to choose one or more files in the OVF folder.

Step 6 Choose the VMDK file in the OVF folder.

Step 7 If you chose a Cisco ACI Virtual Edge OVF file in Step 5, also choose the XML file in the OVF folder.

Step 8 Click **OK**.

Once the OVF file is uploaded to the content library, it appears in the work pane under the **Templates** tab.

What to do next

Perform the tasks in the procedure Deploying Cisco ACI vPod VMs on the ESXi Hosts Using the Cisco ACI vCenter Plug-In, on page 20 in this guide.

Deploying Cisco ACI vPod VMs on the ESXi Hosts Using the Cisco ACI vCenter Plug-In

After you upload the Cisco ACI vPod VM OVF file to VMware vCenter, you deploy the Cisco ACI vPod virtual spine (vSpine) and virtual leaf (vLeaf) virtual machines (VM) on the ESXi hosts and the using the Cisco ACI vCenter plug-in.

For information about other deployment methods, see Cisco ACI vPod Deployment Using the PowerCLI, on page 21 or Cisco ACI vPod Deployment Using Python, on page 25 in this guide.

Before you begin

You must have performed the following tasks:

- Uploaded the Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) VM OVF file to VMware vCenter.

  See the section Uploading the OVF Files to the VMware vCenter Content Library, on page 19 in this guide for instructions.

- Configured connectivity between a physical pod and the Cisco ACI vPod.

  See the section Preparing the Physical Pod IPN Connectivity Using the Cisco APIC GUI, on page 8 in this guide for instructions.

- Added a Cisco ACI vPod in Cisco Application Policy Infrastructure Controller (APIC).

  See the section Adding the Cisco ACI vPod Using the Cisco APIC GUI, on page 14 in this guide for instructions.

- Captured an unexpired Cisco APIC passphrase.

The passphrase displays in Cisco APIC after you add the Cisco ACI vPod. The passphrase is good for 60 minutes. If you need more time between adding the Cisco ACI vPod and deploying it, you can capture a new one that Cisco APIC regenerates every 60 minutes. Go to **System** > **System Settings** > **APIC Passphrase**. The work pane displays the passphrase.

Note If you use VMware vCenter 6.0 Web Client, the pop-up window for browsing to the OVF file may not appear. In that case, upload the OVF and virtual machine disk file (VMDK) to the HTTP server. Then use the OVF file URL from the server to download the OVF file to the content library.

Step 1 Log in to the vSphere Web Client.

Step 2 In the **Home** work pane, click the **Cisco ACI Fabric** icon.

In the **Navigator**, click the **Infrastructure** folder, and in the work pane, choose the **vPod** tab.

Step 3 From the **Select a Virtual Pod** drop-down list, choose a Cisco ACI vPod that you created earlier in Cisco APIC. The **vPod Nodes** area lists the nodes that are provisioned on Cisco APIC.

Step 4 In the **Select Hosts** area, choose the two hosts where you want to deploy the Cisco ACI vPod VMs.

Step 5 In the **Select Hosts** area, perform the following steps:

a) From the **Version** drop-down list, choose the Cisco ACI vPod version that you want to deploy.
b) From the **Mgmt** drop-down list, choose the management port group.
c) From the **Infra** drop-down list, choose the infra port group.
d) From the **Datastore** drop-down list, we recommend that you choose a custom data store.

We recommend that you choose a custom data store because you should deploy Cisco ACI vPod vSpine and vLeaf VMs on the host's local storage only.

e) In the **APIC Passphrase** field, enter your Cisco APIC passphrase.

Step 6 Click **Deploy vPod**.
The work pane displays the deployment progress. It may take several minutes for the Cisco ACI vPod to appear as active.

Cisco ACI vPod Deployment Using the PowerCLI

After you fulfill the preinstallation prerequisites, you can use the VMware PowerCLI to install Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod).

You first download the .zip file containing the VMware PowerCLI file, import the Cisco ACI vPod, then deploy the new Cisco ACI vPod VM from the VMware vCenter content library.

Setting Up the PowerCLI Environment

Before you can use the PowerCLI to deploy the Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) or Cisco Application Centric Infrastructure (ACI) Virtual Edge virtual machines (VMs), you import the `CiscoAVE` PowerCLI module and establish a connection to the VMware vCenter.

Before you begin

Make sure that you have PowerCLI 6.0 Release 3 or later.

Step 1 Download the `CiscoAVE` .zip file containing the high-level configuration files for Cisco ACI vPod or Cisco ACI Virtual Edge.

The zip file contains the following:

- `CiscoAVE.psm1`: The `CiscoAVE` VMware Power CLI module file
- `lib/`: The module library

Step 2 Import the `CiscoAVE` PowerCLI module using the **Import-Module** command.

Example:

```
PowerCLI C:\> Import-Module CiscoAVE.psm1
```

Step 3 Connect to the VMware vCenter using the standard PowerCLI commands: **Connect-VIServer** and **Connect-CisServer**.

The **Connect-CisServer** command is required for features such as tagging and managing the VMware vCenter content library.

Example:

```
PowerCLI C:\> Connect-VIServer -Server 172.23.143.235 -User admin -Password lab

Name    Port   User
----    ----   ----
172.23.143.235  443   admin
```

Example:

```
PowerCLI C:\> Connect-CisServer -Server 172.23.143.235 -User admin -Password lab

Name              User             Port
----              ----             ----
172.23.143.235    admin@localos    443
```

Managing the VMware vCenter Content Library Using the VMware PowerCLI

Upload the Open Virtualization Format (OVF) file to the VMware vCenter content library so the scripts in the file to deploy the virtual machines (VMs).

You can use an existing content library or create one. You create a new content library in the VMware vSphere Web Client UI or with the PowerCLI commands in this section.

Step 1 Create a new VMware vCenter content library using the **New-LocalContentLibrary** command.

The following text shows the command syntax:

```
New-LocalContentLibrary [-Name] Object [-Datastore] Object [-Datacenter] Object [CommonParameters]
```

Example:

```
PowerCLI C:\> New-LocalContentLibrary -Name ave-lib -Datastore 129-local -Datacenter mininet
Connecting to vCenter.....................................................[ok]
Creating content library 'ave-lib'........................................[ok]
```

Step 2 Upload an OVF file to the VMware vCenter content library using the **New-ContentLibraryItem** command.

The OVF (or .ova) file must be available on the local machine where you run the command.

The following text shows the command syntax:

```
New-ContentLibraryItem [-Name] Object [-ContentLibrary] Object [-Ovf] Object [CommonParameters]
```

Example:

```
PowerCLI C:\> New-ContentLibraryItem -Name vpod-ova -ContentLibrary ave-lib -Ovf
L:\ova\aci-vpod.14.0.0.84.ova
Connecting to vCenter.....................................................[ok]
Extracting OVA............................................................[ok]
Validating................................................................[ok]
Uploading aci-vpod.14.0.0.84-disk1.vmdk...................................[ok]
Uploading aci-vpod.14.0.0.84.ovf..........................................[ok]
Finishing up..............................................................[ok]
```

Step 3 Remove an item from the VMware vCenter content library using the **Remove-LocalContentLibraryItem** command:

The following text shows the command syntax:

```
Remove-LocalContentLibraryItem [-Name] Object [-ContentLibrary] Object [CommonParameters]
```

Example:

```
PowerCLI C:\> Remove-LocalContentLibraryItem -Name vpod-14.0.0.84 -ContentLibrary vpod-ova
Connecting to vCenter.....................................................[ok]
Deleting content library item 'vpod-14.0.0.84'............................[ok]
```

Deploying Cisco ACI vPod Using the VMware PowerCLI

Use the VMware PowerCLI to deploy a pair of virtual spine (vSpine) and virtual leaf (vLeaf) virtual machines (VMs) on given hosts. You can also get a list of deployed Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) VMs.

