Cisco ACI with VMware VDS Integration

This chapter contains the following sections:

Configuring Virtual Machine Networking Policies

Cisco Application Policy Infrastructure Controller (APIC) integrates with third-party VM managers (VMMs)—such as VMware vCenter—to extend the benefits of Cisco Application Centric Infrastructure (ACI) to the virtualized infrastructure. Cisco APIC enables the administrator to use Cisco ACI policies inside the VMM system.

The following modes of Cisco ACI and VMware VMM integration are supported:

- VMware VDS: When integrated with Cisco ACI, the VMware vSphere Distributed Switch (VDS) enables you to configure VM networking in the Cisco ACI fabric.
- Cisco ACI Virtual Edge: For information about how to install and configure Cisco ACI Virtual Edge, see the *Cisco ACI Virtual Edge Installation Guide* and the *Cisco ACI Virtual Edge Configuration Guide* on Cisco.com.
- Cisco Application Virtual Switch (AVS): For information about how to install and configure Cisco AVS with Cisco ACI, see Cisco AVS documentation on Cisco.com.

Note When a Cisco APIC is connected to a VMware vCenter with many folders, you may see a delay when pushing new port groups from the Cisco APIC to the vCenter.

However, if you are running Cisco APIC 3.2(6) or later, you can disable or leave disabled the collection of VM folders, which can remediate the delay in pushing new port groups.

The VM folder collection feature is disabled by default but can be enabled when you create or edit a VMware vCenter domain. If you use or want to use VM folders as a microsegmentation (uSeg) matching attribute, you can enable VM folder data retrieval. However, if you do not use VM folders as a uSeg matching attribute, you can disable collection.

APIC Supported VMware VDS Versions

See the Cisco ACI Virtualization Compatibility Matrix for information about the compatibility of VMware components with Cisco APIC.

Note VMware vSphere version 6.7 includes vCenter 6.7, ESXi 6.7, and DVS 6.6.

Note When adding additional VMware ESXi hosts to the VMM domain with VMware vSphere Distributed Switch (VDS), ensure that the version of ESXi host is compatible with the Distributed Virtual Switch (DVS) version already deployed in the vCenter. For more information about VMware VDS compatibility requirements for ESXi hosts, see the VMware documentation.

If the ESXi host version is not compatible with the existing DVS version, vCenter will not be able to add the ESXi host to the DVS, and an incompatibility error will occur. Modification of the existing DVS version setting from the Cisco APIC is not possible. To lower the DVS version in the vCenter, you need to remove and reapply the VMM domain configuration with a lower setting.

Important If you have ESXi 6.5 hosts running UCS B-Series or C-Series server with VIC cards, some of the vmnics may go down on a port state event, such as a link flap or a TOR reload. To prevent this problem, do not use the default eNIC driver but install it from the VMware website: https://my.vmware.com/web/vmware/details?downloadGroup=DT-ESXI65-CISCO-NENIC-1020&productId=614.

Guidelines for Upgrading VMware DVS from 5.x to 6.x and VMM Integration

This section describes the guidelines for upgrading VMware Distributed Virtual Switch (DVS) from 5.x to 6.x and VMM integration.

- DVS versioning is only applicable to the VMware DVS and not the Cisco Application Virtual Switch (AVS). DVS upgrades are initiated from VMware vCenter, or the relevant orchestration tool and not ACI. The **Upgrade Version** option appears grayed out for AVS switches within vCenter.

- If you are upgrading the DVS from 5.x to 6.x, you must upgrade the vCenter Server to version 6.0 and all hosts connected to the distributed switch to ESXi 6.0. For full details on upgrading your vCenter and Hypervisor hosts, see VMware's upgrade documentation. To upgrade the DVS go to the Web Client: **Home** > **Networking** > **DatacenterX** > **DVS-X** > **Actions Menu** > **Upgrade Distributed Switch**.
- There is no functional impact on the DVS features, capability, performance and scale if the DVS version shown in vCenter does not match the VMM domain DVS version configured on the APIC. The APIC and VMM Domain DVS Version is only used for initial deployment.

Guidelines for VMware VDS Integration

Follow the guidelines in this section when integrating VMware vSphere Distributed Switch (VDS) into Cisco Application Centric Infrastructure (ACI).

- Do not change the following settings on a VMware VDS configured for VMM integration:
  - VMware vCenter hostname (if you are using DNS).
  - VMware vCenter IP address (if you are using IP).
  - VMware vCenter credentials used by Cisco APIC.
  - Data center name
  - Folder, VDS, or portgroup name.
  - Folder structure containing the VMware VDS.

    For example, do not put the folder in another folder.
  - Uplink port-channel configuration, including LACP/port channel, LLDP, and CDP configuration
  - VLAN on a portgroup
  - Active uplinks for portgroups pushed by Cisco APIC.
  - Security parameters (promiscuous mode, MAC address changes, forged transmits) for portgroups pushed by Cisco APIC.
- Use supported versions of VMware vCenter/vSphere with the version of Cisco ACI that you are running.
- If you are adding or removing any portgroups, use Cisco APIC or the Cisco ACI vCenter plug-in in VMware vCenter.
- Know that Cisco APIC may overwrite some changes that are made in VMware vCenter.

  For example, when Cisco APIC updates a portgroup, port binding, promiscuous mode, and load-balancing can be overwritten

Mapping Cisco ACI and VMware Constructs

Table 1: Mapping of Cisco Application Centric Infrastructure (ACI) and VMware Constructs

Cisco ACI Terms	VMware Terms
Endpoint group (EPG)	Port group
LACP Active	• Route based on IP hash (downlink port group) • LACP Enabled/Active (uplink port group)
LACP Passive	• Route based on IP hash (downlink port group) • LACP Enabled/Active (uplink port group)
MAC Pinning	• Route based on originating virtual port • LACP Disabled
MAC Pinning-Physical-NIC-Load	• Route based on physical NIC load • LACP Disabled
Static Channel - Mode ON	• Route Based on IP Hash (downlink port group) • LACP Disabled
Virtual Machine Manager (VMM) Domain	vSphere Distributed Switch (VDS)
VM controller	vCenter (Datacenter)

VMware VDS Parameters Managed By APIC

VDS Parameters Managed by APIC

See the section Mapping Cisco ACI and VMware Constructs in this guide for a table of corresponding Cisco Application Centric Infrastructure (ACI) and VMware terminology.

VMware VDS	Default Value	Configurable Using Cisco APIC Policy?
Name	VMM domain name	Yes (Derived from Domain)
Description	"APIC Virtual Switch"	No
Folder Name	VMM domain name	Yes (Derived from Domain)
Version	Highest supported by vCenter	Yes
Discovery Protocol	LLDP	Yes

VMware VDS	Default Value	Configurable Using Cisco APIC Policy?
Uplink Ports and Uplink Names	8	No
Uplink Name Prefix	uplink	No
Maximum MTU	9000	Yes
LACP policy	disabled	Yes
Port mirroring	0 sessions	Yes
Alarms	2 alarms added at the folder level	No

VDS Port Group Parameters Managed by APIC

VMware VDS Port Group	Default Value	Configurable using APIC Policy
Name	Tenant Name | Application Profile Name | EPG Name	Yes (Derived from EPG)
Port binding	Static binding	No
VLAN	Picked from VLAN pool	Yes
Load balancing algorithm	Derived based on port-channel policy on APIC	Yes
Promiscuous mode	Disabled	Yes
Forged transmit	Disabled	Yes
Mac change	Disabled	Yes
Block all ports	False	No

Creating a VMM Domain Profile

VMM domain profiles specify connectivity policies that enable virtual machine controllers to connect to the Cisco ACI fabric. They group VM controllers with similar networking policy requirements. For example, VM controllers can share VLAN pools and application endpoint groups (EPGs). The Cisco APIC communicates with the controller to publish network configurations such as port groups that are then applied to the virtual workloads. For details, see the Cisco Application Centric Infrastructure Fundamentals on Cisco.com.

Beginning with Cisco APIC Release 3.1(1), you also can create a read-only VMM domain. A read-only VMM domain enables you to view inventory information for a VDS in the VMware vCenter that Cisco APIC does not manage. Procedures to configure a read-only VMM domain differ slightly from procedures to create other VMM domains. However, the same workflow and prerequisites apply.

Note In this section, examples of a VMM domain are vCenter domain.

GUI Tasks

This section shows how to perform tasks using GUI.

- For references to REST API tasks, refer to REST API Tasks, on page 28.
- For references to NX-OS Style CLI tasks, refer to NX-OS Style CLI Tasks, on page 35.

