



FlashStack Virtual Server Infrastructure Deployment Guide: Cisco PowerTool Addendum

February 2017

Contents

Executive Summary	4
Introduction	4
FlashStack VSI Solution Overview	4
Cisco UCS PowerTool Suite for Microsoft PowerShell	5
Installing Cisco UCS PowerTool	6
Using Cisco UCS PowerTool	7
Configuring Cisco UCS in FlashStack VSI	9
Configure Cisco UCS Manager: Initial Steps	9
Configure Anonymous Reporting	9
PowerTool cmdlet Steps: Anonymous Reporting (Turned On).....	10
PowerTool cmdlet Steps: Anonymous Reporting (Turned Off).....	10
Synchronize Cisco UCS with NTP.....	11
PowerTool cmdlet Steps: Synchronize Cisco UCS with NTP	11
Configure Cisco UCS Servers	12
Edit Chassis Discovery Policy	12
PowerTool cmdlet Steps: Edit Chassis Discovery Policy	12
Enable Server and Uplink Ports	13
PowerTool cmdlet Steps: Enable Server and Uplink Ports.....	14
Acknowledge Cisco UCS Chassis.....	15
PowerTool cmdlet Steps: Acknowledge Cisco UCS Chassis	16
Create Pools	16
Create MAC Address Pools	16
PowerTool cmdlet Steps: Create MAC Address Pools.....	19
Create UUID Suffix Pool.....	19
PowerTool cmdlet Steps: Create UUID Suffix Pools	20
Create Server Pool.....	20
PowerTool cmdlet Steps: Create Server Pool	22
Add a Block of IP Addresses for KVM Access	22
PowerTool cmdlet Steps: Add a Block of IP Addresses for KVM Access.....	22
Create a WWNN Pool	22
PowerTool cmdlet Steps: Create a WWNN Pool.....	23
Create WWPN Pools.....	24
PowerTool cmdlet Steps: Create WWPN Pools	26
Set Packages and Policies	26
Create Host Firmware Package	26
PowerTool cmdlet Steps: Create Host Firmware Package.....	27
Create Server Pool Qualification Policy (Optional)	27
PowerTool cmdlet Steps: Create Server Pool Qualification Policy (Optional)	28
Download Cisco Custom Image for VMware ESXi 6.0 U2	28
Create vMedia Policy for VMware ESXi 6.0 U2 Install Boot (Optional If You Are Manually Attaching ISO Image Through KVM)	28
PowerTool cmdlet Steps: Create vMedia Policy for VMware ESXi 6.0 U2 Install Boot	30
Create Server BIOS Policy	30
PowerTool cmdlet Steps: Create Server BIOS Policy	31
Update the Default Maintenance Policy	31
PowerTool cmdlet Steps: Update the Default Maintenance Policy.....	32
Create Local Disk Configuration Policy (Optional).....	32
PowerTool cmdlet Steps: Create Local Disk Configuration Policy	33
Create vNIC and vHBA Placement Policy for Virtual Machine Infrastructure Hosts	33
PowerTool cmdlet Steps: Create vNIC and vHBA Placement Policy for Virtual Machine Infrastructure Hosts	34
Create Network Control Policy for Cisco Discovery Protocol	34
PowerTool cmdlet Steps: Create Network Control Policy for Cisco Discovery Protocol.....	35

Configure Cisco UCS LAN Connectivity	35
Create Uplink Port Channels	35
PowerTool cmdlet Steps: Create Uplink Port Channels	38
Create VLANs	38
PowerTool cmdlet Steps: Create VLANs.....	41
Create vNIC Templates	41
PowerTool cmdlet Steps: Create vNIC Templates	52
Set Jumbo Frames in Cisco UCS Fabric.....	53
PowerTool cmdlet Steps: Set Jumbo Frames in Cisco UCS Fabric	54
Create LAN Connectivity Policy.....	54
PowerTool cmdlet Steps: Create LAN Connectivity Policy	59
Configure Cisco UCS SAN Connectivity	60
Configure Unified Ports	60
PowerTool cmdlet Steps: Configure Unified Ports.....	61
Create VSANs	62
PowerTool cmdlet Steps: Create VSANs	63
Create Fibre Channel Port Channels	63
PowerTool cmdlet Steps: Create Fibre Channel Port Channels.....	67
Create vHBA Templates.....	68
PowerTool cmdlet Steps: Create vHBA Templates	69
Create SAN Connectivity Policy	69
PowerTool cmdlet Steps: Create SAN Connectivity Policy	72
Create Boot Policies.....	72
PowerTool cmdlet Steps: Create Boot Policies	79
Create a Service Profile Template.....	80
PowerTool cmdlet Steps: Create a Service Profile Template.....	86
Create Service Profiles.....	87
PowerTool cmdlet Steps: Create Service Profiles	88
Conclusion	88
For More Information.....	88

Executive Summary

This document describes the configuration of Cisco Unified Computing System™ (Cisco UCS®) components detailed in the Cisco® Validated Design for FlashStack Virtual Server Infrastructure (VSI) design and deployment guides for VMware vSphere 6.0 U2 using cmdlets from the Cisco UCS PowerTool Suite for Microsoft PowerShell.

FlashStack VSI runs VMware vSphere using the Pure Storage FlashArray//M all-flash array, Cisco UCS, Cisco Nexus® 9000 Series Switches, and Cisco MDS 9000 Family Fibre Channel switches.

The scope of this document is limited to Cisco UCS PowerTool configuration for Cisco UCS in FlashStack VSI. For the complete FlashStack VSI deployment, see the FlashStack VSI deployment guide at

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/ucs_flashstack_vsi_vm6.html.

Introduction

Cisco and Pure Storage worked together to produce the FlashStack VSI Cisco Validated Design for VMware vSphere. The design uses best-in-class storage, server, and network components as the foundation for virtualized workloads, enabling efficient architectural designs that can be quickly and confidently deployed.

This document adds to the implementation of the FlashStack VSI a simplified option for configuring the Cisco UCS elements using the Cisco UCS Manager module of Cisco UCS PowerTool for Microsoft PowerShell. The Cisco UCS PowerTool Suite is a set of PowerShell modules that helps automate all aspects of Cisco UCS Manager, Cisco UCS Central Software, and Cisco Integrated Management Controller (IMC). It can also help automate server, network, storage, and hypervisor management.

The steps presented in this document show the specific cmdlets for configuring the resources detailed in the FlashStack VSI validated designs. These cmdlet invocations can be adjusted to accommodate connectivity and component changes that differ from the equipment used in the FlashStack VSI validated designs, but details of these change options are not covered in this document and will need to be researched independently. For additional information about the Cisco UCS PowerTool Suite, including release notes and related documentation, see

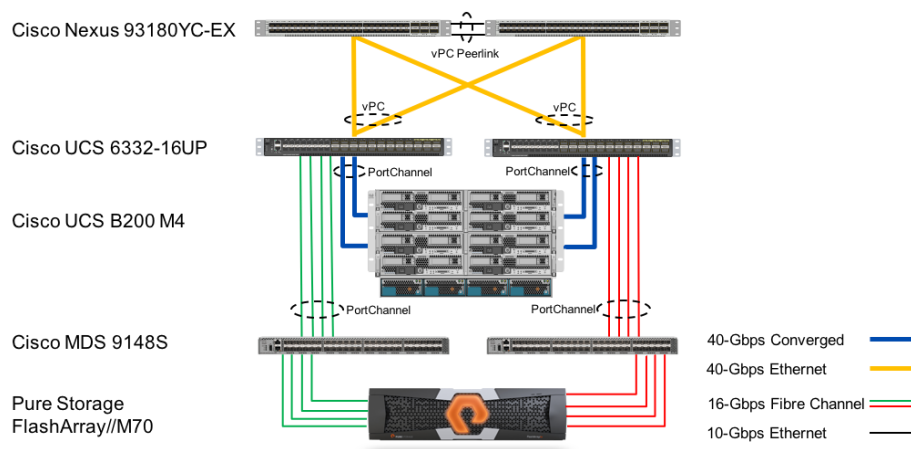
https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/msft_tools/All_Plugin_RN/PowerTool/2x/b_Cisco_UCS_PowerTool_Suite_Release_Notes_2x.html.

FlashStack VSI Solution Overview

FlashStack Virtual Server Infrastructure is a validated reference architecture developed by Cisco and Pure Storage to serve enterprise data centers. The solution is built to deliver a VMware vSphere–based environment using the Cisco UCS platform, Cisco Nexus switches, Cisco MDS 9000 Family multilayer fabric switches, and Pure Storage FlashArray.

The architecture brings together a simple, wire-once solution that is SAN booted and highly resilient at each layer of the design. This approach creates an infrastructure that is well suited for a variety of virtual application deployments that can reliably scale when expansion is needed. **Error! Reference source not found.** shows the base physical architecture used in FlashStack VSI.

Figure 1. FlashStack with Cisco UCS 6332-16UP Fabric Extender and Pure Storage FlashArray//M70



The reference hardware configuration includes:

- Two Cisco Nexus 93180YC-EX Switches
- Two Cisco UCS 6332-16UP Fabric Interconnects
- Cisco UCS 5108 Chassis with two Cisco UCS 2304 Fabric Extenders
- Cisco UCS B200 M4 Blade Servers
- Two Cisco MDS 9148S Multilayer Fabric Switches
- Pure Storage FlashArray//M70

The virtual environment that this configuration supports uses VMware vSphere 6.0 U2. Virtual management and automation components from Cisco and Pure Storage can be either built in to the solution or installed as optional add-ons.

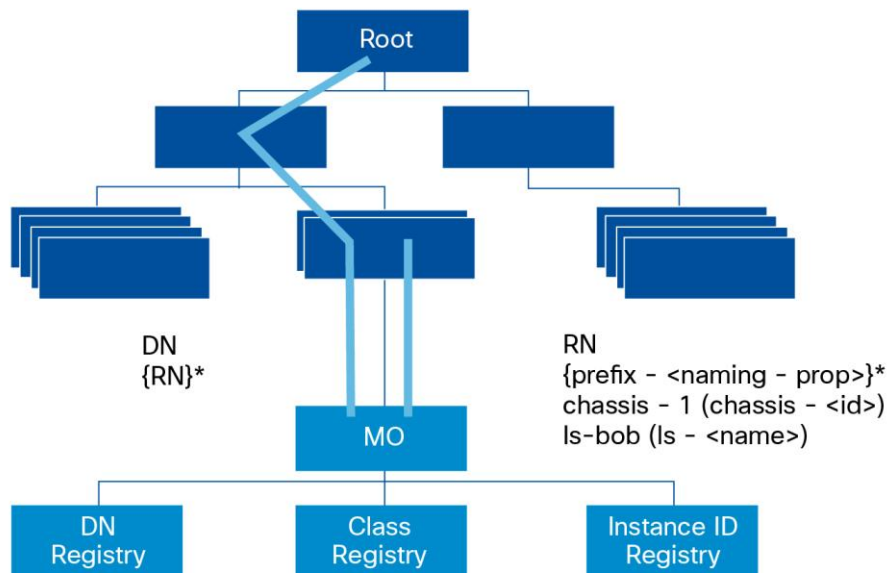
For a more thorough discussion of the design, refer to the FlashStack VSI Design Guide for VMware vSphere 6.0 U2 at

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/ucs_flashstack_vsi_vm6_designs.html.

Cisco UCS PowerTool Suite for Microsoft PowerShell

The Cisco UCS PowerTool Suite is a set of modules for Microsoft PowerShell that makes available cmdlets that can be used for Cisco UCS Manager, IMC, and Cisco UCS Central Software operations from within PowerShell. The cmdlets work within the Cisco UCS Manager management information tree (MIT), performing operations on the managed objects within the tree.

Figure 2. Cisco UCS Management Information Tree



For a more thorough discussion of the implementation, refer to the Cisco UCS Manager PowerTool User Guide at http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/msft_tools/powertools/ucs_powertool_book/2x/b_Cisco_UCSM_PowerTool_UG_Release_2x/b_Cisco_UCSM_PowerTool_UG_Release_2x_chapter_00.html.

Installing Cisco UCS PowerTool

Microsoft PowerShell is required to run the Cisco UCS PowerTool cmdlets. PowerShell 3.0 can be downloaded from Microsoft at <https://www.microsoft.com/en-us/download/details.aspx?id=34595>.

The Cisco UCS PowerTool Suite for Microsoft PowerShell comes as a download from Cisco.com and can be found at <https://software.cisco.com/download/release.html?i=!y&mdfid=286305108&softwareid=284574017&release=2.1.1>.

The complete Microsoft Installer (MSI) installation package installs:

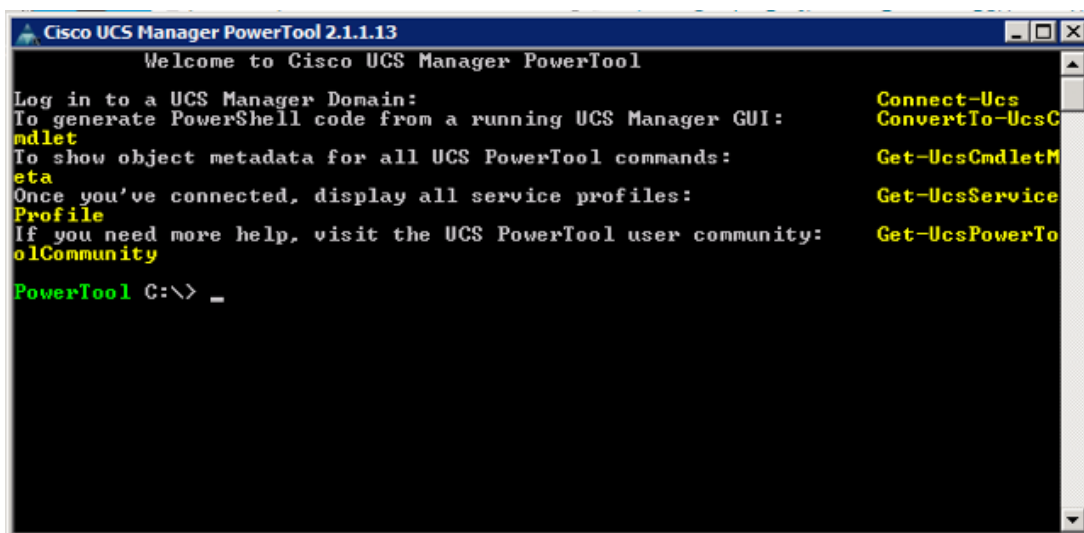
- Cisco UCS Manager PowerTool
- Cisco IMC PowerTool
- Cisco UCS Central PowerTool
- Cisco UCS Desired State Configuration (DSC) Resource

You can select the Custom installation option to install just the Cisco UCS Manager module for PowerTool, or you can select the Complete setup option to install all modules.

Using Cisco UCS PowerTool

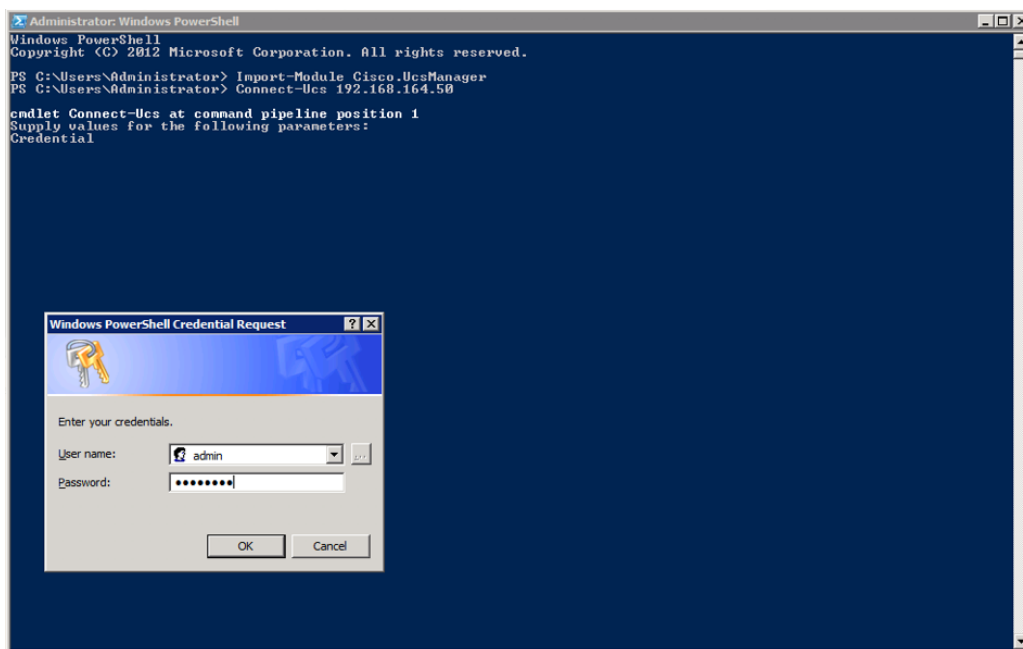
With the installation package in place, you can run cmdlets from the Cisco UCS Manager PowerTool terminal that will be installed (Figure 3).

Figure 3. Cisco UCS Manager PowerTool Terminal



However, if you prefer you can use the native Microsoft PowerShell terminal after you import the PowerTool module with the **Import-Module Cisco.UcsManager** command (Figure 4).

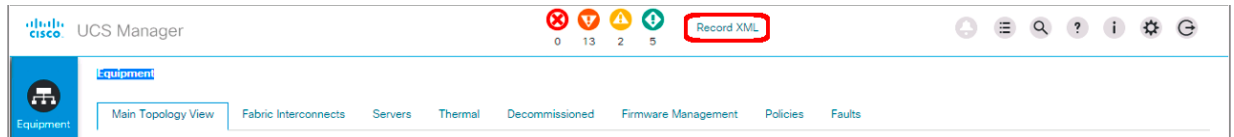
Figure 4. Microsoft PowerShell Terminal importing the Cisco UCS Manager PowerTool Module and Connecting to Cisco UCS Manager



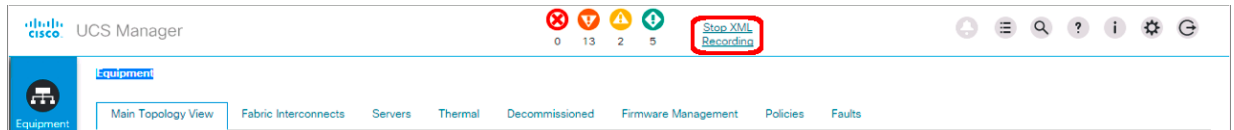
You can display a list of the cmdlets from within PowerShell by using the command **Get-Command -Module Cisco.UcsManager**. In addition, you can explore examples of use in the [PowerTool user guide](#) and samples published by at the [Cisco Communities website](#).

A quick way to get started is to generate XML from the Cisco UCS Manager HTML interface.

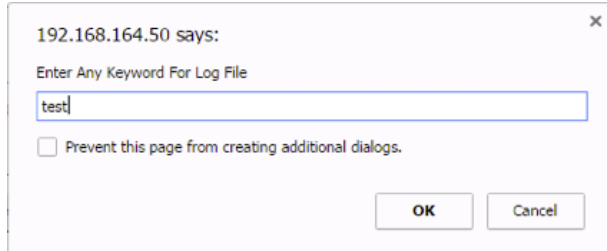
1. With the Cisco UCS Manager HTML interface open, capture the XML command by pressing the command sequence Ctrl+Alt+Q. Then click the Record XML button in Cisco UCS Manager.