Before you begin

You must have done the following:

- Uploaded the Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) Open Virtualization Format (OVF) to the VMware vCenter content library.

  See the section Uploading the OVF Files to the VMware vCenter Content Library, on page 19 in this guide for instructions.

- Configured connectivity between a physical pod and the Cisco ACI vPod.

  See the section Preparing the Physical Pod IPN Connectivity Using the Cisco APIC GUI, on page 8 in this guide for instructions.

- Added a Cisco ACI vPod in Cisco Application Policy Infrastructure Controller (APIC).

  See the section Adding the Cisco ACI vPod Using the Cisco APIC GUI, on page 14 in this guide for instructions.

- Captured an unexpired Cisco APIC passphrase.

The passphrase displays in Cisco APIC after you add the Cisco ACI vPod. The passphrase is good for 60 minutes. If you need more time between adding the Cisco ACI vPod and deploying it, you can capture a new one that Cisco APIC regenerates every 60 minutes. Go to **System** > **System Settings** > **APIC Passphrase**. The work pane displays the passphrase.

- Captured all the vLeaf and vSpine serial numbers from the Cisco ACI vPod created on Cisco APIC.

Step 1 Deploy the vSpine and vLeaf VMs using the **New-VPodVM** command.

Run the command twice, each time on a different host, to deploy one pair of vSpine and vLeaf VMs on each host.

The following text shows the command syntax:

```
New-VPodVM [-HostName] Object [-MgmtPortgroupName] Object [-InfraPortgroupName] Object [-AuthMode]
Object [-AuthKey] SecureString
[-OvfItem] Object [-VpodId] Object [[-VspineSerial] String] [[-VleafSerial] String] [[-Library]
String] [[-DatastoreName]
String] [[-VspineIp] String] [[-VspineNetmask] String] [[-VspineGateway] String] [[-VspineNameserver]
 String] [[-VleafIp]
String] [[-VleafNetmask] String] [[-VleafGateway] String] [[-VleafNameserve r] String]
[CommonParameters]
```

Example:

Note For details about each individual parameter, enter the command **Get-Help New-VPodVM -detailed** and review the output.

```
PowerCLI C:\> $pass = Read-Host -AsSecureString
********
PowerCLI C:\> PowerCLI C:\> New-VPodVM -HostName 172.23.143.129 -MgmtPortgroupName "my-vds/mgmt-pg"
 -InfraPortgroupName "vpod-infra" -DatastoreName 129-local -AuthKey $pass -OvfItem vpod-ova -VPodId
 2 -VspineSerial SPINE201-SWJI -VleafSerial LEAF203-VIWE
Connecting to vCenter.....................................................[ok]
Validating configuration..................................................[ok]
Deploying vSpine & vLeaf (this might take several minutes).............[ok]
Performing configuration..................................................[ok]
Powering On VM 'cisco-vPod2-spine1'.....................................[ok]
Powering On VM 'cisco-vPod2-leaf1'.....................................[ok]
```

Step 2 Get a list of deployed Cisco ACI vPod VMs using the **Get-VPodVM** command.

The following text shows the command syntax:

```
Get-VPodVM [CommonParameters]
```

Example:

```
PowerCLI C:\> Get-VpodVM | Format-Table
VirtualMachine   role  serial   pod  HostName   ManagementIp
--------------   ----  ------   --- --------   ------------
cisco-vPod2-leaf1  leaf  VLEAF1-2-OBQ9L  2 172.23.143.129  172.23.143.156
cisco-vPod2-spine1  spine VSPINE1-2-I9IYL  2 172.23.143.129  172.23.143.159
```

Note To use a static IP address for the management IP address of the VM, use the `-VSpineIp` and `-VleafIp` parameters. For example:

```
-VSpineIp 172.23.150.100 -VSpineNetmask 255.255.255.0 -VSpineGateway 172.23.150.254 -VLeafIp
 172.23.150.101 -VLeafNetmask 255.255.255.0 -VLeafGateway 172.23.150.254
```

Cisco ACI vPod Deployment Using Python

After you fulfill the preinstallation prerequisites, you can use Python to install Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod)

You first download the zip file containing the Python files, set up the environment to run Python, and then use Python commands to create a content library on VMware vCenter, upload the Cisco ACI vPod virtual machine (VM) Open Virtualization Format (OVF) file to the VMware vCenter content library, and then deploy the new VMs from the content library.

Setting Up the Python Environment

Set up the Python environment so you can use Python to install Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) or Cisco Application Centric Infrastructure (ACI) Virtual Edge.

Note We strongly recommend that you use a virtual environment to avoid any Python dependency problems.

Before you begin

You must have done the following:

- Made sure that you have Python 2.7.9 or a later version.
- Made sure that you have VMware vCenter 6.0 GA U3 or later.
- Made sure that you have Git and PIP installed.

Step 1 Download the .zip file containing the high-level Python configuration scripts for deploying Cisco ACI vPod and Cisco ACI Virtual Edge.

The .zip file contains the following:

- `get-avevm.py`: Gets the list of Cisco ACI Virtual Edge virtual machines (VMs) currently deployed.
- `new-avevm.py`: Deploy a new Cisco ACI Virtual Edge VM.
- `remove-avevm.py`: Removes a Cisco ACI Virtual Edge VM.
- `content-library.py`: Interact with the VMware vCenter content library.
- `get-vpodvm.py`: Get a list of Cisco ACI vPod VMs currently deployed.
- `new-vpodvm.py`: Deploy a new pair (one virtual spine [vSpine] and one virtual leaf [vLeaf]) of Cisco ACI vPod VMs.
- `remove-vpodvm.py`: Remove all Cisco ACI vPod VMs.
- `requirements.txt`: Python dependencies list used by the PIP package management system.

Step 2 (Optional but recommended) Set up a Python virtual environment.

a) Enter the following commands:

Example:

```
$ pip install virtualenv
$ virtualenv venv
```

b) Enter one of the following commands:

- If you have a Linux or Macintosh system, enter the following command:

```
$ . venv/bin/activate
```

- If you have a Windows system, enter the following command:

```
> ven\Scripts\activate
```

Step 3 Install the VMware vSphere Automation software development kit (SDK).

a) Download the VMware vSphere Automation SDK from GitHub; there is currently no up-to-date version in the Python Package Index (PyPi).

Example:

```
(venv) $ git clone https://github.com/vmware/vsphere-automation-sdk-python.git
(venv) $ cd vsphere-automation-sdk-python

Linux:

(venv) $ pip install --upgrade -r requirements.txt --extra-index-url file://`pwd`/lib

Windows:

> pip install --upgrade --force-reinstall -r requirements.txt --extra-index-url
file:///absolute_dir_to_sdk/lib
```

Step 4 Install all other dependencies.

Example:

```
(venv) $ cd ../
(venv) $ pip install -r requirements.txt
```

The `requirements.txt` file contains all the dependencies that the script relies on. Installing the dependencies in this file is a one-time task.

Managing the VMware vCenter Content Library Using Python

You upload the Open Virtualization Format (OVF) file to the VMware vCenter content library so the scripts in the file can deploy the virtual machines (VMs).

You can use an existing library or create a new one. You create a new content library in the VMware vSphere Web Client UI or with the Python commands in this section.

Step 1 Create a new content library using the subcommand `Create`.