Prerequisites for Creating a VMM Domain Profile

To configure a VMM domain profile, you must meet the following prerequisites:

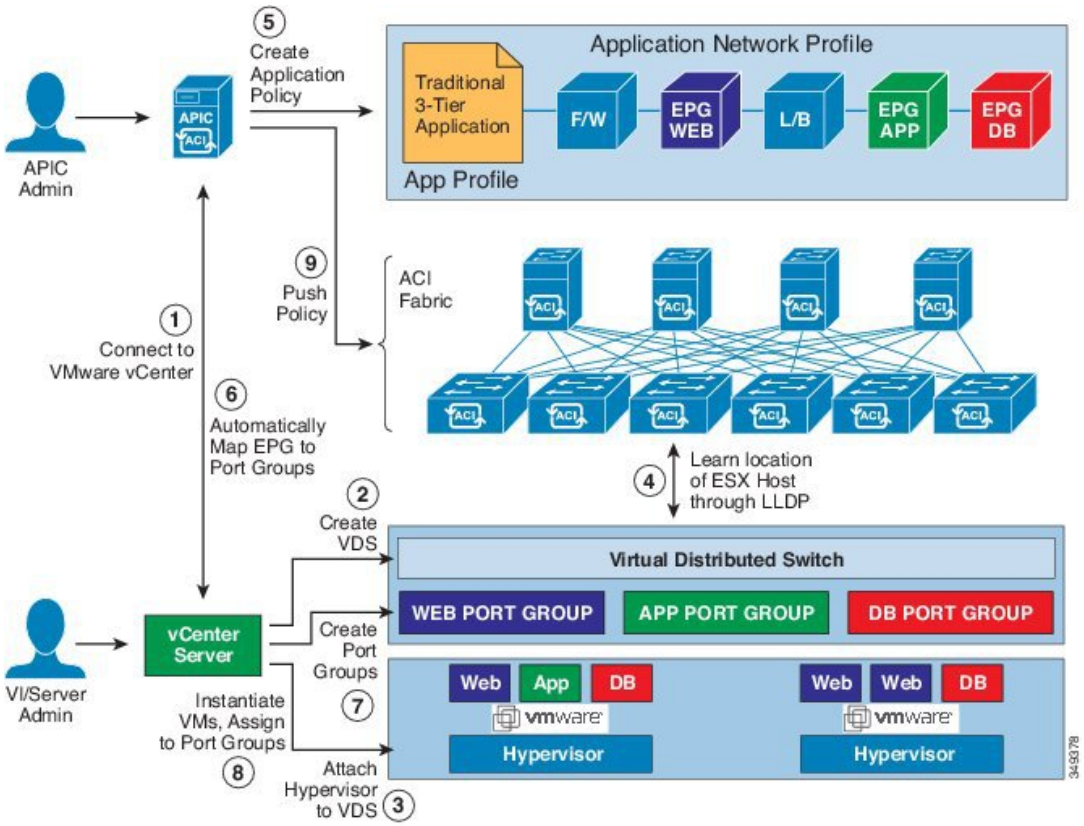
- All fabric nodes are discovered and configured.
- Inband (inb) or out-of-band (oob) management has been configured on the APIC.
- A Virtual Machine Manager (VMM) is installed, configured, and reachable through the inb/oob management network (for example, a vCenter).
- You have the administrator/root credentials to the VMM (for example vCenter).

  Note If you prefer not to use the vCenter admin/root credentials, you can create a custom user account with minimum required permissions. See Custom User Account with Minimum VMware vCenter Privileges, on page 24 for a list of the required user privileges.

- A DNS policy for the APIC must be configured if you plan to reference the VMM by hostname rather than an IP address.

vCenter Domain Operational Workflow

Figure 1: A Sequential Illustration of the vCenter Domain Operational Workflow



The APIC administrator configures the vCenter domain policies in the APIC. The APIC administrator provides the following vCenter connectivity information:

- The vCenter IP address, vCenter credentials, VMM domain policies, and VMM domain SPAN
- Policies (VLAN pools, domain type such as VMware VDS, Cisco Nexus 1000V switch)
- Connectivity to physical leaf inerfaces (using attach entity profiles)

1. The APIC automatically connects to the vCenter.
2. The APIC creates the VDS—or uses an existing VDS if there is one already created—matching the name of the VMM domain.

Note If you use an existing VDS, the VDS must be inside a folder with the same name.

Note If you want to see an existing VDS from the vCenter, you can do so by specifying the **Read Only Mode** in the **Access Mode** area when you create a VMM domain with the same name as the VDS in vCenter using the Cisco APIC. This VMM in **Read Only Mode** is not managed by APIC. You may not be able to modify any properties of this VMM domain except vCenter user credentials and vCenter IP address.

3. The vCenter administrator or the compute management tool adds the ESX host or hypervisor to the APIC VDS and assigns the ESX host hypervisor ports as uplinks on the APIC VDS. These uplinks must connect to the ACI leaf switches.
4. The APIC learns the location of the hypervisor host to the leaf connectivity using LLDP or CDP information of the hypervisors.
5. The APIC administrator creates and associates application EPG policies.
6. The APIC administrator associates EPG policies to VMM domains.
7. The APIC automatically creates port groups in the VMware vCenter under the VDS. This process provisions the network policy in the VMware vCenter.

Note
- The port group name is a concatenation of the tenant name, the application profile name, and the EPG name.
- The port group is created under the VDS, and it was created earlier by the APIC.

8. The vCenter administrator or the compute management tool instantiates and assigns VMs to the port groups.
9. The APIC learns about the VM placements based on the vCenter events. The APIC automatically pushes the application EPG and its associated policy (for example, contracts and filters) to the ACI fabric.

Creating a vCenter Domain Profile Using the GUI

An overview of the tasks that you perform to create a vCenter Domain are as follows (details are in the steps that follow):

- Create or select a switch profile.
- Create or select an interface profile.
- Create or select an interface policy group.
- Create or select VLAN pool.
- Create vCenter domain.
- Create vCenter credentials.

Procedure

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

Step 2 In the navigation pane, click **Quick Start**, and then in the central pane click **Configure an interface, PC, and VPC**.

Step 3 In the **Configure an interface, PC, and VPC** dialog box, perform the following actions:

a) Expand **Configured Switch Interfaces**.
b) Click the **+** icon.
c) Make sure that the **Quick** radio button is chosen.
d) From the **Switches** drop-down list, choose the appropriate leaf ID.

In the **Switch Profile Name** field, the switch profile name automatically populates.

e) Click the **+** icon to configure the switch interfaces.
f) In the **Interface Type** area, check the appropriate radio button.
g) In the **Interfaces** field, enter the desired interface range.
h) In the **Interface Selector Name** field, the selector name automatically populates.
i) In the **Interface Policy Group** area, choose the **Create One** radio button.
j) From the **Link Level Policy** drop-down list, choose the desired link level policy.
k) From the **CDP Policy** drop-down list, choose the desired CDP policy.

Note Similarly choose the desired interface policies from the available policy areas.

l) In the **Attached Device Type** area, choose **ESX Hosts**.
m) In the **Domain** area, make sure that the **Create One** radio button is chosen.
n) In the **Domain Name** field, enter the domain name.
o) In the **VLAN** area, make sure that the **Create One** radio button is chosen.
p) In the **VLAN Range** field, enter the VLAN range as appropriate.

Note We recommend a range of at least 200 VLAN numbers. Do not define a range that includes your manually assigned infra VLAN. If you do so, it can trigger a fault, depending on your version of Cisco Application Policy Infrastructure Controller (APIC). There are specific use cases and options to be set if your infra VLAN needs to be extended as part of an OpFlex integration.

q) In the **vCenter Login Name** field, enter the login name.
r) (Optional) From the **Security Domains** drop-down list, choose the appropriate security domain.
s) In the **Password** field, enter a password.
t) In the **Confirm Password** field, reenter the password.
u) Expand **vCenter**.

Step 4 In the **Create vCenter Controller** dialog box, enter the appropriate information, and click **OK**.

Step 5 In the **Configure Interface, PC, And VPC** dialog box, complete the following actions:

If you do not specify policies in the **Port Channel Mode** and the **vSwitch Policy** areas, the same policies that you configured earlier in this procedure will take effect for the vSwitch.

a) From the **Port Channel Mode** drop-down list, choose a mode.
b) In the **vSwitch Policy** area, click the desired radio button to enable CDP or LLDP.
c) From the **NetFlow Exporter Policy** drop-down list, choose a policy or create one.

A NetFlow exporter policy configures the external collector reachability.

d) Choose values from the **Active Flow TimeOut**, **Idle Flow Timeout**, and **Sampling Rate** drop-down lists.
e) Click **SAVE** twice and then click **SUBMIT**.

Step 6 Verify the new domain and profiles, by performing the following actions:

a) On the menu bar, choose **Virtual Networking** > **Inventory**.
b) In the **Navigation** pane, expand **VMM Domains** > **VMware** > ***Domain_name*** > **vCenter_name**.

In the work pane, under **Properties**, view the VMM domain name to verify that the controller is online. In the **Work** pane, the vCenter properties are displayed including the operational status. The displayed information confirms that connection from the APIC controller to the vCenter Server is established, and the inventory is available.

Creating a Read-Only VMM Domain

Beginning in Cisco APIC Release 3.1(1), you can create a read-only VMM domain. Doing so enables you to view inventory information for a VDS in the VMware vCenter that Cisco APIC does not manage.

After you create the read-only VMM domain, you can view hypervisors, VMs, NIC status, and other inventory information, as with regular VMM domains. You can associate an EPG to the VMM domain and configure policies for it. However, policies are not pushed from the read-only VMM domain to the VDS. Also, no faults are raised for a read-only VMM domain.