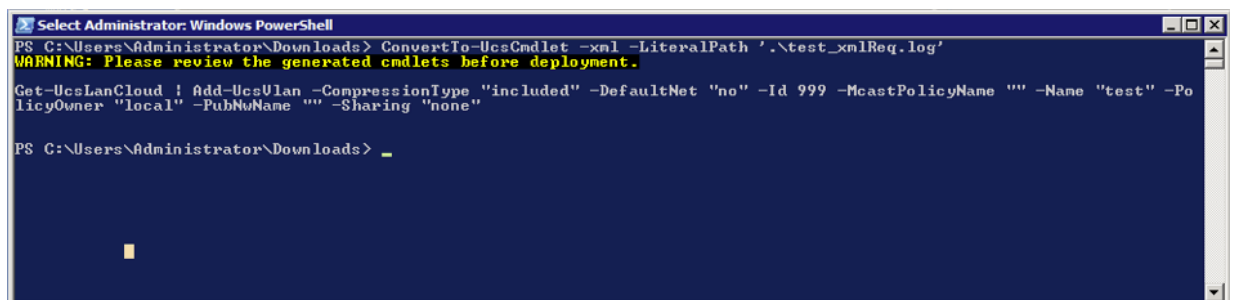
2. With the recording started, commands invoked through the Cisco UCS Manager HTML GUI will be collected as XML equivalents. To stop recording and save the commands to a file, click Stop XML Recording.



3. Stopping the recording displays a prompt asking you to name the generated XML file. Enter a keyword to name the file and then click OK to save the file.



4. The resulting XML log file will be named <keyword>_xmlReq.log. You can use it to generate the equivalent cmdlets by entering **ConvertTo-UcsCmdlet -xml -LiteralPath <XML_LogFile>**.

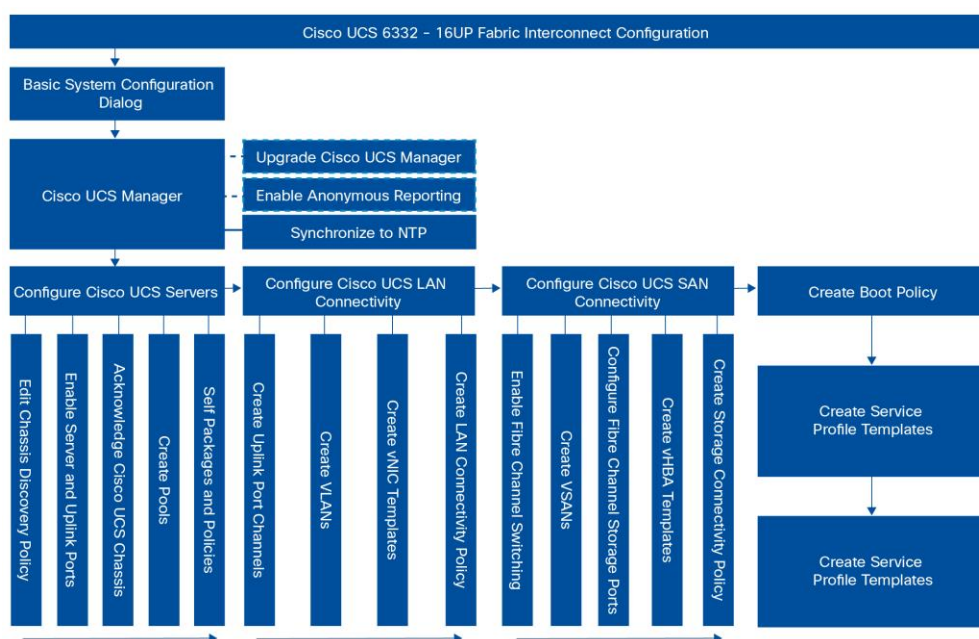


Configuring Cisco UCS in FlashStack VSI

This section presents the steps for configuring FlashStack VSI. The Cisco UCS Manager GUI configuration steps are presented first, and the equivalent PowerTool cmdlets are presented immediately following each set of instructions. These steps are appropriate for the specific physical cabling and network configuration for FlashStack VSI. They are provided as examples and will need to be adjusted if your environment differs.

This section presents the steps shown in **Error! Reference source not found.** with the exception of those for the Basic System Configuration Dialog and Upgrade Cisco UCS Manager workflows.

Figure 5. Cisco UCS Configuration Workflow from the FlashStack VSI Deployment Guide



The steps shown in **Error! Reference source not found.** will be shown with the exception of the Basic System Configuration Dialog and the Upgrade of Cisco UCS Manager. All other steps are included as follows:

Configure Cisco UCS Manager: Initial Steps

This section presents the initial steps for configuring Cisco UCS Manager.

Configure Anonymous Reporting

When you first connect to the Cisco UCS Manager GUI, a pop-up window appears asking whether you want to allow Cisco to collect anonymous information about your use to help with future development. To configure anonymous reporting, complete the following step:

- In the Anonymous Reporting window, select Yes or No to indicate whether you want to send anonymous data to Cisco to help improve future products:

Anonymous Reporting

Cisco Systems, Inc. will be collecting feature configuration and usage statistics which will be sent to Cisco Smart Call Home server anonymously. This data helps us prioritize the features and improvements that will most benefit our customers.
If you decide to enable this feature in future, you can do so from the "Anonymous Reporting" in the Call Home settings under the Admin tab.
[View Sample Data](#)

Do you authorize the disclosure of this information to Cisco Smart CallHome?
☒ Yes ☐ No

SMTP Server

Host (IP Address or Hostname):

Port:

☐ Don't show this message again.

If you later want to enable or disable Anonymous Reporting, you can find the configuration in Cisco UCS Manager at Admin > Communication Management > Call Home. Click the tab at the far right for Anonymous Reporting.

PowerTool cmdlet Steps: Anonymous Reporting (Turned On)

```
Start-UcsTransaction
Add-UcsManagedObject -ModifyPresent -ClassId CallhomeAnonymousReporting -PropertyMap @{AdminState="on"; Dn="call-home/anonymousreporting"; }
Add-UcsManagedObject -ModifyPresent -ClassId CallhomeSmtplib -PropertyMap @{Dn="call-home/smtplib"; Host="192.168.164.25"; }
Complete-UcsTransaction
```

PowerTool cmdlet Steps: Anonymous Reporting (Turned Off)

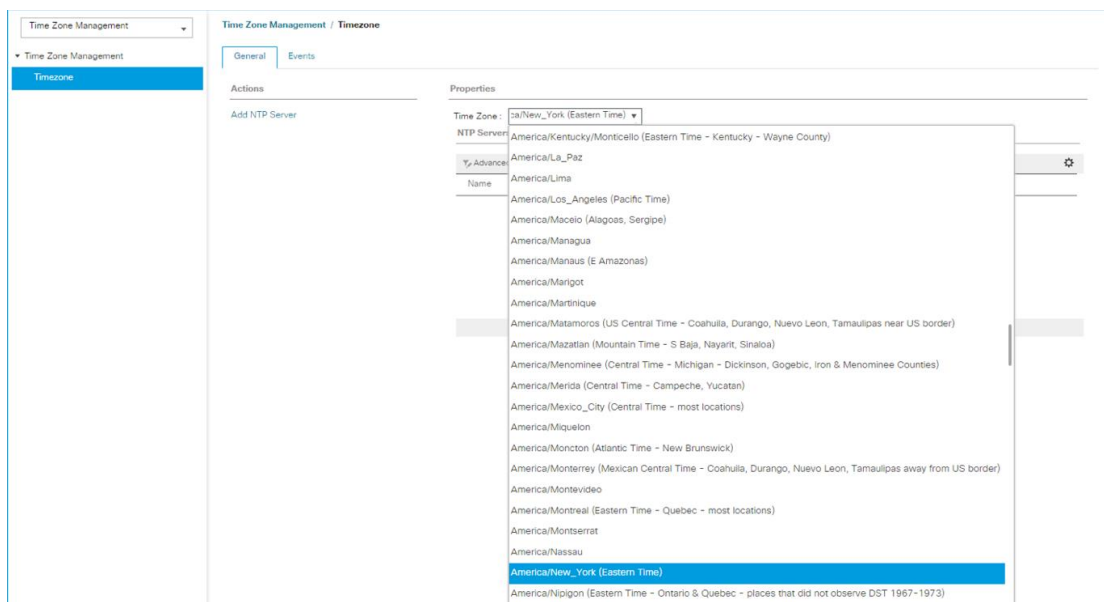
```
Add-UcsManagedObject -ModifyPresent -ClassId CallhomeAnonymousReporting -PropertyMap @{AdminState="off"; Dn="call-home/anonymousreporting"; }
```

Note: These cmdlets do not disable the Anonymous Reporting pop-up in the Cisco UCS Manager GUI or HTML interface. To disable the pop-up in the manager, you will need to be disable them from the Cisco UCS Manager GUI or HTML interface.

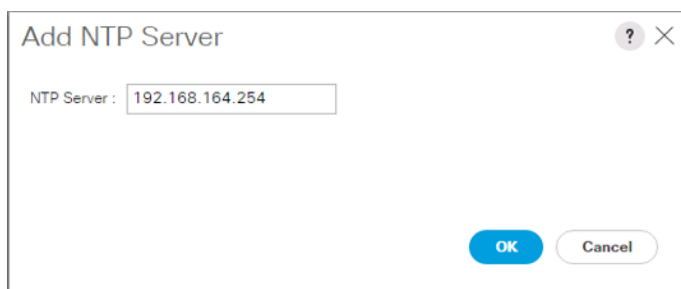
Synchronize Cisco UCS with NTP

To synchronize the Cisco UCS environment with the Network Time Protocol (NTP) server, complete the following steps:

1. In Cisco UCS Manager, click the Admin tab in the navigation pane.
2. Select All > Timezone Management.



3. In the Properties pane, select the appropriate time zone in the Timezone menu.
4. Click Save Changes and then click OK.
5. Click Add NTP Server.
6. Enter a valid NTP server address and click OK.



7. Click OK.

PowerTool cmdlet Steps: Synchronize Cisco UCS with NTP

```
Get-UcsSvcEp | Add-UcsManagedObject -ModifyPresent -ClassId CommDateTime -  
PropertyMap @{Timezone="America/New_York (Eastern Time)"};  
Get-UcsSvcEp | Get-UcsTimezone | Add-UcsNtpServer -Name "192.168.164.254"
```

Configure Cisco UCS Servers

This section presents steps for configuring the Cisco UCS servers.

Edit Chassis Discovery Policy

Setting the discovery policy simplifies the addition of Cisco UCS B-Series Blade Server Chassis. To modify the chassis discovery policy, complete the following steps:

1. In Cisco UCS Manager, click the Equipment tab in the navigation pane and select Equipment in the list on the left under the pull-down menu.
2. In the right pane, click the Policies tab.
3. Under Global Policies, set the Chassis/FEX Discovery Policy to match the number of uplink ports that are cabled between the chassis or fabric extenders (FEXes) and the fabric interconnects.
4. Set the Link Grouping Preference to Port Channel.

The screenshot shows the Cisco UCS Manager web interface. The browser address bar displays `ucs-6332-16up - Unified C: x` and `192.168.164.50/app/3_1_2b/index.html#`. The page title is "UCS Manager". The left navigation pane has a blue sidebar with icons for Equipment, Servers, LAN, SAN, VM, Storage, Chassis, and Admin. The "Equipment" tab is selected. The main content area shows the "Policies" tab. Under "Global Policies", the "Chassis/FEX Discovery Policy" is configured. The settings are as follows:

- Chassis/FEX Discovery Policy**
 - Action: ☐ 2 Link
 - Link Grouping Preference: ☐ None ☒ Port Channel
 - Backplane Speed Preference: ☒ 40G ☐ 4x10G
- Rack Server Discovery Policy**
 - Action: ☒ Immediate ☐ User Acknowledged
 - Scrub Policy:
- Rack Management Connection Policy**
 - Action: ☒ Auto Acknowledged ☐ User Acknowledged
- Power Policy**
 - Redundancy: ☐ Non Redundant ☒ N+1 ☐ Grid
- MAC Address Table Aging**
 - Aging Time: ☐ Never ☒ Mode Default ☐ other
- Global Power Allocation Policy**
 - Allocation Method: ☐ Manual Blade Level Cap ☒ Policy Driven Chassis Group Cap
- Firmware Auto Sync Server Policy**
 - Sync State: ☒ No Actions ☐ User Acknowledge
- Global Power Profiling Policy**
 - Profile Power:
- Info Policy**
 - Action: ☒ Disabled ☐ Enabled

At the bottom right, there are two buttons: "Save Changes" and "Reset Values".

5. Leave other settings alone or change if appropriate to your environment.
6. Click Save Changes.
7. Click OK.

PowerTool cmdlet Steps: Edit Chassis Discovery Policy

```
Add-UcsManagedObject -ModifyPresent -ClassId ComputeChassisDiscPolicy -  
PropertyMap @{LinkAggregationPref="port-channel"; Action="2-link"; Dn="org-  
root/chassis-discovery"; }
```

Enable Server and Uplink Ports

To enable server and uplink ports, complete the following steps:

1. In Cisco UCS Manager, click the Equipment tab in the navigation pane.
2. Select Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module.
3. Expand Ethernet Ports.
4. Select the ports that are connected to the chassis, right-click them, and select Configure as Server Port.

The screenshot shows the Cisco UCS Manager interface. The 'Equipment' tab is selected, and the navigation pane shows 'Fabric Interconnects' > 'Fabric Interconnect A (primary)' > 'Fixed Module'. The 'Ethernet Ports' section is expanded, showing a list of ports from Port 7 to Port 39. A right-click context menu is open over Port 17, with the option 'Configure as Server Port' highlighted. The table below shows the details of the ports.

Name	Address	IF Role	IF Type	Overall Status	Admin State
▼ Fabric Interconnect A (primary)					
▼ Fixed Module					
▼ Ethernet Ports					
Port 7	00:DE:FB:07:C9:92	Unconfigured	Physical	Stp Not Present	Disabled
Port 8	00:DE:FB:07:C9:93	Unconfigured	Physical	Stp Not Present	Disabled
Port 9	00:DE:FB:07:C9:94	Unconfigured	Physical	Stp Not Present	Disabled
Port 10	00:DE:FB:07:C9:95	Unconfigured	Physical	Stp Not Present	Disabled
Port 11	00:DE:FB:07:C9:96	Unconfigured	Physical	Stp Not Present	Disabled
Port 12	00:DE:FB:07:C9:97	Unconfigured	Physical	Stp Not Present	Disabled
Port 13	00:DE:FB:07:C9:98	Unconfigured	Physical	Stp Not Present	Disabled
Port 14	00:DE:FB:07:C9:99	Unconfigured	Physical	Stp Not Present	Disabled
Port 15	00:DE:FB:07:C9:9A	Unconfigured	Physical	Stp Not Present	Disabled
Port 16	00:DE:FB:07:C9:9B	Unconfigured	Physical	Stp Not Present	Disabled
Port 17	00:DE:FB:07:C9:9C	Unconfigured	Physical	Admin Down	Disabled
Port 18	00:DE:FB:07:C9:9D	Unconfigured	Physical	Admin Down	Disabled
Port 19	00:DE:FB:07:C9:9E	Unconfigured	Physical	Admin Down	Disabled
Port 20	00:DE:FB:07:C9:9F	Unconfigured	Physical	Admin Down	Disabled
Port 21	00:DE:FB:07:C9:A0	Unconfigured	Physical	Stp Not Present	Disabled
Port 22	00:DE:FB:07:C9:A1	Unconfigured	Physical	Stp Not Present	Disabled
Port 23	00:DE:FB:07:C9:A2	Unconfigured	Physical	Stp Not Present	Disabled
Port 24	00:DE:FB:07:C9:A3	Unconfigured	Physical	Stp Not Present	Disabled
Port 25	00:DE:FB:07:C9:A4	Unconfigured	Physical	Stp Not Present	Disabled
Port 26	00:DE:FB:07:C9:A5	Unconfigured	Physical	Stp Not Present	Disabled
Port 27	00:DE:FB:07:C9:A6	Unconfigured	Physical	Stp Not Present	Disabled
Port 28	00:DE:FB:07:C9:A7	Unconfigured	Physical	Stp Not Present	Disabled
Port 29	00:DE:FB:07:C9:A8	Unconfigured	Physical	Stp Not Present	Disabled
Port 30	00:DE:FB:07:C9:A9	Unconfigured	Physical	Stp Not Present	Disabled
Port 31	00:DE:FB:07:C9:AA	Unconfigured	Physical	Stp Not Present	Disabled
Port 32	00:DE:FB:07:C9:AB	Unconfigured	Physical	Stp Not Present	Disabled
Port 33	00:DE:FB:07:C9:AC	Unconfigured	Physical	Stp Not Present	Disabled
Port 34	00:DE:FB:07:C9:AD	Unconfigured	Physical	Stp Not Present	Disabled
Port 35	00:DE:FB:07:C9:AE	Unconfigured	Physical	Stp Not Present	Disabled
Port 36	00:DE:FB:07:C9:AF	Unconfigured	Physical	Stp Not Present	Disabled
Port 37	00:DE:FB:07:C9:B0	Unconfigured	Physical	Stp Not Present	Disabled
Port 38	00:DE:FB:07:C9:B1	Unconfigured	Physical	Stp Not Present	Disabled
Port 39	00:DE:FB:07:C9:B2	Unconfigured	Physical	Stp Not Present	Disabled
Port 40	00:DE:FB:07:C9:B3	Unconfigured	Physical	Stp Not Present	Disabled

5. Click Yes to confirm server ports and click OK.
6. Verify that the ports connected to the chassis are now configured as server ports.
7. Select ports 39 and 40 that are connected to the Cisco Nexus switches, right-click them, and select Configure as Uplink Port.

Equipment

Main Topology View Fabric Interconnects Servers Thermal Decommissioned Firmware Management Policies Faults

+ - Advanced Filter Export Print

Name	Address	If Role	If Type	Overall Status	Admin State
Port 17	00:DE:FB:07:C9:9C	Server	Physical	Up	Enabled
Port 18	00:DE:FB:07:C9:A0	Server	Physical	Up	Enabled
Port 19	00:DE:FB:07:C9:A4	Unconfigured	Physical	Admin Down	Disabled
Port 20	00:DE:FB:07:C9:A8	Unconfigured	Physical	Admin Down	Disabled
Port 21	00:DE:FB:07:C9:AC	Unconfigured	Physical	Stp Not Present	Disabled
Port 22	00:DE:FB:07:C9:B0	Unconfigured	Physical	Stp Not Present	Disabled
Port 23	00:DE:FB:07:C9:B4	Unconfigured	Physical	Stp Not Present	Disabled
Port 24	00:DE:FB:07:C9:B8	Unconfigured	Physical	Stp Not Present	Disabled
Port 25	00:DE:FB:07:C9:BC	Unconfigured	Physical	Stp Not Present	Disabled
Port 26	00:DE:FB:07:C9:C0	Unconfigured	Physical	Stp Not Present	Disabled
Port 27	00:DE:FB:07:C9:C4	Unconfigured	Physical	Stp Not Present	Disabled
Port 28	00:DE:FB:07:C9:C8	Unconfigured	Physical	Stp Not Present	Disabled
Port 29	00:DE:FB:07:C9:CC	Unconfigured	Physical	Stp Not Present	Disabled
Port 30		Unconfigured	Physical	Stp Not Present	Disabled
Port 31		Unconfigured	Physical	Stp Not Present	Disabled
Port 32		Unconfigured	Physical	Stp Not Present	Disabled
Port 33		Unconfigured	Physical	Stp Not Present	Disabled
Port 34		Unconfigured	Physical	Stp Not Present	Disabled
Port 35		Unconfigured	Physical	Stp Not Present	Disabled
Port 36		Unconfigured	Physical	Stp Not Present	Disabled
Port 37		Unconfigured	Physical	Stp Not Present	Disabled
Port 38		Unconfigured	Physical	Stp Not Present	Disabled
Port 39		Unconfigured	Physical	Admin Down	Disabled
Port 40	00:DE:FB:07:C9:E9	Unconfigured	Physical	Admin Down	Disabled

FC Ports

Fabric Interconnect B (subordinate)

Add Delete Info

Save Changes Reset Values

- Click Yes to confirm uplink ports and click OK.
- Select Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module.
- Expand Ethernet Ports.
- Select the ports that are connected to the chassis, right-click them, and select Configure as Server Port.
- Click Yes to confirm server ports and click OK.
- Select ports 39 and 40 that are connected to the Cisco Nexus switches, right-click them, and select Configure as Uplink Port.
- Click Yes to confirm the uplink ports and click OK.