The following text shows the command usage:

```
usage: content-library.py [-h] --vcenter VCENTER --vc-username VC_USERNAME
[--vc-password VC_PASSWORD] [--silent] Create --name NAME --datacenter DATACENTER
--datastore DATASTORE
```

Example:

```
(venv) $ python content-library.py --vcenter 172.23.143.235 --vc-username admin --vcpassword
lab Create --name ave_repo --datacenter mininet --datastore 129-local
Connecting to vCenter.....................................................[ok]
Creating content library 'ave_repo'.....................................[ok]
```

Step 2 Copy the `ave vmdk` file to the datastore of any of the host in the VMware vCenter.

Example:

```
scp cisco-ave-2.1.1.321-disk1.vmdk root@10.23.238.203:/vmfs/volumes/datastore2/
```

Step 3 Upload the OVF file to the VMware vCenter content library using the subcommand **Upload**.

The OVF file must be available on the local machine where you run the Python script. Provide the full datastore path of the copied `vmdk` file in `–vmdk-ds-path`.

The following text shows the command usage:

```
usage: content-library.py [-h] --vcenter VCENTER --vc-username VC_USERNAME
[--vc-password VC_PASSWORD] [--silent] Upload --library LIBRARY --item ITEM --path PATH
[--vmdk-ds-path VMDK_DS_PATH]
```

Example:

```
(venv) $ python content-library.py --vcHost 10.23.219.150 --vcUser 'administrator' --vcPwd 'lab'
Upload --library repo --item cisco-ave-2.1.1.321.ovf --path /Users/User/dev/ovf/cisco-ave-2.1.1.321.ovf
 --vmdk-ds-path ds:///vmfs/volumes/59348426-b1a50255-8787-cc167ee18b76/cisco-ave-2.1.1.321-disk1.vmdk
Connecting to vCenter.....................................................[ok]
Extracting OVA............................................................[ok]
Validating................................................................[ok]
Uploading aci-vpod.14.0.0.84-disk1.vmdk...................................[ok]
Uploading aci-vpod.14.0.0.84.ovf..........................................[ok]
Finishing up..............................................................[ok]
```

Step 4 Remove an item from the content library using the subcommand **Remove**.

The following text shows the command usage:

```
usage: content-library.py [-h] --vcenter VCENTER --vc-username VC_USERNAME
[--vc-password VC_PASSWORD] [--silent] Remove --library LIBRARY --item ITEM
```

Example:

```
(venv) $ python content-library.py --vcenter 172.23.143.235 --vc-username admin --vcpassword
lab Remove --library repo --item vpod-14.0.0.84
Connecting to vCenter.....................................................[ok]
Deleting content library item 'vpod-14.0.0.84'.....................[ok]
```

Deploying Cisco ACI vPod VMs Using Python

Use Python to deploy a pair of virtual spine (vSpine) and virtual leaf (vLeaf) virtual machines (VMs) on given hosts. You can also get a list of deployed Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) VMs.

Note Enter the Python command twice to deploy two pairs of virtual spine (vSpine) and virtual leaf (vLeaf) virtual machines (VMs). Choose a different host each time you enter the command to deploy the vSpine and vLeaf pairs on different hosts.

Before you begin

You must have done the following:

- Uploaded the Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) Open Virtualization Format (OVF) to the VMware vCenter content library.

  See the section Uploading the OVF Files to the VMware vCenter Content Library, on page 19 in this guide for instructions.

- Configured connectivity between a physical pod and the Cisco ACI vPod.

  See the section Preparing the Physical Pod IPN Connectivity Using the Cisco APIC GUI, on page 8 in this guide for instructions.

- Created a Cisco ACI vPod in Cisco Application Policy Infrastructure Controller (APIC).

  See the section Adding the Cisco ACI vPod Using the Cisco APIC GUI, on page 14 in this guide for instructions.

- Captured an unexpired Cisco APIC passphrase.

  The passphrase displays in Cisco APIC after you add the Cisco ACI vPod. The passphrase is good for 60 minutes. If you need more time between adding the Cisco ACI vPod and deploying it, you can capture a new one that Cisco APIC regenerates every 60 minutes. Go to **System** > **System Settings** > **APIC Passphrase**. The work pane displays the passphrase, and you can click the refresh icon to ensure that you get a newly generated one.

- Captured all the vLeaf and vSpine serial numbers from the Cisco ACI vPod created on Cisco APIC.

Step 1 Deploy the vSpine and vLeaf VMs using the Python script `new-vpodvm.py`.

The following text shows the script usage:

```
usage: new-vpodvm.py [-h] [--silent] --vcenter VCENTER --vc-username
VC_USERNAME [--vc-password VC_PASSWORD] --host-name
HOST_NAME --mgmt-pg MGMT_PG --infra-pg INFRA_PG
--ovf-item OVF_ITEM --vpod-id VPOD_ID
[--auth-key AUTH_KEY] [--vspine-serial VSPINE_SERIAL]
[--vleaf-serial VLEAF_SERIAL] [--library LIBRARY]
[--datastore DATASTORE] [--vspine-ip VSPINE_IP]
[--vspine-netmask VSPINE_NETMASK]
[--vspine-gateway VSPINE_GATEWAY]
[--vspine-nameserver VSPINE_NAMESERVER]
[--vleaf-ip VLEAF_IP] [--vleaf-netmask VLEAF_NETMASK]
[--vleaf-gateway VLEAF_GATEWAY]
[--vleaf-nameserver VLEAF_NAMESERVER]
```

Example:

Note For details about each individual parameter, enter the command **python new-vpodvm.py -h** and review the output.

```
(venv) $ python new-vpodvm.py --vcenter 172.23.143.235 --vc-username admin --vc-password lab --host-name
 172.23.143.129 --mgmt-pg 'my-vds/mgmt-pg' --infra-pg 'vpod-infra' --ovf-item vpod-ova --vpod-id 2
--datastore 129-local --auth-key 3NWG4NDP4DESTZL2 --vspine-serial 'SPINE201-SWJI' --vleaf-serial
'LEAF203-VIWE'

Connecting to vCenter.....................................................[ok]
Validating configuration..................................................[ok]
Deploying vSpine & vLeaf (this might take several minutes).............[ok]
Performing configuration..................................................[ok]
Powering On VM 'cisco-vPod2-spine1'.....................................[ok]
Powering On VM 'cisco-vPod2-leaf1'......................................[ok]
```

Step 2 Get a list of deployed Cisco ACI vPod VMs using the `get-vpodvm.py` script.

The following text shows the script usage:

```
usage: get-vpodvm.py [-h] [--silent] --vcenter VCENTER --vc-username
VC_USERNAME [--vc-password VC_PASSWORD]
```

Example:

```
(venv) $ python get-vpodvm.py --vcenter 172.23.143.235 --vc-username admin --vc-password lab

+--------------------+----------------+-----+-------+--------------+----------------
-+
| Virtual Machine | Host | POD | Role | Management IP | Serial Number
|
+--------------------+----------------+-----+-------+--------------+----------------
-+
| cisco-vPod2-leaf1 | 172.23.143.129 | 2 | leaf | None | VLEAF1-2-G9DPB
|
| cisco-vPod2-spine1 | 172.23.143.129 | 2 | spine | None | VSPINE1-2-8BH4M
|
+--------------------+----------------+-----+-------+--------------+----------------
```

Note To use a static IP management IP address, use the `--vspine-ip` and `--vleaf-ip` parameters. Example:

```
--vspine-ip 172.23.150.100 --vspine-netmask 255.255.255.0 --vspine-gateway 172.23.150.254
--vleaf-ip 172.23.150.101 --vleaf-netmask 255.255.255.0 --vleaf-gateway 172.23.150.254
```

Verifying the Cisco ACI vPod Deployment

After you deploy Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod), verify the deployment by ensuring that the interface that is used to communicate with Cisco ACI Virtual Edge (kni0) has a virtual tunnel endpoint (VTEP) IP address.