You can create a read-only VMM domain using the Cisco APIC GUI, the NX-OS style CLI, or REST API. See the following sections in this guide for instructions:

- Creating a Read-Only VMM Domain Using the Cisco APIC GUI, on page 10
- Creating a Read-Only VMM Domain Using the REST API, on page 30
- Creating a Read-Only VMM Domain Using the NX-OS Style CLI, on page 37

Creating a Read-Only VMM Domain Using the Cisco APIC GUI

In order to create a read-only VMM domain, you create the domain in the **Create vCenter Domain** dialog box under the **Virtual Networking** tab. Do not follow the procedure in the section Creating a vCenter Domain Profile Using the GUI, on page 8 to create the domain. That procedure does not enable you to set an access mode for the VMM domain.

Before you begin

- Fulfill the prerequisites in the section Prerequisites for Creating a VMM Domain Profile, on page 6.
- In the VMware vCenter, ensure that under the **Networking** tab, the VDS is contained by a folder.

  Also ensure that the folder and the VDS have the exact same name of the read-only VMM domain that you plan to create.

Procedure

Step 1 Log in to Cisco APIC.

Step 2 Choose **Virtual Networking** > **Inventory** and then expand the **VMM Domains** folder.

Step 3 Right-click the **VMM Domains** folder and choose **Create vCenter Domain**.

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

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

Note The name of the read-only domain must be the same as the name of the VDS and the folder that contains in the VMware vCenter.

b) In the **Virtual Switch** area, choose **VMware vSphere Distributed Switch**.

c) In the **Access Mode** area, choose **Read Only Mode**.

d) In the **vCenter Credentials** area, click the **+** (plus) icon, and then create the VMware vCenter credentials for the domain.

e) In the **vCenter** area, click the **+** (plus) icon, and then add a vCenter controller for the domain.

f) Click **Submit**.

What to do next

You can attach an EPG to the read-only VMM domain and configure policies for it. However, those policies are not pushed to the VDS in the VMware vCenter.

Enhanced LACP Policy Support

In Cisco Application Policy Infrastructure Controller (APIC) Release 3.2(7), you can improve uplink load balancing by applying different Link Aggregation Control Protocol (LACP) policies to different distributed virtual switch (DVS) uplink port groups.

Cisco APIC now supports VMware's Enhanced LACP feature, which is available for DVS 5.5 and later. Previously, the same LACP policy applied to all DVS uplink port groups. Before Cisco APIC Release 3.2(7), it was not possible to manage VMware link aggregation groups (LAGs) with Cisco APIC.

You can choose from up to 20 different load-balancing algorithms when you create a VMware vCenter virtual machine manager (VMM) domain for Cisco Application Centric Infrastructure (ACI) Virtual Edge or VMware VDS. You apply different policies to different uplink portgroups.

You have eight DVS uplink portgroups, and you must configure at least two uplinks in the same policy. So you can have up to four different LACP policies for each DVS. Enhanced LACP supports only active and passive LACP modes.

Note For Cisco ACI Virtual Edge VXLAN mode, it is mandatory to use a load-balancing algorithm having a UDP port. We recommend the algorithm **Source and Destination TCP/UDP Port**. In VLXAN mode, traffic is always sent between VTEP to the FTEP IP. So communication is always between one pair of IP address. So for VXLAN traffic, the only way to distinguish traffic is using the UDP port number.

The following sections provide instructions for configuring multiple LACP policies for DVS uplinks using the Cisco APIC GUI, NX-OS style CLI, or REST API.

Enhanced LACP Limitations

Be aware of the following limitations when using enhanced Link Aggregation Control Protocol (LACP) policies.

- You cannot fall back to the previous version of LACP after upgrading to enhanced LACP.
- You cannot downgrade to a version of Cisco Application Policy Infrastructure Controller (APIC) earlier than 3.2(7) without removing the enhanced LACP configuration. See the procedure Remove the Enhanced LACP Configuration Before a Downgrade, on page 16 in this guide.
- Cisco Application Centric Infrastructure (ACI) Virtual Edge, VXLAN mode traffic always uses the source IP address as the TEP IP address. To ensure proper load balancing, we recommend the algorithm **Source and Destination TCP/UDP Port**.

Create LAGs for DVS Uplink Port Groups Using the Cisco APIC GUI

Improve distributed virtual switch (DVS) uplink port group load balancing by putting the port groups into link aggregation groups (LAGs) and associating them with specific load-balancing algorithms. You can perform this task using the Cisco Application Policy Infrastructure Controller (APIC) GUI.

Before you begin

- You must have created a VMware vCenter virtual machine manager (VMM) domain for VMware VDS or Cisco Application Centric Infrastructure (ACI) Virtual Edge.
- If a vSwitch policy container does not exist, create one.

Procedure

Step 1 Log into the Cisco APIC.

Step 2 Go to **Virtual Networking** > **Inventory** > **VMM Domains** > **VMware** > ***domain*** .

Step 3 In the work pane, choose **Policy** > **VSwitch Policy**.

Step 4 If you have not already done so, in the **Properties** area, choose a policy.

Step 5 In the **Enhanced LAG Policy** area, click the **+** (plus) icon and then complete the following steps:

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

b) From the **Mode** drop-down list, choose **LACP Active** or **LACP Passive**.

c) From the **Load Balancing Mode** drop-down list, choose a load-balancing method.

d) In the **Number of Links** selector, choose how many DVS uplink port groups to include in the LAG.

You can put two to eight uplink port groups into a LAG.

e) Click **Update** and then click **Submit**.

Step 6 Repeat Step 5 to create other LAGs for the DVS.

What to do next

If you are using VMware VDS, associate endpoint groups (EPGs) to the domain with the enhanced LACP policy. If you are using Cisco Application Centric Infrastructure (ACI) Virtual Edge, associate internally created inside and outside port groups with the enhanced LACP policy, then associate EPGs to the domain with the policy.

Create LAGs for DVS Uplink Port Groups Using the NX-OS Style CLI

Improve distributed virtual switch (DVS) uplink port group load balancing by putting the port groups into link aggregation groups (LAGs) and associating them with specific load-balancing algorithms. You can perform this task using the NX-OS style CLI.

Before you begin

You must have created a VMware vCenter virtual machine manager (VMM) domain for VMware VDS or Cisco Application Centric Infrastructure (ACI) Virtual Edge.

Procedure

Create or delete an enhanced LACP policy.

Example:

```
apic1(config-vmware)# enhancedlacp  LAG name
apic1(config-vmware-enhancedlacp)# lbmode loadbalancing mode
apic1(config-vmware-enhancedlacp)# mode mode
apic1(config-vmware-enhancedlacp)# numlinks max number of uplinks
apic1(config-vmware)# no enhancedlacp LAG name to delete
```

What to do next

If you are using VMware VDS, associate endpoint groups (EPGs) to the domain with the enhanced LACP policy. If you are using Cisco Application Centric Infrastructure (ACI) Virtual Edge, associate internally created inside and outside port groups with the enhanced LACP policy, then associate EPGs to the domain with the policy.

Create LAGs for DVS Uplink Port Groups Using REST API

Improve distributed virtual switch (DVS) uplink port group load balancing by putting the port groups into link aggregation groups (LAGs) and associating them with specific load-balancing algorithms. You can perform this task using REST API.

Before you begin

You must have created a VMware vCenter virtual machine manager (VMM) domain for VMware VDS or Cisco Application Centric Infrastructure (ACI) Virtual Edge.

Procedure

Step 1 Create the the LAG and associate it with a load-balancing algorithm.

Example:

```
<polUni>
<vmmProvP vendor="VMware">
    <vmmDomP name="mininetlacpavs">
        <vmmVSwitchPolicyCont>
            <lacpEnhancedLagPol name="lag2" mode="passive" lbmode="vlan" numLinks="4">
            </lacpEnhancedLagPol>
        </vmmVSwitchPolicyCont>
```

```
    </vmmDomP>
</vmmProvP>
</polUni>
```

Step 2 Repeat the step to create other LAGs for the DVS.

What to do next

If you are using VMware VDS, associate endpoint groups (EPGs) to the domain with the enhanced LACP policy. If you are using Cisco Application Centric Infrastructure (ACI) Virtual Edge, associate internally created inside and outside port groups with the enhanced LACP policy, then associate EPGs to the domain with the policy.

Associate Application EPGs to VMware vCenter Domains with Enhanced LACP Policies Using the Cisco APIC GUI

Associate application endpoint groups (EPGs) with the VMware vCenter domain with LAGs and a load-balancing algorithm. You can perform this task using the Cisco Application Policy Infrastructure Controller (APIC) GUI.

Before you begin

You must have created link aggregation groups (LAGs) for distributed virtual switch (DVS) uplink port groups and associated a load-balancing algorithm to the LAGs.

Note This procedure assumes that you have not yet associated an application EPG with a VMware vCenter domain. If you have already done so, you edit the domain association.

Procedure

Step 1 Log into Cisco APIC.

Step 2 Go to **Tenants** > ***tenant*** > **Application Profiles** > ***application_profile*** > **Application EPGs** > ***EPG*** > **Domains (VMs and Bare-Metals)**.