PowerTool cmdlet Steps: Enable Server and Uplink Ports

```
Start-UcsTransaction
```

```
$mo = Add-UcsManagedObject -ModifyPresent -ClassId FabricDceSwSrv -PropertyMap @{"Id"="A"; Dn="fabric/server/sw-A"; }
```

```
$mo_1 = $mo | Add-UcsServerPort -AdminState "enabled" -AutoNegotiate "yes" -Name "" -PortId 17 -SlotId 1 -UsrLbl ""
```

```
$mo_2 = $mo | Add-UcsServerPort -AdminState "enabled" -AutoNegotiate "yes" -Name "" -PortId 18 -SlotId 1 -UsrLbl ""
```

```
Complete-UcsTransaction
```

```
Start-UcsTransaction
```

```
$mo = Add-UcsManagedObject -ModifyPresent -ClassId FabricEthLan -PropertyMap @{"Id"="A"; Dn="fabric/lan/A"; }
```

```
$mo_1 = $mo | Add-UcsUplinkPort -ModifyPresent -AdminSpeed "10gbps" -AdminState "enabled" -AutoNegotiate "yes" -EthLinkProfileName "default" -FlowCtrlPolicy "default" -Name "" -PortId 39 -SlotId 1 -UsrLbl ""
```

```

$mo_2 = $mo | Add-UcsUplinkPort -ModifyPresent -AdminSpeed "10gbps" -AdminState
"enabled" -AutoNegotiate "yes" -EthLinkProfileName "default" -FlowCtrlPolicy
"default" -Name "" -PortId 40 -SlotId 1 -UsrLbl ""
Complete-UcsTransaction

Start-UcsTransaction
$mo = Add-UcsManagedObject -ModifyPresent -ClassId FabricDceSwSrv -PropertyMap
@{Id="B"; Dn="fabric/server/sw-B"; }
$mo_1 = $mo | Add-UcsServerPort -AdminState "enabled" -AutoNegotiate "yes" -Name
"" -PortId 17 -SlotId 1 -UsrLbl ""
$mo_2 = $mo | Add-UcsServerPort -AdminState "enabled" -AutoNegotiate "yes" -Name
"" -PortId 18 -SlotId 1 -UsrLbl ""
Complete-UcsTransaction

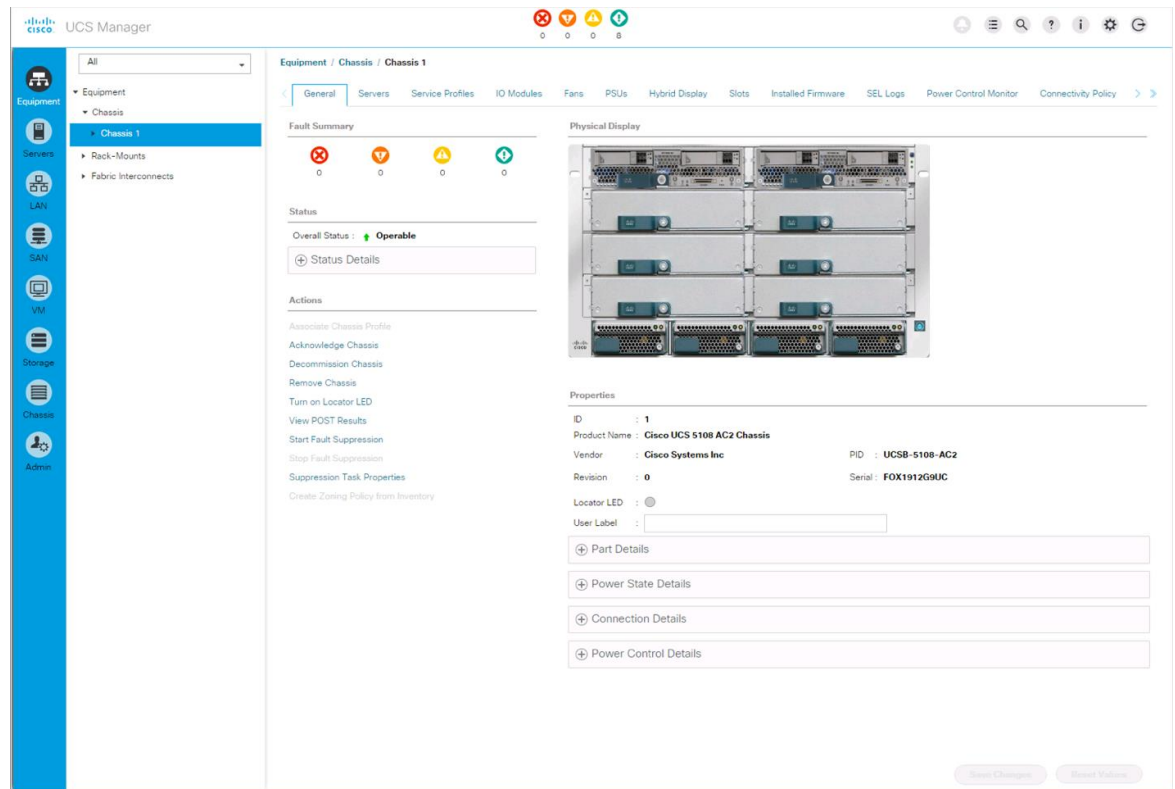
Start-UcsTransaction
$mo = Add-UcsManagedObject -ModifyPresent -ClassId FabricEthLan -PropertyMap
@{Id="B"; Dn="fabric/lan/B"; }
$mo_1 = $mo | Add-UcsUplinkPort -ModifyPresent -AdminSpeed "10gbps" -AdminState
"enabled" -AutoNegotiate "yes" -EthLinkProfileName "default" -FlowCtrlPolicy
"default" -Name "" -PortId 39 -SlotId 1 -UsrLbl ""
$mo_2 = $mo | Add-UcsUplinkPort -ModifyPresent -AdminSpeed "10gbps" -AdminState
"enabled" -AutoNegotiate "yes" -EthLinkProfileName "default" -FlowCtrlPolicy
"default" -Name "" -PortId 40 -SlotId 1 -UsrLbl ""
Complete-UcsTransaction

```

Acknowledge Cisco UCS Chassis

To acknowledge all Cisco UCS chassis, complete the following steps:

1. In Cisco UCS Manager, click the Equipment tab in the navigation pane.
2. Expand Chassis and select each chassis that is listed.
3. Right-click each chassis and select Acknowledge Chassis.



4. Click Yes and then click OK to complete acknowledgement of the chassis.

PowerTool cmdlet Steps: Acknowledge Cisco UCS Chassis

```
Add-UcsManagedObject -ModifyPresent -ClassId EquipmentChassis -PropertyMap
@{Id=1; AdminState="re-acknowledge"; Dn="sys/chassis-1"; }
```

Create Pools

This section presents the steps for creating pools.

Create MAC Address Pools

To configure the necessary MAC address pools for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Pools > root.

Note: In this procedure, two MAC address pools are created: one for each switching fabric.

3. Right-click MAC Pools under the root organization.
4. Select Create MAC Pool to create the MAC address pool.
5. Enter **MAC_Pool_A** as the name of the MAC address pool.
6. Optional: Enter a description for the MAC address pool.
7. For Assignment Order, select Sequential.

Create MAC Pool [?] X

1 Define Name and Description

Name :

Description :

Assignment Order : ☐ Default ☒ Sequential

< Prev Next > Finish Cancel

8. Click Next.
9. Click Add.
10. Specify a starting MAC address.
11. Specify a size for the MAC address pool that is sufficient to support the available blade or server resources.

Create MAC Pool [?] X

2 Add MAC Addresses

Advanced Filter Export Print

Name	From	To
[Empty Table]		

Create a Block of MAC Addresses [?] X

First MAC Address : Size :

To ensure uniqueness of MACs in the LAN fabric, you are strongly encouraged to use the following MAC prefix:
00:25:B5:xx:xx:xx

OK Cancel

+ Add Delete

< Prev Next > Finish Cancel

12. Click OK.
13. Click Finish.
14. In the confirmation message, click OK.
15. Right-click MAC Pools under the root organization.
16. Select Create MAC Pool to create the MAC address pool.
17. Enter **MAC_Pool_B** as the name of the MAC address pool.

18. Optional: Enter a description for the MAC address pool.

The screenshot shows the 'Create MAC Pool' dialog box with a sidebar on the left containing two steps: '1 Define Name and Description' (highlighted in blue) and '2 Add MAC Addresses'. The main area contains the following fields and controls:

- Name :** A text box containing 'MAC_Pool_B'.
- Description :** An empty text box.
- Assignment Order :** Two radio buttons, 'Default' (unselected) and 'Sequential' (selected).
- Navigation buttons:** '< Prev', 'Next >', 'Finish', and 'Cancel'.

19. Click Next.

20. Click Add.

21. Specify a starting MAC address.

22. Specify a size for the MAC address pool that is sufficient to support the available blade or server resources.

The screenshot shows the 'Create MAC Pool' dialog box with the sidebar step '2 Add MAC Addresses' highlighted. A sub-dialog box titled 'Create a Block of MAC Addresses' is open in the foreground. The sub-dialog contains:

- First MAC Address :** A text box containing '00:25:B5:91:18:00'.
- Size :** A dropdown menu showing '32'.
- Text:** 'To ensure uniqueness of MACs in the LAN fabric, you are strongly encouraged to use the following MAC prefix: 00:25:B5:xx:xx:xx'.
- Buttons:** 'OK' and 'Cancel'.

The background dialog box shows a table with columns 'Name', 'From', and 'To'. Below the table are '+ Add' and '- Delete' buttons. At the bottom of the background dialog are '< Prev', 'Next >', 'Finish', and 'Cancel' buttons.

23. Click OK.

24. Click Finish.

25. In the confirmation message, click OK.

PowerTool cmdlet Steps: Create MAC Address Pools

```
Start-UcsTransaction

$mo = Get-UcsOrg -Level root | Add-UcsMacPool -AssignmentOrder "sequential" -
Name "MAC_Pool_A"

$mo_1 = $mo | Add-UcsMacMemberBlock -From "00:25:B5:91:1A:00" -To
"00:25:B5:91:1A:1F"

Complete-UcsTransaction


Start-UcsTransaction

$mo = Get-UcsOrg -Level root | Add-UcsMacPool -AssignmentOrder "sequential" -
Name "MAC_Pool_B"

$mo_1 = $mo | Add-UcsMacMemberBlock -From "00:25:B5:91:1B:00" -To
"00:25:B5:91:1B:1F"

Complete-UcsTransaction
```

Create UUID Suffix Pool

To configure the necessary universally unique identifier (UUID) suffix pool for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Pools > root.
3. Right-click UUID Suffix Pools.
4. Select Create UUID Suffix Pool.
5. Enter **UUID_Pool** as the name of the UUID suffix pool.

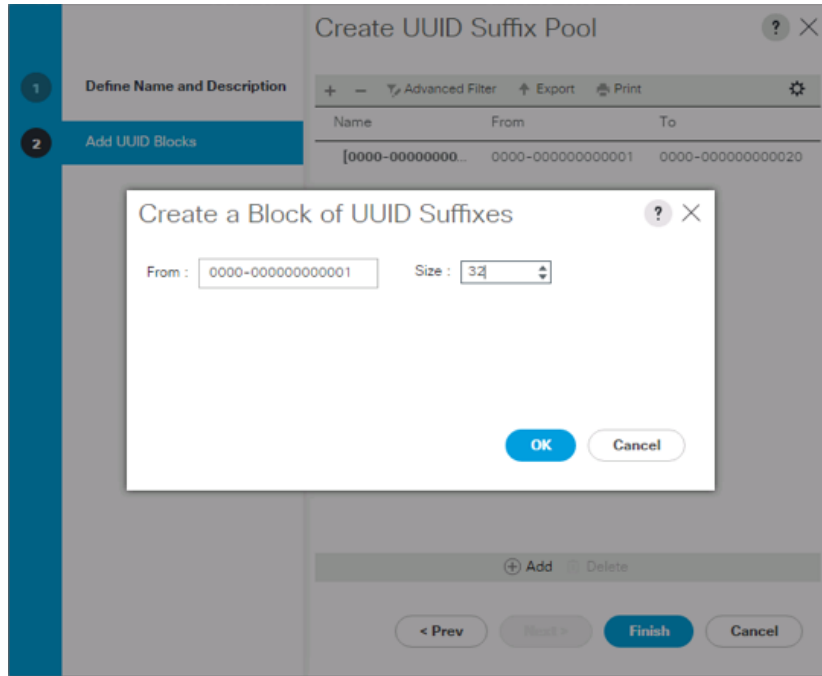
The screenshot shows the 'Create UUID Suffix Pool' dialog box. The left sidebar indicates the current step is '1 Define Name and Description'. The main form contains the following fields and options:

- Name:** A text box containing 'UUID_Pool'.
- Description:** An empty text box.
- Prefix:** Radio buttons for 'Derived' (selected) and 'other'.
- Assignment Order:** Radio buttons for 'Default' and 'Sequential' (selected).

At the bottom of the dialog are four buttons: '< Prev', 'Next >', 'Finish', and 'Cancel'.

6. Optional: Enter a description for the UUID suffix pool.
7. For Prefix, use the Derived option.
8. For Assignment Order, select Sequential.

9. Click Next.
10. Click Add to add a block of UUIDs.



11. Keep the From field at the default setting.
12. Specify a size for the UUID block that is sufficient to support the available blade or server resources.
13. Click OK.
14. Click Finish.
15. Click OK.

PowerTool cmdlet Steps: Create UUID Suffix Pools

```
Start-UcsTransaction
$mo = Get-UcsOrg -Level root | Add-UcsUuidSuffixPool -AssignmentOrder
"sequential" -Name "UUID_Pool"
$mo_1 = $mo | Add-UcsUuidSuffixBlock -From "0000-000000000001" -To "0000-
000000000020"
Complete-UcsTransaction
```

Create Server Pool

To configure the necessary server pool for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Pools > root.
3. Right-click Server Pools.
4. Select Create Server Pool.
5. Enter **Infra_Pool** as the name of the server pool.

Create Server Pool

1 Set Name and Description

2 Add Servers

Name : Infra_Pool

Description :

< Prev Next > Finish Cancel

6. Optional: Enter a description for the server pool.
7. Click Next.
8. Select two (or more) servers to be used for the VMware management cluster and click >> to add them to the Infra_Pool server pool.

Create Server Pool

1 Set Name and Description

2 Add Servers

Servers

...	SI...	R...	U...	PID	A...	S...	C...
1	1		U...	U...	F...	28	
1	2		U...	U...	F...	28	

>>

Pooled Servers

...	SI...	R...	U...	PID	A...	S...	C...
No data available							

<<

Model: UCSB-B200-M4
Serial Number: FLM2023J7L5
Vendor: Cisco Systems Inc

Model:
Serial Number:
Vendor:

< Prev Next > Finish Cancel

9. Click Finish.
10. Click OK.

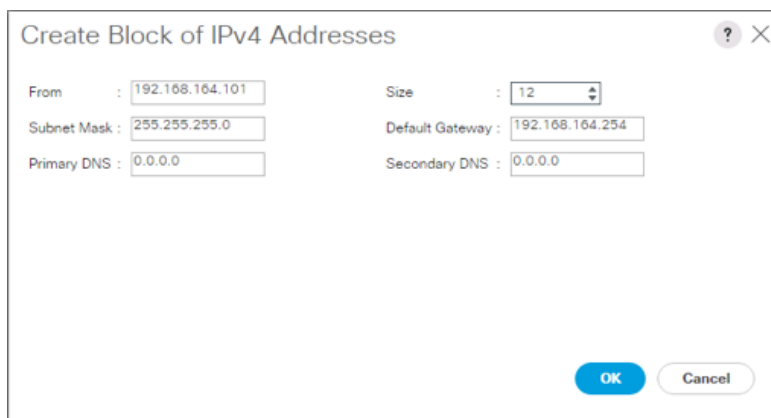
PowerTool cmdlet Steps: Create Server Pool

```
Start-UcsTransaction
$mo = Get-UcsOrg -Level root | Add-UcsServerPool -Name "Infra_Pool"
$mo_1 = $mo | Add-UcsComputePooledSlot -ModifyPresent -ChassisId "1" -SlotId 1
$mo_2 = $mo | Add-UcsComputePooledSlot -ModifyPresent -ChassisId "1" -SlotId 2
Complete-UcsTransaction
```

Add a Block of IP Addresses for KVM Access

To create a block of IP addresses for in-band server keyboard, video, and mouse (KVM) access in the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Pools > root > IP Pools.
3. Right-click IP Pool ext-mgmt and select Create Block of IPv4 Addresses.



4. Enter the starting IP address of the block, the number of IP addresses required, and the subnet and gateway information.
5. Click OK to create the block of IP addresses.
6. Click OK.

PowerTool cmdlet Steps: Add a Block of IP Addresses for KVM Access

```
Get-UcsOrg -Level root | Get-UcsIpPool -Name "ext-mgmt" -LimitScope | Add-
UcsIpPoolBlock -DefGw "192.168.164.254" -From "192.168.164.101" -To
"192.168.164.112"
```

Create a WWNN Pool

To configure the necessary worldwide node name (WWNN) pool for the Cisco UCS environment, complete the following steps:

1. Select the SAN tab on the left.
2. Select Pools > root.
3. Right-click WWNN Pools under the root organization.
4. Select Create WWNN Pool to create the WWNN pool.
5. Enter **WWNN_Pool** as the name of the WWNN pool.

6. Optional: Enter a description for the WWNN pool.
7. For Assignment Order, select Sequential.

8. Click Next.
9. Click Add.
10. Modify the From field as necessary for your Cisco UCS environment.
11. Specify a size of the WWNN block sufficient to support the available server resources.

