Configure VMM Domain Integration with ACI and UCS B Series

Contents

Introduction
Prerequisites
Requirements
Components Used
Configure
Create the VMM Domain
Verify the DVS is Created in vCenter
Create/Verify that CDP or LLDP is Enabled on the UCS vNICs
Configure the vSwitch Policies on APIC for UCS B
Verify
Troubleshoot

Introduction

This document describes the configuration steps that are required in order to integrate a Cisco Unified Computing System (UCS) B Series into an Application Centric Infrastructure (ACI) fabric that leverages Virtual Machine Manager (VMM) domain integration.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these hardware and software versions:

- An ACI fabric that consists of two spine switches and two leaf switches
- A UCS B Series chassis with two fabric interconnects
- UCS B Series blades with VMware ESXi
- An Application Policy Infrastructure Controller (APIC)

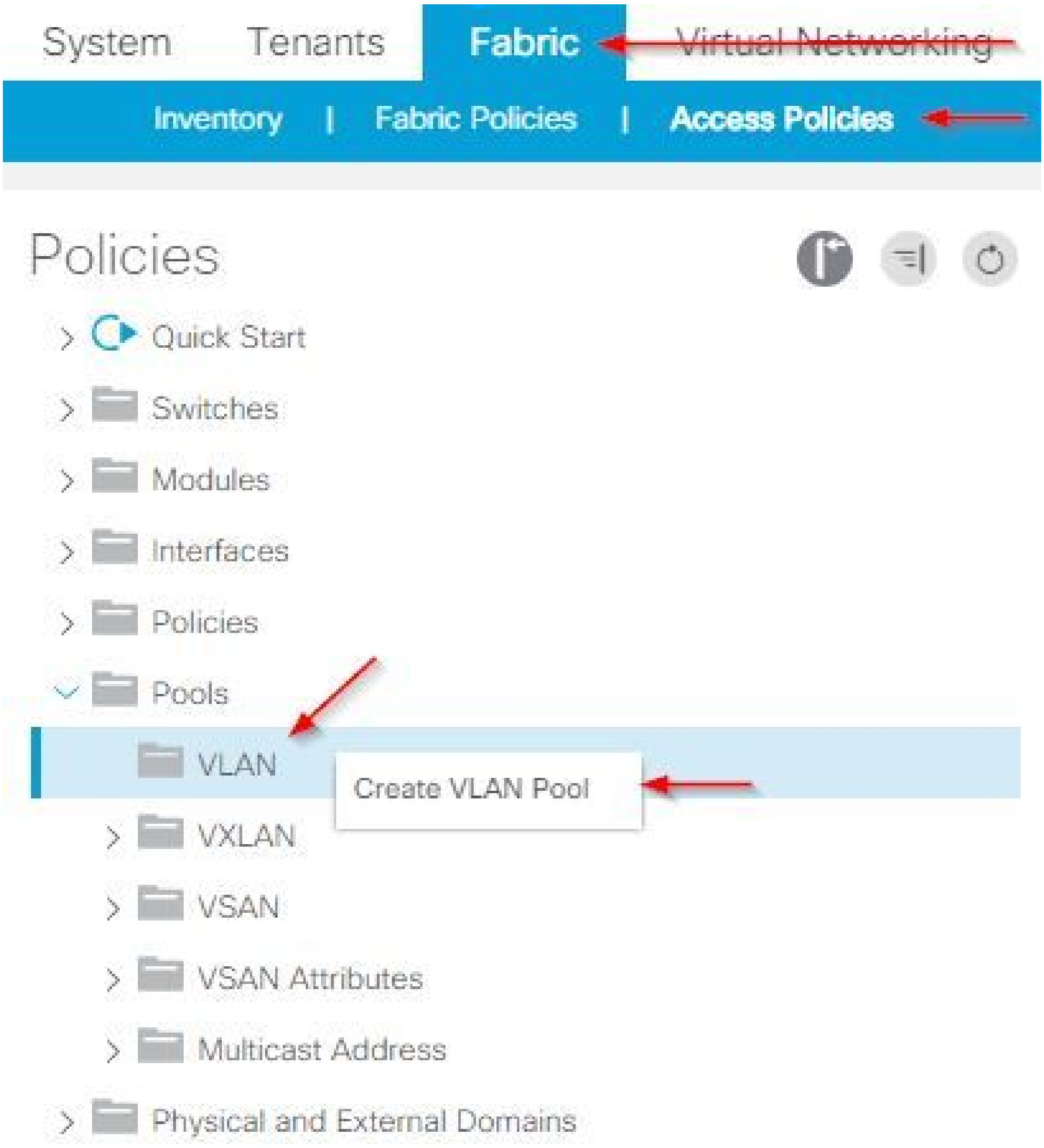
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

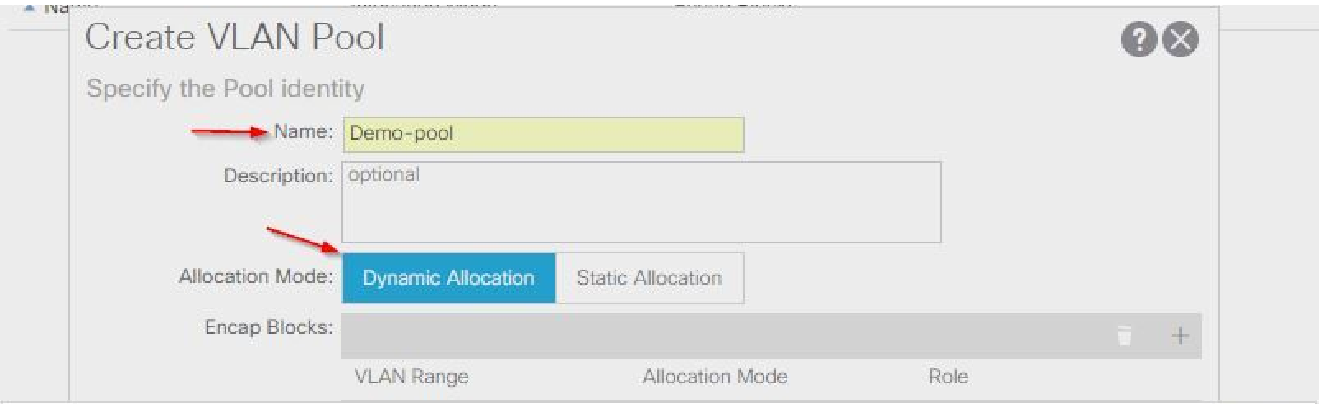
Create the VMM Domain

Most of this configuration is similar to the deployment of a VMM domain on any server hardware. There are certain limitations for which the workaround is to configure the APIC a certain way. These workaround configurations are called out specifically in this procedure.

1. Create a dynamic VLAN pool. From the APIC user interface, choose **Fabric** > **Access Policies** > **Pools** > **VLAN** > **Create VLAN Pool**.



2. When the Create VLAN Pool window opens, enter this information: Enter the name of the pool in the Name field.Click **Dynamic Allocation**.Click the **Encap Blocks (+)** plus symbol and enter the Encap Block Range in the Range fields of the Create Ranges dialog box.Click **Dynamic Allocation** for the Allocation Mode field.Click **External or On the wire encapsulations.**Click **OK**.Click
Submit.



Create VLAN Pool

Specify the Pool identity

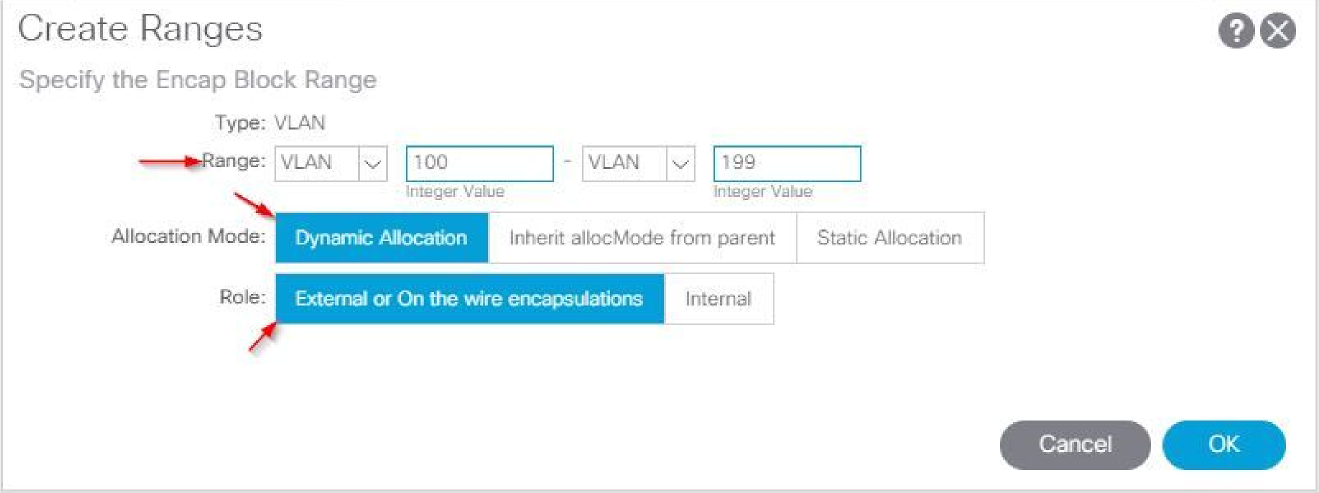
Name: Demo-pool

Description: optional

Allocation Mode: Dynamic Allocation | Static Allocation

Encap Blocks:

VLAN Range | Allocation Mode | Role



Create Ranges

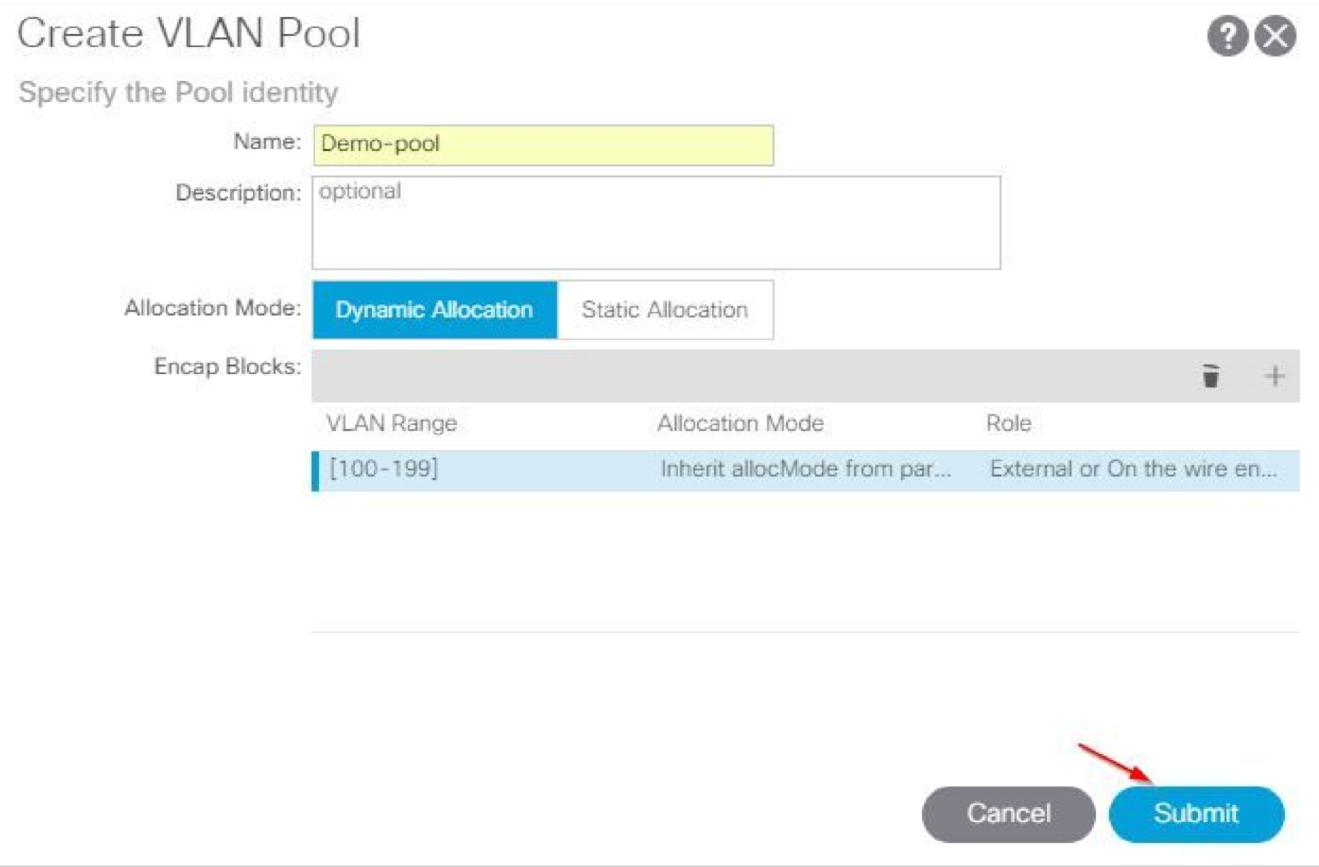
Specify the Encap Block Range

Type: VLAN

Range: VLAN 100 (Integer Value) - VLAN 199 (Integer Value)

Allocation Mode: Dynamic Allocation | Inherit allocMode from parent | Static Allocation

