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.

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 VMware vCenter.

Cisco APIC Supported VMware VDS Versions

Different versions of VMware vSphere Distributed Switch (DVS) support different versions of Cisco Cisco Application Policy Infrastructure Controller (APIC). See the Cisco ACI Virtualization Compatibility Matrix for information about the compatibility of VMware components with Cisco APIC.

VMware vSphere

See the ACI Virtualization Compatibility Matrix for the supported release versions.

Adding ESXi Host Considerations

When adding additional VMware ESXi hosts to the virtual machine manager (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.

ESXi 6.5 Hosts with VIC Cards and UCS Servers

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.

VMware vCenter High Availability

VMware vCenter High Availability (VCHA), introduced in VMware vSphere 6.5, eliminates the single point of failure of VMware vCenter.

With VCHA, if the VMware vCenter active node fails, the passive node takes over. The passive node has the same IP address, credentials, and other information as the active node. No new VMM configuration is needed to take advantage of VCHA. Once the passive node takes over, and is reachable, Cisco APIC automatically reconnects.

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.

- VMM integration for DVS mode allows you to configure port-channels between leaf switch ports and ESXi hypervisor ports from APIC. LACP is either supported in enhanced or basic mode for port channels. Here is the matrix of support on ACI and VMware side:

Table 1: LACP Support

	ACI release prior to 3.2.7	ACI release after 3.2.7	VMware DVS release prior to 6.6	VMware DVS release after 6.6
Basic LACP	Yes	Yes	Yes	No
Enhanced LACP	No	Yes	Yes	Yes

When VMware side DVS is upgraded to version 6.6 or higher, LACP has to be reconfigured from Basic mode to Enhanced mode. If you have already configured enhanced LACP (eLACP) with prior versions of DVS (prior to 6.6), you need not reconfigure eLACP when upgrading to DVS 6.6.

Note Beginning with DVS version 6.6, basic LACP is not supported.

Migrating LACP from basic to enhanced, can result in traffic loss; perform the migration during a maintenance window. For the detailed migration procedure, see Migrating Basic LACP to Enhanced LACP , on page 16.

For more details about eLACP, and to add eLACP to a VMM domain, see the *Enhanced LACP Policy Support* section, later in this chapter.

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 2: 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
Uplink Ports and Uplink Names	8	Yes (From Cisco APIC Release 4.2(1))
Uplink Name Prefix	uplink	Yes (From Cisco APIC Release 4.2(1))
Maximum MTU	9000	Yes
LACP policy	disabled	Yes
Alarms	2 alarms added at the folder level	No

Note Cisco APIC does not manage port mirroring. You can configure port mirroring directly from VMware vCenter. Cisco APIC does not override the configuration. If Cisco APIC manages the configuration, Cisco APIC raises a fault. If Cisco APIC does not manage the configuration, Cisco APIC does not raise a fault.

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	Yes
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 Application Centric Infrastructure (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 Application Policy Infrastructure Controller (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.

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

Pushing the VMM Domain After Deleting It

You may accidentally delete the VMware Distributed Virtual Switch (DVS) that you created in Cisco APIC from the VMware vCenter. If that occurs, the Cisco APIC policy is not pushed again to VMware vCenter.

To push the VMM domain again to the VMware vCenter, disconnect the Cisco APIC VMware vCenter connectivity. Doing so ensures that after reconnection, Cisco APIC again pushes the VMM domain to the VMware vCenter and the DVS is recreated in VMware vCenter.

Read-Only VMM Domains

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.