12. Click OK.
13. Click Finish to create the WWNN Pool.
14. Click OK.

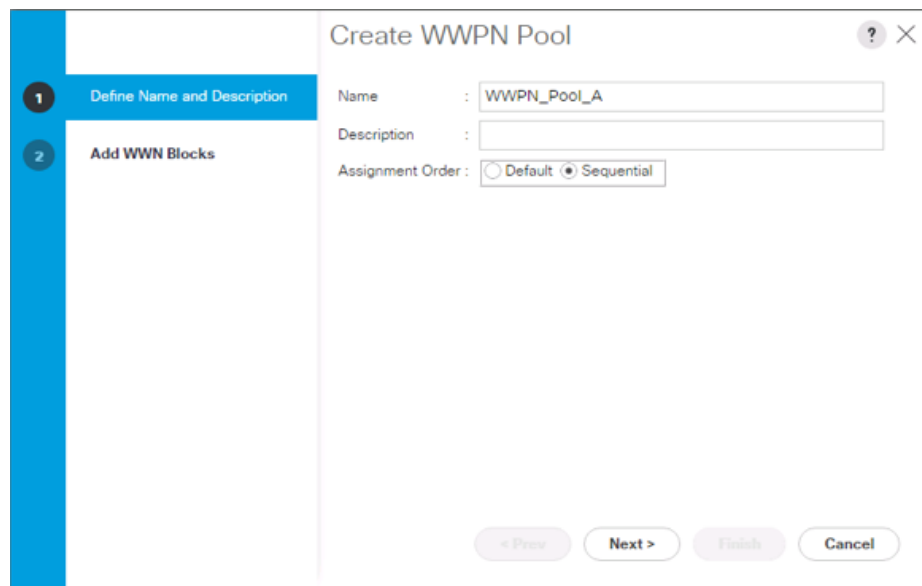
PowerTool cmdlet Steps: Create a WWNN Pool

```
Start-UcsTransaction
$mo = Get-UcsOrg -Level root | Add-UcsWnnPool -AssignmentOrder "sequential" -
Name "WWNN_Pool" -Purpose "node-wnn-assignment"
$mo_1 = $mo | Add-UcsWnnMemberBlock -From "20:00:00:25:B5:01:00:00" -To
"20:00:00:25:B5:01:00:1F"
Complete-UcsTransaction
```

Create WWPN Pools

To configure the necessary worldwide port name (WWPN) pools for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
2. Select Pools > root.
3. In this procedure, two WWPN pools are created: one for each switching fabric.
4. Right-click WWPN Pools under the root organization.
5. Select Create WWPN Pool to create the first WWPN pool.
6. Enter **WWPN_Pool_A** as the name of the WWPN pool.
7. Optional: Enter a description for the WWPN pool.
8. For Assignment Order, select Sequential.

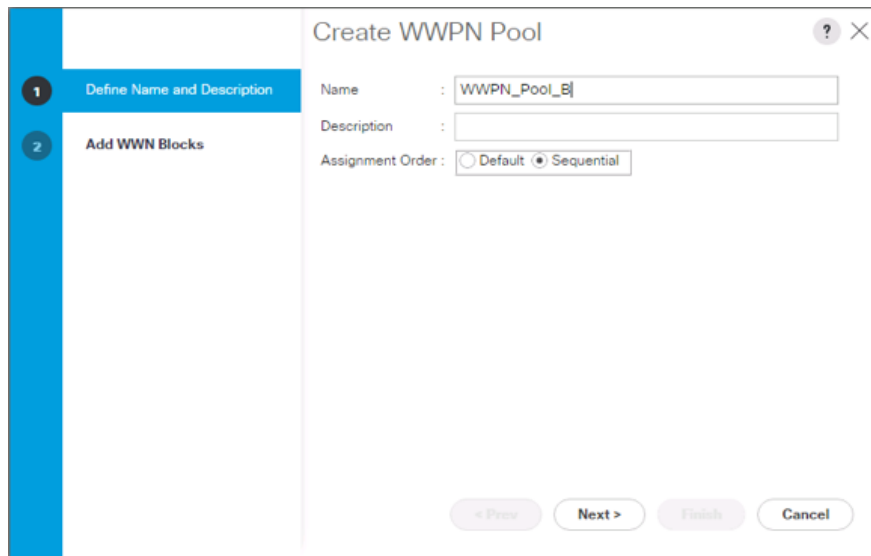


9. Click Next.
10. Click Add.
11. Specify a starting WWPN.
12. Specify a size for the WWPN pool that is sufficient to support the available blade or server resources.



13. Click OK.

14. Click Finish.
15. In the confirmation message, click OK.
16. Right-click WWPN Pools under the root organization.
17. Select Create WWPN Pool to create the second WWPN pool.
18. Enter **WWPN_Pool_B** as the name of the WWPN pool.
19. Optional: Enter a description for the WWPN pool.
20. For Assignment Order, select Sequential.



21. Click Next.
22. Click Add.
23. Specify a starting WWPN.
24. Specify a size for the WWPN address pool that is sufficient to support the available blade or server resources.



25. Click OK.
26. Click Finish.
27. In the confirmation message, click OK.

PowerTool cmdlet Steps: Create WWPN Pools

```
Start-UcsTransaction

$mo = Get-UcsOrg -Level root | Add-UcsWwnPool -AssignmentOrder "sequential" -
Name "WWPN_Pool_A"

$mo_1 = $mo | Add-UcsWwnMemberBlock -From "20:00:00:25:B5:01:0A:00" -To
"20:00:00:25:B5:01:0A:1F"

Complete-UcsTransaction


Start-UcsTransaction

$mo = Get-UcsOrg -Level root | Add-UcsWwnPool -AssignmentOrder "sequential" -
Name "WWPN_Pool_B"

$mo_1 = $mo | Add-UcsWwnMemberBlock -From "20:00:00:25:B5:01:0B:00" -To
"20:00:00:25:B5:01:0B:1F"

Complete-UcsTransaction
```

Set Packages and Policies

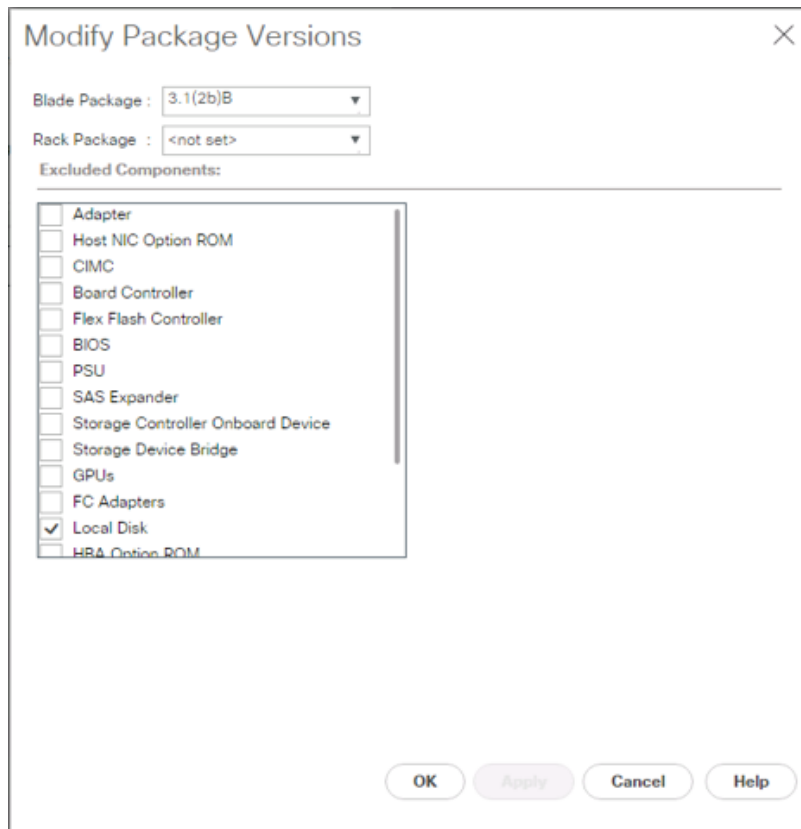
This section presents steps for configuring packages and policies.

Create Host Firmware Package

Firmware management policies allow the administrator to select the corresponding packages for a given server configuration. These policies often include packages for adapter, BIOS, board controller, Fibre Channel adapter, host bus adapter (HBA) option ROM (to enable the HBA firmware called by the system BIOS), and storage controller properties.

To create a firmware management policy for a given server configuration in the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Expand Host Firmware Packages.
4. Select default.
5. In the Actions pane, select Modify Package Versions.
6. Select Version 3.1(2b)B for Blade Package and leave Rack Package not set.
7. Leave Excluded Components with only Local Disk selected.



8. Click OK to modify the host firmware package.

PowerTool cmdlet Steps: Create Host Firmware Package

```
Get-UcsOrg -Level root | Add-UcsFirmwareComputeHostPack -ModifyPresent -
BladeBundleVersion "3.1(2b)B" -Name "default"
```

Create Server Pool Qualification Policy (Optional)

To create an optional server pool qualification policy for the Cisco UCS environment, complete the following steps:

Note: This example creates a policy for Cisco UCS B-Series Blade Servers and Cisco UCS C-Series Rack Servers with Intel® Xeon® processor E2660 v4 Xeon Broadwell CPUs.

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click Server Pool Policy Qualifications.
4. Select Create Server Pool Policy Qualification.
5. Name the policy **UCS-Broadwell**.
6. Select Create CPU/Core Qualifications.
7. Select Xeon for the Processor/Architecture.
8. Select UCS-CPU-E52660E as the part number (PID).
9. Click OK to create the CPU/Core qualification.

10. Click OK to create the policy. Click OK again to confirm.

PowerTool cmdlet Steps: Create Server Pool Qualification Policy (Optional)

```
Start-UcsTransaction
$mo = Get-UcsOrg -Level root | Add-UcsServerPoolQualification -Name "UCS-
Broadwell"
$mo_1 = $mo | Add-UcsCpuQualification -Model "UCS-CPU-E52660E"
Complete-UcsTransaction
```

Download Cisco Custom Image for VMware ESXi 6.0 U2

You will need to download the VMware Cisco Custom image for use during installation by manually accessing the Cisco UCS Kernel-based Virtual Machine (KVM) virtual media (vMedia) or by using the vMedia policy covered in the next subsection.

To download the Cisco Custom image, perform the following steps:

1. Log in to VMware by clicking the following link: [VMware login page](#).
2. Type your email address or customer number and password. Then click Log in.
3. Download the Cisco Custom image by clicking the following link: [Cisco Custom Image 6.0 U2](#).
4. Click Download Now.
5. Save the image file in your destination folder.

Create vMedia Policy for VMware ESXi 6.0 U2 Install Boot (Optional If You Are Manually Attaching ISO Image Through KVM)

You need a separate HTTP web server to automate the availability of the ESXi image for each service profile at power-up. The creation of this web server is not covered in this document, but you can use any existing web server that can serve files through HTTP that are accessible on the out-of-band network on which the ESXi image resides.

Place the Cisco Custom image VMware ESXi 6.0 U2 ISO on the HTTP server and complete the following steps to create a vMedia policy:

1. In Cisco UCS Manager, select the Servers tab.
2. Select Policies > root.
3. Right-click vMedia Policies.
4. Select Create vMedia Policy.
5. Name the policy **ESXi-6.0U2-HTTP**.
6. In the Description field, enter **Mounts Cisco Custom ISO for ESXi 6.0 U2**.
7. Leave Yes selected for Retry on Mount Failure.

Create vMedia Policy

Name : ESXi-6.0U2-HTTP

Description : Mount Cisco Custom ISO for ESXi 6.0 U2

Retry on Mount Failure : ☐ No ☒ Yes

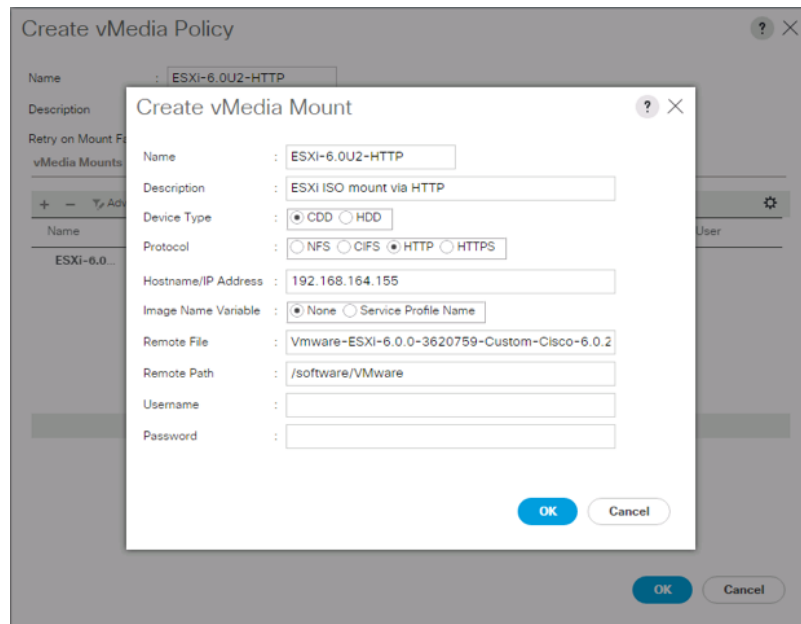
vMedia Mounts

Name	Type	Protocol	Authenticati...	Server	Filename	Remote Path	User
No data available							

+ Add - Delete Info

OK Cancel

8. Click Add.
9. Name the mount **ESXi-6.0U2-HTTP**.
10. In the Description field, enter **ESXi ISO mount via HTTP**.
11. Select CDD Device Type.
12. Select HTTP Protocol.
13. Enter the IP address of the web server.
14. Leave None selected for Image Name Variable.
15. Enter Vmware-ESXi-6.0.0-3620759-Custom-Cisco-6.0.2.1.iso as the remote file name.
16. Enter the web server path to the ISO file in the Remote Path field.
17. Leave the Username and Password fields blank.



18. Click OK to create the vMedia mount.

19. Click OK. Then click OK again to complete the creation the vMedia policy.

PowerTool cmdlet Steps: Create vMedia Policy for VMware ESXi 6.0 U2 Install Boot

```
Start-UcsTransaction
$mo = Get-UcsOrg -Level root | Add-UcsVmediaPolicy -Descr "Mounts Cisco Custom
ISO for ESXi 6.0 U2" -Name "ESXi-6.0U2-HTTP"
$mo_1 = $mo | Add-UcsVmediaMountEntry -DeviceType "cdd" -ImageFileName "Vmware-
ESXi-6.0.0-3620759-Custom-Cisco-6.0.2.1.iso" -ImagePath "/software/VMware" -
MappingName "ESXi-6.0U2-HTTP" -MountProtocol "http" -RemoteIpAddress
"192.168.164.155"
Complete-UcsTransaction
```

Create Server BIOS Policy

To create a server BIOS policy for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click BIOS Policies.
4. Select Create BIOS Policy.
5. Enter **VM-Host-Infra** as the BIOS policy name.
6. Leave Reboot on BIOS Setting Change unselected.
7. Change the Quiet Boot setting to disabled.
8. Change Consistent Device Naming to enabled.

9. Click Finish to create the BIOS policy.
10. Click OK.

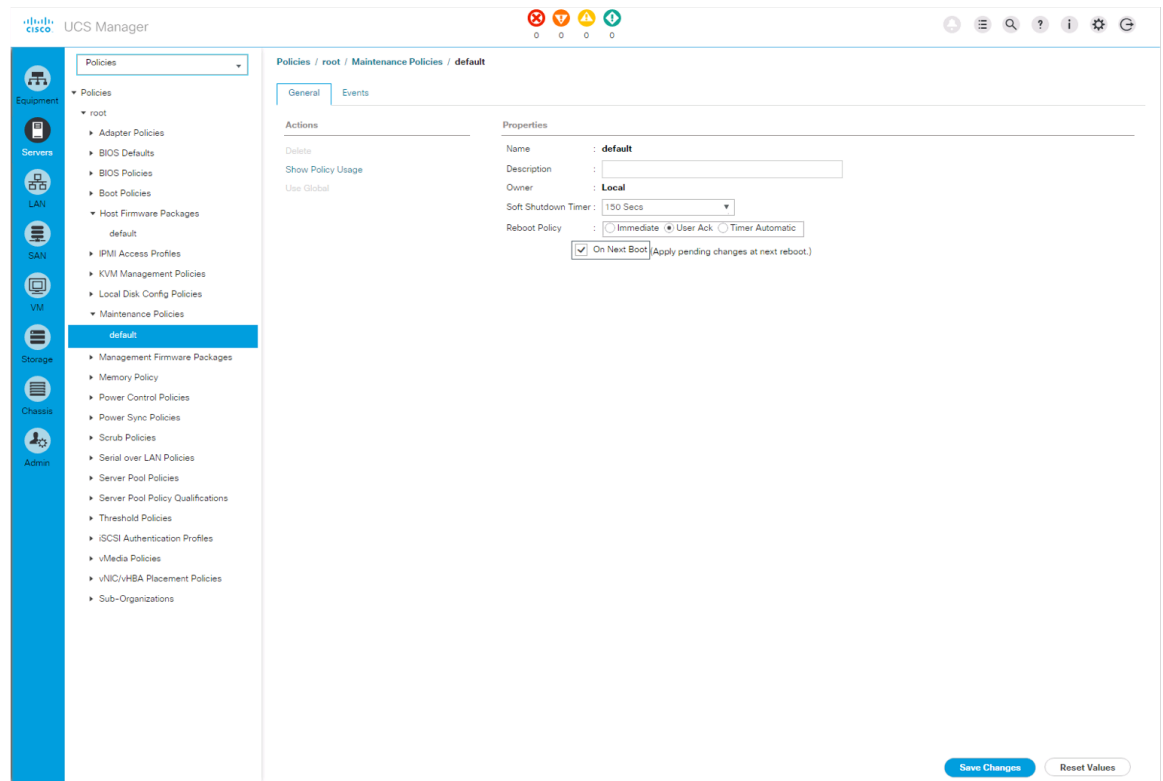
PowerTool cmdlet Steps: Create Server BIOS Policy

```
Start-UcsTransaction
$mo = Get-UcsOrg -Level root | Add-UcsBiosPolicy -Name "VM-Host-Infra"
$mo_1 = $mo | Set-UcsBiosVfQuietBoot -VpQuietBoot "disabled"
$mo_2 = $mo | Set-UcsBiosVfPOSTErrorPause -VpPOSTErrorPause "platform-default"
$mo_3 = $mo | Set-UcsBiosVfResumeOnACPowerLoss -VpResumeOnACPowerLoss "platform-default"
$mo_4 = $mo | Set-UcsBiosVfFrontPanelLockout -VpFrontPanelLockout "platform-default"
$mo_5 = $mo | Set-UcsBiosVfConsistentDeviceNameControl -VpCDNControl "enabled"
Complete-UcsTransaction
```

Update the Default Maintenance Policy

To update the default maintenance policy, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Select Maintenance Policies > default.
4. Change Reboot Policy to User Ack.
5. Optional: Click On Next Boot to delegate maintenance windows to server owners.



6. Click Save Changes.
7. Click OK to accept the change.

PowerTool cmdlet Steps: Update the Default Maintenance Policy

```
Get-UcsOrg -Level root | Add-UcsMaintenancePolicy -ModifyPresent -Name
"default" -TriggerConfig "on-next-boot" -UptimeDisr "user-ack"
```

Create Local Disk Configuration Policy (Optional)

You need to create a local disk configuration policy for the Cisco UCS environment if the servers in the environment do not have a local disk. To create a local disk configuration policy, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click Local Disk Config Policies.
4. Select Create Local Disk Configuration Policy.
5. Enter **SAN-Boot** as the local disk configuration policy name.
6. Change the mode to No Local Storage.
7. Click OK to create the local disk configuration policy.