Role: External or On the wire encapsulations | Internal



Create VLAN Pool

Specify the Pool identity

Name: Demo-pool

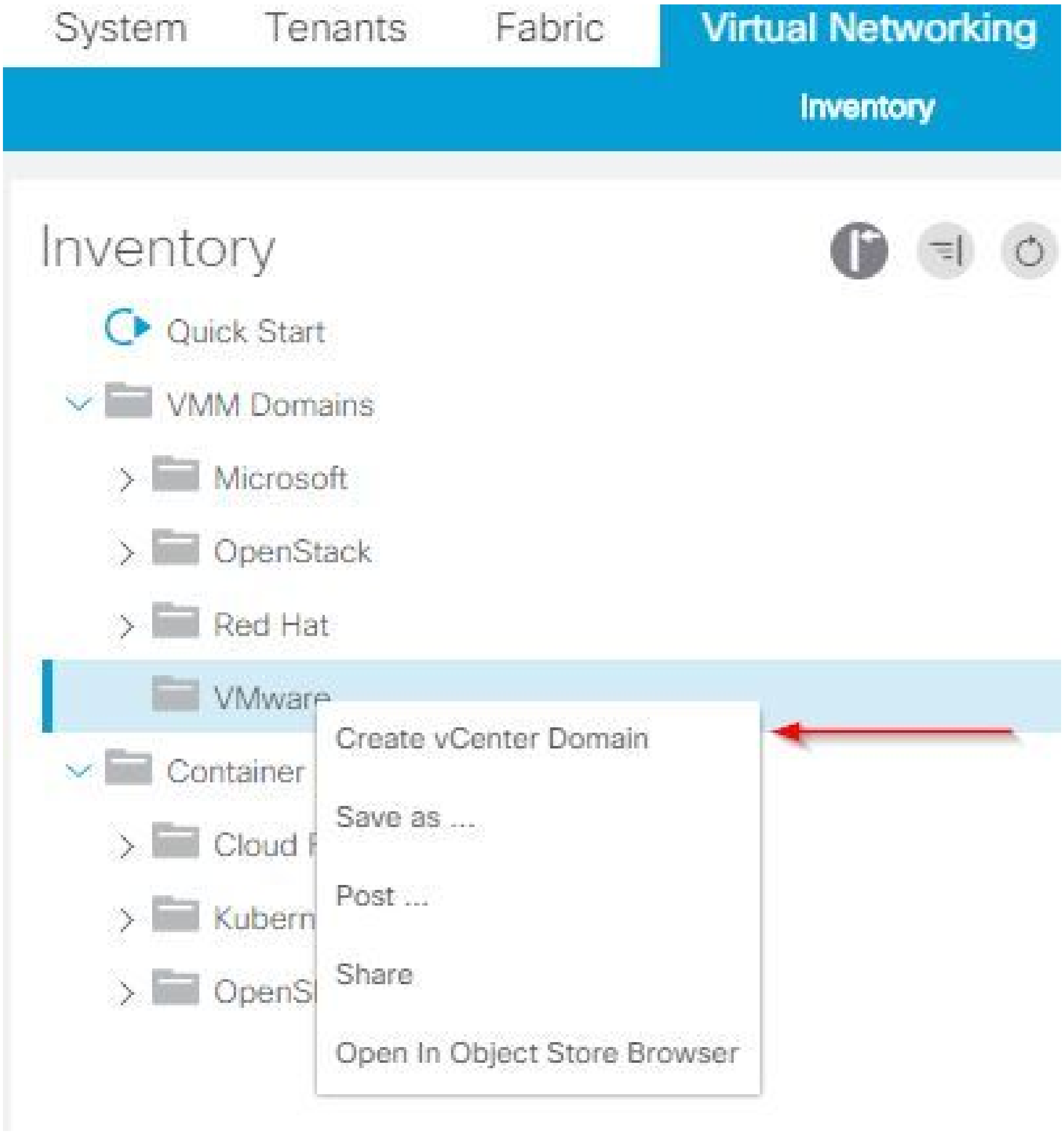
Description: optional

Allocation Mode: Dynamic Allocation | Static Allocation

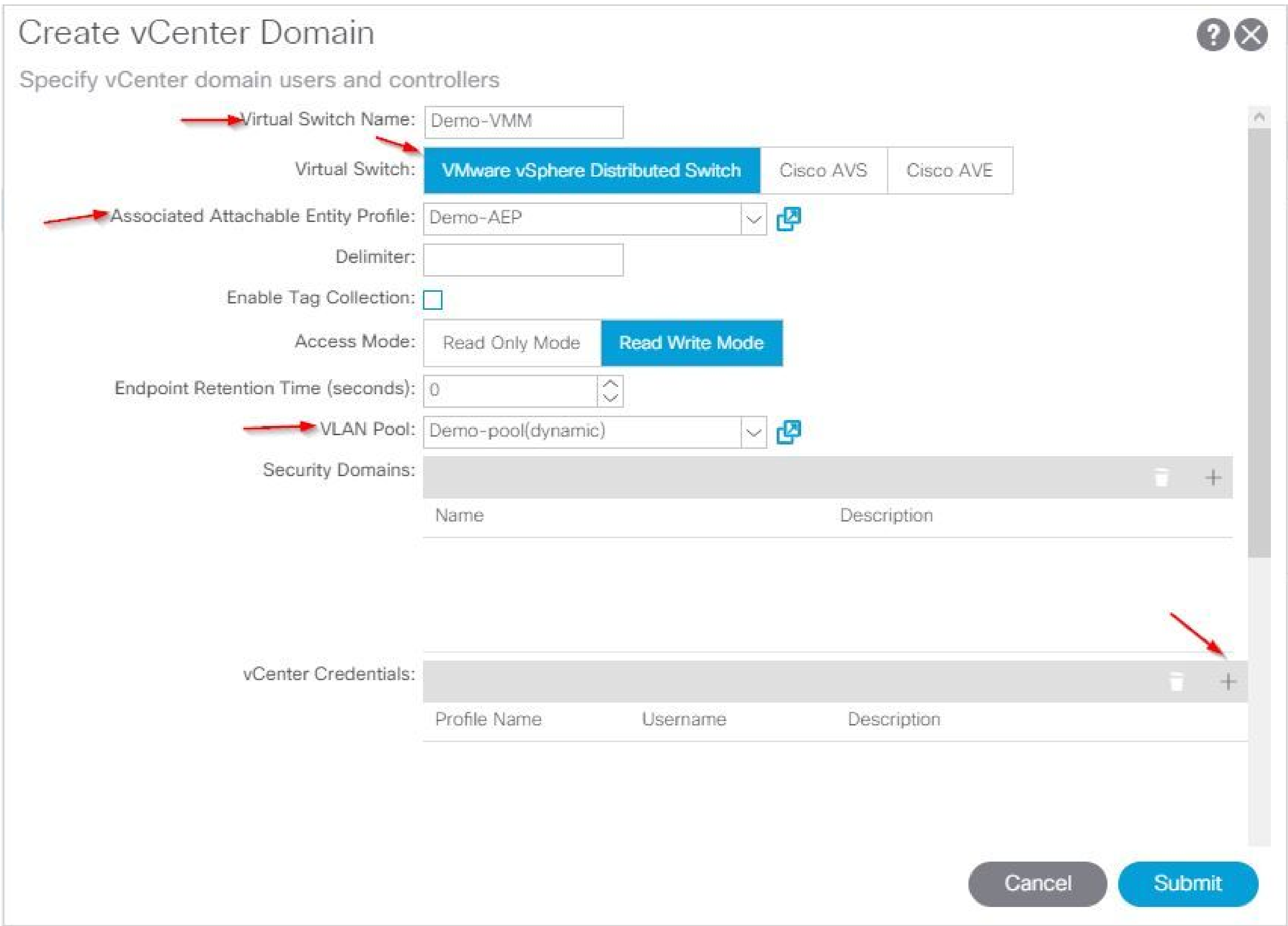
Encap Blocks:

VLAN Range	Allocation Mode	Role
[100-199]	Inherit allocMode from par...	External or On the wire en...

3. From the APIC user interface, choose **Virtual Networking > VMM Domains > VMware > Create vCenter Domain**.



4. When the Create vCenter Domain window appears, enter this information: Enter the domain name in the Virtual Switch Name field.Click **VMWare vSphere Distributed Switch**.Choose (create if needed) **Demo-AEP** from the Associated Attachable Entity Profile drop-down list.Choose **Demo-Pool (dynamic)** from the VLAN Pool drop-down list.Click the **vCenter Credentials (+)** plus symbol and enter your vCenter Credential information in the Create vCenter Credential dialog box.Click **OK**.Click
Submit.



Create vCenter Domain

Specify vCenter domain users and controllers

Virtual Switch Name: Demo-VMM

Virtual Switch: VMware vSphere Distributed Switch | Cisco AVS | Cisco AVE

Associated Attachable Entity Profile: Demo-AEP

Delimiter:

Enable Tag Collection: □

Access Mode: Read Only Mode | Read Write Mode

Endpoint Retention Time (seconds): 0

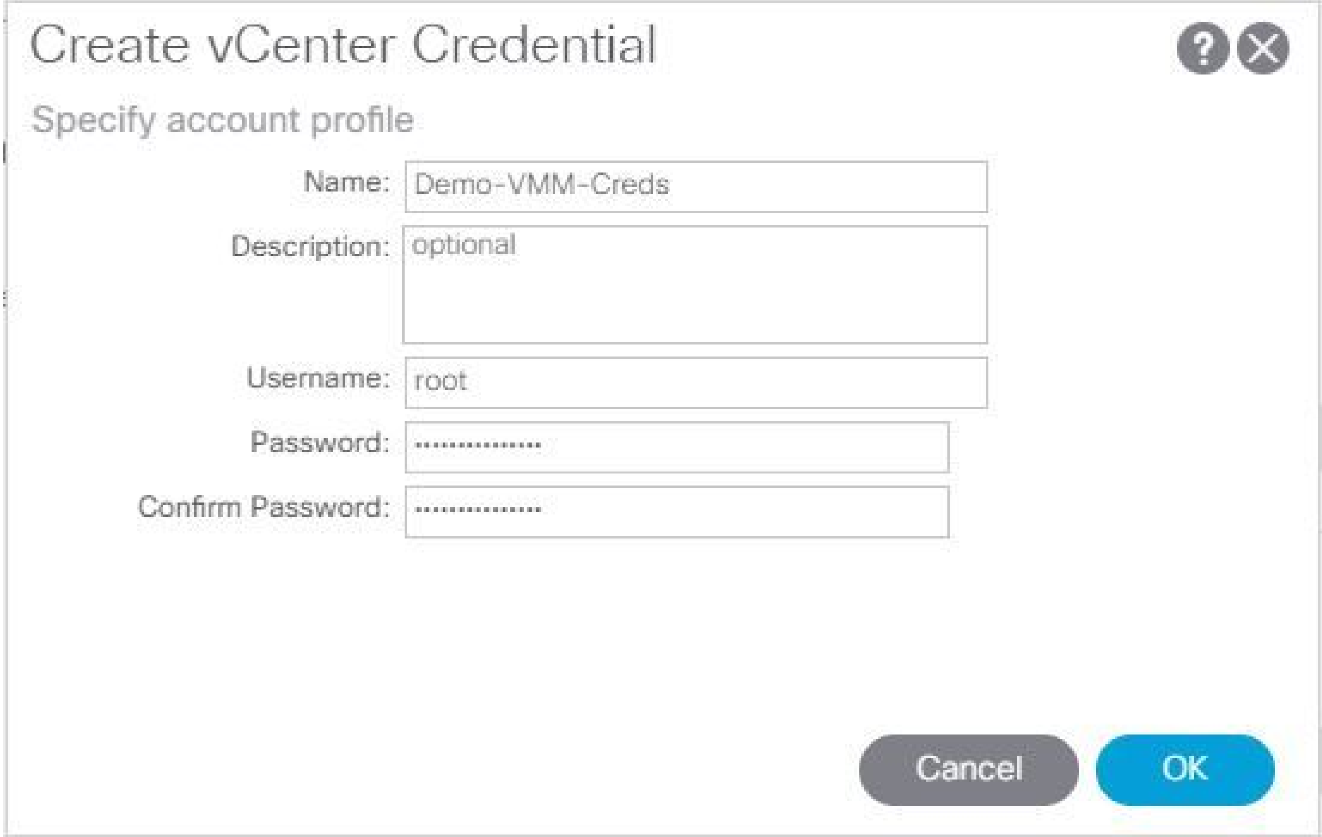
VLAN Pool: Demo-pool(dynamic)

Security Domains:

Name	Description

vCenter Credentials:

Profile Name	Username	Description



Create vCenter Credential

Specify account profile

Name: Demo-VMM-Creds

Description: optional

Username: root

Password: ••••••••••••••••

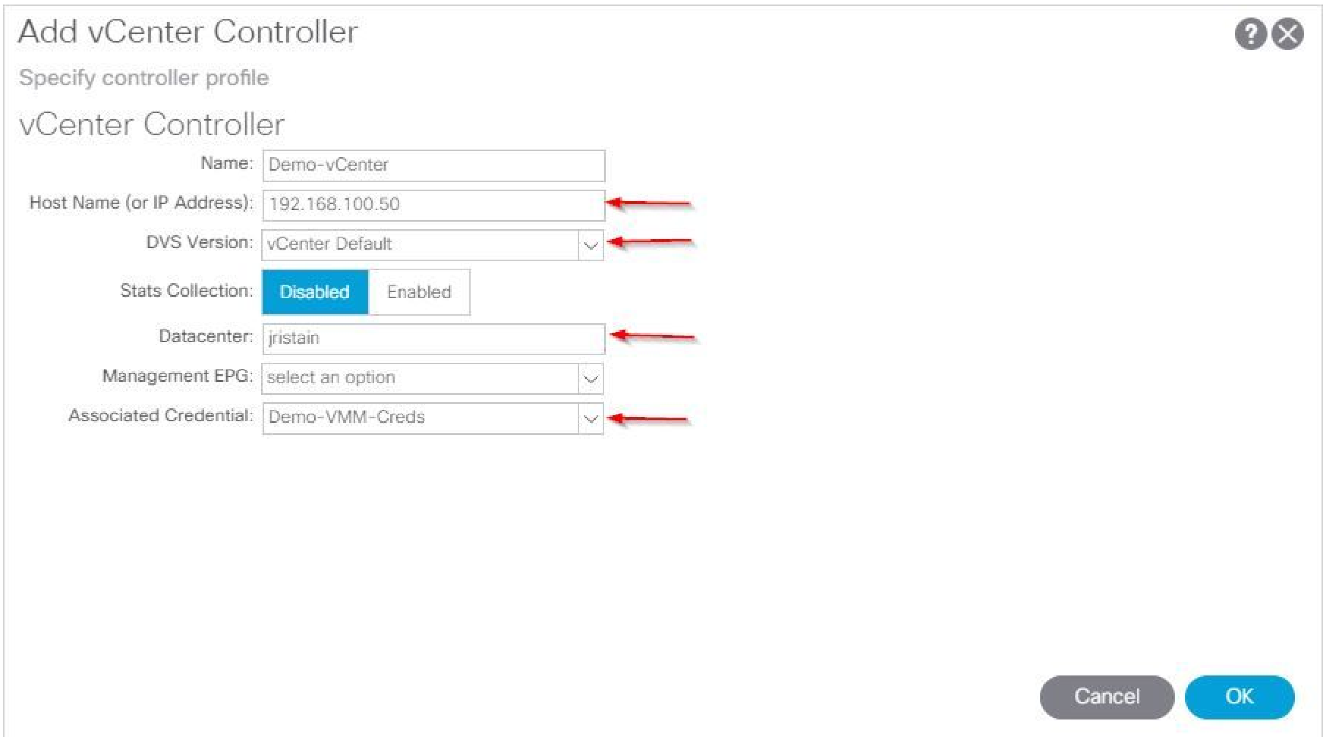
Confirm Password: ••••••••••••••••

5. Click the **(+)** plus symbol by vCenter heading from the Create vCenter Domain window, it may be required to scroll down to see it. Enter this information when the Create vCenter Controller window appears:

vCenter:

Name	IP	Type	Stats Collection

Enter the host name or IP address in the Host Name (or IP Address) field.Choose **vCenter Default** from the DVS Version drop-down list.Enter the name of the datacenter in the Datacenter field.Choose **Demo-VMM-Creds** from the Associated Credential drop-down list.Click **OK**.Click **Submit**.