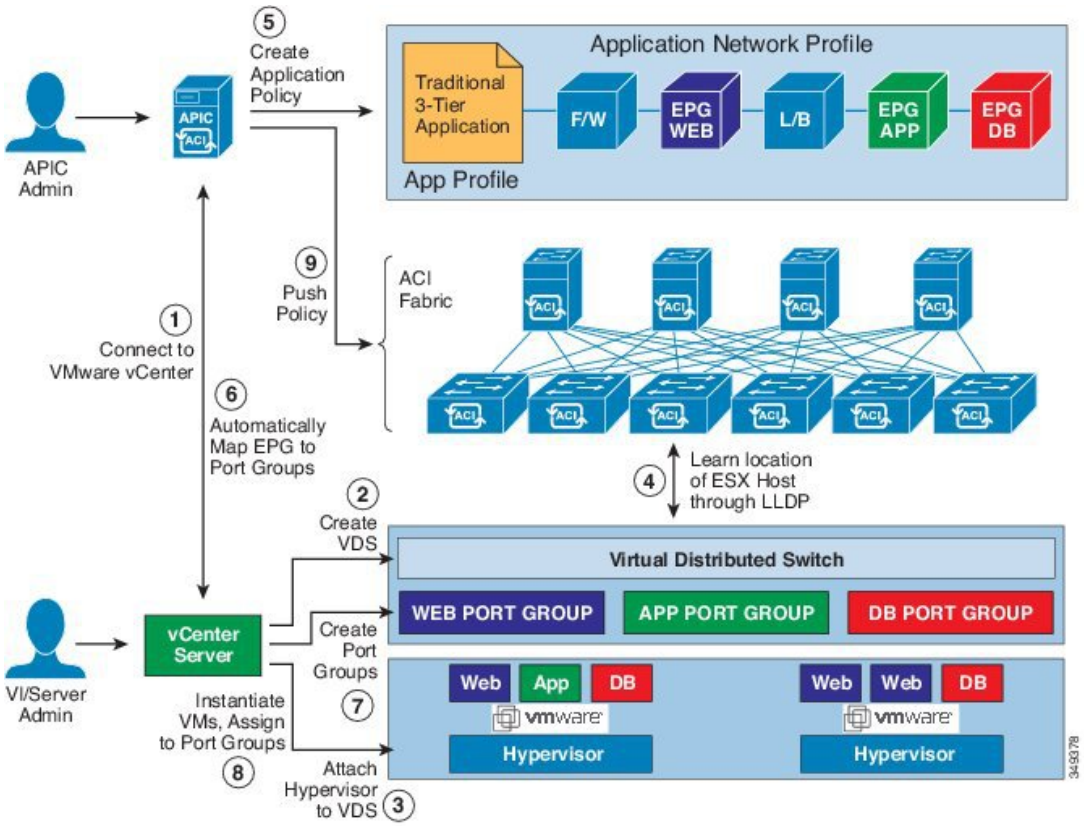
Prerequisites for Creating a VMM Domain Profile

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).

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 Time0ut**, **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
- Creating a Read-Only VMM Domain Using the NX-OS Style CLI

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.

Promoting a Read-Only VMM Domain to Read-Write

Beginning in Cisco APIC Release 4.0(1), you can promote an existing read-only VMM domain to a fully managed read-write VMM domain. Doing so enables you to not only view the inventory information for a VDS in the VMware vCenter, but also have Cisco APIC manage it.

Creating read-only VMM domains is described in Creating a Read-Only VMM Domain, on page 10.

Before you promote an existing read-only VMM domain, carefully consider the guidelines and limitations described in Promoting a Read-Only VMM Domain Caveats, on page 11.

Promoting a VMM domain from Read-Only to Read-Write will allow the APIC to monitor and manage the VMM domain as well as allow you to associate EPGs to it as Port Groups. You can promote a read-only VMM domain using the Cisco APIC GUI, the NX-OS style CLI, or REST API. See this section for the Cisco APIC GUI procedure. See the appendices for the procedures Promoting a Read-Only VMM Domain Using the NX-OS Style CLI and Promoting a Read-Only VMM Domain Using the REST API.

Promoting a Read-Only VMM Domain Caveats

When promoting a read-only VMM domain to read-write, keep in mind the following caveats:

- Promoting a read-only domain requires a specific network folder structure for the domain's VDS on the vCenter server. If your existing VDS is not contained in a network folder but is located directly under the datacenter, you will need to create a network folder with the same name as the VDS and move the VDS into that network folder before promoting the domain to read-write in order for APIC to properly manage it. Promoting a domain whose VDS is configured directly under the datacenter will cause APIC to create a new VDS inside a new network folder instead.
- When creating port-groups in vCenter for the read-only VMM domains you plan to promote to fully managed, it is recommended that you name them in the `<tenant-name>|<application-name>|<EPG-name>` format.

When you promote a VMM domain to fully managed and associate an EPG with the domain, any port-groups that are named in this standard format will be automatically added to the EPG.