Step 3 Right-click **Domains (VMs and Bare-Metals)** and choose **Add VMM Domain Association**.

Step 4 In the **Add VMM Domain Association** dialog box, complete the following steps:

a) From the **VMM Domain Profile** drop-down list, choose the domain that you want to associate the EPG to.

b) From the **Enhanced Lag Policy**, choose the policy configured for the domain that you want to apply to the EPG.

c) (Optional) In the **Delimiter** field, enter one of the following: **|**, **~**, **!**, **@**, **^**, **+**, or **=**.

If you do not enter a symbol, the system default **|** delimiter will appear in the policy.

d) Add remaining values as desired for the domain association, and then click **Submit**.

Step 5 Repeat Step 2 through Step 4 for other application EPGs in the tenant as desired.

Associate Application EPGs to VMware vCenter Domains with Enhanced LACP Policies Using the NX-OS Style CLI

Associate application endpoint groups (EPGs) with the VMware vCenter domain with LAGs and a load-balancing algorithm. You can perform this task using NX-OS style CLI. You can also deassociate application EPGs from the domain.

Before you begin

You must have created link aggregation groups (LAGs) for distributed virtual switch (DVS) uplink port groups and associated a load-balancing algorithm to the LAGs.

Procedure

Step 1 Associate an application EPG with the domain or deassociate it from the domain.

Example:

```
apic1(config-tenant-app-epg-domain)#  lag-policy name of the LAG policy to associate
apic1(config-tenant-app-epg-domain)# no  lag-policy name of the LAG policy to deassociate
```

Step 2 Repeat Step 1 for other application EPGs in the tenant as desired.

Associate Application EPGs to VMware vCenter Domains with Enhanced LACP Policies Using REST API

Associate application endpoint groups (EPGs) with the VMware vCenter domain with LAGs and a load-balancing algorithm. You can perform this task using REST API. You can also deassociate application EPGs from the domain.

Before you begin

You must have created link aggregation groups (LAGs) for distributed virtual switch (DVS) uplink port groups and associated a load-balancing algorithm to the LAGs.

Procedure

Step 1 Associate an EPG to a VMware vCenter domain with LAGs associated to a load-balancing algorithm.

Example:

```
<polUni>
  <fvTenant
    dn="uni/tn-coke"
    name="coke">
    <fvCtx name="cokectx"/>
    <fvAp
      dn="uni/tn-coke/ap-sap"
      name="sap">
      <fvAEPg
        dn="uni/tn-coke/ap-sap/epg-web3"
        name="web3" >
          <fvRsBd tnFvBDName="cokeBD2" />
```

```
            <fvRsDomAtt resImedcy="immediate" switchingMode="native"
              tDn="uni/vmmp-VMware/dom-mininetlacpavs">
              <fvAEPgLagPolAtt >
                <fvRsVmmVSwitchEnhancedLagPol
tDn="uni/vmmp-VMware/dom-mininetlacpavs/vswitchpolcont/enlacplagp-lag2"/>
              </fvAEPgLagPolAtt>
            </fvRsDomAtt>
      </fvAEPg>
    </fvAp>
  </fvTenant>
</polUni>
```

Step 2 Repeat Step 1 for other application EPGs in the tenant, as desired.

Remove the Enhanced LACP Configuration Before a Downgrade

Before you downgrade Cisco Application Policy Infrastructure Controller (APIC) to a release earlier than 3.2(7), you must remove the enhanced LACP configuration. Complete the steps in this procedure to remove the configuration.

Procedure

Step 1 Reassign uplinks on all ESXi hosts from link aggregation groups (LAGs) to normal uplinks.

Step 2 Remove LAG associations from all EPGs associated with the distributed virtual switch (DVS).

You can expect traffic loss while performing this step.

Step 3 Change port channel settings to static channel or MAC pinning, which will cause traffic to recover once the port channel is up.

Step 4 Remove all LAG-related configuration from the virtual machine manager (VMM).

Step 5 Verify that all LAG-related policies are deleted from VMware vCenter.

What to do next

Downgrade to a Cisco APIC release earlier than 4.0(1).

Endpoint Retention Configuration

After you create a vCenter domain, you can configure endpoint retention. This feature enables you to delay the deletion of an endpoint, reducing the chances of dropped traffic.

You configure endpoint retention in the APIC GUI or with the NX-OS style CLI or the REST API. For information, see the following sections in this guide:

- Configuring Endpoint Retention Using the GUI, on page 17
- Configure Endpoint Retention Using the NX-OS Style CLI, on page 17
- Configuring Endpoint Retention Using the REST API, on page 33

Configuring Endpoint Retention Using the GUI

Before you begin

You must have created a vCenter domain.

Procedure

Step 1 Log in to Cisco APIC.

Step 2 Choose **VM Networking** > **Inventory**.

Step 3 In the left navigation pane, expand the **VMware** folder and then click the vCenter domain that you created earlier.

Step 4 In the central **Domain** work pane, make sure that the **Policy** and **General** tabs are selected.

Step 5 In the **End Point Retention Time (seconds)** counter, choose the number of seconds to retain endpoints before they are detached.

You can choose between 0 and 600 seconds. The default is 0.

Step 6 Click **Submit**.

Configure Endpoint Retention Using the NX-OS Style CLI

Before you begin

You must have created a vCenter domain.

Procedure

Step 1 In the CLI, enter configuration mode:

Example:

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

Step 2 Configure a retention time for detached endpoints:

You can choose a delay of between 0 and 600 seconds. The default is 0.

Example:

```
apic1(config)# vmware-domain <domainName>

apic1(config-vmware)# ep-retention-time <value>
```

Creating VDS Uplink Port Groups

Each VMM domain appears in the vCenter as a vSphere Distributed Switch (VDS). The virtualization administrator associates hosts to the VDS created by the APIC and selects which vmnics to use for the specific VDS. The configuration of the VDS uplinks are performed from the APIC controller by changing the vSwitch configuration from the Attach Entity Profile (AEP) that is associated with the VMM domain. You can find the AEP in the APIC GUI in the Fabric Access Policies configuration area.

Note When working with ACI and vSphere VMM integration, Link Aggregation Groups (LAGs) are not a supported method of creating interface teams on distributed switches created by the APIC. The APIC pushes the necessary interface teaming configuration based on the settings in the Interface Policy Group and/or AEP vSwitch policy. It is not supported or required to manually create interface teams in vCenter.

Creating a Trunk Port Group

Creating a Trunk Port Group Using the GUI

This section describes how to create a trunk port group using the GUI.

Before you begin

- Trunk port group must be tenant independent.

Procedure

Step 1 Log in to the APIC GUI.

Step 2 On the menu bar, choose **Virtual Networking**.

Step 3 In the navigation pane, choose **VMM Domains** > **VMware** > **Domain_name** > **Trunk Port Groups** and right-click **Create Trunk Port Group**.

Step 4 In the **Create Trunk Port Group** dialog box, perform the following actions:

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

b) For the **Promiscuous Mode** buttons, click either **Disabled** or **Enabled**. The default is **Disabled**.

c) For the **Trunk Portgroup Immediacy** buttons, click either **Immediate** or **On Demand**. The default is **On Demand**.

d) For the **MAC changes** buttons, click either **Disabled** or **Enabled**. The default is **Enabled**.

e) For the **Forged transmits** buttons, click either **Disabled** or **Enabled**. The default is **Enabled**.

f) In the **VLAN Ranges** field, choose the **+** icon and enter the VLAN range (vlan-100 vlan-200).

Note If you do not specify a VLAN Range, the VLAN list will be taken from the domain's VLAN namespace.

g) Click **Update**.

Step 5 Click **Submit**.

Creating a Trunk Port Group Using the NX-OS Style CLI

This section describes how to create a trunk port group using the NX-OS Style CLI.

Before you begin

- Trunk port groups must be tenant independent.

Procedure

Step 1 Go to the vmware-domain context, enter the following command:

Example:

```
apic1(config-vmware)# vmware-domain ifav2-vcenter1
```

Step 2 Create a trunk port group, enter the following command:

Example:

```
apic1(config-vmware)# trunk-portgroup trunkpg1
```

Step 3 Enter the VLAN range:

Example:

```
apic1(config-vmware-trunk)# vlan-range 2800-2820, 2830-2850
```

Note If you do not specify a VLAN range, the VLAN list will be taken from the domain's VLAN namespace.