Add vCenter Controller

Specify controller profile

vCenter Controller

Name: Demo-vCenter

Host Name (or IP Address): 192.168.100.50

DVS Version: vCenter Default

Stats Collection: [✓ Disabled] Enabled

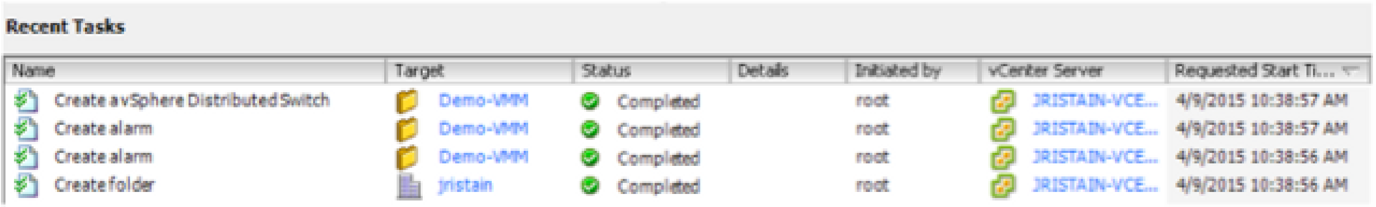
Datacenter: jristain

Management EPG: select an option

Associated Credential: Demo-VMM-Creds

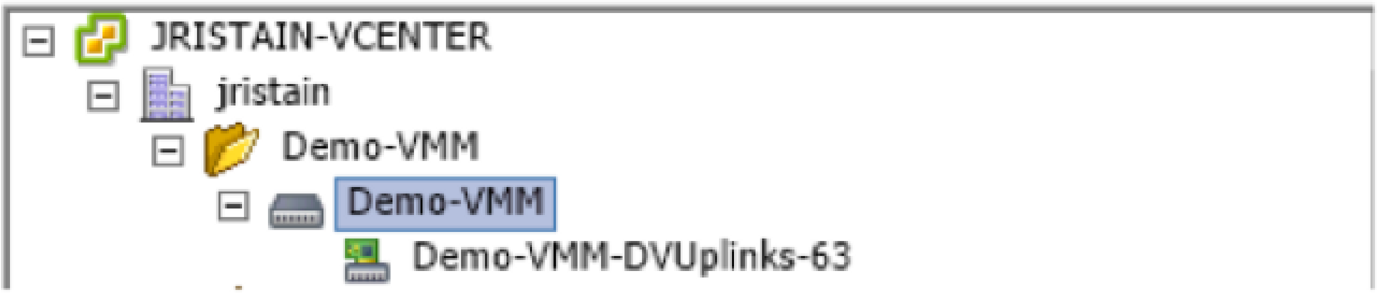
Verify the DVS is Created in vCenter

You should see a few new tasks in the Recent Tasks window and the addition of a Distributed Virtual Switch (DVS) in the vCenter Server:



Recent Tasks

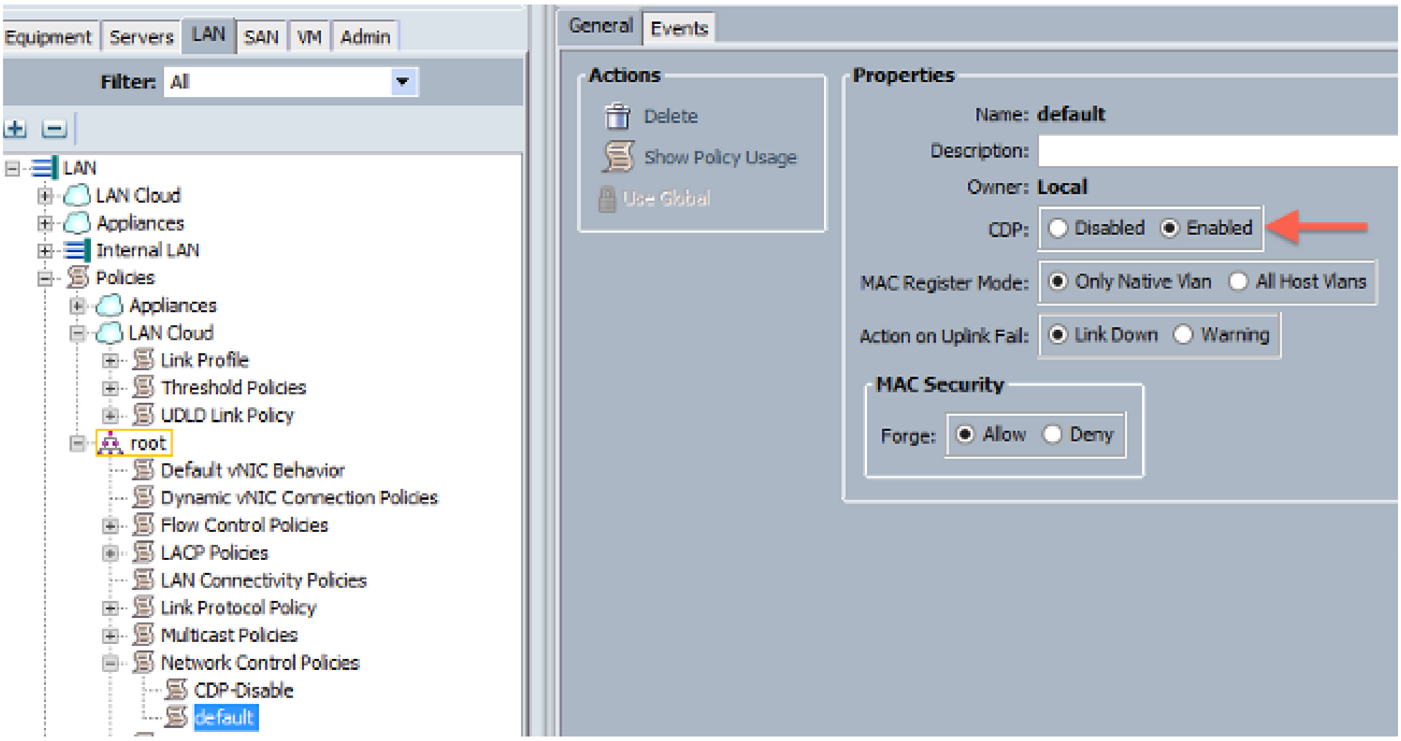
Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Ti...
Create a vSphere Distributed Switch	Demo-VMM	Completed		root	JRISTAIN-VCE...	4/9/2015 10:38:57 AM
Create alarm	Demo-VMM	Completed		root	JRISTAIN-VCE...	4/9/2015 10:38:57 AM
Create alarm	Demo-VMM	Completed		root	JRISTAIN-VCE...	4/9/2015 10:38:56 AM
Create folder	jristain	Completed		root	JRISTAIN-VCE...	4/9/2015 10:38:56 AM



Create/Verify that CDP or LLDP is Enabled on the UCS vNICs

When you deploy UCS B in ACI, you can choose the discovery protocol you would like to use to discover the hosts. This section walks you through how to configure each type in the UCS Manager.