Create Local Disk Configuration Policy ? X

Name : SAN-Boot

Description :

Mode : No Local Storage ▼

FlexFlash

FlexFlash State : ☒ Disable ☐ Enable

If **FlexFlash State** is disabled, SD cards will become unavailable immediately.
Please ensure SD cards are not in use before disabling the FlexFlash State.

FlexFlash RAID Reporting State : ☒ Disable ☐ Enable

OK Cancel

8. Click OK.

PowerTool cmdlet Steps: Create Local Disk Configuration Policy

```
Get-UcsOrg -Level root | Add-UcsLocalDiskConfigPolicy -Mode "no-local-storage" -
Name "SAN-Boot"
```

Create vNIC and vHBA Placement Policy for Virtual Machine Infrastructure Hosts

To create a virtual network interface card (vNIC) and virtual HBA (vHBA) placement policy for the infrastructure hosts, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click vNIC/vHBA Placement Policies.
4. Select Create Placement Policy.
5. Enter **VM-Host-Infra** as the name of the placement policy.
6. Click 1 and select Assigned Only for Selection Preference.

Create Placement Policy

Name : VM-Host-Infra

Virtual Slot Mapping Scheme : ☒ Round Robin ☐ Linear Ordered

Advanced Filter Export Print

Virtual Slot	Selection Preference
1	Assigned Only
2	All
3	Assigned Only
4	Exclude Dynamic
	Exclude Unassigned
	Exclude usNIC

OK Cancel

- Click OK. Then click OK again.

PowerTool cmdlet Steps: Create vNIC and vHBA Placement Policy for Virtual Machine Infrastructure Hosts

```
Start-UcsTransaction
$mo = Get-UcsOrg -Level root | Add-UcsPlacementPolicy -Name "VM-Host-Infra"
$mo_1 = $mo | Add-UcsFabricVCon -ModifyPresent -Fabric "NONE" -Id "1" -InstType
"auto" -Placement "physical" -Select "assigned-only" -Share "shared" -Transport
"ethernet","fc"
$mo_2 = $mo | Add-UcsFabricVCon -ModifyPresent -Fabric "NONE" -Id "2" -InstType
"auto" -Placement "physical" -Select "all" -Share "shared" -Transport
"ethernet","fc"
$mo_3 = $mo | Add-UcsFabricVCon -ModifyPresent -Fabric "NONE" -Id "3" -InstType
"auto" -Placement "physical" -Select "all" -Share "shared" -Transport
"ethernet","fc"
$mo_4 = $mo | Add-UcsFabricVCon -ModifyPresent -Fabric "NONE" -Id "4" -InstType
"auto" -Placement "physical" -Select "all" -Share "shared" -Transport
"ethernet","fc"
Complete-UcsTransaction
```

Create Network Control Policy for Cisco Discovery Protocol

To create a network control policy that enables Cisco Discovery Protocol (CDP) on virtual network ports, complete the following steps:

- In Cisco UCS Manager, click the LAN tab in the navigation pane.
- Select Policies > root.
- Right-click Network Control Policies.
- Select Create Network Control Policy.
- Enter **Enable_CDP** as the policy name.
- For CDP, select the Enabled option.
- Click OK to create the network control policy.

8. Click OK.

PowerTool cmdlet Steps: Create Network Control Policy for Cisco Discovery Protocol

```
Start-UcsTransaction
$mo = Get-UcsOrg -Level root | Add-UcsNetworkControlPolicy -Cdp "enabled" -Name
"Enable_CDP"
$mo_1 = $mo | Add-UcsPortSecurityConfig -ModifyPresent -Descr "" -Forge "allow" -
Name "" -PolicyOwner "local"
Complete-UcsTransaction
```

Configure Cisco UCS LAN Connectivity

This section presents steps for configuring LAN connectivity in the Cisco UCS environment.

Create Uplink Port Channels

To configure the necessary port channels in the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.

Note: In this procedure, two port channels are created: one from fabric A to both Cisco Nexus switches, and one from fabric B to both Cisco Nexus switches.

2. Under LAN > LAN Cloud, expand the Fabric A tree.
3. Right-click Port Channels.
4. Select Create Port Channel.
5. Enter a unique ID for the port channel, (**151** in this example to correspond with the upstream Cisco Nexus port channel).
6. With 151 selected, enter **vPC-151-Nexus** as the name of the port channel.

Create Port Channel

1 Set Port Channel Name

ID : 151

Name : vPC-151-Nexus

2 Add Ports

< Prev Next > Finish Cancel

7. Click Next.
8. Select the following ports to be added to the port channel:
 - Slot ID 1 and port 39
 - Slot ID 1 and port 40

Create Port Channel

1 Set Port Channel Name

2 Add Ports

Ports			
Slot ID	Aggr. Po...	Port	MAC
1	0	40	00:DE:F...
1	0	39	00:DE:F...

>> <<

Ports in the port channel			
Slot ID	Aggr. Po...	Port	MAC
No data available			

< Prev Next > Finish Cancel

9. Click >> to add the ports to the port channel.
10. Click Finish to create the port channel.
11. Click OK.
12. In the navigation pane, under LAN > LAN Cloud, expand the Fabric B tree.
13. Right-click Port Channels.
14. Select Create Port Channel.
15. Enter a unique ID for the port channel, (**152** in this example to correspond with the upstream Cisco Nexus port channel).
16. With 152 selected, enter **vPC-152-Nexus** as the name of the port channel.

Create Port Channel

1 Set Port Channel Name

2 Add Ports

ID : 152

Name : vPC-152-Nexus

< Prev Next > Finish Cancel

17. Click Next.

18. Select the following ports to be added to the port channel:

- Slot ID 1 and port 39
- Slot ID 1 and port 40

Create Port Channel

1 Set Port Channel Name

2 Add Ports

Ports			
Slot ID	Aggr. Po...	Port	MAC
1	0	39	00:DE:F...
1	0	40	00:DE:F...

>> <<

Ports in the port channel			
Slot ID	Aggr. Po...	Port	MAC
No data available			

< Prev Next > Finish Cancel

19. Click >> to add the ports to the port channel.

20. Click Finish to create the port channel.

21. Click OK.

PowerTool cmdlet Steps: Create Uplink Port Channels

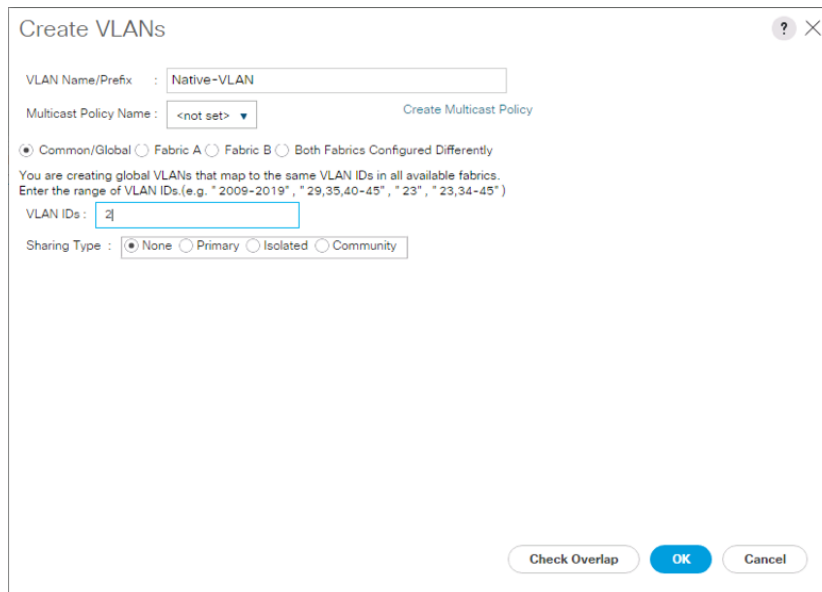
```
Start-UcsTransaction
$mo = Get-UcsFisLanCloud -Id "A" | Add-UcsUplinkPortChannel -Name "vPC-151-Nexus"
-PortId 151
$mo_1 = $mo | Add-UcsUplinkPortChannelMember -ModifyPresent -AdminState "enabled"
-AutoNegotiate "yes" -EthLinkProfileName "default" -Name "" -PortId 39 -SlotId 1
$mo_2 = $mo | Add-UcsUplinkPortChannelMember -ModifyPresent -AdminState "enabled"
-AutoNegotiate "yes" -EthLinkProfileName "default" -Name "" -PortId 40 -SlotId 1
Complete-UcsTransaction

Start-UcsTransaction
$mo = Get-UcsFisLanCloud -Id "B" | Add-UcsUplinkPortChannel -Name "vPC-152-Nexus"
-PortId 152
$mo_1 = $mo | Add-UcsUplinkPortChannelMember -ModifyPresent -AdminState "enabled"
-AutoNegotiate "yes" -EthLinkProfileName "default" -Name "" -PortId 39 -SlotId 1
$mo_2 = $mo | Add-UcsUplinkPortChannelMember -ModifyPresent -AdminState "enabled"
-AutoNegotiate "yes" -EthLinkProfileName "default" -Name "" -PortId 40 -SlotId 1
Complete-UcsTransaction
```

Create VLANs

To configure the necessary virtual local area networks (VLANs) for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select LAN > LAN Cloud.
3. Right-click VLANs.
4. Select Create VLANs.
5. Enter **Native-VLAN** as the name of the VLAN to be used as the native VLAN.
6. Keep the Common/Global option selected as the scope of the VLAN.
7. Enter the native VLAN ID.
8. Keep Sharing Type set to None.



Create VLANs [?] [X]

VLAN Name/Prefix : Native-VLAN

Multicast Policy Name : <not set> [Create Multicast Policy](#)

☒ Common/Global ☐ Fabric A ☐ Fabric B ☐ Both Fabrics Configured Differently

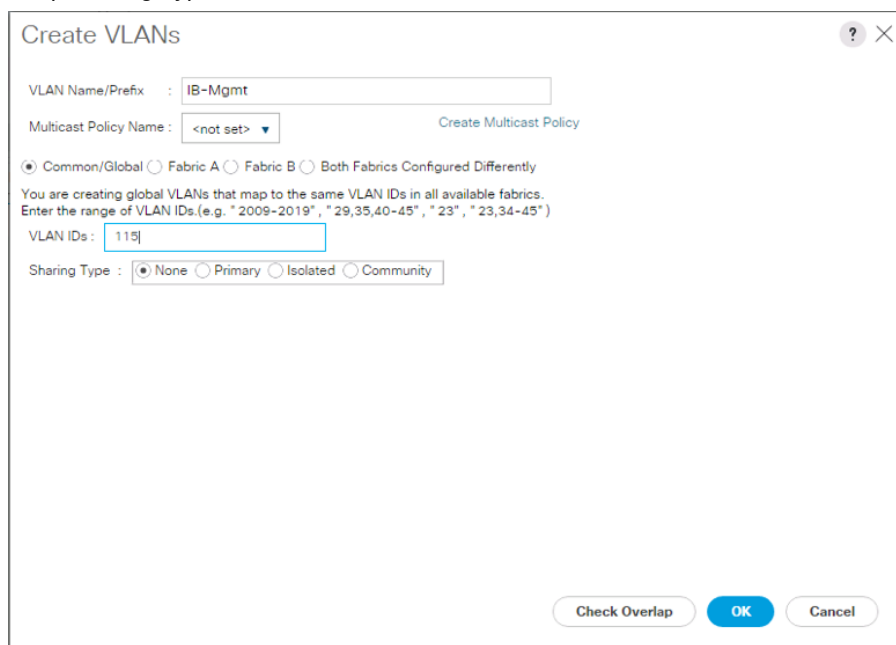
You are creating global VLANs that map to the same VLAN IDs in all available fabrics.
Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")

VLAN IDs : 2

Sharing Type : ☒ None ☐ Primary ☐ Isolated ☐ Community

[Check Overlap](#) [OK](#) [Cancel](#)

9. Click OK. Then click OK again.
10. Expand the list of VLANs in the navigation pane, right-click the newly created Native-VLAN, and select Set as Native VLAN.
11. Click Yes. Then click OK again.
12. Right-click VLANs.
13. Select Create VLANs.
14. Enter **IB-Mgmt** as the name of the VLAN to be used for management traffic.
15. Keep the Common/Global option selected as the scope of the VLAN.
16. Enter the in-band management VLAN ID.
17. Keep Sharing Type set to None.



Create VLANs [?] [X]

VLAN Name/Prefix : IB-Mgmt

Multicast Policy Name : <not set> [Create Multicast Policy](#)

☒ Common/Global ☐ Fabric A ☐ Fabric B ☐ Both Fabrics Configured Differently

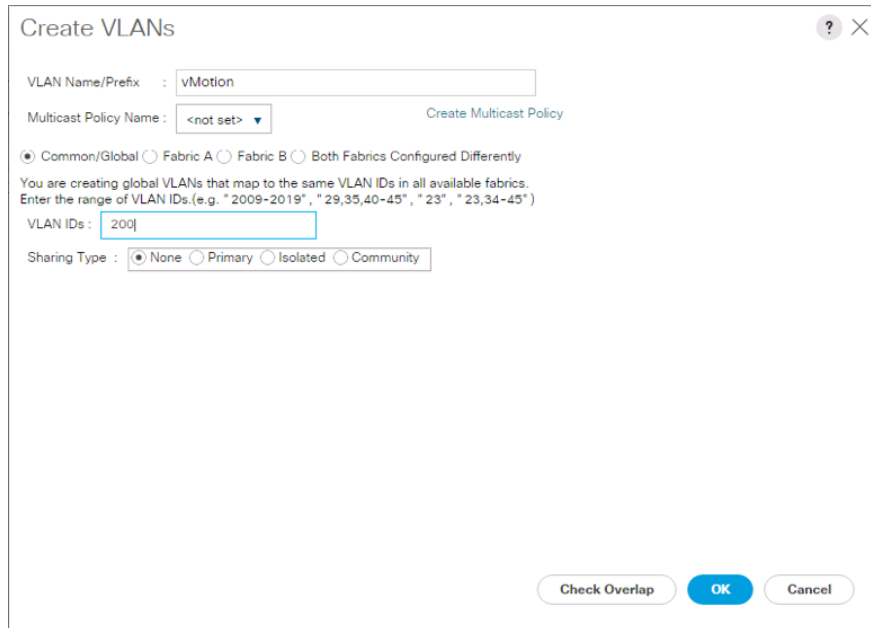
You are creating global VLANs that map to the same VLAN IDs in all available fabrics.
Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")

VLAN IDs : 115

Sharing Type : ☒ None ☐ Primary ☐ Isolated ☐ Community

[Check Overlap](#) [OK](#) [Cancel](#)

18. Click OK. Then click OK again.
19. Right-click VLANs.
20. Select Create VLANs.
21. Enter **vMotion** as the name of the VLAN to be used for VMware vMotion.
22. Keep the Common/Global option selected as the scope of the VLAN.
23. Enter the vMotion VLAN ID.
24. Keep Sharing Type set to None.



The screenshot shows a 'Create VLANs' dialog box with the following fields and options:

- VLAN Name/Prefix :** vMotion
- Multicast Policy Name :** <not set> (with a 'Create Multicast Policy' link)
- Scope:** ☒ Common/Global, ☐ Fabric A, ☐ Fabric B, ☐ Both Fabrics Configured Differently
- Instructions:** You are creating global VLANs that map to the same VLAN IDs in all available fabrics. Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")
- VLAN IDs :** 200
- Sharing Type :** ☒ None, ☐ Primary, ☐ Isolated, ☐ Community
- Buttons:** Check Overlap, OK, Cancel

25. Click OK/ Then click OK again.
26. Right-click VLANs.
27. Select Create VLANs.
28. Enter **VM-App-1** as the name of the VLAN to be used for virtual machine traffic.
29. Keep the Common/Global option selected as the scope of the VLAN.
30. Enter the virtual machine traffic VLAN ID.
31. Keep Sharing Type set to None.

Create VLANs

VLAN Name/Prefix : VM-App-1

Multicast Policy Name : <not set> [Create Multicast Policy](#)

☒ Common/Global ☐ Fabric A ☐ Fabric B ☐ Both Fabrics Configured Differently

You are creating global VLANs that map to the same VLAN IDs in all available fabrics.
Enter the range of VLAN IDs (e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")

VLAN IDs : 201

Sharing Type : ☒ None ☐ Primary ☐ Isolated ☐ Community

[Check Overlap](#) **OK** [Cancel](#)

32. Click OK. Then click OK again.

33. Repeat these steps as needed for any additional VLANs created on the upstream Cisco Nexus switches.

PowerTool cmdlet Steps: Create VLANs

```
Get-UcsLanCloud | Add-UcsVlan -CompressionType "included" -DefaultNet "no" -Id 2
-McastPolicyName "" -Name "Native-VLAN" -PolicyOwner "local" -PubNwName "" -
Sharing "none"

Get-UcsLanCloud | Add-UcsVlan -CompressionType "included" -DefaultNet "no" -Id
115 -McastPolicyName "" -Name "IB-Mgmt" -PolicyOwner "local" -PubNwName "" -
Sharing "none"

Get-UcsLanCloud | Add-UcsVlan -CompressionType "included" -DefaultNet "no" -Id
200 -McastPolicyName "" -Name "vMotion" -PolicyOwner "local" -PubNwName "" -
Sharing "none"

Get-UcsLanCloud | Add-UcsVlan -CompressionType "included" -DefaultNet "no" -Id
201 -McastPolicyName "" -Name "VM-App-1" -PolicyOwner "local" -PubNwName "" -
Sharing "none"

Get-UcsLanCloud | Add-UcsVlan -CompressionType "included" -DefaultNet "no" -Id
202 -McastPolicyName "" -Name "VM-App-2" -PolicyOwner "local" -PubNwName "" -
Sharing "none"

Get-UcsLanCloud | Add-UcsVlan -CompressionType "included" -DefaultNet "no" -Id
203 -McastPolicyName "" -Name "VM-App-3" -PolicyOwner "local" -PubNwName "" -
Sharing "none"
```

Create vNIC Templates

To create multiple vNIC templates for the Cisco UCS environment, complete the following steps. A total of six vNIC templates will be created.

Create a Management vNIC Template

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template.
5. Enter **vNIC_Mgmt_A** as the vNIC template name.
6. Keep Fabric A selected.
7. Do not select the Enable Failover checkbox.
8. Select Primary Template for Redundancy Type.
9. Leave Peer Redundancy Template not set.
10. Under Target, make sure that the virtual machine (VM) checkbox is not selected.
11. Select Updating Template for Template Type.
12. Under VLANs, select the checkboxes for IB-MGMT and Native-VLAN VLANs.

Create vNIC Template

Name : vNIC_Mgmt_A

Description :

Fabric ID : ☒ Fabric A ☐ Fabric B ☐ Enable Failover

Redundancy

Redundancy Type : ☐ No Redundancy ☒ Primary Template ☐ Secondary Template

Peer Redundancy Template : <not set>

Target

☒ Adapter

☐ VM

Warning

If VM is selected, a port profile by the same name will be created.
If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type : ☐ Initial Template ☒ Updating Template

VLANs

Select	Name	Native VLAN
☐	default	☐
☒	IB-Mgmt	☐
☒	Native-VLAN	☒

OK Cancel

13. Set Native-VLAN as the native VLAN.
14. Leave vNIC Name selected as the content delivery network (CDN) source.
15. Leave 1500 set for the maximum transmission unit (MTU).
16. In the MAC Pool list, select MAC_Pool_A.
17. In the Network Control Policy list, select Enable_CDP.