Before you begin

You must have added a Cisco ACI vPod in Cisco Application Policy Infrastructure Controller (APIC) and deployed the Cisco ACI vPod VMs in VMware vCenter.

Run the **ifconfig** command and examine the output:

The example shows the output for a virtual leaf (vLeaf), which would be eth1-49. A virtual spine (vSpine) would be eth5-1.

Example:

```
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.9.3  netmask 255.255.252.0  broadcast 192.168.11.255
        inet6 fe80::250:56ff:fea7:fac  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:a7:0f:ac  txqueuelen 1000  (Ethernet)
        RX packets 374443  bytes 52541802 (50.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 161054  bytes 20000611 (19.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

What to do next

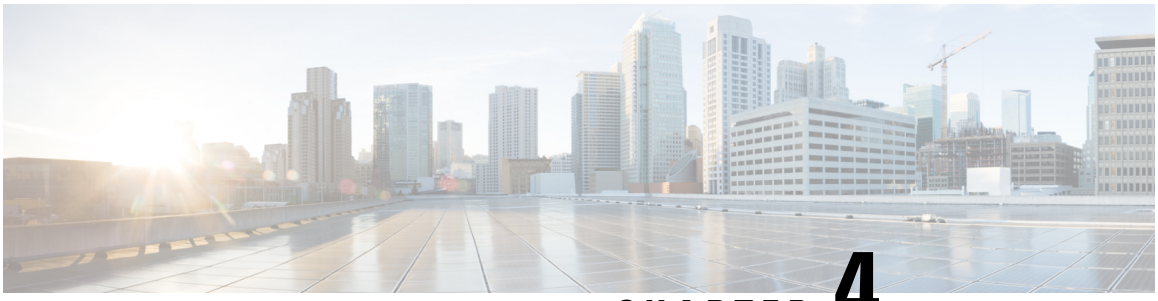
Read the Key Post-Installation Configuration Tasks, on page 31 in this guide.

Cisco ACI Virtual Edge Installation

After you create the Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) and deploy its virtual machines (VMs), you install Cisco Application Centric Infrastructure (ACI) Virtual Edge and set it to work with the Cisco ACI vPod.

Follow the instructions in the installation chapter of the *Cisco ACI Virtual Edge Installation Guide*, making sure that you fulfill the prerequisites and follow the guidelines. When you deploy the Cisco ACI Virtual Edge VMs, set the Cisco ACI Virtual Edge to cloud mode and choose the Cisco ACI vPod that you want it to become part of.

Note When you deploy the Cisco ACI Virtual Edge VM on the ESXi host, OpFlex immediately comes online. Do not attach VMkernel ports to the Infra port group.



CHAPTER 4

Key Post-Installation Configuration Tasks

Key Cisco ACI vPod Post-Installation Configuration Tasks

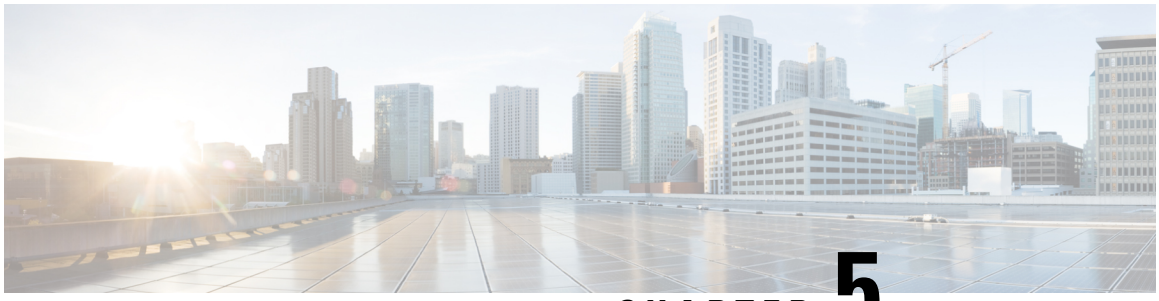
After you install Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod), it becomes a virtual fabric in the remote location. You can use each Cisco Application Centric Infrastructure (ACI) Virtual Edge that it contains as you would use Cisco ACI Virtual Edge in the on-premises data center.

However, before you do so, you first perform the following key configuration tasks for each Cisco ACI Virtual Edge in the Cisco ACI Virtual Pod:

- Deploy an application profile, which includes creating a tenant, application profile, endpoint groups (EPGs), filters, and contracts, and assigning port groups to VMs. Then verify the application profile.
- If you want to use Distributed Firewall, Enable it after installation. See the chapter "Distributed Firewall" in the Cisco ACI Virtual Edge Configuration Guide for instructions.
- Configure Network Time Protocol (NTP) on the Cisco ACI vPod virtual leafs (vLeafs).

  See the section "Time Synchronization and NTP" in the *Cisco APIC Basic Configuration Guide* on Cisco.com.

Note When you use Cisco ACI Virtual Edge as part of Cisco ACI Virtual Pod, it has most of the same functionality as it does when it is not part of Cisco ACI Virtual Pod. See the *Cisco ACI Virtual Pod Release Notes* for more information.



CHAPTER 5

Cisco ACI vPod Upgrade

Cisco ACI vPod Updgrade

You use the Cisco Application Policy Infrastructure Controller (APIC) GUI to upgrade the software on Cisco ACI Virtual Pod (vPod). The upgrade is done in two stages: You first download the new version of Cisco ACI vPod firmware ISO to Cisco APIC and then upgrade the Cisco ACI vPod virtual spines and virtual leafs.

Prerequisites for Upgrading Cisco ACI vPod

1. Download the ISO version of the Cisco ACI vPod firmware that you want to upgrade to; you can download it to a local machine or a remote server.
2. Note the location of the downloaded ISO file.

Guidelines for Upgrading Cisco ACI vPod

You may want to upgrade Cisco APIC one virtual leaf and virtual spine pair at a time to prevent traffic disruption.

Importing the Cisco ACI vPod Firmware ISO Image

You import the Cisco ACI vPod ISO firmware image so you can update the Cisco ACI vPod virtual spines and leafs.

Before you begin

You must have downloaded the Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) firmware ISO image from Cisco.com to a local machine or remote server.

Step 1 Log in to Cisco APIC.

Step 2 On the menu bar, choose **Admin** > **Firmware**.

Step 3 Click the **Images** tab, then click the **Tools** icon and choose **Add Firmware to APIC** from the drop-down menu.

The **Add Firmware to APIC.** dialog box appears; perform the following steps in the dialog box.

Step 4 In the **Firmware Image Location** field, complete one of the following series of steps:

Option	Description
If you want to import the Cisco ACI vPod ISO firmware image...	Then...
From your local machine	**a.** Click **Local**. . **b.** Click **Browse**, navigate to the folder on your local system with the Cisco ACI vPod ISO firmware image that you want to import. **c.** Click **Submit**. **d.** Go to the section Upgrading the Cisco ACI vPod Virtual Leafs and Spines, on page 35 in this guide.
From a remote server	**a.** Click **Remote**. **b.** Continue with the following steps.

a) Click **Submit**.

Wait for the Cisco ACI vPod ISO firmware image to download.

Step 5 In the **Download Name** field, choose an existing download from the drop-down menu or enter a name for the Cisco ACI vPod ISO firmware image file to create a new download (for example, *vpod_image*).

Step 6 In the **Protocol** field, click either the **HTTP** or the **Secure copy** radio button.

The following fields appear if you are creating a new download.

Step 7 In the **URL** field, enter the URL from where the image will be downloaded.

Option	Description
In the previous step, if you chose...	Then...
HTTP	**a.** Enter the HTTP source that you want to use to download the software image. For example, `10.67.82.87:/home/username/ACI/aci-vpod-dk9.14.2.0.73.iso`. **b.** Click **Submit**. **c.** Go to the section Upgrading the Cisco ACI vPod Virtual Leafs and Spines, on page 35 in this guide.