By default, Cisco Discovery Protocol (CDP) is disabled on the UCS virtual Network Interface Card (vNIC) because the default Network Control Policy has CDP disabled. In order to enable CDP, you can either modify the default Network Control Policy, or create a new one with CDP enabled. Then apply that policy to each vNIC in each Service Profile. In this example, the default Network Control Policy is modified since all of the Service Profiles use that by default:



Properties

Name: **default**

Description:

Owner: **Local**

CDP: ○ Disabled ● Enabled

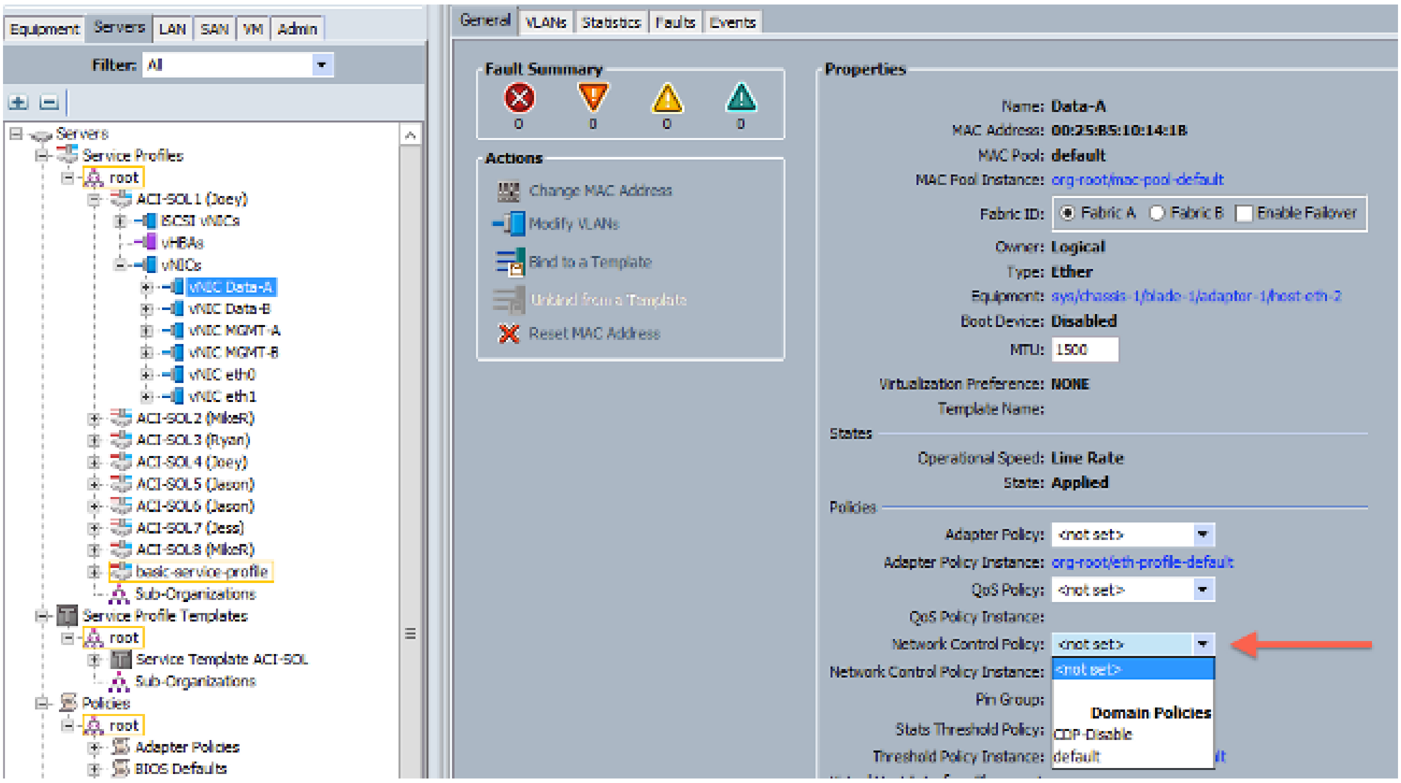
MAC Register Mode: ● Only Native Vlan ○ All Host Vlans

Action on Uplink Fail: ● Link Down ○ Warning

MAC Security

Forge: ● Allow ○ Deny

If you use a different policy, ensure you add that policy to the vNICs in each Service Profile:



Properties

Name: **Data-A**

MAC Address: **00:25:B5:10:14:1B**

MAC Pool: **default**

MAC Pool Instance: org-root/mac-pool-default

Fabric ID: ● Fabric A ○ Fabric B □ Enable Failover

Owner: **Logical**

Type: **Ether**

Equipment: sys/chassis-1/blade-1/adaptor-1/host-eth-2

Boot Device: **Disabled**

MTU: 1500

Virtualization Preference: **NONE**

Template Name:

States

Operational Speed: **Line Rate**

State: **Applied**

Policies

Adapter Policy: <not set>

Adapter Policy Instance: org-root/eth-profile-default

QoS Policy: <not set>

QoS Policy Instance:

Network Control Policy: <not set>

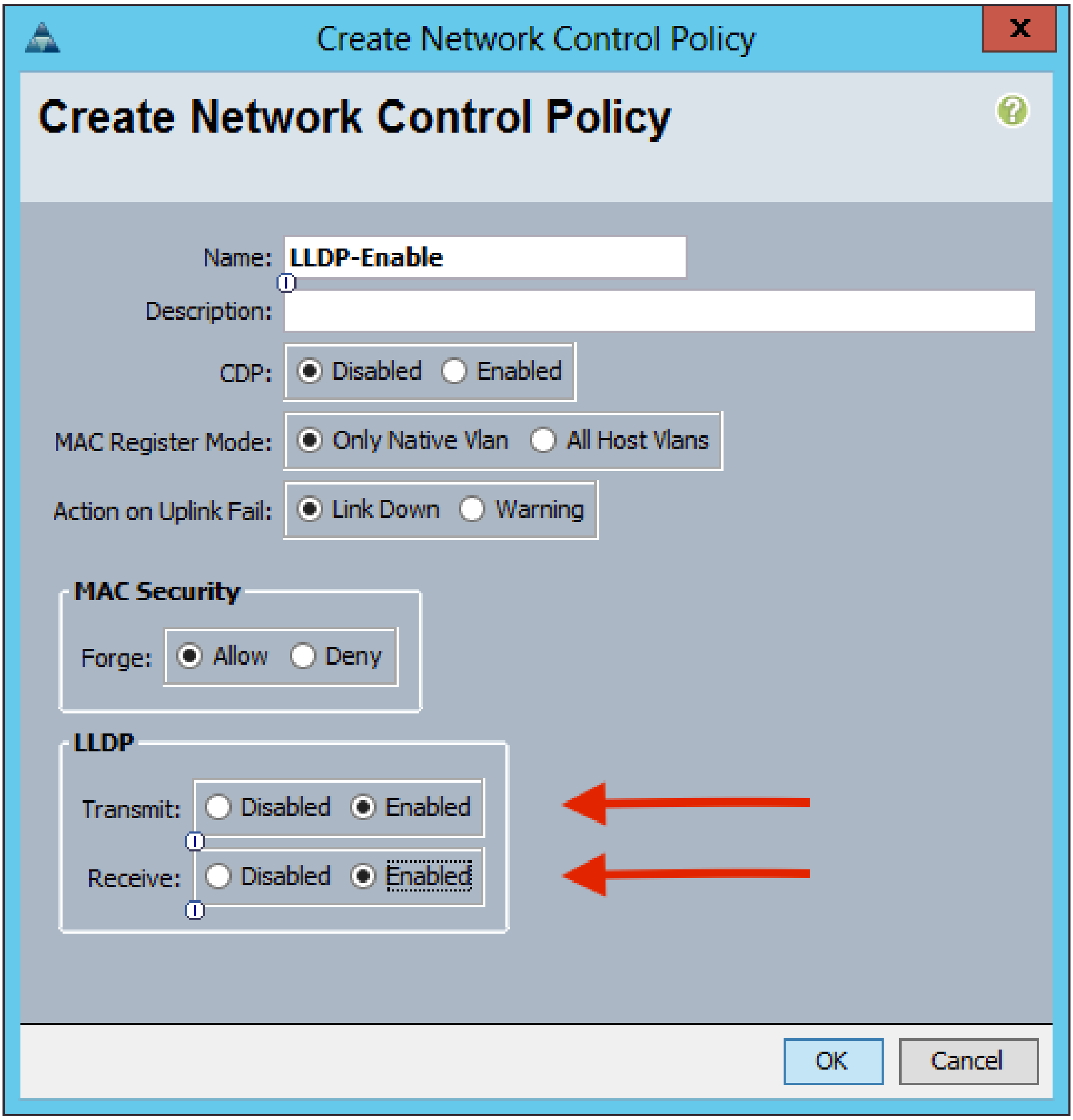
Network Control Policy Instance:

Pin Group:

Stats Threshold Policy:

Threshold Policy Instance:

In Version 2.2(4b) and later, the UCS supports Link Layer Discovery Protocol (LLDP) from the Fabric Interconnects down to the blades. This means that you can also use LLDP in order to discover the hosts in vCenter and the fabric if you run this version or later. The configuration is the exact same as above, but you would enable LLDP in both directions:



Create Network Control Policy

Name: LLDP-Enable

Description:

CDP: ● Disabled ○ Enabled

MAC Register Mode: ● Only Native Vlan ○ All Host Vlans

Action on Uplink Fail: ● Link Down ○ Warning

MAC Security

Forge: ● Allow ○ Deny

LLDP

Transmit: ○ Disabled ● Enabled

Receive: ○ Disabled ● Enabled

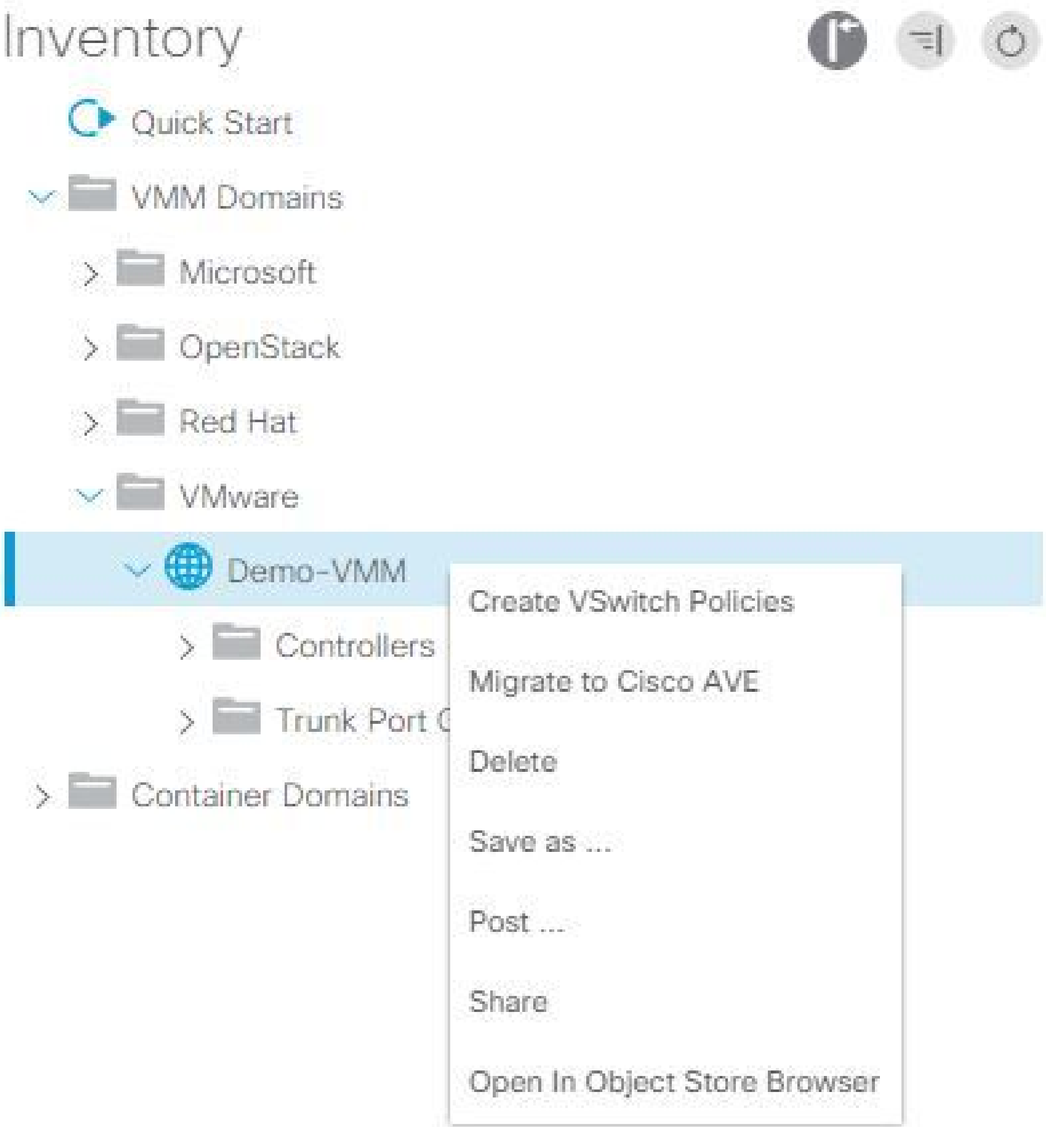
Configure the vSwitch Policies on APIC for UCS B

By default on the DVS, the Discovery Protocol used is LLDP. This is fine for any servers that support LLDP, but the UCS B series blades only support LLDP on UCSM version 2.2(4b) and later. Because of this, ESXi cannot report LLDP information to the APIC, unless you are on the correct code.

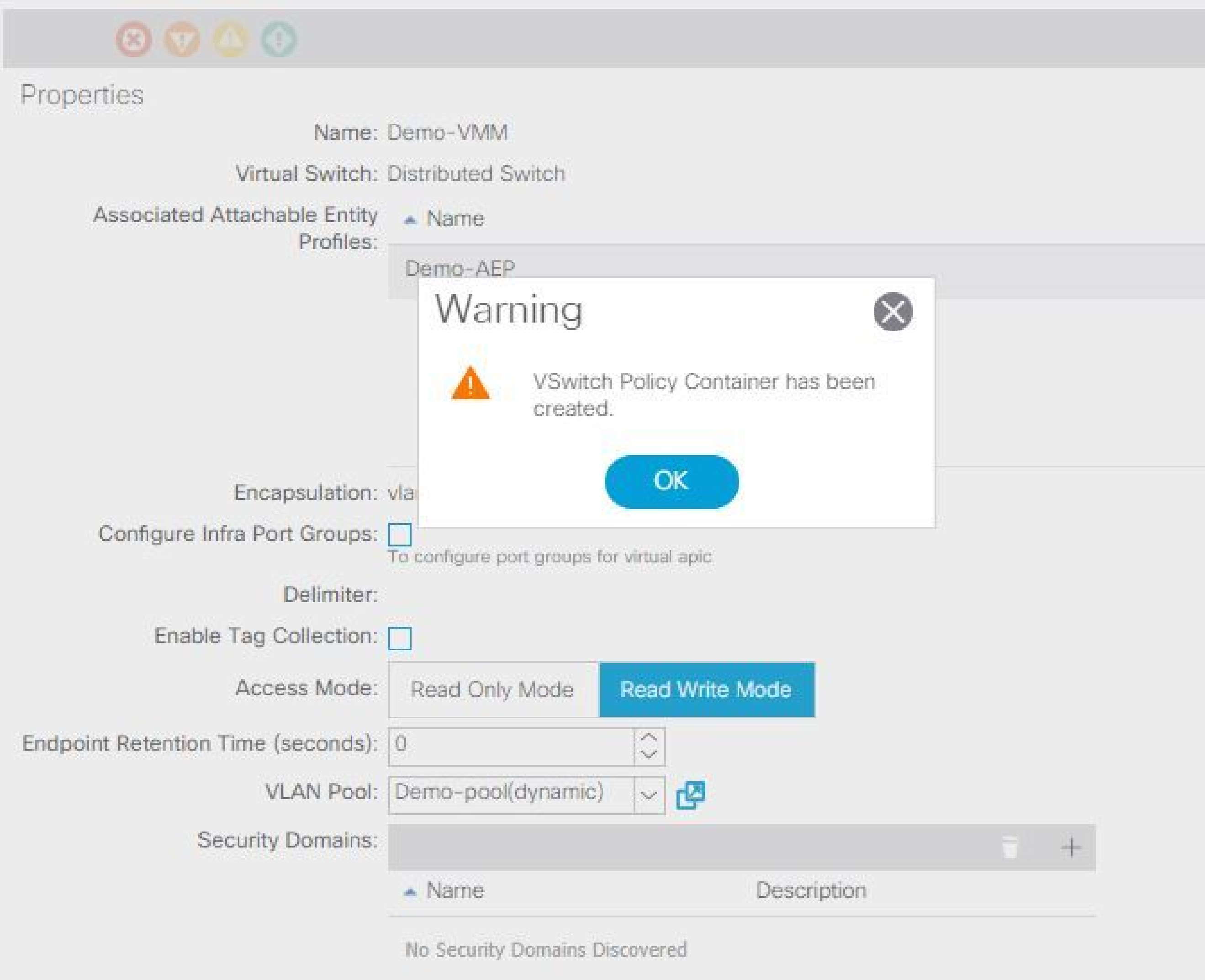
As an alternative to LLDP, use CDP in order to discover the hosts. In order to get the DVS to use CDP, configure a vSwitch policy on the VMM Domain that has CDP enabled and LLDP disabled.

Along with this, the only supported load balancing mechanism when UCS B series is used is Route Based on Originating Virtual Port. If you configure a **mac-pinning** policy, it programs the port groups to use this mechanism. This is very important in order to prevent packet loss.

1. From the APIC user interface, choose **Virtual Networking > VMM Domains > VMware > Configured Domain > Create VSwitch Policies**.



2. At this point, a warning will be displayed to alert you that a default VSwitch policy has been created.



Properties

Name: Demo-VMM

Virtual Switch: Distributed Switch

Associated Attachable Entity Profiles: Name: Demo-AEP

Encapsulation: vla

Configure Infra Port Groups: □ To configure port groups for virtual apic

Delimiter:

Enable Tag Collection: □

Access Mode: Read Only Mode | **Read Write Mode**

Endpoint Retention Time (seconds): 0

VLAN Pool: Demo-pool(dynamic)

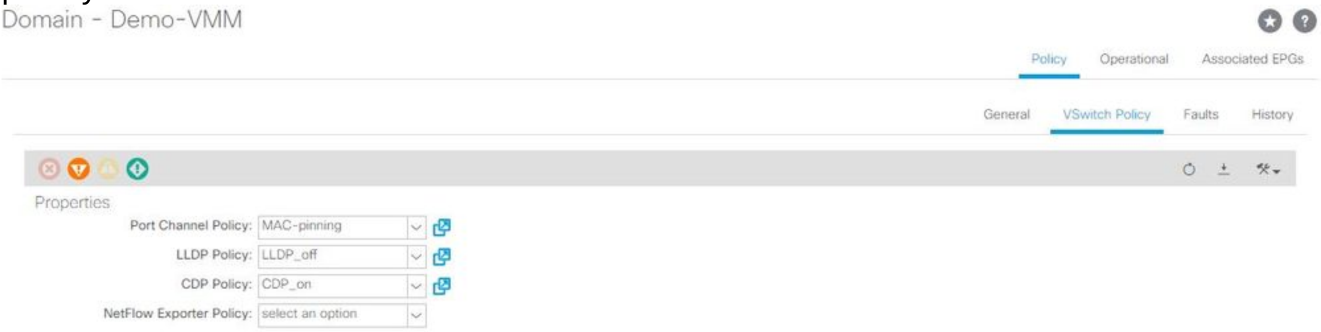
Security Domains:

Name	Description
No Security Domains Discovered	

Warning

VSwitch Policy Container has been created.

3. Accept the warning message and navigate to the **Vswitch Policy** tab under the VMM Domain: Choose or create a **CDP Policy** where **CDP is enabled**.Choose or create a **Port Channel Policy** with **mac-pinning** mode selected.Choose or create an **LLDP Policy** where **CDP is disabled**.Click **Submit**.**Note**: If you are on UCSM 2.2(4b) or later, and you want to use LLDP, you can turn on LLDP in this vSwitch policy since the UCS supports it. This example is only for UCSM versions that do not support LLDP, or if CDP is desired. If both LLDP and CDP are enabled, LLDP takes
priority.