Create vNIC Template

VLANs

Advanced Filter Export Print

Select	Name	Native VLAN
☒	IB-Mgmt	
☒	Native-VLAN	☒
☐	VM-App-1	☐
☐	VM-App-2	☐
☐	VM-App-3	☐
☐	vMotion	☐

CDN Source : ☒ vNIC Name ☐ User Defined

MTU : 1500

MAC Pool : MAC_Pool_A(32/32)

QoS Policy : <not set>

Network Control Policy : Enable_CDP

Pin Group : <not set>

Stats Threshold Policy : default

Connection Policies

☒ Dynamic vNIC ☐ usNIC ☐ VMO

Dynamic vNIC Connection Policy : <not set>

OK Cancel

18. Click OK to create the vNIC template.

19. Click OK.

Create the vNIC_Mgmt_B Template

1. In the navigation pane, select the LAN tab.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template
5. Enter **vNIC_Mgmt_B** as the vNIC template name.
6. Select Fabric B.
7. Do not select the Enable Failover checkbox.
8. Select Secondary Template for Redundancy Type.
9. From the Peer Redundancy Template pull-down menu, select vNIC_Mgmt_A.
10. Under Target, make sure that the VM checkbox is not selected.
11. Select Updating Template as the template type.
12. Under VLANs, select the checkboxes for IB-MGMT and Native-VLAN VLANs.

?

×

Create vNIC Template

Name

:

vNIC_Mgmt_B

Description

:

Fabric ID

:

☐ Fabric A
☒ Fabric B
☐ Enable Failover

Redundancy

:

☐ No Redundancy
☐ Primary Template
☒ Secondary Template

Peer Redundancy Template

:

<not set>

Target

:

☒ Adapter
☐ VM

<not set>

Domain Policies

vNIC_Mgmt_A

Warning

:

If **VM** is selected, a port profile by the same name will be created.

If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type

:

☐ Initial Template
☒ Updating Template

VLANs

:

Advanced Filter

Export

Print

⚙

Select	Name	Native VLAN
☐	default	☐
☒	IB-Mgmt	☐
☒	Native-VLAN	☒
☐	...	☐

OK

Cancel

13. Set default as the native VLAN.
14. Leave vNIC Name selected as the CDN source.
15. Leave 1500 set for the MTU.
16. In the MAC Pool list, select MAC_Pool_B.
17. In the Network Control Policy list, select Enable_CDP.

Create vNIC Template

VLANs

Advanced Filter Export Print

Select	Name	Native VLAN
☒	IS-Mgmt	
☒	Native-VLAN	☒
☐	VM-App-1	☐
☐	VM-App-2	☐
☐	VM-App-3	☐
☐	vMotion	☐

CDN Source : ☒ vNIC Name ☐ User Defined

MTU : 1500

MAC Pool : MAC_Pool_B(32/32)

QoS Policy : <not set>

Network Control Policy : Enable_CDP

Pin Group : <not set>

Stats Threshold Policy : default

Connection Policies

☒ Dynamic vNIC ☐ usNIC ☐ VMO

Dynamic vNIC Connection Policy : <not set>

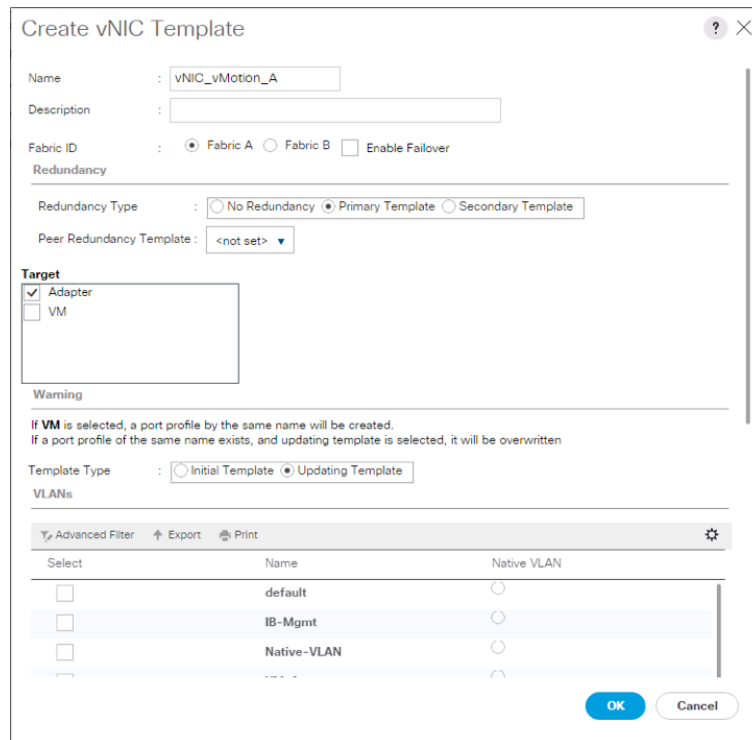
OK Cancel

18. Click OK to create the vNIC template.

19. Click OK.

Create a vMotion vNIC Template

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template.
5. Enter **vNIC_vMotion_A** as the vNIC template name.
6. Keep Fabric A selected.
7. Do not select the Enable Failover checkbox.
8. Select Primary Template for Redundancy Type.
9. Leave Peer Redundancy Template not set.
10. Under Target, make sure that the VM checkbox is not selected.
11. Select Updating Template for Template Type.



Create vNIC Template

Name : vNIC_vMotion_A

Description :

Fabric ID : ☒ Fabric A ☐ Fabric B ☐ Enable Failover

Redundancy

Redundancy Type : ☐ No Redundancy ☒ Primary Template ☐ Secondary Template

Peer Redundancy Template : <not set>

Target

☒ Adapter

☐ VM

Warning

If **VM** is selected, a port profile by the same name will be created.
If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type : ☐ Initial Template ☒ Updating Template

VLANs

Advanced Filter Export Print

Select	Name	Native VLAN
☐	default	☐
☐	IB-Mgmt	☐
☐	Native-VLAN	☐

OK Cancel

12. Under VLANs, select the checkbox for vMotion as the only VLAN.
13. Set vMotion as the native VLAN.
14. For MTU, enter **9000**.
15. In the MAC Pool list, select MAC_Pool_A.
16. In the Network Control Policy list, select Enable_CDP.

Create vNIC Template

VLANs

Advanced Filter Export Print

Select	Name	Native VLAN
☐	IS-Mgmt	Native VLAN
☐	Native-VLAN	Native VLAN
☐	VM-App1	Native VLAN
☐	VM-App2	Native VLAN
☐	VM-App3	Native VLAN
☒	vMotion	Native VLAN

CDN Source : ☒ vNIC Name ☐ User Defined

MTU : 9000

MAC Pool : MAC_Pool_A(16/32)

QoS Policy : <not set>

Network Control Policy : Enable_CDP

Pin Group : <not set>

Stats Threshold Policy : default

Connection Policies

☒ Dynamic vNIC ☐ usNIC ☐ VMQ

Dynamic vNIC Connection Policy : <not set>

OK Cancel

17. Click OK to create the vNIC template.

18. Click OK.

Create the vNIC_vMotion_B Template

1. In the navigation pane, select the LAN tab.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template
5. Enter **vNIC_vMotion_B** as the vNIC template name.
6. Select Fabric B.
7. Do not select the Enable Failover checkbox.
8. Select Secondary Template for Redundancy Type.
9. From the Peer Redundancy Template pull-down menu, select vNIC_vMotion_A.
10. Under Target, make sure that the VM checkbox is not selected.
11. Select Updating Template as the template type.
12. Under VLANs, select the checkbox for the vMotion VLAN.

?

×

Create vNIC Template

Name

:

vNIC_vMotion_B

Description

:

Fabric ID

:

☐ Fabric A
☒ Fabric B
☐ Enable Failover

Redundancy

:

☐ No Redundancy
☐ Primary Template
☒ Secondary Template

Peer Redundancy Template

:

<not set>

Target

:

☒ Adapter
☐ VM

<not set>

Domain Policies

vNIC_Mgmt_A

vNIC_vMotion_A

Warning

:

If **VM** is selected, a port profile by the same name will be created.

If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type

:

☐ Initial Template
☒ Updating Template

VLANs

:

Advanced Filter

Export

Print

⚙

Select	Name	Native VLAN
☐	default	☐
☐	IB-Mgmt	☐
☐	Native-VLAN	☐
☐	...	☐

OK

Cancel

13. Select vNIC Name for CDN Source.
14. For MTU, enter **9000**.
15. In the MAC Pool list, select MAC_Pool_B.
16. In the Network Control Policy list, select Enable_CDP.

Create vNIC Template

VLANs

Advanced Filter Export Print

Select	Name	Native VLAN
☐	ib-mgmt	
☐	Native-VLAN	
☐	VM-App1	
☐	VM-App2	
☐	VM-App3	
☒	vMotion	

CDN Source : ☒ vNIC Name ☐ User Defined

MTU : 9000

MAC Pool : MAC_Pool_B(16/32)

QoS Policy : <not set>

Network Control Policy : Enable_CDP

Pin Group : <not set>

Stats Threshold Policy : default

Connection Policies

☒ Dynamic vNIC ☐ usNIC ☐ VMQ

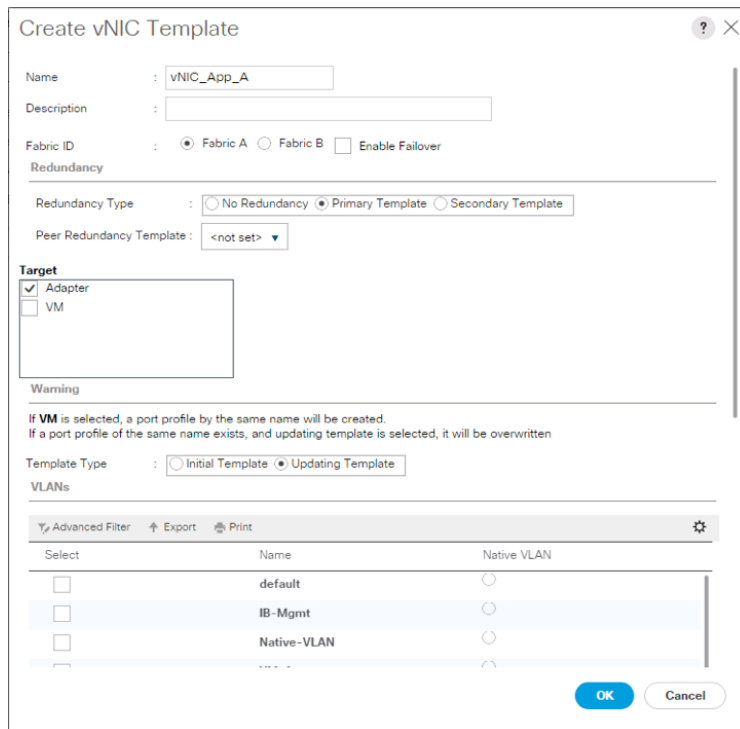
Dynamic vNIC Connection Policy : <not set>

OK Cancel

17. Click OK to create the vNIC template.
18. Click OK.

Create an Application vNIC Template

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template.
5. Enter **vNIC_App_A** as the vNIC template name.
6. Keep Fabric A selected.
7. Do not select the Enable Failover checkbox.
8. Select Primary Template for Redundancy Type.
9. Leave Peer Redundancy Template not set.
10. Under Target, make sure that the VM checkbox is not selected.
11. Select Updating Template for Template Type.
12. Under VLANs, select the checkboxes for any application or production VLANs that should be delivered to the ESXi hosts.



Create vNIC Template

Name : vNIC_App_A

Description :

Fabric ID : ☒ Fabric A ☐ Fabric B ☐ Enable Failover

Redundancy

Redundancy Type : ☐ No Redundancy ☒ Primary Template ☐ Secondary Template

Peer Redundancy Template : <not set>

Target

☒ Adapter

☐ VM

Warning

If VM is selected, a port profile by the same name will be created.
If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type : ☐ Initial Template ☒ Updating Template

VLANs

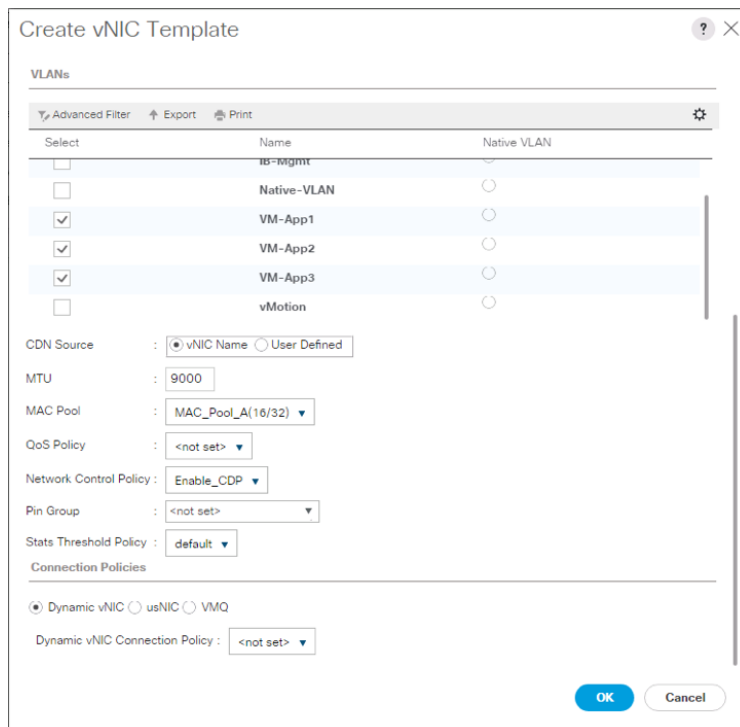
Select	Name	Native VLAN
☐	default	☐
☐	IB-Mgmt	☐
☐	Native-VLAN	☐

OK Cancel

13. For MTU, enter **9000**.

14. In the MAC Pool list, select MAC_Pool_A.

15. In the Network Control Policy list, select Enable_CDP.



Create vNIC Template

VLANs

Select	Name	Native VLAN
☐	IB-Mgmt	☐
☐	Native-VLAN	☐
☒	VM-App1	☐
☒	VM-App2	☐
☒	VM-App3	☐
☐	vMotion	☐

CDN Source : ☒ vNIC Name ☐ User Defined

MTU : 9000

MAC Pool : MAC_Pool_A(16/32)

QoS Policy : <not set>

Network Control Policy : Enable_CDP

Pin Group : <not set>

Stats Threshold Policy : default

Connection Policies

☒ Dynamic vNIC ☐ usNIC ☐ VMQ

Dynamic vNIC Connection Policy : <not set>

OK Cancel

16. Click OK to create the vNIC template.

17. Click OK.

Create the vNIC_App_B Template

1. In the navigation pane, select the LAN tab.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template
5. Enter **vNIC_App_B** as the vNIC template name.
6. Select Fabric B.
7. Do not select the Enable Failover checkbox.
8. Select Secondary Template for Redundancy Type.
9. From the Peer Redundancy Template pull-down menu, select vNIC_App_A.
10. Under Target, make sure the VM checkbox is not selected.

Create vNIC Template

Name : vNIC_App_B

Description :

Fabric ID : ☐ Fabric A ☒ Fabric B ☐ Enable Failover

Redundancy

Redundancy Type : ☐ No Redundancy ☐ Primary Template ☒ Secondary Template

Peer Redundancy Template : <not set>

Target

☒ Adapter ☐ VM

Warning

If **VM** is selected, a port profile by the same name will be created.
If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type : ☐ Initial Template ☒ Updating Template

VLANs

Select	Name	Native VLAN
☐	default	☐
☐	IB-Mgmt	☐
☐	Native-VLAN	☐

OK Cancel

11. Select Updating Template as the template type.
12. Under VLANs, select the same checkboxes for the application or production VLANs selected for the vNIC_App_A vNIC Template.
13. Set default as the native VLAN.
14. Select vNIC Name for CDN Source.
15. For MTU, enter **9000**.
16. In the MAC Pool list, select MAC_Pool_B.
17. In the Network Control Policy list, select Enable_CDP.

Create vNIC Template

VLANs

Advanced Filter Export Print

Select	Name	Native VLAN
☐	ib-mgmt	☐
☐	Native-VLAN	☐
☒	VM-App1	☐
☒	VM-App2	☐
☒	VM-App3	☐
☐	vMotion	☐

CDN Source : ☒ vNIC Name ☐ User Defined

MTU : 9000

MAC Pool : MAC_Pool_B(16/32)