If you chose a different format for the port-group names, you will need to manually re-assign all the VMs from the existing port-group to the new one created by the APIC for the EPG after you promote the domain:

- Create an EPG and associate it with the VMM domain.

  A fault will be raised on the VMM domain as it cannot find an EPG policy for the port-group

- Remove the virtual machines (VMs) from the existing port-group and attach them to the EPG.

Note This may cause traffic loss during the process.

- Once the VMs have been detached from port-group, delete the old port-group from the vCenter.

  All VMs must be detached from the port-group before you can delete it.

- When migrating a domain from read-only to read-write, it is recommended that you use a VLAN range that is unique and separate from the physical domain range in order to avoid potentially running out of available VLANs during migration process.
- If you want to use the same EPG on multiple VMMs and VMware vCenters, configure a link aggregation group (LAG) policy with the same name as the domain. An EPG can be connected to only one LAG policy. If you want to use different LAG policies, you must associate each one with a different EPG.

  See the section Enhanced LACP Policy Support, on page 13 in this guide for more information.

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

You can use the Cisco APIC GUI to promote a read-only VMM domain.

Before you begin

Instructions for promoting a read-only VMM domain to a managed domain assume you have completed the following prerequisites:

- Fulfill the prerequisites in the section Prerequisites for Creating a VMM Domain Profile, on page 6.
- Configure a read-only domain as described in Creating a Read-Only VMM Domain, on page 10.
- In the VMware vCenter, under the **Networking** tab, ensure that the VDS is contained by a network folder of the exact same name of the read-only VMM domain that you plan to promote.

Procedure

Step 1 Log in to Cisco APIC.

Step 2 Associate an Access Entity Profile (AEP) with the read-only VMM domain.

a) Navigate to **Fabric** > **Access Policies** > **Policies** > **Global** > **Attachable Access Entity Profiles**.

b) Select an AEP and associate it with the read-only VMM domain you plan to promote to fully managed.

Step 3 Promote the VMM domain.

a) Navigate to **Virtual Networking** > **Inventory**.
b) Expand the **VMM Domains** > **VMware** folder.
c) Select the read-only VMM Domain you want to promote.
d) Change the **Access Mode** setting to *Read Write Mode*.
e) Select a **VLAN Pool** from the drop down menu to associate a VLAN pool with the domain.
f) Click **Submit** to save changes.

Step 4 Create a new Link Aggregation Group (LAG) policy.

If you are using vCenter version 5.5 or later, you must create a LAG policy for the domain to use Enhanced LACP feature, as described in Create LAGs for DVS Uplink Port Groups Using the Cisco APIC GUI, on page 15.

Otherwise, you can skip this step.

Step 5 Associate the LAG policy with appropriate EPGs.

If you are using vCenter version 5.5 or later, you must associate the LAG policy with the EPGs to use Enhanced LACP feature, as described in Associate Application EPGs to VMware vCenter Domains with Enhanced LACP Policies Using the Cisco APIC GUI, on page 15.

Otherwise, you can skip this step.

What to do next

Any EPGs you attach to the VMM domain and any policies you configure will now be 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.

When you enable Enhanced LACP policy on the ACI side, it will push the configuration to DVS. Later, even if you remove the policy on the ACI side, enhanced LACP is still available on the DVS side, because after an enhanced LACP policy is enabled, it can not be reverted.

Note Enhanced LACP can be enabled either on the ACI or DVS side.

You can choose from up to 20 different load-balancing algorithms when you create a VMware vCenter virtual machine manager (VMM) domain for 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.

Beginning with Cisco APIC Release 5.2(1), Enhanced LACP policy is supported on interfaces of Layer 4 to Layer 7 service devices used in service graphs. See *Defining a Logical Device* section in the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*.

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 17 in this guide.
- Traffic is disrupted when an enhanced LACP LAG policy name conflicts with the name of a previous enhanced LACP link aggregation group (LAG) policy uplink. If you have an enhanced LACP LAG policy that is named ELACP-DVS for a DVS domain, its uplink is automatically named ELACP-DVS-1, ELACP-DVS-2, ELACP-DVS-3, and so on, depending on the number uplinks configured in the policy.