Step 4 The mac changes is accept by default. If you choose to not to accept the mac changes, enter the following command:

Example:

```
apic1(config-vmware-trunk)# no mac-changes accept
```

Step 5 The forged transmit is accept by default. If you choose to not to accept the forged transmit, enter the following command:

Example:

```
apic1(config-vmware-trunk)# no forged-transmit accept
```

Step 6 The promiscuous mode is disable by default. If you choose to enable promiscuous mode on the trunk port group:

Example:

```
apic1(config-vmware-trunk)# allow-promiscuous enable
```

Step 7 The trunk port group immediacy is set to on-demand by default. If you want to enable immediate immediacy, enter the following command:

Example:

```
apic1(config-vmware-trunk)# immediacy-immediate enable
```

Step 8 Show the VMware domain:

Example:

```
apic1(config-vmware)# show vmware domain name mininet
Domain Name                          : mininet
Virtual Switch Mode                  : VMware Distributed Switch
Switching Encap Mode                 : vlan
Vlan Domain                          : mininet (2800-2850, 2860-2900)
Physical Interfaces                  :
Number of EPGs                       : 2
Faults by Severity                   : 0, 2, 4, 0
LLDP override                        : no
CDP override                         : no
Channel Mode override                : no

vCenters:
Faults: Grouped by severity (Critical, Major, Minor, Warning)
 vCenter               Type      Datacenter            Status    ESXs   VMs    Faults

 --------------------  --------  --------------------  --------  -----  -----  ---------------

 172.22.136.195        vCenter   mininet               online    2      57     0,0,4,0


Trunk Portgroups:
 Name                                          VLANs

 --------------------------------------------  --------------------------------------------

 epgtr1                                        280-285

 epgtr2                                        280-285

 epgtr3                                        2800-2850


apic1(config-vmware)# show vmware domain name mininet trunk-portgroup

 Name                           Aggregated EPG
 -----------------------------  ---------------------------------------------
 epgtr1                         test|wwwtestcom3|test830
 epgtr2
 epgtr3                         test|wwwtestcom3|test830
                                test|wwwtestcom3|test833


apic1(config-vmware)# )# show vmware domain name ifav2-vcenter1 trunk-portgroup name trunkpg1
Name                           Aggregated EPG                 Encap
 -----------------------------  -----------------------------  ------------
 trunkpg1                       LoadBalance|ap1|epg1           vlan-318
                                LoadBalance|ap1|epg2           vlan-317
                                LoadBalance|ap1|failover-epg   vlan-362
                                SH:l3I:common:ASAv-HA:test-    vlan-711
                                rhi|rhiExt|rhiExtInstP
                                SH:l3I:common:ASAv-HA:test-    vlan-712
                                rhi|rhiInt|rhiIntInstP
                                test-dyn-ep|ASA_FWctxctx1bd-   vlan-366
                                inside|int
                                test-dyn-ep|ASA_FWctxctx1bd-   vlan-888
                                inside1|int
                                test-dyn-ep|ASA_FWctxctx1bd-   vlan-365
                                outside|ext
```

```
test-dyn-ep|ASA_FWctxctx1bd-    vlan-887
outside1|ext
test-inb|FW-Inbctxtrans-        vlan-886
vrfinside-bd|int
test-inb|FW-Inbctxtrans-        vlan-882
vrfoutside-bd|ext
test-inb|inb-ap|inb-epg         vlan-883
test-pbr|pbr-ap|pbr-cons-epg    vlan-451
test-pbr|pbr-ap|pbr-prov-epg    vlan-452
test1|ap1|epg1                  vlan-453
test1|ap1|epg2                  vlan-485
test1|ap1|epg3                  vlan-454
test2-scale|ASA-                vlan-496
Trunkctxctx1bd-inside1|int
test2-scale|ASA-                vlan-811
Trunkctxctx1bd-inside10|int
```

```
apic1(config-vmware)# show running-config vmware-domain mininet
# Command: show running-config vmware-domain mininet
# Time: Wed May 25 21:09:13 2016
  vmware-domain mininet
    vlan-domain member mininet type vmware
    vcenter 172.22.136.195 datacenter mininet
      exit
    configure-dvs
      exit
    trunk-portgroup epgtr1 vlan 280-285
    trunk-portgroup epgtr2 vlan 280-285
    trunk-portgroup epgtr3 vlan 2800-2850
    exit
```

Creating a Trunk Port Group Using the REST API

This section describes how to create a trunk port group using the REST API.

Before you begin

- Trunk port groups must be tenant independent.

Procedure

Create a trunk port group:

Example:

```
<vmmProvP vendor="VMware">
 <vmmDomP name=”DVS1">
  <vmmUsrAggr name="EPGAggr_1">
   <fvnsEncapBlk name="blk0" from="vlan-100” to="vlan-200"/>
  </vmmUsrAggr>
```

```
 </vmmDomP>
</vmmProvP>
```

Working with Blade Servers

Guidelines for Cisco UCS B-Series Servers

When integrating blade server systems into Cisco ACI for purposes of VMM integration (for example, integrating Cisco UCS blade servers or other non-Cisco blade servers) you must consider the following guidelines:

Note This example shows how to configure a port channel access policy for integrating Cisco UCS blade servers. You can use similar steps to set up a virtual port channel or individual link access policies depending upon how your Cisco UCS blade server uplinks are connected to the fabric. If no port channel is explicitly configured on the APIC for the UCS blade server uplinks, the default behavior will be mac-pinning.

- The VM endpoint learning relies on either the CDP or LLDP protocol. If supported, CDP must be enabled all the way from the leaf switch port through any blade switches and to the blade adapters.
- Ensure the management address type, length, and value (TLV) is enabled on the blade switch (CDP or LLDP protocol) and advertised towards servers and fabric switches. Configuration of management TLV address must be consistent across CDP and LLDP protocols on the blade switch.
- The APIC does not manage fabric interconnects and the blade server, so any UCS specific policies such as CDP or port channel policies must be configured from the UCS Manager.
- VLANs defined in the VLAN pool used by the attachable access entity profile on the APIC, must also be manually created on the UCS and allowed on the appropriate uplinks connecting to the fabric. This must include the infrastructure VLAN if applicable. For details, see the *Cisco UCS Manager GUI Configuration Guide*.
- When you are working with the Cisco UCS B-series server and using an APIC policy, Link Layer Discovery Protocol (LLDP) is not supported.
- Cisco Discovery Protocol (CDP) is disabled by default in Cisco UCS Manager. In Cisco UCS Manager, you must enable CDP by creating a Network Control Policy.
- Do not enable fabric failover on the adapters in the UCS server service profiles. Cisco recommends that you allow the hypervisor to handle failover at the virtual switch layer so that load balancing of traffic is appropriately performed.

Note Symptom: The change of management IP of the unmanaged node such as blade switch or fabric interconnect gets updated in the VMware vCenter, but the VMware vCenter does not send any events to APIC.

Condition: This causes the APIC to be out of sync with VMware vCenter.

Workaround: You need to trigger an inventory pull for the VMware vCenter controller that manages ESX servers behind the unmanaged node.

Setting up an Access Policy for a Blade Server Using the GUI

Before you begin

To operate with the Cisco APIC, the Cisco UCS Fabric Interconnect must be at least a version 2.2(1c). All components, such as the BIOS, CIMC, and the adapter must be a version 2.2(1c) or later. For further details, see the *Cisco UCS Manager CLI Configuration Guide*.

Procedure

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

Step 2 In the navigation pane, click **Quick Start**.

Step 3 In the central pane, click **Configure an interface, PC, and VPC**.

Step 4 In the **Configure Interface, PC, and VPC** dialog box, click the **+** icon to select switches.

Step 5 In the **Switches** field, from the drop-down list, choose the desired switch IDs.

Step 6 Click the **+** icon to configure the switch interfaces.

Step 7 In the **Interface Type** field, click the **VPC** radio button.

Step 8 In the **Interfaces** field, enter the appropriate interface or interface range that is connected to the blade server.

Step 9 In the **Interface Selector Name** field, enter a name.

Step 10 From the **CDP Policy** drop-down list, choose default

The default CDP policy is set to disabled. (Between the leaf switch and the blade server, CDP must be disabled.)

Step 11 From the **LLDP Policy** drop-down list, choose default.

The default LLDP policy is set to enabled for the receive and transmit states. (Between the leaf switch and the blade server, LLDP must be enabled.)

Step 12 From the **LACP Policy** drop-down list, choose **Create LACP Policy**.

Between the leaf switch and the blade server, the LACP policy must be set to active.

Step 13 In the **Create LACP Policy** dialog box, perform the following actions:

a) In the **Name** field, enter a name for the policy.
b) In the **Mode** field, the **Active** radio button is checked.
c) Keep the remaining default values and click **Submit**.

Step 14 From the **Attached Device Type** field drop-down list, choose ***ESX Hosts*** .

Step 15 In the **Domain Name** field, enter a name as appropriate.

Step 16 In the **VLAN Range** field, enter the range.

Step 17 In the **vCenter Login Name** field, enter the login name.

Step 18 In the **Password** field, and the **Confirm Password** field, enter the password.

Step 19 Expand the **vCenter** field, and in the **Create vCenter Controller** dialog box, enter the desired content and click **OK**.

Step 20 In the **vSwitch Policy** field, perform the following actions:

Between the blade server and the ESX hypervisor, CDP must be enabled, LLDP must be disabled, and LACP must be disabled so Mac Pinning must be set.

a) Check the **MAC Pinning** check box.
b) Check the **CDP** check box.
c) Leave the **LLDP** check box unchecked because LLDP must remain disabled.

Step 21 Click **Save**, and click **Save** again. Click **Submit**.
The access policy is set.