Domain - Demo-VMM

Properties

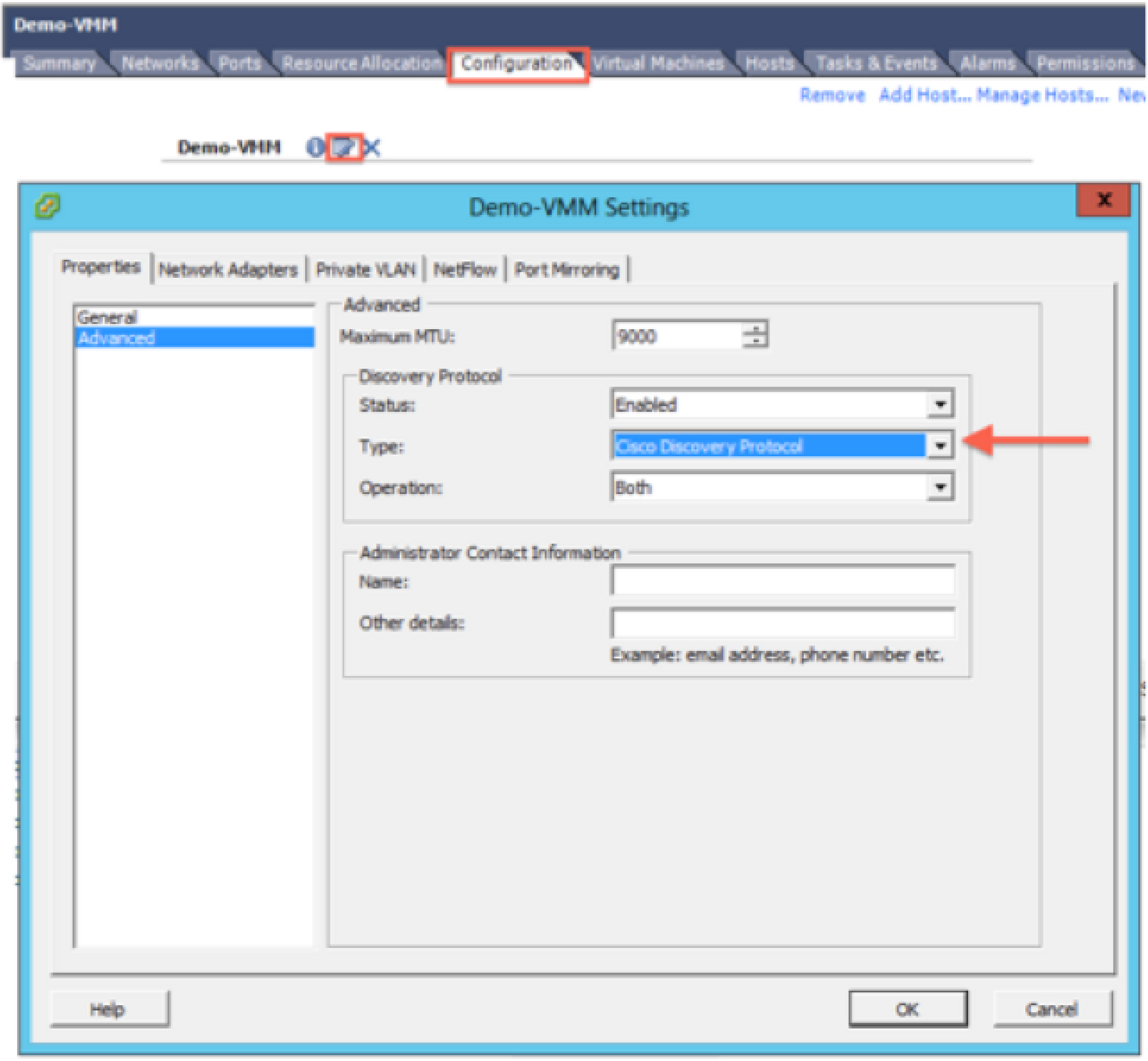
Port Channel Policy: MAC-pinning

LLDP Policy: LLDP_off

CDP Policy: CDP_on

NetFlow Exporter Policy: select an option

After you click **Submit**, you can see that the DVS is reconfigured in the
vCenter:



Advanced

Maximum MTU: 9000

Discovery Protocol

Status: Enabled

Type: Cisco Discovery Protocol

Operation: Both

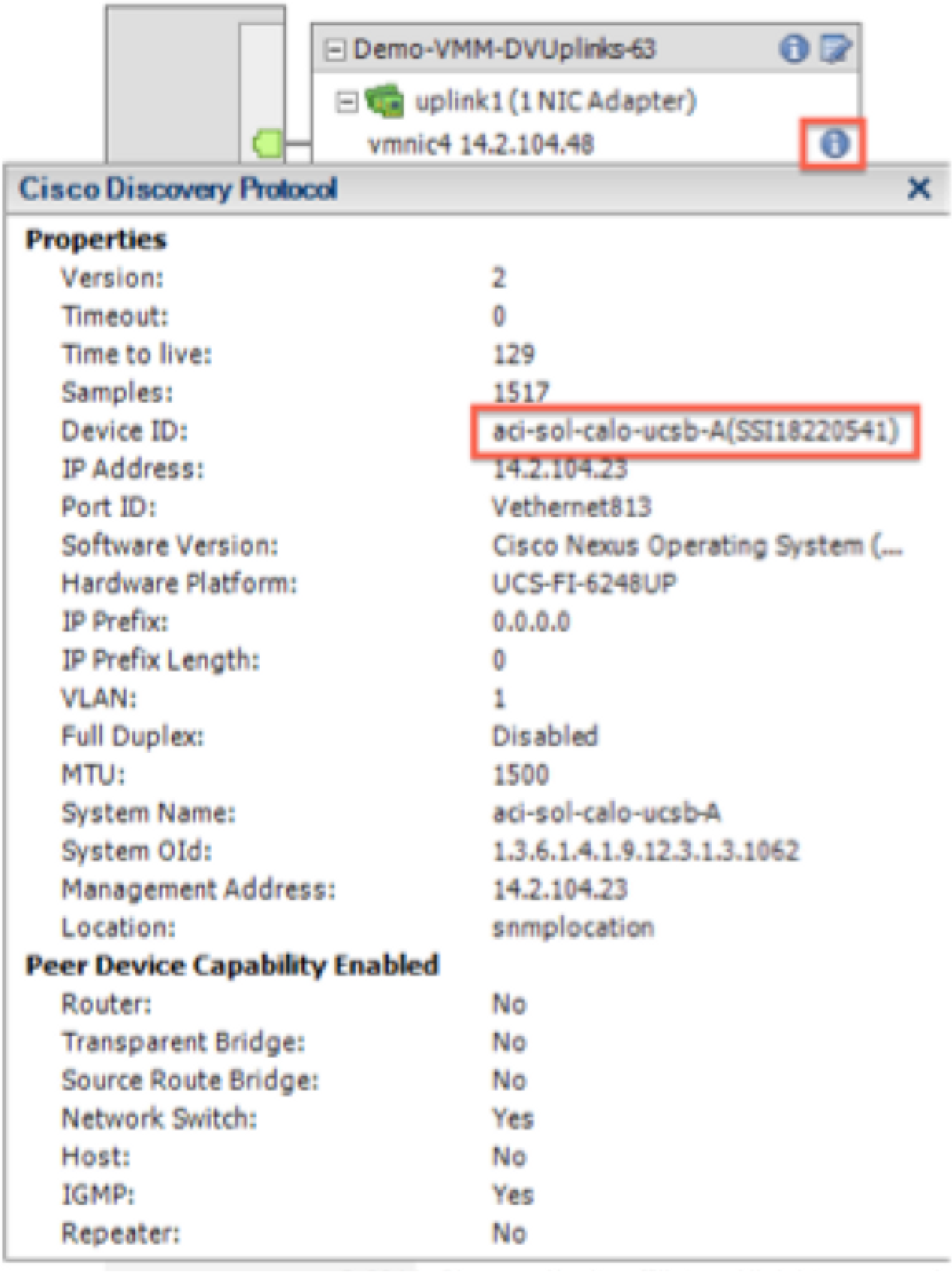
Administrator Contact Information

Name:

Other details:

Example: email address, phone number etc.