  Traffic loss occurs if you then try to configure of add another enhanced LAG policy with a name that conflicts with a previous policy uplink name. To remedy the issue, delete the LAG policy and re-create it with a different name.
- Interfaces of Layer 4 to Layer 7 service devices support LAG policy from Cisco APIC Release 5.2(1). However, if you have a Layer 4 to Layer 7 service device in a VMM domain, you will not be able to use enhanced LAG in that entire VMM domain (applicable for releases prior to 5.2(1)). This is because, you can not have uplinks attached to enhanced LAG while the interfaces of Layer 4 to Layer 7 service devices are not using LAG.

  Downgrading from Release 5.2(1)

To Release	LAG Used On	Required Action
Release earlier than 5.2(1)	EPG(s)	No action required.
Release earlier than 5.2(1)	EPGs and interfaces of Layer 4 to Layer 7 service devices	Remove LAG from entire VMM domain.
Release earlier than 3.2(7)	EPGs and/or interfaces of Layer 4 to Layer 7 service devices	Remove LAG from entire VMM domain.

- Enhanced LACP configuration is available only for VMware vDS VMM domain with switching mode set to *native.*

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.
- If a vSwitch policy container does not exist, create one.

Note You must configure a port channel policy before you create an enhanced LAG policy. You can create a port channel policy when you create a vCenter domain profile.

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.

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.

Migrating Basic LACP to Enhanced LACP

Use this procedure to migrate basic LACP to enhanced LACP on an existing VMware vCenter domain VDS.

As explained in the earlier sections, *Create LAGs for DVS Uplink Port Groups Using the Cisco APIC GUI* and *Associate Application EPGs to VMware vCenter Domains with Enhanced LACP Policies Using the Cisco APIC GUI*, enhanced LACP configurations include these vital procedures:

- Configure Enhanced Lag Policy in VSwitch Policy of the VMware VMM Domain.
- Select Enhanced Lag Policy at VMware VMM Domain association for each EPG.

Unless both of the above steps are performed, traffic is not forwarded properly. The second step takes care of the active uplinks configuration in teaming and failover of the port-group for each EPG and it needs to be done for all EPGs that use the VMware VMM Domain.

Migrating LACP from basic to enhanced can result in traffic loss even with automation, and it is recommended to perform the migration during a maintenance window. This procedure is to minimize traffic loss, even when the migration is performed during a maintenance window.

Procedure

Step 1 Upgrade the DVS to enhanced LACP on VMware vCenter (not through APIC). Complete the following steps:

a) Select **Networking** from the **Menu** and locate the DVS.

b) Right-click the DVS, and in the pop-up screen that is displayed, select **Upgrade** > **Enhance LACP Support**.

This step creates LACP configuration , *ELAG*, and automatically updates the active uplinks configuration of the port-group to use the *ELAG* group. You can expect traffic loss while performing this step because the configuration of the physical network adapters are getting updated. APIC raises a fault, F3290.

c) Verify the updated LACP confguration on VDS.

To verify, select **DVS** > **Configure** > **Settings** > **LACP**.

Step 2 Ensure to create the same enhanced LAG policy (*ELAG*) in the vSwitch policy of the existing VMware VMM domain. See the *Create LAGs for DVS Uplink Port Groups Using the Cisco APIC GUI* procedure for details about creating LAG policies.

Fault F3290 clears.

Step 3 Select the Enhanced Lag Policy at VMware VMM Domain association for each EPG. See the *Associate Application EPGs to VMware vCenter Domains with Enhanced LACP Policies Using the Cisco APIC GUI* procedure for details.

Step 4 Verify if the forwarding is working fine.

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.

Note Before downgrading, see Enhanced LACP Limitations, on page 14 section for the required action, based on LAG support.

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 and interfaces of L4-L7 service devices used in service graphs, 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 3.2(7).

Port Binding

Port Binding is a parameter which determines the connection between the virtual machines and virtual network adapters to a vDS and how to to use those virtual machines.

You can configure the binding type for an EPG. Depending on the binding type, you can also configure the number of ports and port allocation. Port binding is not configurable for non user-configured EPGs such as EPGs created by system and service EPGs.