Troubleshooting the Cisco ACI and VMware VMM System Integration

For troubleshooting information, see the following links:

- Cisco APIC Troubleshooting Guide
- ACI Troubleshooting Book

Additional Reference Sections

Custom User Account with Minimum VMware vCenter Privileges

Setting VMware vCenter privileges allows the Cisco Application Policy Infrastructure Controller (APIC) to send VMware API commands to VMware vCenter for the creation of the DVS/Cisco Application Virtual Switch (AVS). Setting privileges also allows Cisco APIC to create the VMK interface (AVS), publish port groups, and relay all necessary alerts.

To configure the VMware vCenter from Cisco APIC, your credentials must allow the following minimum set of privileges within the VMware vCenter:

- **Alarms**

  Cisco APIC creates two alarms in the folder, one for DVS and another for port-group. The alarm is raised when the EPG or Domain policy is deleted on Cisco APIC. However, the alarms cannot be deleted for DVS or port-group because of the virtual machines (VMs) that are attached.

- **Distributed Switch**
- **dvPort Group**

- **Folder**
- **Network**

  Cisco APIC manages the network settings such as add or delete port-groups, setting host/DVS MTU, LLDP/CDP, LACP.

- **Host**

  If you use Cisco AVS, in addition to the already listed privileges, you need Host privileges on the data center where Cisco APIC creates the DVS.

  - **Host.Configuration.Advanced settings**
  - **Host.Local operations.Reconfigure virtual machine**
  - **Host.Configuration.Network configuration**

    This privilege is needed for Cisco AVS and the auto-placement feature for virtual Layer 4 to Layer 7 Service VMs. For Cisco AVS, APIC creates the VMK interface and places it in the 'vtep' port-group, which is used for OpFlex.

- **Virtual machine**

  If you use Service Graph in addition to the already listed privileges, you need the **Virtual machine** privilege for the virtual appliances that are used for Service Graph.

  - **Virtual machine.Configuration.Modify device settings**
  - **Virtual machine.Configuration.Settings**

If you want to deploy service VMs using the service VM orchestration feature, enable the following privileges in addition to the preceding privileges.

For information about the feature, see the "Service VM Orchestration" chapter of the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide* .

- **Datastore**
  - **Allocate space**
  - **Browse datastore**
  - **Low level file operations**
  - **Remove file**
- **Host**
  - **Local operations.Delete virtual machine**
  - **Local operations.Reconfigure virtual machine**
- **Resource**
  - **Assign virtual machine to resource pool**
- **Virtual machine**

- **Inventory.Create new**
- **Inventory.Create from existing**
- **Inventory.Remove**
- **Configuration.Add new disk**
- **Provisioning.Deploy template**
- **Provisioning.Clone template**
- **Provisioning.Clone virtual machine**
- **Provisioning.Customize**
- **Interaction (all)**

- **Global**
  - **Manage Custom Attributes**
  - **Set Custom Attribute**

Quarantine Port Groups

The quarantine port group feature provides a method to clear port group assignments under certain circumstances. In the VMware vCenter, when a VMware vSphere Distributed Switch (VDS) is created, a quarantine port group is created in the VDS by default. The quarantine port group default policy is to block all ports.

As part of integration with Layer 4 to Layer 7 virtual service appliances, such as a load balancer or firewall, the Application Policy Infrastructure Controller (APIC) creates service port groups in vCenter for service stitching and orchestrates placement of virtual appliances, such as service virtual machines (VMs), in these service port groups as part of the service graph rendering mechanism. When the service graph is deleted, the service VMs are automatically moved to the quarantine port group. This auto-move to a quarantine port group on delete is only done for service VMs, which are orchestrated by the APIC.

You can take further action with the port in quarantine port group as desired. For example, you can migrate all of the ports from the quarantine port group to another port group, such as a VM network.

The quarantine port group mechanism is not applicable to regular tenant endpoint groups (EPGs) and their associated port groups and tenant VMs. Therefore, if the tenant EPG is deleted, any tenant VMs present in the associated port group remains intact and they will not be moved to the quarantine port group. The placement of tenant VMs into the tenant port group is outside the realm of the APIC.

On-Demand VMM Inventory Refresh

Triggered Inventory provides a manual trigger option to pull and refresh Cisco Application Policy Infrastructure Controller (APIC) inventory from the virtual machine manager (VMM) controller. It is not required in normal scenarios. Use it with discretion only when errors occur.

When there is a process restart, leadership change, or background periodic 24-hour inventory audit, Cisco APIC pulls inventory to keep VMM inventory aligned with the VMM controller inventory. At certain times, VMware vCenter APIs can error out, and Cisco APIC may not have fully downloaded the inventory from the

VMware vCenter despite retries. Cisco APIC indicates this condition with a user-visible fault. In this case, triggered inventory allows you to start an inventory pull from the Cisco APIC VMM to the VMware vCenter.

Cisco APIC does not maintain any synchronization between the VMM configuration and the VMware vCenter VDS configuration. If you directly change VDS settings from the VMware vCenter, Cisco APIC does not try to overwrite the user settings (except for PVLAN configuration).

Physically Migrating the ESXi Host

Complete the tasks in this procedure to physically migrate ESXi hosts.

Procedure

Step 1 Put the host into maintenance mode or evacuate the virtual machine (VM) workload by another method.

Step 2 Remove the ESXi host from the VMware VDS, Cisco Application Centric Infrastructure (ACI) Virtual Edge, or Cisco Application Virtual Switch.

Step 3 Physically recable the ESXi host to the new leaf switch or pair of leaf switches

Step 4 Add the ESXi host back to the VMware VDS, Cisco Application Centric Infrastructure (ACI) Virtual Edge, or Cisco Application Virtual Switch.

Guidelines for Migrating a vCenter Hypervisor VMK0 to an ACI Inband VLAN

Follow the guidelines below to migrate the default vCenter hypervisor VMK0 out of bound connectivity to ACI inband ports. An ACI fabric infrastructure administrator configures the APIC with the necessary policies, then the vCenter administrator migrates the VMK0 to the appropriate ACI port group.

Create the Necessary Management EPG Policies in APIC

As an ACI fabric infrastructure administrator, use the following guidelines when creating the management tenant and VMM domain policies:

- Choose a VLAN to use for ESX management.
- Add the VLAN chosen for ESX management to a range (or Encap Block) in the VLAN pool associated with the target VMM domain. The range where this VLAN is added must have allocation mode set to static allocation.
- Create a management EPG in the ACI management tenant (mgmt).
- Verify that the bridge domain associated with the management EPG is also associated with the private network (inb).
- Associate the management EPG with the target VMM domain as follows:
    - Use resolution immediacy as pre-provision.
    - Specify the management VLAN in the Port Encap field of the VM domain profile association.

As a result, APIC creates the port group under vCenter with VLAN specified by the user. APIC also automatically pushes the policies on the leaf switches associated with the VMM domain and Attach Entity Profile (AEP).

Migrate the VMK0 to the Inband ACI VLAN

By default vCenter configures the default VMK0 on the hypervisor management interface. The ACI polices created above enable the vCenter administrator to migrate the default VMK0 to the port group that is created by APIC. Doing so frees up the hypervisor management port.

REST API Tasks

This section shows how to perform tasks using REST API.

- For references to GUI tasks, refer to sections, Creating a VMM Domain Profile, on page 5 and Setting up an Access Policy for a Blade Server Using the GUI, on page 23.
- For references to NX-OS Style CLI tasks, refer to NX-OS Style CLI Tasks, on page 35.

Creating a vCenter Domain Profile Using the REST API

Procedure

Step 1 Configure a VMM domain name, a controller, and user credentials.

Example:

```
 POST URL: https://<api-ip>/api/node/mo/.xml

<polUni>
<vmmProvP vendor="VMware">
<!-- VMM Domain -->
<vmmDomP name="productionDC">
<!-- Association to VLAN Namespace -->
<infraRsVlanNs tDn="uni/infra/vlanns-VlanRange-dynamic"/>
<!-- Credentials for vCenter -->
<vmmUsrAccP name="admin" usr="administrator" pwd="admin" />
<!-- vCenter IP address -->
<vmmCtrlrP name="vcenter1" hostOrIp="<vcenter ip address>" rootContName="<Datacenter Name
in vCenter>">
<vmmRsAcc tDn="uni/vmmp-VMware/dom-productionDC/usracc-admin"/>
</vmmCtrlrP>
</vmmDomP>
</vmmProvP>
```

Example:

```
<polUni>
<vmmProvP vendor="VMware">
    <vmmDomP name="mininet" delimiter="@" >
   </vmmDomP>
</vmmProvP>
</polUni>
```

Step 2 Create an attachable entity profile for VLAN namespace deployment.

Example:

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml
<infraInfra>
<infraAttEntityP name="profile1">
<infraRsDomP tDn="uni/vmmp-VMware/dom-productionDC"/>
</infraAttEntityP>
</infraInfra>
```

Step 3 Create an interface policy group and selector.

Example:

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml

<infraInfra>
    <infraAccPortP name="swprofile1ifselector">
        <infraHPortS name="selector1" type="range">
            <infraPortBlk name="blk"
             fromCard="1" toCard="1" fromPort="1" toPort="3">
            </infraPortBlk>
     <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-group1" />
        </infraHPortS>
    </infraAccPortP>

    <infraFuncP>
        <infraAccPortGrp name="group1">
            <infraRsAttEntP tDn="uni/infra/attentp-profile1" />
        </infraAccPortGrp>
    </infraFuncP>
</infraInfra>
```

Step 4 Create a switch profile.