You can also verify that the vmnics see CDP information from the Fabric Interconnect:



Cisco Discovery Protocol

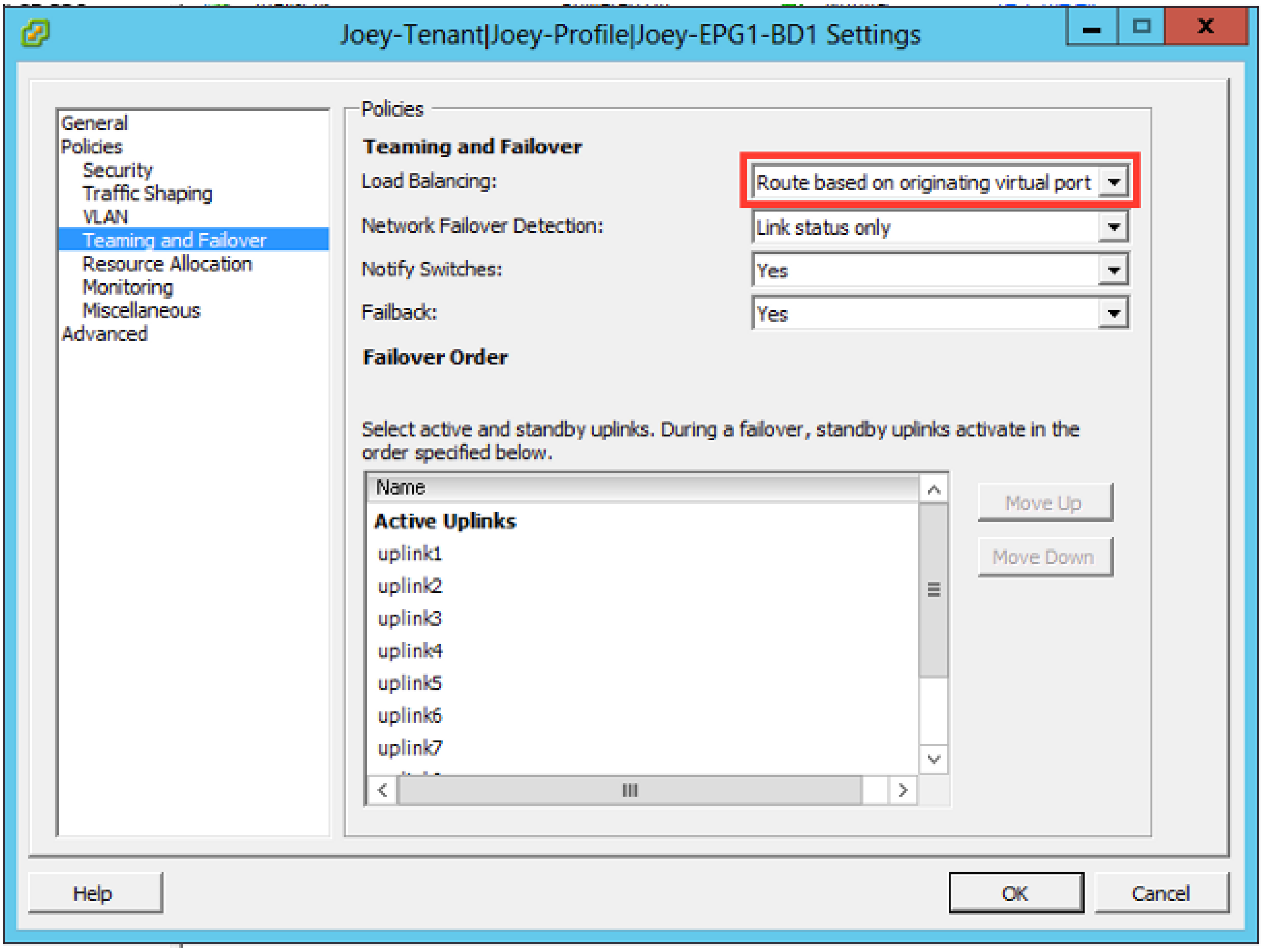
Properties

Version:	2
Timeout:	0
Time to live:	129
Samples:	1517
Device ID:	aci-sol-calo-ucsb-A(SSI18220541)
IP Address:	14.2.104.23
Port ID:	Vethernet813
Software Version:	Cisco Nexus Operating System (...
Hardware Platform:	UCS-FI-6248UP
IP Prefix:	0.0.0.0
IP Prefix Length:	0
VLAN:	1
Full Duplex:	Disabled
MTU:	1500
System Name:	aci-sol-calo-ucsb-A
System OId:	1.3.6.1.4.1.9.12.3.1.3.1062
Management Address:	14.2.104.23
Location:	snmplocation

Peer Device Capability Enabled

Router:	No
Transparent Bridge:	No
Source Route Bridge:	No
Network Switch:	Yes
Host:	No
IGMP:	Yes
Repeater:	No

4. Verify that "Route based on originating virtual port" is programmed on the port groups. Right-click a port group in the Networking tab, and edit the setting in order to verify this:



Joey-Tenant|Joey-Profile|Joey-EPG1-BD1 Settings

Policies

Teaming and Failover

Load Balancing: Route based on originating virtual port

Network Failover Detection: Link status only

Notify Switches: Yes

Failback: Yes

Failover Order

Select active and standby uplinks. During a failover, standby uplinks activate in the order specified below.

Name

Active Uplinks

uplink1

uplink2

uplink3

uplink4

uplink5

uplink6

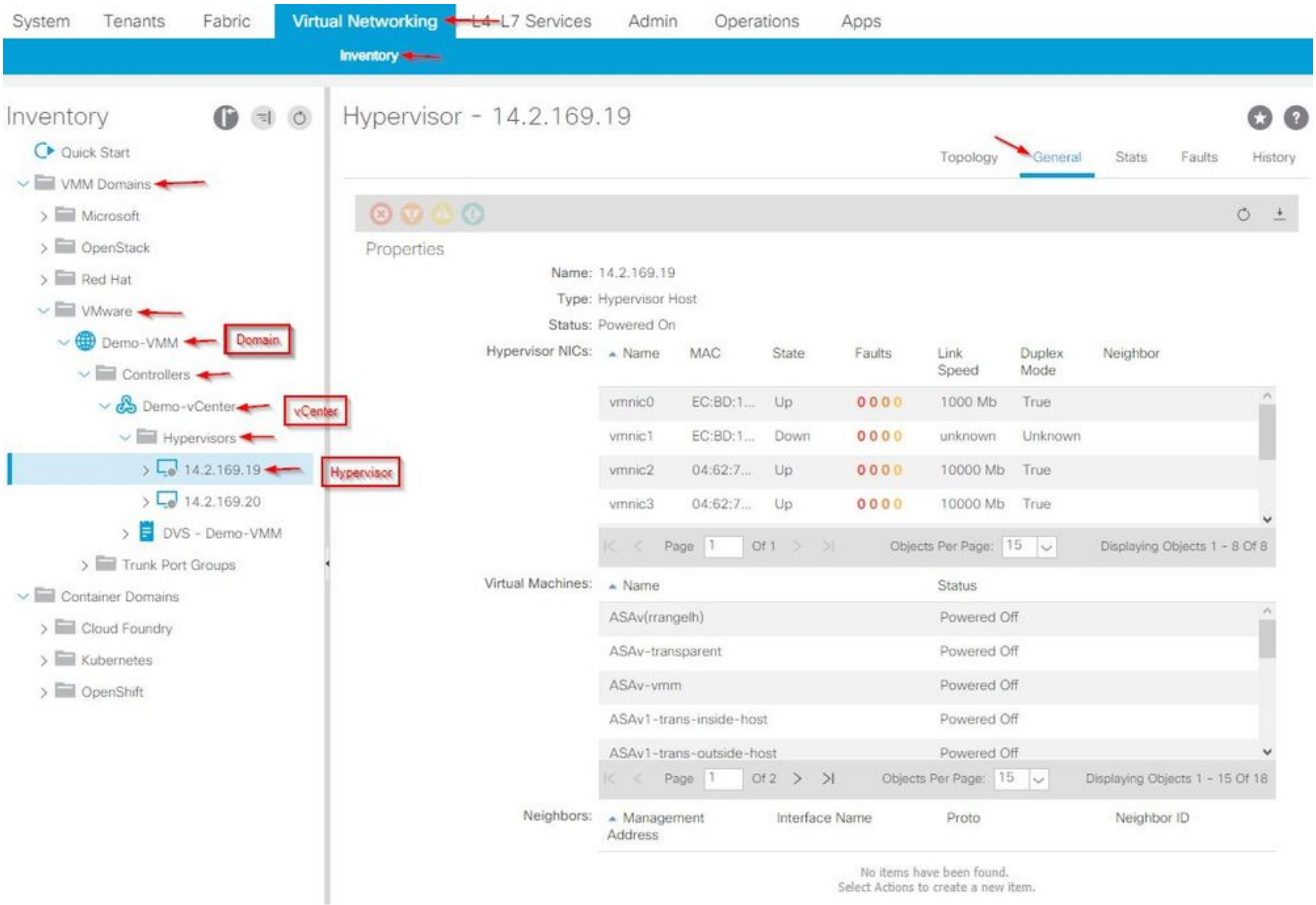
uplink7

Verify

Use this section to confirm that your configuration works properly.

After these changes are made, the APIC should be notified by the vCenter about the CDP information. In order to verify this, check the inventory of the VMM domain.

From the APIC user interface, choose **Virtual Networking** > **Inventory** > **VMM Domains > VMware** > **Domain** > **Controllers** > **vCenter** > **Hypervisors** > **Hypervisor** > **General** in order to view the Properties window.



Name: 14.2.169.19
Type: Hypervisor Host
Status: Powered On

Hypervisor NICs:

Name	MAC	State	Faults	Link Speed	Duplex Mode	Neighbor
vmnic0	EC:BD:1...	Up	0 0 0 0	1000 Mb	True	
vmnic1	EC:BD:1...	Down	0 0 0 0	unknown	Unknown	
vmnic2	04:62:7...	Up	0 0 0 0	10000 Mb	True	
vmnic3	04:62:7...	Up	0 0 0 0	10000 Mb	True	

Page 1 Of 1 Objects Per Page: 15 Displaying Objects 1 - 8 Of 8

Virtual Machines:

Name	Status
ASAv(rrangelh)	Powered Off
ASAv-transparent	Powered Off
ASAv-vmm	Powered Off
ASAv1-trans-inside-host	Powered Off
ASAv1-trans-outside-host	Powered Off

Page 1 Of 2 Objects Per Page: 15 Displaying Objects 1 - 15 Of 18

Neighbors:

Management Address	Interface Name	Proto	Neighbor ID

No items have been found.
Select Actions to create a new item.

At this point, you can change your VM Network settings to add the adapter to the proper port group and test connectivity. Pings should be successful. If pings are not successful, verify all settings in vCenter and in the APIC are correct for CDP neighbor discovery.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.