Types of Binding

These three different types of port binding determine when ports in a port group are assigned to virtual machines:

- Static Binding— When you connect a virtual machine to a port group configured with static binding, a port is immediately assigned and reserved for it, guaranteeing connectivity at all times. The port is disconnected only when the virtual machine is removed from the port group. You can connect a virtual machine to a static-binding port group only through the vCenter server. In static binding type, there are two types of port allocation: Fixed and Elastic. If port allocation is fixed, only a limited number of VMs can be attached, based on the number of ports. If you try adding more number of VMs than the number of ports, the following error is displayed— *No free port available*. But in case of elastic port allocation, when an attempt is made to attach more VMs than the number of ports specified, the number of ports is automatically increased by 8. The default values for binding type is static and number of ports is 0. If the binding type is static, then, typically, the port allocation is elastic. The port allocation can be changed/updated by the user on fvRsDomAtt (EPG to VMM Domain association). If the binding type is static and port allocation is fixed, you can change the number of ports. But if the binding type is static and port allocation is elastic, you can configure only once and the number of ports cannot be updated. This is because, in elastic mode, vCenter takes care of dynamically increasing the ports and there is no need to modify it from the APIC.
- Dynamic Binding— In a port group configured with dynamic binding, a port is assigned to a virtual machine only when the virtual machine is powered on and its NIC is in a connected state. The port is disconnected when the virtual machine is powered off or the NIC of the virtual machine is disconnected. Virtual machines connected to a port group configured with dynamic binding must be powered on and off through vCenter. Dynamic binding can be used in environments where you have more virtual machines than available ports, but do not plan to have a greater number of virtual machines active than the available ports. For example, if you have 300 virtual machines and 100 available ports, but will not have more than 90 virtual machines active at one time, dynamic binding is appropriate for your port group. Dynamic binding type does not support port allocation. So, only the type and number of ports can be modified using the VMM domain association configuration (fvRsDomAtt) on APIC.

Note The Dynamic Binding option (lateBinding in vSphere) has been deprecated as of vSphere 5.0, and is not available on the VMware vSphere GUI.

- Ephemeral Binding— In a port group configured with ephemeral binding, a port is created and assigned to a virtual machine by the host when the virtual machine is powered on and its NIC is in a connected state. When the virtual machine powers off or the NIC of the virtual machine is disconnected, the port is deleted. In ephemeral, the number of ports option disappears on vCenter and that is because if the binding type is ephemeral, then all the ports on the switch can be used.

Configure Port Binding Using the GUI

Use this procedure to configure port binding for a VMM domain.

Procedure

Step 1 Login to Cisco APIC.

Step 2 Go to **Tenants** > ***tenant*** > **Application Profile** > ***application profile*** > **Application EPGs** > ***application EPG***.

Step 3 Right-click the application EPG that you want to associate with a VMM domain, and then choose **Add VMM Domain Association**.

Step 4 In the **Add VMM Domain Association** dialog box, select the required port binding. The available options are:

- Dynamic Binding— a port is assigned to a virtual machine only when the virtual machine is powered on and its NIC is in a connected state. The port is disconnected when the virtual machine is powered off or the NIC of the virtual machine is disconnected.
- Ephemeral— a port is created and assigned to a virtual machine by the host when the virtual machine is powered on and its NIC is in a connected state. When the virtual machine powers off or the NIC of the virtual machine is disconnected, the port is deleted.
- Default—behavior is similar to the behavior when you choose static binding.
- Static Binding— a port is immediately assigned and reserved for it, guaranteeing connectivity at all times. The port is disconnected only when the virtual machine is removed from the port group.
- Port Allocation— this field is displayed only when Static Binding is selected. The options are, Fixed and Elastic.
  - **a.** Elastic—the default number of ports is set to eight. When all ports are assigned, a new set of eight ports is created.
  - **b.** Fixed—the default number of ports is set to eight. No additional ports are created when all ports are assigned.
- Number of Ports— this field is displayed when Dynamic Binding or Static Binding is selected. The default value is 0; recommended value is 8.

For more details about the types of port binding, see Types of Binding, on page 18.

Step 5 Click **Submit**.