Example:

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml

<infraInfra>
    <infraNodeP name="swprofile1">
        <infraLeafS name="selectorswprofile11718" type="range">
            <infraNodeBlk name="single0" from_="101" to_="101"/>
            <infraNodeBlk name="single1" from_="102" to_="102"/>
        </infraLeafS>
        <infraRsAccPortP tDn="uni/infra/accportprof-swprofile1ifselector"/>
    </infraNodeP>
</infraInfra>
```

Step 5 Configure the VLAN pool.

Example:

```
 POST URL: https://<apic-ip>/api/node/mo/.xml

<polUni>
<infraInfra>
<fvnsVlanInstP name="VlanRange" allocMode="dynamic">
   <fvnsEncapBlk name="encap" from="vlan-100" to="vlan-400"/>
</fvnsVlanInstP>
</infraInfra>
</polUni>
```

Step 6 Locate all the configured controllers and their operational state.

Example:

```
GET:
https://<apic-ip>/api/node/class/compCtrlr.xml?
<imdata>
<compCtrlr apiVer="5.1" ctrlrPKey="uni/vmmp-VMware/dom-productionDC/ctrlr-vcenter1"
deployIssues="" descr="" dn="comp/prov-VMware/ctrlr-productionDC-vcenter1" domName="
productionDC"
hostOrIp="esx1" mode="default" model="VMware vCenter Server 5.1.0 build-756313"
name="vcenter1" operSt="online" port="0" pwd="" remoteOperIssues="" scope="vm"
usr="administrator" vendor="VMware, Inc." ... />
</imdata>
```

Step 7 Locate the hypervisor and VMs for a vCenter with the name 'vcenter1' under a VMM domain called 'ProductionDC'.

Example:

```
GET:
https://<apic-ip>/api/node/mo/comp/prov-VMware/ctrlr-productionDC-vcenter1.xml?query-target=children

<imdata>
<compHv descr="" dn="comp/prov-VMware/ctrlr-productionDC-vcenter1/hv-host-4832" name="esx1"
state="poweredOn" type="hv" ... />
<compVm descr="" dn="comp/prov-VMware/ctrlr-productionDC-vcenter1/vm-vm-5531" name="AppVM1"
state="poweredOff" type="virt" .../>
<hvsLNode dn="comp/prov-VMware/ctrlr-productionDC-vcenter1/sw-dvs-5646" lacpEnable="yes"
lacpMode="passive" ldpConfigOperation="both" ldpConfigProtocol="lldp" maxMtu="1500"
mode="default" name="apicVswitch" .../>
</imdata>
```

Step 8 (Optional) Configure a retention time for detached endpoints:

You can choose a delay of between 0 and 600 seconds. The default is 0 seconds.

Example:

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml
<vmmProvP vendor="VMware" >
<vmmDomP name="mininetavs" mode="n1kv" enfPref="sw" epRetTime=”60”>
<infraRsVlanNs tDn="uni/infra/vlanns-inst-dynamic"/>
<vmmUsrAccP
name="defaultAccP"
usr="administrator"
pwd="admin"
/>
</vmmDomP>
</vmmProvP>
```

Creating a Read-Only VMM Domain Using the REST API

You can use REST API to create a read-only VMM domain.

Before you begin

- Fulfill the prerequisites in the section Prerequisites for Creating a VMM Domain Profile, on page 6.
- In the VMware vCenter, ensure that under the **Networking** tab, the VDS is contained by a folder.

Also ensure that the folder and the VDS have the exact same name of the read-only VMM domain that you plan to create.

Procedure

Step 1 Configure a VMM domain name, a controller, and user credentials.

Example:

```
POST URL: https://<api-ip>/api/node/mo/.xml
<polUni>
<vmmProvP vendor="VMware">
<!-- VMM Domain -->
<vmmDomP name="productionDC" accessMode="read-only">
<!-- Association to VLAN Namespace -->
<infraRsVlanNs tDn="uni/infra/vlanns-VlanRange-dynamic"/>
<!-- Credentials for vCenter -->
<vmmUsrAccP name="admin" usr="administrator" pwd="admin" />
<!-- vCenter IP address -->
<vmmCtrlrP name="vcenter1" hostOrIp="<vcenter ip address>" rootContName="<Datacenter Name
in vCenter>">
<vmmRsAcc tDn="uni/vmmp-VMware/dom-productionDC/usracc-admin"/>
</vmmCtrlrP>
</vmmDomP>
</vmmProvP>
```

Example:

```
<polUni>
<vmmProvP vendor="VMware">
    <vmmDomP name="mininet" delimiter="@" >
   </vmmDomP>
</vmmProvP>
</polUni>
```

Step 2 Create an attachable entity profile for VLAN namespace deployment.

Example:

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml
<infraInfra>
<infraAttEntityP name="profile1">
<infraRsDomP tDn="uni/vmmp-VMware/dom-productionDC"/>
</infraAttEntityP>
</infraInfra>
```

Step 3 Create an interface policy group and selector.

Example:

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml

<infraInfra>
    <infraAccPortP name="swprofile1ifselector">
        <infraHPortS name="selector1" type="range">
            <infraPortBlk name="blk"
             fromCard="1" toCard="1" fromPort="1" toPort="3">
            </infraPortBlk>
     <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-group1" />
        </infraHPortS>
    </infraAccPortP>
```

```
    <infraFuncP>
        <infraAccPortGrp name="group1">
            <infraRsAttEntP tDn="uni/infra/attentp-profile1" />
        </infraAccPortGrp>
    </infraFuncP>
</infraInfra>
```

Step 4 Create a switch profile.

Example:

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml

<infraInfra>
    <infraNodeP name="swprofile1">
        <infraLeafS name="selectorswprofile11718" type="range">
            <infraNodeBlk name="single0" from_="101" to_="101"/>
            <infraNodeBlk name="single1" from_="102" to_="102"/>
        </infraLeafS>
        <infraRsAccPortP tDn="uni/infra/accportprof-swprofile1ifselector"/>
    </infraNodeP>
</infraInfra>
```

Step 5 Configure the VLAN pool.

Example:

```
 POST URL: https://<apic-ip>/api/node/mo/.xml

<polUni>
<infraInfra>
<fvnsVlanInstP name="VlanRange" allocMode="dynamic">
   <fvnsEncapBlk name="encap" from="vlan-100" to="vlan-400"/>
</fvnsVlanInstP>
</infraInfra>
</polUni>
```

Step 6 Locate all the configured controllers and their operational state.

Example:

```
GET:
https://<apic-ip>/api/node/class/compCtrlr.xml?
<imdata>
<compCtrlr apiVer="5.1" ctrlrPKey="uni/vmmp-VMware/dom-productionDC/ctrlr-vcenter1"
deployIssues="" descr="" dn="comp/prov-VMware/ctrlr-productionDC-vcenter1" domName="
productionDC"
hostOrIp="esx1" mode="default" model="VMware vCenter Server 5.1.0 build-756313"
name="vcenter1" operSt="online" port="0" pwd="" remoteOperIssues="" scope="vm"
usr="administrator" vendor="VMware, Inc." ... />
</imdata>
```

Step 7 Locate the hypervisor and VMs for a vCenter with the name 'vcenter1' under a VMM domain called 'ProductionDC'.

Example:

```
GET:
https://<apic-ip>/api/node/mo/comp/prov-VMware/ctrlr-productionDC-vcenter1.xml?query-target=children

<imdata>
```

```
<compHv descr="" dn="comp/prov-VMware/ctrlr-productionDC-vcenter1/hv-host-4832" name="esx1"
state="poweredOn" type="hv" ... />
<compVm descr="" dn="comp/prov-VMware/ctrlr-productionDC-vcenter1/vm-vm-5531" name="AppVM1"
state="poweredOff" type="virt" .../>
<hvsLNode dn="comp/prov-VMware/ctrlr-productionDC-vcenter1/sw-dvs-5646" lacpEnable="yes"
lacpMode="passive" ldpConfigOperation="both" ldpConfigProtocol="lldp" maxMtu="1500"
mode="default" name="apicVswitch" .../>
</imdata>
```

Step 8 (Optional) Configure a retention time for detached endpoints:

You can choose a delay of between 0 and 600 seconds. The default is 0 seconds.

Example:

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml
<vmmProvP vendor="VMware" >
<vmmDomP name="mininetavs" mode="n1kv" enfPref="sw" epRetTime=”60”>
<infraRsVlanNs tDn="uni/infra/vlanns-inst-dynamic"/>
<vmmUsrAccP
name="defaultAccP"
usr="administrator"
pwd="admin"
/>
</vmmDomP>
</vmmProvP>
```

What to do next

You can attach an EPG to the read-only VMM domain and configure policies for it. However, those policies are not pushed to the VDS in the VMware vCenter.