QoS Policy : <not set>

Network Control Policy : Enable_CDP

Pin Group : <not set>

Stats Threshold Policy : default

Connection Policies

☒ Dynamic vNIC ☐ usNIC ☐ VMQ

Dynamic vNIC Connection Policy : <not set>

OK Cancel

18. Click OK to create the vNIC template.

19. Click OK.

PowerTool cmdlet Steps: Create vNIC Templates

```
Start-UcsTransaction
$mo = Get-UcsOrg -Level root | Add-UcsVnicTemplate -IdentPoolName "MAC_Pool_A" -
Name "vNIC_Mgmt_A" -NwCtrlPolicyName "Enable_CDP" -RedundancyPairType "primary" -
TemplType "updating-template"
$mo_1 = $mo | Add-UcsVnicInterface -ModifyPresent -DefaultNet "no" -Name "IB-
Mgmt"
$mo_2 = $mo | Add-UcsVnicInterface -ModifyPresent -DefaultNet "yes" -Name
"Native-VLAN"
Complete-UcsTransaction
Start-UcsTransaction
$mo = Get-UcsOrg -Level root | Add-UcsVnicTemplate -IdentPoolName "MAC_Pool_B" -
Name "vNIC_Mgmt_B" -NwCtrlPolicyName "Enable_CDP" -PeerRedundancyTemplName
"vNIC_Mgmt_A" -RedundancyPairType "secondary" -SwitchId "B" -TemplType "updating-
template"
$mo_1 = $mo | Add-UcsVnicInterface -ModifyPresent -DefaultNet "no" -Name "IB-
Mgmt"
$mo_2 = $mo | Add-UcsVnicInterface -ModifyPresent -DefaultNet "yes" -Name
"Native-VLAN"
Complete-UcsTransaction
Start-UcsTransaction
$mo = Get-UcsOrg -Level root | Add-UcsVnicTemplate -IdentPoolName "MAC_Pool_A" -
Mtu 9000 -Name "vNIC_vMotion_A" -NwCtrlPolicyName "Enable_CDP" -
RedundancyPairType "primary" -TemplType "updating-template"
```

```

$mo_1 = $mo | Add-UcsVnicInterface -ModifyPresent -DefaultNet "no" -Name
"vMotion"

Complete-UcsTransaction

Start-UcsTransaction

$mo = Get-UcsOrg -Level root | Add-UcsVnicTemplate -IdentPoolName "MAC_Pool_B" -
Mtu 9000 -Name "vNIC_vMotion_B" -NwCtrlPolicyName "Enable_CDP" -
PeerRedundancyTemplName "vNIC_vMotion_A" -RedundancyPairType "secondary" -
SwitchId "B" -TemplType "updating-template"

$mo_1 = $mo | Add-UcsVnicInterface -ModifyPresent -DefaultNet "no" -Name
"vMotion"

Complete-UcsTransaction

Start-UcsTransaction

$mo = Get-UcsOrg -Level root | Add-UcsVnicTemplate -IdentPoolName "MAC_Pool_A" -
Mtu 9000 -Name "vNIC_App_A" -NwCtrlPolicyName "Enable_CDP" -RedundancyPairType
"primary" -TemplType "updating-template"

$mo_1 = $mo | Add-UcsVnicInterface -ModifyPresent -DefaultNet "no" -Name "VM-App-
1"

$mo_2 = $mo | Add-UcsVnicInterface -ModifyPresent -DefaultNet "no" -Name "VM-App-
2"

$mo_3 = $mo | Add-UcsVnicInterface -ModifyPresent -DefaultNet "no" -Name "VM-App-
3"

Complete-UcsTransaction

Start-UcsTransaction

$mo = Get-UcsOrg -Level root | Add-UcsVnicTemplate -IdentPoolName "MAC_Pool_B" -
Mtu 9000 -Name "vNIC_App_B" -NwCtrlPolicyName "Enable_CDP" -
PeerRedundancyTemplName "vNIC_App_A" -RedundancyPairType "secondary" -SwitchId
"B" -TemplType "updating-template"

$mo_1 = $mo | Add-UcsVnicInterface -ModifyPresent -DefaultNet "no" -Name "VM-App-
1"

$mo_2 = $mo | Add-UcsVnicInterface -ModifyPresent -DefaultNet "no" -Name "VM-App-
2"

$mo_3 = $mo | Add-UcsVnicInterface -ModifyPresent -DefaultNet "no" -Name "VM-App-
3"

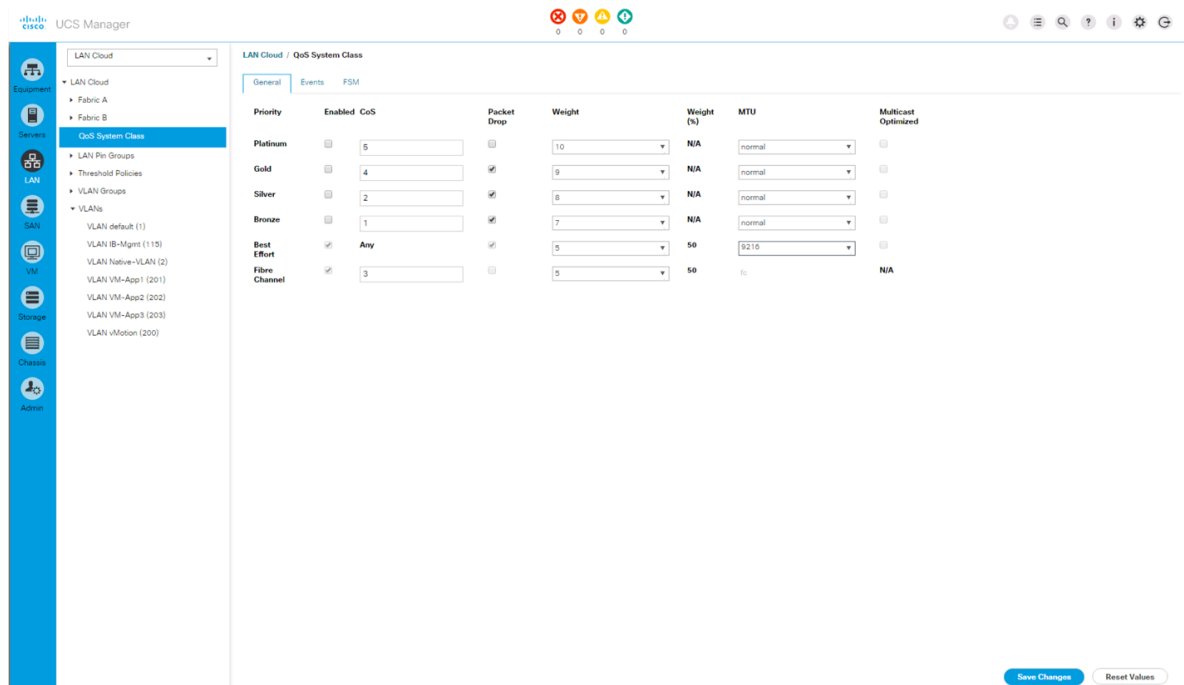
Complete-UcsTransaction

```

Set Jumbo Frames in Cisco UCS Fabric

To configure jumbo frames and enable quality of service (QoS) in the Cisco UCS fabric, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select LAN > LAN Cloud > QoS System Class.
3. In the right pane, click the General tab.
4. On the Best Effort row, enter **9216** in the box in the MTU column.
5. Click Save Changes at the bottom of the window.



6. Click OK.

PowerTool cmdlet Steps: Set Jumbo Frames in Cisco UCS Fabric

```
Add-UcsManagedObject -ModifyPresent -ClassId QosclassEthBE -PropertyMap
@{Dn="fabric/lan/classes/class-best-effort"; Mtu="9216"; }
```

Create LAN Connectivity Policy

To configure the necessary Infrastructure LAN connectivity policy, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select LAN > Policies > root.
3. Right-click LAN Connectivity Policies.
4. Select Create LAN Connectivity Policy.
5. Enter **Infra-LAN-Policy** as the name of the policy.
6. Click the upper Add button to add a vNIC.
7. In the Create vNIC dialog box, enter **00-Mgmt-A** as the name of the vNIC.
8. Select the Use vNIC Template checkbox.
9. In the vNIC Template list, select vNIC_Mgmt_A.
10. In the Adapter Policy list, select VMware.

Create vNIC

Name : 00-Mgmt-A

Use vNIC Template : ☒

Redundancy Pair : ☐

vNIC Template : vNIC_Mgmt_A

Peer Name :

Adapter Performance

Adapter Policy

Domain Policies

vNIC_App_A

vNIC_App_B

vNIC_App_Temp_A

vNIC_App_Temp_B

vNIC_Mgmt_A

vNIC_Mgmt_B

vNIC_Template_A

vNIC_Template_B

vNIC_vMotion_A

vNIC_vMotion_B

Create Ethernet Adapter Policy

OK Cancel

11. Click OK to add this vNIC to the policy.
12. Click the upper Add button to add another vNIC to the policy.
13. In the Create vNIC box, enter **01-Mgmt-B** as the name of the vNIC.
14. Select the Use vNIC Template checkbox.
15. In the vNIC Template list, select vNIC_Mgmt_B.
16. In the Adapter Policy list, select VMWare.
17. Click OK to add the vNIC to the policy.

Create vNIC

Name : 01-Mgmt-B

Use vNIC Template : ☒

Redundancy Pair : ☐

vNIC Template : <not set>

Peer Name :

Adapter Policy

Domain Policies

- vNIC_App_A
- vNIC_App_B
- vNIC_App_Temp_A
- vNIC_App_Temp_B
- vNIC_Mgmt_A
- vNIC_Mgmt_B**
- vNIC_Template_A
- vNIC_Template_B
- vNIC_vMotion_A
- vNIC_vMotion_B

Create Ethernet Adapter Policy

OK Cancel

18. Click the upper Add button to add a vNIC.
19. In the Create vNIC dialog box, enter **02-vMotion-A** as the name of the vNIC.
20. Select the Use vNIC Template checkbox.
21. In the vNIC Template list, select vNIC_vMotion_A.
22. In the Adapter Policy list, select VMware.
23. Click OK to add this vNIC to the policy.

Create vNIC

Name : 02-vMotion-A

Use vNIC Template : ☒

Redundancy Pair : ☐

Peer Name :

Create vNIC Template

vNIC Template : <not set>

Adapter Policy : <not set>

Domain Policies

Adapter Policy

vNIC_App_A

vNIC_App_B

vNIC_App_Temp_A

vNIC_App_Temp_B

vNIC_Mgmt_A

vNIC_Mgmt_B

vNIC_Template_A

vNIC_Template_B

vNIC_vMotion_A

vNIC_vMotion_B

Create Ethernet Adapter Policy

OK Cancel

24. Click the upper Add button to add a vNIC to the policy.
25. In the Create vNIC dialog box, enter **03-vMotion-B** as the name of the vNIC.
26. Select the Use vNIC Template checkbox.
27. In the vNIC Template list, select vNIC_vMotion_B.
28. In the Adapter Policy list, select VMware.

Create vNIC

Name : 03-vMotion-B

Use vNIC Template : ☒

Redundancy Pair : ☐

Peer Name :

Create vNIC Template

vNIC Template : <not set>

Adapter Policy : <not set>

Domain Policies

Adapter Policy

vNIC_App_A

vNIC_App_B

vNIC_App_Temp_A

vNIC_App_Temp_B

vNIC_Mgmt_A

vNIC_Mgmt_B

vNIC_Template_A

vNIC_Template_B

vNIC_vMotion_A

vNIC_vMotion_B

Create Ethernet Adapter Policy

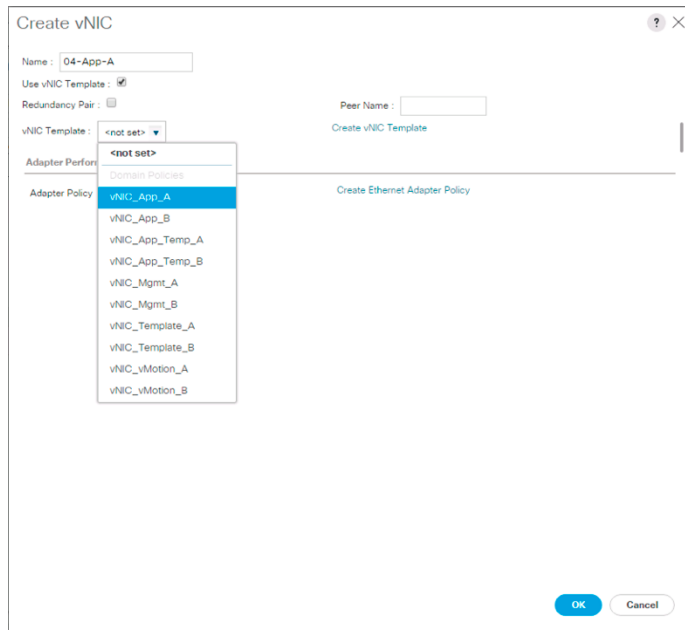
OK Cancel

29. Click OK to add this vNIC to the policy.
30. Click the upper Add button to add a vNIC.
31. In the Create vNIC dialog box, enter **04-App-A** as the name of the vNIC.
32. Select the Use vNIC Template checkbox.

33. In the vNIC Template list, select vNIC_App_A.

34. In the Adapter Policy list, select VMware.

35. Click OK to add this vNIC to the policy.



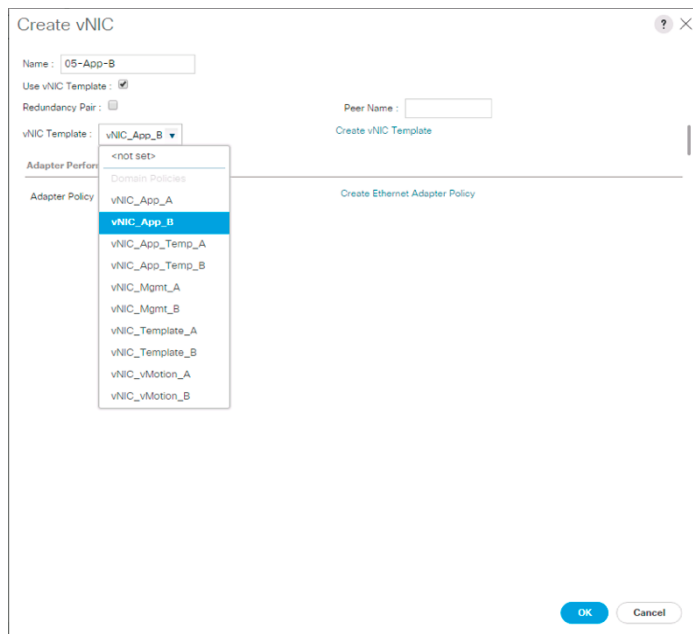
36. Click the upper Add button to add a vNIC to the policy.

37. In the Create vNIC dialog box, enter **05-App-B** as the name of the vNIC.

38. Select the Use vNIC Template checkbox.

39. In the vNIC Template list, select vNIC_App_B.

40. In the Adapter Policy list, select VMware.



41. Click OK to add this vNIC to the policy.

Create LAN Connectivity Policy

Name : Infra-LAN-Policy

Description :

Click **Add** to specify one or more vNICs that the server should use to connect to the LAN.

Name	MAC Address	Native VLAN
vNIC 05-App-B	Derived	
vNIC 04-App-A	Derived	
vNIC 03-vMotion-B	Derived	
vNIC 02-vMotion-A	Derived	
vNIC 01-Mgmt-B	Derived	
vNIC 00-Mgmt-A	Derived	

Delete Add Modify

+ Add iSCSI vNICs

OK Cancel

42. Click OK to create the LAN connectivity policy.

43. Click OK.

PowerTool cmdlet Steps: Create LAN Connectivity Policy

```
Start-UcsTransaction
```

```
$mo = Get-UcsOrg -Level root | Add-UcsVnicLanConnPolicy -Name "Infra-LAN-Policy"
```

```
$mo_1 = $mo | Add-UcsVnic -AdaptorProfileName "VMWare" -Name "00-Mgmt-A" -  
NwTemplateName "vNIC_Mgmt_A" -Order "1"
```

```
$mo_2 = $mo | Add-UcsVnic -AdaptorProfileName "VMWare" -Name "01-Mgmt-B" -  
NwTemplateName "vNIC_Mgmt_B" -Order "2" -SwitchId "B"
```

```
$mo_3 = $mo | Add-UcsVnic -AdaptorProfileName "VMWare" -Name "02-vMotion-A" -  
NwTemplateName "vNIC_vMotion_A" -Order "3"
```

```
$mo_4 = $mo | Add-UcsVnic -AdaptorProfileName "VMWare" -Name "03-vMotion-B" -  
NwTemplateName "vNIC_vMotion_B" -Order "4" -SwitchId "B"
```

```
$mo_5 = $mo | Add-UcsVnic -AdaptorProfileName "VMWare" -Name "04-App-A" -  
NwTemplateName "vNIC_App_A" -Order "5"
```

```
$mo_6 = $mo | Add-UcsVnic -AdaptorProfileName "VMWare" -Name "05-App-B" -  
NwTemplateName "vNIC_App_B" -Order "6" -SwitchId "B"
```

```
Complete-UcsTransaction
```

Configure Cisco UCS SAN Connectivity

This section presents the steps for configuring SAN connectivity in the Cisco UCS environment.

Configure Unified Ports

The Cisco UCS 6332-16UP Fabric Interconnects have a slider mechanism in the Cisco UCS Manager GUI that controls the 16 ports. You can enable and configure the first 6, the first 12, or all 16 of the unified ports.

To configure the Fibre Channel ports, complete the following steps:

1. In Cisco UCS Manager, click the Equipment tab in the navigation pane.
2. Select Equipment > Fabric Interconnects > Fabric Interconnect A (primary)
3. Select Configure Unified Ports.
4. Click Yes in the pop-up window warning that changes to the fixed module will require a reboot of the fabric interconnect and that changes to the expansion module will require a reboot of that module.
5. In the Configured Fixed Ports pop-up window, move the gray slider bar from the left to the right to select 6, 12, or 16 ports to be set as Fibre Channel uplinks.

Configure Unified Ports



Instructions

The position of the slider determines the type of the ports.
All the ports to the left of the slider are Fibre Channel ports (Purple), while the ports to the right are Ethernet ports (Blue).

Port	Transport	If Role or Port Channel Membership	Desired If Role
Port 1	ether	Unconfigured	FC Uplink
Port 2	ether	Unconfigured	FC Uplink
Port 3	ether	Unconfigured	FC Uplink
Port 4	ether	Unconfigured	FC Uplink
Port 5	ether	Unconfigured	FC Uplink
Port 6	ether	Unconfigured	FC Uplink
Port 7	ether	Unconfigured	
Port 8	ether	Unconfigured	
Port 9	ether	Unconfigured	
Port 10	ether	Unconfigured	
Port 11	ether	Unconfigured	
Port 12	ether	Unconfigured	
Port 13	ether	Unconfigured	
Port 14	ether	Unconfigured	
Port 15	ether	Unconfigured	
Port 16	ether	Unconfigured	

OK **Cancel**

6. Click OK to continue.
7. Select Equipment > Fabric Interconnects > Fabric Interconnect B (primary).
8. Select Configure Unified Ports.

9. Click Yes in the pop-up window warning that changes to the fixed module will require a reboot of the fabric interconnect and that changes to the expansion module will require a reboot of that module.
10. In the Configured Fixed Ports pop-up window, move the gray slider bar from the left to the right to select 6, 12, or 16 ports to be set as Fibre Channel uplinks.
11. Click OK to continue.

Note: The fabric interconnects will reboot and then will reconnect to Cisco UCS Manager after they are back up.

PowerTool cmdlet Steps: Configure Unified Ports

```
Start-UcsTransaction
```

```
$mo = Add-UcsManagedObject -ModifyPresent -ClassId FabricFcSan -PropertyMap
@{Id="A"; Dn="fabric/san/A"; }
```

```
$mo_1 = $mo | Add-UcsFcUplinkPort -AdminState "enabled" -AutoNegotiate "yes" -
FillPattern "arbff" -Name "" -PortId 1 -SlotId 1 -UsrLbl ""
```

```
$mo_2 = $mo | Add-UcsFcUplinkPort -AdminState "enabled" -AutoNegotiate "yes" -
FillPattern "arbff" -Name "" -PortId 2 -SlotId 1 -UsrLbl ""
```

```
$mo_3 = $mo | Add-UcsFcUplinkPort -AdminState "enabled" -AutoNegotiate "yes" -
FillPattern "arbff" -Name "" -PortId 3 -SlotId 1 -UsrLbl ""
```

```
$mo_4 = $mo | Add-UcsFcUplinkPort -AdminState "enabled" -AutoNegotiate "yes" -
FillPattern "arbff" -Name "" -PortId 4 -SlotId 1 -UsrLbl ""
```

```
$mo_5 = $mo | Add-UcsFcUplinkPort -AdminState "enabled" -AutoNegotiate "yes" -
FillPattern "arbff" -Name "" -PortId 5 -SlotId 1 -UsrLbl ""
```

```
$mo_6 = $mo | Add-UcsFcUplinkPort -AdminState "enabled" -AutoNegotiate "yes" -
FillPattern "arbff" -Name "" -PortId 6 -SlotId 1 -UsrLbl ""
```

```
Complete-UcsTransaction
```

```
Start-UcsTransaction
```

```
$mo = Add-UcsManagedObject -ModifyPresent -ClassId FabricFcSan -PropertyMap
@{Id="B"; Dn="fabric/san/B"; }
```

```
$mo_1 = $mo | Add-UcsFcUplinkPort -AdminState "enabled" -AutoNegotiate "yes" -
FillPattern "arbff" -Name "" -PortId 1 -SlotId 1 -UsrLbl ""
```

```
$mo_2 = $mo | Add-UcsFcUplinkPort -AdminState "enabled" -AutoNegotiate "yes" -
FillPattern "arbff" -Name "" -PortId 2 -SlotId 1 -UsrLbl ""
```

```
$mo_3 = $mo | Add-UcsFcUplinkPort -AdminState "enabled" -AutoNegotiate "yes" -
FillPattern "arbff" -Name "" -PortId 3 -SlotId 1 -UsrLbl ""
```

```
$mo_4 = $mo | Add-UcsFcUplinkPort -AdminState "enabled" -AutoNegotiate "yes" -
FillPattern "arbff" -Name "" -PortId 4 -SlotId 1 -UsrLbl ""
```

```
$mo_5 = $mo | Add-UcsFcUplinkPort -AdminState "enabled" -AutoNegotiate "yes" -
FillPattern "arbff" -Name "" -PortId 5 -SlotId 1 -UsrLbl ""
```

```
$mo_6 = $mo | Add-UcsFcUplinkPort -AdminState "enabled" -AutoNegotiate "yes" -
FillPattern "arbff" -Name "" -PortId 6 -SlotId 1 -UsrLbl ""
```

```
Complete-UcsTransaction
```

```
#
```

```
#
```

```
# Wait for FIs to reboot before proceeding
```

```
# (Credentials may need to be re-established within PowerShell after reboot)
```

```
#
```

```
#
```

Create VSANs

To configure the necessary virtual storage area networks (VSANs) for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the SAN tab in the navigation pane.