Configure Port Binding Using the REST API

Use the following to configure port binding using REST API. The example below displays the port binding as *staticBinding*.

```
<fvAp name="ap">
 <fvAEPg name="Epg1">
  <fvRsBd tnFvBDName="BD1" />
    <fvRsDomAtt resImedcy="immediate" switchingMode="native"
bindingType="staticBinding" numPorts="12" portAllocation="fixed"
    tDn="uni/vmmp-VMware/dom-mininetlacp2">
  </fvRsDomAtt>
 </fvAEPg>
</fvAp>
```

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 20
- Configure Endpoint Retention Using the NX-OS Style CLI
- Configuring Endpoint Retention Using the REST API

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**.

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

Trunk Port Group

You use a trunk port group to aggregate the traffic of endpoint groups (EPGs) for VMware virtual machine manager (VMM) domains.

For details about trunk port groups, see the section About Trunk Port Group.

For procedures to create trunk port groups, see the following sections:

- Creating a Trunk Port Group Using the GUI, on page 21
- Creating a Trunk Port Group Using the NX-OS Style CLI
- Creating a Trunk Port Group Using the REST API

Creating a Trunk Port Group Using the GUI

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

Before you begin

Ensure that the trunk port group is 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** > **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 virtual machines attached to the trunk port group receives unicast traffic not destined to their MAC addresses. The options are:

- **Enabled**
- **Disabled** (default)

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

The field specifies whether policies are resolved immediately or when needed on the leaf switches. The options are:

- **Immediate**
- **On Demand** (default)

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

The field allows definition of new MAC addresses for the network adapter within the VM. The options are:

- **Enabled** (default)
- **Disabled**

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

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

- **Enabled** (default)
- **Disabled**

f) From the **Enhanced Lag Policy** drop-down list, choose the uplink with the Link Aggregation Control Protocol (LACP) policy that you want to apply.

The policy consists of distributed virtual switch (DVS) uplink port groups configured in link aggregation groups (LAGs) and associated with a load-balancing algorithm. You must have previously applied at least one uplink with an LACP policy to a DVS uplink port group. Doing so enables you to improve uplink load balancing.

For information about enhanced LACP, see the section Enhanced LACP Policy Support, on page 13 in this guide.

g) 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.

h) Click **Update**.

Step 5 Click **Submit**.

Using VMware vSphere vMotion

VMware vSphere vMotion enables you to move a virtual machine (VM) between different physicals hosts without interruption in service.

See the VMware website for information about VMware vSphere vMotion, including documentation.

When you use VMware vMotion to move a VM behind a VMware distributed virtual switch (DVS), traffic is interrupted from several seconds to several minutes. The interruption can last up 15 minutes—the default local endpoint retention interval. The interruption occurs when both of the following two cases are true:

- When virtual switches use only Reverse Address Resolution Protocol (RARP) to indicate VM moves
- When a bridge domain is associated with a First Hop Security (FHS) policy that has the IP Inspection enabled

To work around the issue, disassociate the FHS policy from the bridge domain or change the policy to one in which IP inspection is disabled.

Working with Blade Servers

Guidelines for Cisco UCS B-Series Servers

When integrating blade server systems into Cisco ACI Cisco Application Centric Infrastructure for purposes of VMM integration (for example, integrating Cisco Unified Computing System (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 Cisco Application Policy Infrastructure Controller (APIC) for the UCS blade server uplinks, the default behavior will be mac-pinning.

- The VM endpoint learning relies on either the Cisco Discovery Protocol (CDP) or Link Layer Discovery Protocol (LLDP). 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 Cisco 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 Cisco 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, both CDP and LLDP are supported, beginning from UCSM 2.2.4b. If UCS B-series server is using earlier firmware, LLDP is not supported.
- 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 Cisco APIC.

Condition: This causes the Cisco 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. Setting privileges also allows Cisco APIC to 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** (read/write/modify)

  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** (read/write/modify)
- **dvPort Group** (read/write/modify)
- **Folder** (read/write/modify)
- **Network** (read/write/modify)

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

- **Virtual machine** (read/write/modify)

  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** (read/write/modify)
  - **Allocate space**
  - **Browse datastore**
  - **Low level file operations**
  - **Remove file**
- **Resource** (read/write/modify)
  - **Assign virtual machine to resource pool**

- **Virtual machine** (read/write/modify)
  - **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** (read/write/modify)
  - **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, 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, 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.