Configuring Endpoint Retention Using the REST API

Before you begin

You must have configured a vCenter domain.

Procedure

Configure a retention time for detached endpoints:

You can choose a delay of between 0 and 600 seconds. The default is 0 seconds.

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml
<vmmProvP vendor="VMware" >

<vmmDomP name="mininetavs" epRetTime=”60”>
</vmmDomP>
</vmmProvP>
```

Setting Up an Access Policy for a Blade Server Using the REST API

Procedure

Set up an access policy for a blade server.

Example:

```
POST: https://<ip or hostname APIC>/api/node/mo/uni.xml

<polUni>
                <infraInfra>
                <!-- Define LLDP CDP and LACP policies -->
                <lldpIfPol name="enable_lldp" adminRxSt="enabled" adminTxSt="enabled"/>
                <lldpIfPol name="disable_lldp" adminRxSt="disabled" adminTxSt="disabled"/>
                <cdpIfPol name="enable_cdp" adminSt="enabled"/>
                <cdpIfPol name="disable_cdp" adminSt="disabled"/>
<lacpLagPol name='enable_lacp' ctrl='15' descr='LACP' maxLinks='16' minLinks='1'
mode='active'/>
                <lacpLagPol name='disable_lacp' mode='mac-pin'/>


        <!-- List of nodes. Contains leaf selectors. Each leaf selector contains list of
node blocks -->
        <infraNodeP name="leaf1">
                <infraLeafS name="leaf1" type="range">
                <infraNodeBlk name="leaf1" from_="1017" to_="1017"/>
            </infraLeafS>
            <infraRsAccPortP tDn="uni/infra/accportprof-portselector"/>
        </infraNodeP>


        <!-- PortP contains port selectors. Each port selector contains list of ports. It
also has association to port group policies -->
        <infraAccPortP name="portselector">
                <infraHPortS name="pselc" type="range">
               <infraPortBlk name="blk" fromCard="1" toCard="1" fromPort="39" toPort="40">

                </infraPortBlk>
                <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-leaf1_PC"/>
            </infraHPortS>
        </infraAccPortP>

        <!-- FuncP contains access bundle group policies -->
        <infraFuncP>
                <!-- Access bundle group has relation to PC, LDP policies and to attach
entity profile -->
            <infraAccBndlGrp name="leaf1_PC" lagT='link'>
                <infraRsLldpIfPol tnLldpIfPolName="enable_lldp"/>
                <infraRsLacpPol tnLacpLagPolName='enable_lacp'/>
                <infraRsAttEntP tDn="uni/infra/attentp-vmm-FI2"/>
            </infraAccBndlGrp>
        </infraFuncP>

        <!-- AttEntityP has relation to VMM domain -->
        <infraAttEntityP name="vmm-FI2">
                <infraRsDomP tDn="uni/vmmp-VMware/dom-productionDC"/>
            <!-- Functions -->
            <infraProvAcc name="provfunc"/>
            <!-- Policy overrides for VMM -->
            <infraAttPolicyGroup name="attpolicy">
                <!-- RELATION TO POLICIES GO HERE -->
```

```
                <infraRsOverrideCdpIfPol tnCdpIfPolName="enable_cdp"/>
                <infraRsOverrideLldpIfPol tnLldpIfPolName="disable_lldp"/>
                <infraRsOverrideLacpPol tnLacpLagPolName="disable_lacp"/>
            </infraAttPolicyGroup/>
        </infraAttEntityP>

        </infraInfra>
</polUni>

OUTPUT:
<?xml version="1.0" encoding="UTF-8"?>
<imdata></imdata>
```

NX-OS Style CLI Tasks

This section shows how to perform tasks using NX-OS Style CLI.

- For references to GUI tasks, refer to sections, Creating a VMM Domain Profile, on page 5 and Setting up an Access Policy for a Blade Server Using the GUI, on page 23.
- For references to REST API tasks, refer to REST API Tasks, on page 28.

Creating a vCenter Domain Profile Using the NX-OS Style CLI

Before you begin

This section describes how to create a vCenter domain profile using the NX-OS style CLI:

Procedure

Step 1 In the CLI, enter configuration mode:

Example:

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

Step 2 Configure a VLAN domain:

Example:

```
apic1(config)# vlan-domain dom1 dynamic
apic1(config-vlan)# vlan 150-200 dynamic
apic1(config-vlan)# exit
apic1(config)#
```

Step 3 Add interfaces to this VLAN domain. These are the interfaces to be connected to VMware hypervisor uplink ports:

Example:

```
apic1(config)# leaf 101-102
apic1(config-leaf)# interface ethernet 1/2-3
apic1(config-leaf-if)# vlan-domain member dom1
```

```
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

Step 4 Create a VMware domain and add VLAN domain membership:

Example:

```
apic1(config)# vmware-domain vmmdom1
apic1(config-vmware)# vlan-domain member dom1
apic1(config-vmware)#
```

Create the domain with a specific delimiter:

Example:

```
apic1(config)# vmware-domain vmmdom1 delimiter @
```

Step 5 Configure the domain type to DVS:

Example:

```
apic1(config-vmware)# configure-dvs
apic1(config-vmware-dvs)# exit
apic1(config-vmware)#
```

Step 6 (Optional) Configure a retention time for detached endpoints:

You can choose a delay of between 0 and 600 seconds. The default is 0.

Example:

```
apic1(config)# vmware-domain <domainName>

apic1(config-vmware)# ep-retention-time <value>
```

Step 7 Configure a controller in the domain:

Example:

```
apic1(config-vmware)# vcenter 192.168.66.2 datacenter prodDC
apic1(config-vmware-vc)# username administrator
Password:
Retype password:
apic1(config-vmware-vc)# exit
apic1(config-vmware)# exit
apic1(config)# exit
```

Note When configuring the password, you must precede special characters such as '$' or '!' with a backslash ('\$') to avoid misinterpretation by the Bash shell. The escape backslash is necessary only when configuring the password; the backslash does not appear in the actual password.

Step 8 Verify configuration:

Example:

```
apic1# show running-config vmware-domain vmmdom1
# Command: show running-config vmware-domain vmmdom1
# Time: Wed Sep  2 22:14:33 2015
  vmware-domain vmmdom1
    vlan-domain member dom1
    vcenter 192.168.66.2 datacenter prodDC
      username administrator password *****
```

```
configure-dvs
  exit
exit
```

Creating a Read-Only VMM Domain Using the NX-OS Style CLI

You can use the NX-OS style CLI to create a read-only VMM domain.

Before you begin

- Fulfill the prerequisites in the section Prerequisites for Creating a VMM Domain Profile, on page 6.
- In the VMware vCenter, ensure that under the **Networking** tab, the VDS is contained by a folder.

  Also ensure that the folder and the VDS have the exact same name of the read-only VMM domain that you plan to create.

Procedure

Step 1 In the CLI, enter configuration mode:

Example:

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

Step 2 Configure a VLAN domain:

Example:

```
apic1(config)# vlan-domain dom1 dynamic
apic1(config-vlan)# vlan 150-200 dynamic
apic1(config-vlan)# exit
apic1(config)#
```

Step 3 Add interfaces to this VLAN domain. These are the interfaces to be connected to VMware hypervisor uplink ports:

Example:

```
apic1(config)# leaf 101-102
apic1(config-leaf)# interface ethernet 1/2-3
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

Step 4 Create a VMware domain and add VLAN domain membership:

Example:

```
apic1(config)# vmware-domain vmmdom1 access-mode readonly
apic1(config-vmware)# vlan-domain member dom1
apic1(config-vmware)#
```

Create the domain with a specific delimiter:

Example:

```
apic1(config)# vmware-domain vmmdom1 delimiter @
```

Step 5 Configure the domain type to DVS:

Example:

```
apic1(config-vmware)# configure-dvs
apic1(config-vmware-dvs)# exit
apic1(config-vmware)#
```

Step 6 (Optional) Configure a retention time for detached endpoints:

You can choose a delay of between 0 and 600 seconds. The default is 0.

Example:

```
apic1(config)# vmware-domain <domainName>

apic1(config-vmware)# ep-retention-time <value>
```

Step 7 Configure a controller in the domain:

Example:

```
apic1(config-vmware)# vcenter 192.168.66.2 datacenter prodDC
apic1(config-vmware-vc)# username administrator
Password:
Retype password:
apic1(config-vmware-vc)# exit
apic1(config-vmware)# exit
apic1(config)# exit
```

Note When configuring the password, you must precede special characters such as '$' or '!' with a backslash ('\$') to avoid misinterpretation by the Bash shell. The escape backslash is necessary only when configuring the password; the backslash does not appear in the actual password.

Step 8 Verify configuration:

Example:

```
apic1# show running-config vmware-domain vmmdom1
# Command: show running-config vmware-domain vmmdom1
# Time: Wed Sep  2 22:14:33 2015
  vmware-domain vmmdom1
    vlan-domain member dom1
    vcenter 192.168.66.2 datacenter prodDC
      username administrator password *****
    configure-dvs
      exit
    exit
```

What to do next

You can attach an EPG to the read-only VMM domain and configure policies for it. However, those policies are not pushed to the VDS in the VMware vCenter.