Secure copy	**a.** Enter the Secure Copy Protocol (SCP) source that you want to use to download the software image, using the format `SCP server:/path`. For example, `10.67.82.87:/home/username/ACI/aci-vpod-dk9.14.2.0.73.iso`.

Option	Description
	b. Continue with the following steps.

Step 8 In the **Username** field, enter your username for secure copy.

Step 9 In the **Authentication Type** field, choose the type of authentication for the download:

Option	Description
If you want to...	Then...
Authenticate with a password	**a.** Choose **Use Password**. **b.** In the Password field, enter your password for secure copy. **c.** Click **Submit**. **d.** Go to the section Upgrading the Cisco ACI vPod Virtual Leafs and Spines, on page 35 in this guide.
Authenticate with an SSH public or private key	**a.** Choose **Use SSH Public/Private Key Files**. **b.** Enter the SSH key information in the **SSH Key Contents** field; the **SSH Key Passphrase** can remain empty. **c.** Click **Submit**.

What to do next

Check the progress of the image import:

1. Go to **Admin** > **Firmware** > **Images**.
2. In the **Firmware** central pane, view the **Status** of the image you imported.

   If the image has not finished downloading, you can check progress the **Download Percent(%)** column.

Upgrading the Cisco ACI vPod Virtual Leafs and Spines

After you import the Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) firmware ISO image, you update the virtual spines and switches.

Before you begin

You must have imported the new Cisco ACI vPod firmware ISO image. See the section Importing the Cisco ACI vPod Firmware ISO Image, on page 33 in this guide.

Step 1 Log in to Cisco APIC.

Step 2 On the menu bar, choose **Admin** > **Firmware**.

Step 3 Click the **Infrastructure** tab, and then click the **Nodes** sub-tab.
The **Firmware** central pane lists all the pods by name, function, model, current firmware, upgrade group, and status.

Step 4 Click the tools icon and choose **Schedule Node Upgrade**.

Step 5 In the **Schedule Node Upgrade** dialog box, perform the following steps:

a) In the **Group Type** field, choose **Switch** or **vPpod**.

b) In the **Upgrade Group Name** field, choose an existing upgrade group from the drop-down menu, or click the **x** in the corner of the field to clear the field, and then enter a name for the upgrade group.

Note If you select an existing POD maintenance group, fields that are associated with that maintenance group are automatically filled in.

c) From the **Target Firmware Version** drop-down list, choose the desired image version to which you want to upgrade the switches.

d) Check the **Ignore Compatibility Check** check box.

e) Check the **Graceful Maintenance** check box to change the node to the Graceful Insertion and Removal (GIR) mode before performing the upgrade.

f) In the **Run Mode** field, choose the run mode to proceed automatically to the next set of nodes once the set of nodes has gone through the maintenance process successfully.

The options are:

- **Do not pause on failure and do not wait on cluster health**
- **Pause only Upon Upgrade Failure**

The default is **Pause only Upon Upgrade Failure**.

g) In the **Upgrade Start Time** field, select **Now** or **Schedule for Later**.

If you select **Schedule for Later**, select the trigger value using the Scheduler scroll-down menu.

h) In the **Node Selection** field,choose **Range** or **Manual**.

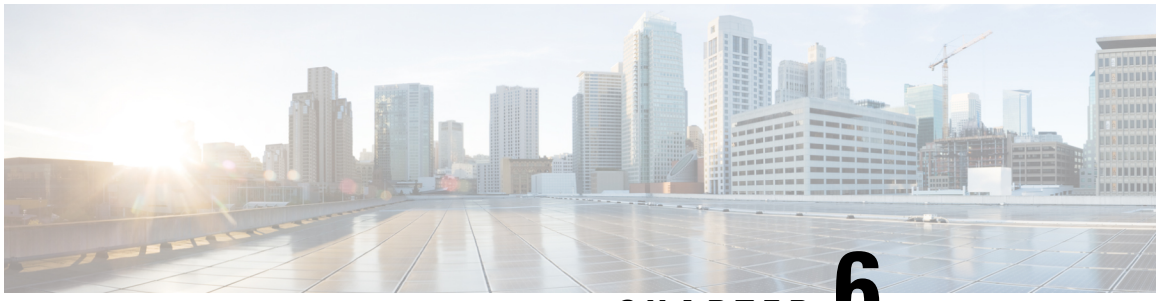
- If you select **Range**, enter the range in the **Group Node Ids** field.
- If you choose **Manual**, a list of available leaf switches and spine switches appears in the **All Nodes** area. Choose the nodes that you want to include in this upgrade.

i) In the **Group Node IDs** field, enter the ID numbers of the nodes that you want to upgrade.

j) Click **Submit**.

What to do next

1. Check the progress of the upgrade by going to **Admin** > **Firmware** > **Infrastructure** > **Nodes** and viewing the percentage in the **Upgrade Progress** column.
2. (Optional) Repeat this procedure to upgrade other nodes.



CHAPTER 6

Cisco ACI vPod Uninstallation

About Cisco ACI vPod Uninstallation

You might need to remove Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) for testing or if you need to remove all configuration from the Cisco ACI fabric, resetting the fabric to its initial state.

You can uninstall Cisco ACI vPod using the Cisco ACI vCenter Plug-in, the VMware PowerCLI, or a Python script.

Note To use the Cisco ACI vPod management tools (the ACI vCenter Plug-in, the VMware PowerCLI, and Python scripts), we recommend that you use vCenter 6.0 Update 3 or later.

You also need to remove any external tunnel endpoint (TEP) pools.

Uninstalling Cisco ACI vPod Using the Cisco ACI vCenter Plug-in

Before you begin

Remove all the Cisco Application Centric Infrastructure (ACI) Virtual Edge virtual machines (VMs) from the hosts. Any Cisco ACI Virtual Edge VMs associated with the Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) stop working when the Cisco ACI vPod is uninstalled.

Step 1 Log in to the VMware vSphere Web Client.

Step 2 In the Navigator, choose **Cisco ACI Fabric** > **Infrastructure**.

Step 3 In the work pane, choose **vPod**, and then from the **Select a Virtual Pod** drop-down list, choose the Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) that you want to uninstall.

Step 4 Click **Remove POD**, and in the **Uninstall vPOD** dialog box, click **Yes**.
The vSpine and vLeaf VMs associated with the Cisco ACI vPod are deleted. In the **vPod Nodes** area of the work pane, you can see that the status of the nodes are now inactive. You can also see that the VMs are not available on VMware vCenter.

Uninstalling Cisco ACI vPod Using the VMware PowerCLI

Before you begin

Remove all the Cisco Application Centric Infrastructure (ACI) Virtual Edge virtual machines (VMs) from the hosts. Any Cisco ACI Virtual Edge VMs associated with the Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) stop working when the Cisco ACI vPod is uninstalled.

Remove the VMs for a given Cisco ACI vPod ID using the **Remove-VPodVM** command.

The following text shows the command syntax:

```
Remove-VpodVM [-VpodId] Object [CommonParameters]
```

Example:

```
PowerCLI C:\> Remove-VpodVM -VpodId 2
Connecting to vCenter.....................................................[ok]
Fetching all vSpine/vLeaf VMs.............................................[ok]
Deleting VM cisco-vPod2-leaf1.............................................[ok]
Deleting VM cisco-vPod2-spine1............................................[ok]
```

Uninstalling Cisco ACI vPod Using Python

Before you begin

Remove all the Cisco Application Centric Infrastructure (ACI) Virtual Edge virtual machines (VMs) from the hosts. Any Cisco ACI Virtual Edge VMs associated with the Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) stop working when the Cisco ACI vPod is uninstalled.

Remove all the Cisco ACI vPod VMs for a given Cisco ACI vPod ID using the `remove-vpodvm.py` script.

The following text shows the usage for the script:

```
(venv) usage: remove-vpodvm.py [-h] [--silent] --vcenter VCENTER --vc-username
VC_USERNAME [--vc-password VC_PASSWORD] --vpod-id VPOD_ID
```

Example:

```
(venv) $ pyhton remove-vpodvm.py --vcenter 172.23.143.235 --vc-username admin --vc-password lab
--vpod-id 2
Connecting to vCenter.....................................................[ok]
Fetching all vSpine/vLeaf VMs.............................................[ok]
```

```
Deleting VM cisco-vPod2-leaf1.....................................[ok]
Deleting VM cisco-vPod2-spine1....................................[ok]
```

Deleting the External TEP Pools Using REST API

In addition to uninstalling Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod), you need to delete any external tunnel endpoint (TEP) pools. You can delete routable subnets gracefully.

In REST API, an external TEP pool is referred to as a routable subnet.

Step 1 Set the state to inactive. When state is set as inactive, no further IP addresses are allocated from this pool.

Example:

```
<fabricExtRoutablePodSubnet pool="192.4.1.0/27" state="inactive"/>
```

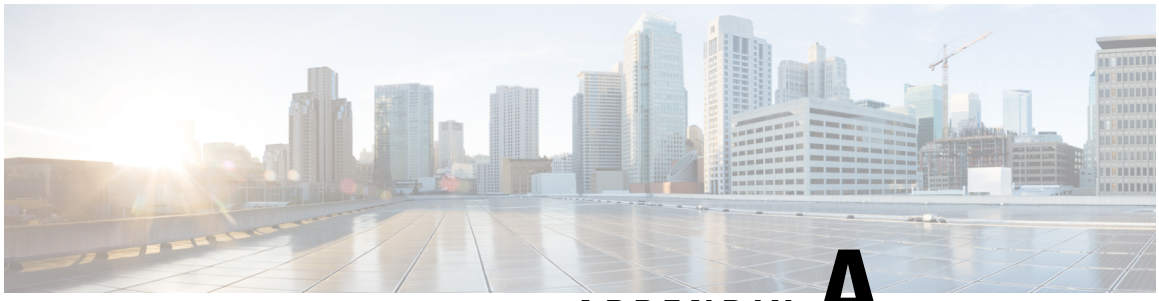
Step 2 Decommission all the virtual nodes (vLeafs and vSpines) of each Cisco ACI vPod.

Step 3 Delete the subnet:

Note You can delete the subnet only if no IP address is used from this pool.

Example:

```
<fabricExtRoutablePodSubnet pool="192.4.1.0/27" status="deleted"/>
```



APPENDIX A

Changing the Gateway IP Address for Cisco ACI vPod

Changing the Gateway IP Address for Cisco ACI vPod

To change the gateway IP address of a Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod), you must perform a clean reboot of the virtual spine (vSpine) and virtual leaf (vLeaf) nodes. Also, reboot the Cisco ACI Virtual Edge virtual machines (VMs) in the Cisco ACI vPod. Otherwise, the gateway IP address is not updated on the vSpine and vLeaf.

Before you begin

Make sure that there is still connectivity through the old gateway IP address.

Step 1 Configure the new gateway IP address on the gateway device.

Step 2 Change the gateway IP address in the Cisco Application Policy Infrastructure Controller (APIC) configuration.

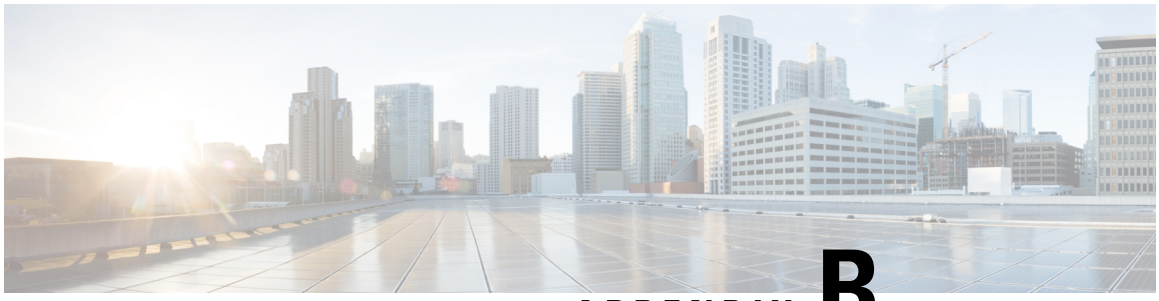
Step 3 Perform a clean reboot of the vSpine and vLeaf nodes.

Alternatively, you can decommission the vSpine and vLeaf nodes and then recommission them.

Step 4 Reboot all the Cisco ACI Virtual Edge VMs in the Cisco ACI vPod.

Step 5 Remove the old gateway IP address from the gateway device.

Changing the Gateway IP Address for Cisco ACI vPod



APPENDIX B

Configuring Cisco ACI to Accept More Routes from the IPN

Configuring Cisco ACI to Accept More Routes From the IPN

When routes are advertised to the physical spines from the interpod network (IPN), Open Shortest Path First (OSPF) restributes those routes only to Intermediate System to Intermediate System (IS-IS). This redistribution happens when IS-IS is part of an existing tunnel endpoint (TEP) pool or part of a subnet that is configured under **Fabric Ext Connection Policies** in the Cisco Application Policy Infrastructure Controller (APIC).

Because of this behavior, spines that are not connected to the IPN cannot reach the vSpines. If your data plane TEP and vSpine router IDs are not part of the Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) TEP pool, you must configure the **Fabric Ext Connection Policies** with those subnets.

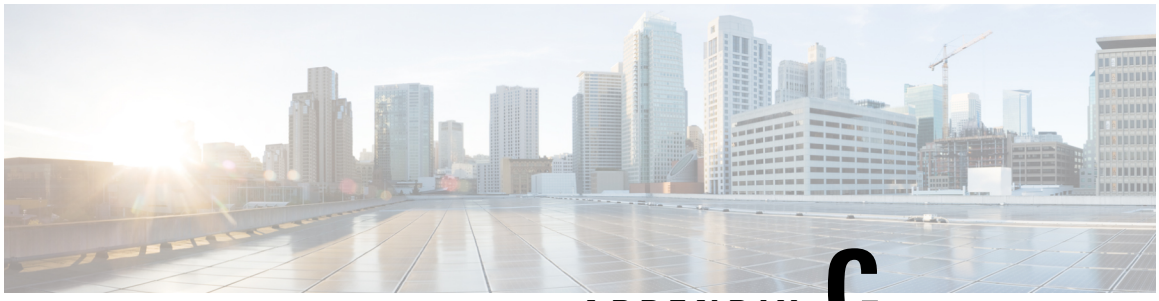
Step 1 Configure the router ID, the data plane (TEP), or both for the vSpine and Cisco ACI vPod as a secondary route on the IPN.

Step 2 Log in to Cisco APIC.

Step 3 Go to **Tenant** > **Infra** > **Policies** > **Protocol** > **Fabric Ext Connection Policies**.

Step 4 Under the configured policy, add the subnets to the **Fabric External Routing Profile**.

Configuring Cisco ACI to Accept More Routes from the IPN



APPENDIX C

Performing Tasks Using REST API

Installation

Preparing the Physical Pod IPN Connectivity Using REST API

The physical spines in the on-premises data center communicate with the Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) virtual spine (vSpines) in the remote site over a Layer 3 interpod network (IPN). Before you create the Cisco ACI vPod on the remote site, you first ensure that a physical pod can communicate with it. You also configure a unique unicast IP address and a routable subnet for each physical pod.

Note The procedures using the Cisco Application Policy Infrastructure Controller (APIC) refer to routable subnets as external tunnel endpoint (TEP) pools.

Step 1 Log in to Cisco APIC:

Example:

```
http://<apic-name/ip>:80/api/aaaLogin.xml

data: <aaaUser name="admin" pwd="password”/>
```

Step 2 Configure the TEP pool:

Example:

```
http://<apic-name/ip>:80/api/policymgr/mo/uni/controller.xml

<fabricSetupPol status=''>
    <fabricSetupP podId="1" tepPool="10.0.0.0/16" />
```

Performing Tasks Using REST API

```
    <fabricSetupP podId="2" tepPool="10.1.0.0/16" status='' />
</fabricSetupPol>
```

Step 3 Configure the node ID policy:

Example:

```
http://<apic-name/ip>:80/api/node/mo/uni/controller.xml

<fabricNodeIdentPol>
<fabricNodeIdentP serial="XXXXXXXXXXX" name="leaf1" nodeId="101" podId="1"/>
<fabricNodeIdentP serial="XXXXXXXXXXX" name="leaf2" nodeId="102" podId="1"/>
<fabricNodeIdentP serial="XXXXXXXXXXX" name="leaf3" nodeId="103" podId="1"/>
<fabricNodeIdentP serial="XXXXXXXXXXX" name="leaf4" nodeId="104" podId="1"/>
<fabricNodeIdentP serial="XXXXXXXXXXX" name="spine1" nodeId="201" podId="1"/>
<fabricNodeIdentP serial="XXXXXXXXXXX" name="spine3" nodeId="202" podId="1"/>
<fabricNodeIdentP serial="XXXXXXXXXXX" name="leaf5" nodeId="105" podId="2"/>
<fabricNodeIdentP serial="XXXXXXXXXXX" name="leaf6" nodeId="106" podId="2"/>
<fabricNodeIdentP serial="XXXXXXXXXXX" name="spine2" nodeId="203" podId="2"/>
<fabricNodeIdentP serial="XXXXXXXXXXX" name="spine4" nodeId="204" podId="2"/>
</fabricNodeIdentPol>
```

Step 4 Configure infra L3Out and external connectivity profile:

Example:

```
http://<apic-name/ip>:80/api/node/mo/uni.xml

<polUni>

<fvTenant descr="" dn="uni/tn-infra" name="infra" ownerKey="" ownerTag="">

   <l3extOut descr="" enforceRtctrl="export" name="multipod" ownerKey="" ownerTag=""
targetDscp="unspecified" status=''>
      <ospfExtP areaId='0' areaType='regular' status=''/>
      <bgpExtP status='' />
      <l3extRsEctx tnFvCtxName="overlay-1"/>
      <l3extProvLbl descr="" name="prov_mp1" ownerKey="" ownerTag="" tag="yellow-green"/>

      <l3extLNodeP name="bSpine">
        <l3extRsNodeL3OutAtt rtrId="201.201.201.201" rtrIdLoopBack="no" tDn="topology/pod-1/node-201">

            <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
            <l3extLoopBackIfP addr="201::201/128" descr="" name=""/>
            <l3extLoopBackIfP addr="201.201.201.201/32" descr="" name=""/>
         </l3extRsNodeL3OutAtt>

        <l3extRsNodeL3OutAtt rtrId="202.202.202.202" rtrIdLoopBack="no" tDn="topology/pod-1/node-202">

            <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
            <l3extLoopBackIfP addr="202::202/128" descr="" name=""/>
            <l3extLoopBackIfP addr="202.202.202.202/32" descr="" name=""/>
         </l3extRsNodeL3OutAtt>

        <l3extRsNodeL3OutAtt rtrId="203.203.203.203" rtrIdLoopBack="no" tDn="topology/pod-2/node-203">

            <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
            <l3extLoopBackIfP addr="203::203/128" descr="" name=""/>
            <l3extLoopBackIfP addr="203.203.203.203/32" descr="" name=""/>
         </l3extRsNodeL3OutAtt>

        <l3extRsNodeL3OutAtt rtrId="204.204.204.204" rtrIdLoopBack="no" tDn="topology/pod-2/node-204">

            <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
            <l3extLoopBackIfP addr="204::204/128" descr="" name=""/>
```

```
            <l3extLoopBackIfP addr="204.204.204.204/32" descr="" name=""/>
          </l3extRsNodeL3OutAtt>

          <l3extLIfP name='portIf'>
             <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-1/paths-201/pathep-[eth1/1]"
encap='vlan-4'  ifInstT='sub-interface' addr="201.1.1.1/30" />
             <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-1/paths-201/pathep-[eth1/2]"
encap='vlan-4'  ifInstT='sub-interface' addr="201.2.1.1/30" />
             <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-1/paths-202/pathep-[eth1/2]"
encap='vlan-4'  ifInstT='sub-interface' addr="202.1.1.1/30" />
             <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-2/paths-203/pathep-[eth1/1]"
encap='vlan-4'  ifInstT='sub-interface' addr="203.1.1.1/30" />
             <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-2/paths-203/pathep-[eth1/2]"
encap='vlan-4'  ifInstT='sub-interface' addr="203.2.1.1/30" />
             <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-2/paths-204/pathep-[eth4/31]"
encap='vlan-4'  ifInstT='sub-interface' addr="204.1.1.1/30" />

            <ospfIfP>
                <ospfRsIfPol tnOspfIfPolName='ospfIfPol'/>
            </ospfIfP>

          </l3extLIfP>
       </l3extLNodeP>

       <l3extInstP descr="" matchT="AtleastOne" name="instp1" prio="unspecified"
targetDscp="unspecified">
           <fvRsCustQosPol tnQosCustomPolName=""/>
       </l3extInstP>
    </l3extOut>

   <fvFabricExtConnP descr="" id="1" name="Fabric_Ext_Conn_Pol1" rt="extended:as2-nn4:5:16" status=''>

       <fvPodConnP descr="" id="1" name="">
          <fvIp addr="100.11.1.1/32"/>
       </fvPodConnP>
       <fvPodConnP descr="" id="2" name="">
          <fvIp addr="200.11.1.1/32"/>
       </fvPodConnP>
       <fvPeeringP descr="" name="" ownerKey="" ownerTag="" type="automatic_with_full_mesh"/>
       <l3extFabricExtRoutingP descr="" name="ext_routing_prof_1" ownerKey="" ownerTag="">
          <l3extSubnet aggregate="" descr="" ip="100.0.0.0/8" name="" scope="import-security"/>
          <l3extSubnet aggregate="" descr="" ip="200.0.0.0/8" name="" scope="import-security"/>
          <l3extSubnet aggregate="" descr="" ip="201.1.0.0/16" name="" scope="import-security"/>
          <l3extSubnet aggregate="" descr="" ip="201.2.0.0/16" name="" scope="import-security"/>
          <l3extSubnet aggregate="" descr="" ip="202.1.0.0/16" name="" scope="import-security"/>
          <l3extSubnet aggregate="" descr="" ip="203.1.0.0/16" name="" scope="import-security"/>
          <l3extSubnet aggregate="" descr="" ip="203.2.0.0/16" name="" scope="import-security"/>
          <l3extSubnet aggregate="" descr="" ip="204.1.0.0/16" name="" scope="import-security"/>
       </l3extFabricExtRoutingP>
    </fvFabricExtConnP>
</fvTenant>
</polUni>
```

Step 5 Configure a routable subnet for each physical pod.

Example:

```
URL: https://<controllername>/api/node/mo/uni/controller/setupPol.xml

POST:

<fabricSetupP podId="1">
<fabricExtRoutablePodSubnet pool="197.16.0.0/25"
    reserveAddressCount = 2/>
</fabricSetupP>
```

In the example, `pool` defines the routable subnet or external TEP pool. You can reserve some of the IP addresses from the start of the pool by the `reserveAddressCount`. Cisco APIC does not manage these IP addresses, which you can configure as desired.

Note the following:

- The minimum size of each routable TEP pool is /28, and the maximum size is /22 for each physical pod.
- Addresses from this TEP pool are allocated to border leafs and spines: physical TEP (PTEP) for border leafs and controller-plane TEP (CP-TEP) for spines.
- Each Cisco APIC is allocated one routable IP address.
- One multicast TEP IP address for each site is allocated from the Pod 1 routable subnet.

Step 6 Configure a unique unicast TEP IP address and an IP addressed used as the Border Gateway Protocol (BGP) next hop for each physical pod:

You can configure these addresses from the reserved portion of the external TEP pool (routable subnet).

Example:

```
<fvTenant name="infra">

     <fvFabricExtConnP id="1" rt="extended:as2-nn4:5:16">
     <fvPodConnP id="1">
  <fvIp addr="108.11.1.1/32"/>
     <fvExtRoutableUcastConnP addr="197.16.0.1/32"/>
</fvFabricExtConnP>
</fvTenant>
```

Step 7 Configure a multiprotocol BGP (MP-BGP) route reflector.

Example:

```
https://<apic-name-or-ip>/api/policymgr/mo/uni.xml

<polUni>
  <fabricInst>
    <fabricPodP name="default">
      <fabricPodS name="default" type="ALL">
        <fabricRsPodPGrp tDn="uni/fabric/funcprof/podpgrp-default"/>
      </fabricPodS>
    </fabricPodP>

    <fabricFuncP name="default">
      <fabricPodPGrp name="default">
        <fabricRsPodPGrpBGPRRP tnBgpInstPolName="default"/>
      </fabricPodPGrp>
    </fabricFuncP>

    <bgpInstPol name="default">
      <bgpAsP asn="200"/>
      <bgpRRP>
        <bgpRRNodePEp id="202" status=""/>
      </bgpRRP>
    </bgpInstPol>
  </fabricInst>
</polUni>
```

If you configure a route reflector and want to remove the spine switch from the controller in the future, you must disable **Route Reflector** on the *BGP Route Reflector* Cisco APIC page before removing the spine switch from the controller. Not doing so results in an error.

To disable a route reflector, right-click on the appropriate route reflector in the **Route Reflector Nodes** area in the **BGP Route Reflector** page and select **Delete**. See the section "Configuring an MP-BGP Route Reflector Using the GUI" in the chapter "MP-BGP Route Reflectors" in the *Cisco APIC Layer 3 Networking Configuration Guide*.

Adding the Cisco ACI vPod Using REST API

To add a Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod), you define the pod ID and tunnel endpoint (TEP) pool. You also configure the virtual spine (vSpine) and virtual leafs (vLeaf) virtual machines (VMs) on the two required nodes.

Before you begin

- You must have prepared a physical pod in the on-premises data center to communicate with Cisco ACI vPod in the remote site. See Preparing the Physical Pod IPN Connectivity Using the Cisco APIC GUI, on page 8 or Preparing the Physical Pod IPN Connectivity Using REST API, on page 11 in this guide.
- We recommend that you create a Cisco Application Centric Infrastructure (ACI) Virtual Edge virtual machine manager (VMM) domain before you create the Cisco ACI vPod.

Step 1 Add the Cisco ACI vPod:

Example:

```
https://<controllername>/api/node/mo/uni/controller/setupPol.xml

<fabricSetupPol>
<fabricSetupP tepPool="196.0.128.0/22" podId="3" podType="virtual">
<fabricSetupAllocP gatewayAddress="196.0.128.1"        reservedAddress="196.0.128.0/27"/>
<fabricAssociatedSetupP pool="20.0.0.0/28" >
<fabricSetupAllocP gatewayAddress="20.0.0.14" reservedAddress="20.0.0.8/29"/>
</fabricAssociatedSetupP>
<fabricPodDhcpServer nodeId="301" serverType="primary”/>
<fabricPodDhcpServer nodeId="303" serverType="secondary”/>
</fabricSetupP>
</fabricSetupPol>
```

Cisco ACI vPod creation: To create the Cisco ACI vPod, you must post the `fabricSetupP` policy with the primary TEP pool of the pod:

```
<fabricSetupP tepPool="196.0.128.0/22" podId="3" podType="virtual">
```

- IP addresses for virtual leafs (vLeafs) and virtual spines (vSpines) will be allocated from the primary TEP pool.
- The primary TEP pool also can be used for Cisco ACI Virtual Edge and Head-End Replicated (HREP) IP addresses.

The minimum size of each TEP pool subnet is /28, and the maximum size is /22.

Gateway IP address: You must specify the gateway IP address and a subnet for Cisco ACI vPod from start or the end of each reserved TEP pool subnet. The gateway will be programmed automatically (using DHCP) by Cisco Application Policy Infrastructure Controller (APIC) in the vLeaf and vSpine. The reserved part of the subnet is not managed by APIC and typically is used for the gateway, HSRP-related IPs, dataplane TEP, and Router ID.

```
<fabricSetupAllocP gatewayAddress="196.0.128.1" reservedAddress="196.0.128.0/27"/>
```

Secondary TEP pools: You can add secondary TEP pools to the Cisco ACI vPod by posting a `fabricAssociatedSetupP` policy. This optional configuration is used only when you want to configure more than one subnet on the Cisco ACI vPod. Secondary subnets are used only for Cisco ACI Virtual Edge in the Cisco ACI vPod.

```
<fabricAssociatedSetupP pool="20.0.0.0/28" >
<fabricSetupAllocP gatewayAddress="20.0.0.14" reservedAddress="20.0.0.8/29"/>
</fabricAssociatedSetupP>
```

The `gatewayAddress` and `reservedAddress` have the same meaning as for the primary subnet.

DHCP server configuration: You must post a `fabricPodDhcpServer` policy to configure DHCP servers running in primary and secondary modes on vLeafs, for example.

```
<fabricPodDhcpServer nodeId="301" serverType="primary”/>
<fabricPodDhcpServer nodeId="303" serverType="secondary”/>
```

Step 2 Add the IP address for the Border Gateway Protocol (BGP) next hop and the BGP password for the Cisco ACI vPod.

Example:

```
<fvFabricExtConnP descr="" id="1" name="Fabric_Ext_Conn_Pol1" rt="extended:as2-nn4:5:16" status=''>

      <fvPodConnP descr="" id="3">
         <fvIp addr="166.11.1.1/32"/>
         <fvPasswordConfig password="12345"/>
      </fvPodConnP>
</fvFabricExtConnP>
```

Uninstallation

Deleting the External TEP Pools Using REST API

In addition to uninstalling Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod), you need to delete any external tunnel endpoint (TEP) pools. You can delete routable subnets gracefully.

In REST API, an external TEP pool is referred to as a routable subnet.

Step 1 Set the state to inactive. When state is set as inactive, no further IP addresses are allocated from this pool.

Example:

```
<fabricExtRoutablePodSubnet pool="192.4.1.0/27" state="inactive"/>
```

Step 2 Decommission all the virtual nodes (vLeafs and vSpines) of each Cisco ACI vPod.

Step 3 Delete the subnet:

Note You can delete the subnet only if no IP address is used from this pool.

Example:

```
<fabricExtRoutablePodSubnet pool="192.4.1.0/27" status="deleted"/>
```