Note: In this procedure, two VSANs are created.

2. Select SAN > SAN Cloud.
3. Right-click VSANs.
4. Select Create VSAN.
5. Enter **VSAN_A** as the name of the VSAN to be used for Fabric A
6. Leave Disabled selected for FC Zoning.
7. Select Fabric A.
8. Enter a unique VSAN ID and a corresponding Fibre Channel over Ethernet (FCoE) VLAN ID. The recommended approach is to use the same ID for both parameters and to use something other than 1.

Create VSAN

Name : VSAN_A

FC Zoning Settings

FC Zoning : ☒ Disabled ☐ Enabled

Do **NOT** enable local zoning if fabric interconnect is connected to an upstream FC/FCoE switch.

☐ Common/Global ☒ Fabric A ☐ Fabric B ☐ Both Fabrics Configured Differently

You are creating a local VSAN in fabric A that maps to a VSAN ID that exists only in fabric A.

Enter the VSAN ID that maps to this VSAN.

VSAN ID : 101

A VLAN can be used to carry FCoE traffic and can be mapped to this VSAN.

Enter the VLAN ID that maps to this VSAN.

FCoE VLAN : 101

OK Cancel

9. Click OK. Then click OK again.
10. Under SAN Cloud, right-click VSANs.
11. Select Create VSAN.
12. Enter **VSAN_B** as the name of the VSAN to be used for Fabric B.
13. Leave Disabled selected for FC Zoning.
14. Select Fabric B.
15. Enter a unique VSAN ID and a corresponding FCoE VLAN ID. The recommended approach is to use the same ID for both parameters and to use something other than 1.

16. Click OK. Then click OK again.

PowerTool cmdlet Steps: Create VSANs

```
Get-UcsFisSanCloud -Id "A" | Add-UcsVsan -FcZoneSharingMode "coalesce" -FcoeVlan
101 -Id 101 -Name "VSAN_A" -PolicyOwner "local" -ZoningState "disabled"

Get-UcsFisSanCloud -Id "B" | Add-UcsVsan -FcZoneSharingMode "coalesce" -FcoeVlan
102 -Id 102 -Name "VSAN_B" -PolicyOwner "local" -ZoningState "disabled"
```

Create Fibre Channel Port Channels

To configure the necessary port channels for the Cisco UCS environment, complete the following steps:

Create a Port Channel for Fabric-A

1. In the navigation pane, under SAN > SAN Cloud, expand the Fabric A tree.
2. Right-click FC Port Channels.
3. Select Create Port Channel.
4. Enter **1** as the ID and **Po1** as the port channel name.

Create FC Port Channel

1 Set FC Port Channel Name

ID : 1

Name : Po1

< Prev Next > Finish Cancel

- Click Next. Then choose appropriate ports and click >> to add the ports to the port channel.

Create FC Port Channel

2 Add Ports

Port Channel Admin Speed : Auto

Ports		
Port	Slot ID	WWPN
1	1	20:01:00:DE...
2	1	20:02:00:DE...
3	1	20:03:00:DE...
4	1	20:04:00:DE...
5	1	20:05:00:DE...
6	1	20:06:00:DE...

>> <<

Ports in the port channel		
Port	Slot ID	WWPN
No data available		

Slot ID: 1
WWPN: 20:01:00:DE:FB:07:C9:80

Slot ID:
WWPN:

< Prev Next > Finish Cancel

- Click Finish.
- Click OK.
- From the VSAN pull-down menu for Port-Channel 1, select VSAN_A 101.

General	Ports	Faults	Events	Statistics
Status Overall Status : Admin Down Additional Info : Administratively down				
Actions Enable Port Channel Disable Port Channel Add Ports				
Properties				
ID : 1				
Fabric ID : A				
Port Type : Aggregation				
Transport Type : Fc				
Name : Fabric_A				
Description :				
VSAN : A/vsan VSAN_A (101)				
Port Channel Admin Speed : Fabric A/vsan VSAN_A (101)				
Operational Speed(Gbps) : Fabric Dual/vsan default (1)				

9. Click Save Changes and then click OK.
10. Create a Port Channel for Fabric-B
11. In the navigation pane, under SAN > SAN Cloud, expand the Fabric B tree.
12. Right-click FC Port Channels.
13. Select Create Port Channel.
14. Enter **2** as the ID and **Po2** as the port channel name.

1

Set FC Port Channel Name

2

Add Ports

Create FC Port Channel

ID : 2

Name : Po2

< Prev

Next >

Finish

Cancel

15. Click Next. Then choose appropriate ports and click >> to add the ports to the port channel.

Create FC Port Channel

Port Channel Admin Speed:

Ports		
Port	Slot ID	WWPN
1	1	20:01:00:DE...
2	1	20:02:00:DE...
3	1	20:03:00:DE...
4	1	20:04:00:DE...
5	1	20:05:00:DE...
6	1	20:06:00:DE...

Ports in the port channel		
Port	Slot ID	WWPN
No data available		

Slot ID: 1
WWPN: 20:01:00:DE:FB:29:F1:00

Slot ID:
WWPN:

< Prev Next > **Finish** Cancel

16. Click Finish.
17. Click OK.
18. From the VSAN pull-down menu for Port-Channel 2, select VSAN_B 102.

SAN / SAN Cloud / Fabric B / FC Port Channels / FC Port-Channel 2 Fabric_B

General Ports Faults Events Statistics

Status

Overall Status : ▼ Failed

Additional Info : **No operational members**

Actions

Enable Port Channel

Disable Port Channel

Add Ports

Properties

ID : **2**

Fabric ID : **B**

Port Type : **Aggregation**

Transport Type : **Fc**

Name :

Description :

VSAN :

Port Channel Admin Speed : **Fabric B/vsan VSAN_B (102)**

Operational Speed(Gbps) : **Fabric Dual/vsan default (1)**

19. Click Save Changes and then click OK.

PowerTool cmdlet Steps: Create Fibre Channel Port Channels

```
Start-UcsTransaction

$mo = Get-UcsFiSanCloud -Id "A" | Add-UcsFcUplinkPortChannel -Name "Po1" -PortId
1

$mo_1 = $mo | Add-UcsFabricFcSanPcEp -ModifyPresent -AdminSpeed "auto" -
AdminState "enabled" -AutoNegotiate "yes" -FillPattern "arbff" -Name "" -PortId 1
-SlotId 1

$mo_2 = $mo | Add-UcsFabricFcSanPcEp -ModifyPresent -AdminSpeed "auto" -
AdminState "enabled" -AutoNegotiate "yes" -FillPattern "arbff" -Name "" -PortId 2
-SlotId 1

$mo_3 = $mo | Add-UcsFabricFcSanPcEp -ModifyPresent -AdminSpeed "auto" -
AdminState "enabled" -AutoNegotiate "yes" -FillPattern "arbff" -Name "" -PortId 3
-SlotId 1

$mo_4 = $mo | Add-UcsFabricFcSanPcEp -ModifyPresent -AdminSpeed "auto" -
AdminState "enabled" -AutoNegotiate "yes" -FillPattern "arbff" -Name "" -PortId 4
-SlotId 1

Complete-UcsTransaction
```

```
Start-UcsTransaction

$mo = Get-UcsFiSanCloud -Id "A" | Add-UcsVsan -ModifyPresent -Name "VSAN_A"

$mo_1 = $mo | Add-UcsVsanMemberFcPortChannel -ModifyPresent -AdminState "enabled"
-Descr "" -Name "" -PortId 1 -SwitchId "A"

Complete-UcsTransaction
```

```
Start-UcsTransaction

$mo = Get-UcsFiSanCloud -Id "B" | Add-UcsFcUplinkPortChannel -Name "Po2" -PortId
2

$mo_1 = $mo | Add-UcsFabricFcSanPcEp -ModifyPresent -AdminSpeed "auto" -
AdminState "enabled" -AutoNegotiate "yes" -FillPattern "arbff" -Name "" -PortId 1
-SlotId 1

$mo_2 = $mo | Add-UcsFabricFcSanPcEp -ModifyPresent -AdminSpeed "auto" -
AdminState "enabled" -AutoNegotiate "yes" -FillPattern "arbff" -Name "" -PortId 2
-SlotId 1

$mo_3 = $mo | Add-UcsFabricFcSanPcEp -ModifyPresent -AdminSpeed "auto" -
AdminState "enabled" -AutoNegotiate "yes" -FillPattern "arbff" -Name "" -PortId 3
-SlotId 1

$mo_4 = $mo | Add-UcsFabricFcSanPcEp -ModifyPresent -AdminSpeed "auto" -
AdminState "enabled" -AutoNegotiate "yes" -FillPattern "arbff" -Name "" -PortId 4
-SlotId 1

Complete-UcsTransaction
```

```
Start-UcsTransaction
```

Create vHBA Templates

To create the necessary vHBA templates for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
2. Select Policies > root.
3. Right-click vHBA Templates.
4. Select Create vHBA Template.
5. Enter **vHBA_Template_A** as the vHBA template name.
6. Keep Fabric A selected.
7. Leave Redundancy Type as No Redundancy.
8. Select VSAN_A.
9. Leave Initial Template as the template type.
10. Select WWPN_Pool_A for WWPN Pool.
11. Click OK to create the vHBA template.

The screenshot shows the 'Create vHBA Template' dialog box with the following configuration:

- Name: vHBA_Template_A
- Description: (empty)
- Fabric ID: ☒ A ☐ B
- Redundancy Type: ☒ No Redundancy ☐ Primary Template ☐ Secondary Template
- Select VSAN: VSAN_A (with a 'Create VSAN' link)
- Template Type: ☒ Initial Template ☐ Updating Template
- Max Data Field Size: 2048
- WWPN Pool: WWPN_Pool_A(24/32)
- QoS Policy: <not set>
- Pin Group: <not set>
- Stats Threshold Policy: default

Buttons: OK, Cancel

12. Click OK.
13. Right-click vHBA Templates.
14. Select Create vHBA Template.
15. Enter **vHBA_Template_B** as the vHBA template name.
16. Select Fabric B for Fabric ID.
17. Select VSAN_B.
18. Leave Redundancy Type as No Redundancy.
19. Leave Initial Template as the template type.
20. Select WWPN_Pool_B for WWPN Pool.

21. Click OK to create the vHBA template.

Create vHBA Template

Name : vHBA_Template_B

Description :

Fabric ID : ☐ A ☒ B

Redundancy

Redundancy Type : ☒ No Redundancy ☐ Primary Template ☐ Secondary Template

Select VSAN : VSAN_B [Create VSAN](#)

Template Type : ☒ Initial Template ☐ Updating Template

Max Data Field Size : 2048

WWPN Pool : WWPN_Pool_B(24/32)

QoS Policy : <not set>

Pin Group : <not set>

Stats Threshold Policy : default

OK Cancel

22. Click OK.

PowerTool cmdlet Steps: Create vHBA Templates

```
Start-UcsTransaction
$mo = Get-UcsOrg -Level root | Add-UcsVhbaTemplate -IdentPoolName "WWPN_Pool_A"
-Name "vHBA_Template_A"
$mo_1 = $mo | Add-UcsVhbaInterface -ModifyPresent -Name "VSAN_A"
Complete-UcsTransaction

Start-UcsTransaction
$mo = Get-UcsOrg -Level root | Add-UcsVhbaTemplate -IdentPoolName "WWPN_Pool_B"
-Name "vHBA_Template_B" -SwitchId "B"
$mo_1 = $mo | Add-UcsVhbaInterface -ModifyPresent -Name "VSAN_B"
Complete-UcsTransaction
```

Create SAN Connectivity Policy

To configure the necessary Infrastructure SAN connectivity policy, complete the following steps:

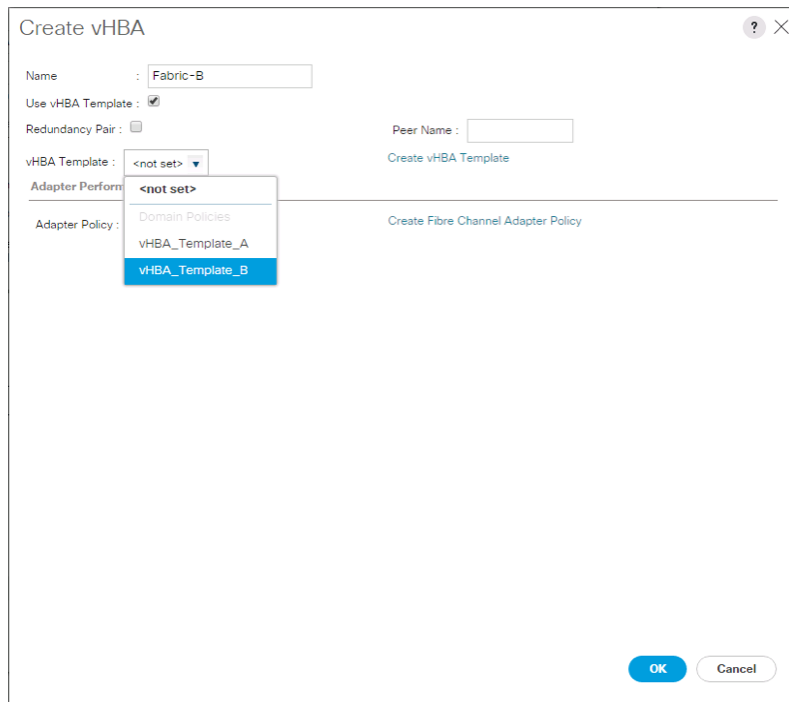
1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
2. Select SAN > Policies > root.
3. Right-click SAN Connectivity Policies.
4. Select Create SAN Connectivity Policy.
5. Enter **Infra-SAN-Policy** as the name of the policy.
6. Select the previously created WWNN_Pool for the WWNN assignment.
7. Click the Add button at the bottom to add a vHBA.
8. In the Create vHBA dialog box, enter **Fabric-A** as the name of the vHBA.

9. Select the Use vHBA Template checkbox.
10. Leave Redundancy Pair unselected.
11. In the vHBA Template list, select vHBA_Template_A.

The screenshot shows the 'Create vHBA' dialog box with the following fields and options:

- Name:** Fabric-A
- Use vHBA Template:** ☒
- Redundancy Pair:** ☐
- Peer Name:** (empty field)
- vHBA Template:** <not set> (dropdown menu open, showing vHBA_Template_A selected)
- Adapter Policy:** (dropdown menu open, showing VMware selected)
- Buttons:** OK (highlighted), Cancel

12. In the Adapter Policy list, select VMware.
13. Click OK.
14. Click the Add button at the bottom to add a second vHBA.
15. In the Create vHBA dialog box, enter **Fabric-B** as the name of the vHBA.
16. Select the Use vHBA Template checkbox.
17. Leave Redundancy Pair unselected.
18. In the vHBA Template list, select vHBA_Template_B.



Create vHBA

Name :

Use vHBA Template : ☒

Redundancy Pair : ☐ Peer Name :

vHBA Template : [Create vHBA Template](#)

Adapter Perform :

Adapter Policy : [Create Fibre Channel Adapter Policy](#)

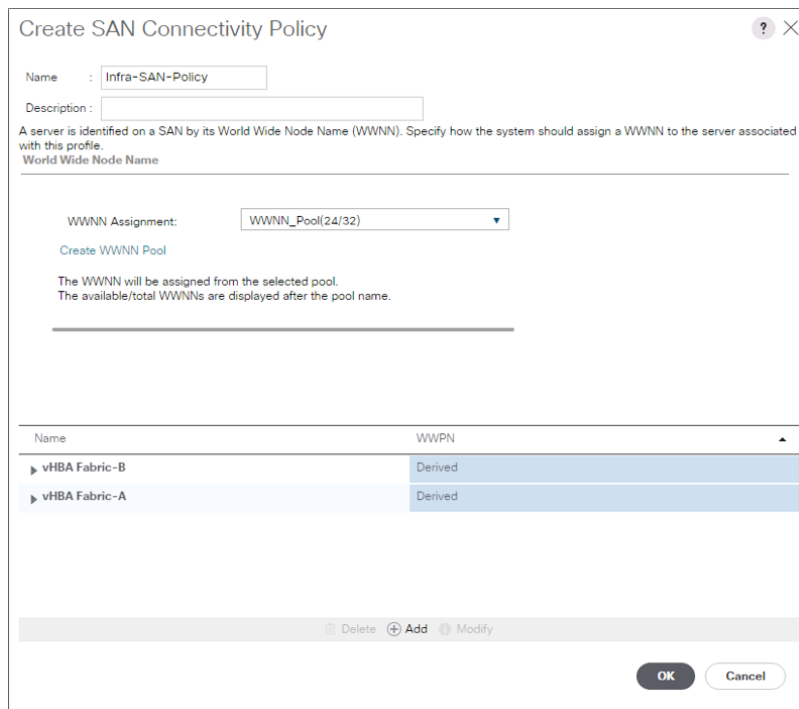
[vHBA_Template_A](#)

[vHBA_Template_B](#)

[OK](#) [Cancel](#)

19. In the Adapter Policy list, select VMware.

20. Click OK.



Create SAN Connectivity Policy

Name :

Description :

A server is identified on a SAN by its World Wide Node Name (WWNN). Specify how the system should assign a WWNN to the server associated with this profile.

World Wide Node Name

WWNN Assignment: [Create WWNN Pool](#)

The WWNN will be assigned from the selected pool.
The available/total WWNNs are displayed after the pool name.

Name	WWPN
▶ vHBA Fabric-B	Derived
▶ vHBA Fabric-A	Derived

[Delete](#) [Add](#) [Modify](#)

[OK](#) [Cancel](#)

21. Click OK to create the SAN connectivity policy.

22. Click OK to confirm the policy creation.

PowerTool cmdlet Steps: Create SAN Connectivity Policy

```
Start-UcsTransaction

$mo = Get-UcsOrg -Level root | Add-UcsVnicSanConnPolicy -Name "Infra-SAN-Policy"

$mo_1 = $mo | Add-UcsVnicFcNode -ModifyPresent -Addr "pool-derived" -
IdentPoolName "WWNN_Pool"

$mo_2 = $mo | Add-UcsVhba -AdaptorProfileName "VMWare" -Name "Fabric-A" -
NwTemplName "vHBA_Template_A" -Order "1"

$mo_2_1 = $mo_2 | Add-UcsVhbaInterface -ModifyPresent -Name "default"

$mo_3 = $mo | Add-UcsVhba -AdaptorProfileName "VMWare" -Name "Fabric-B" -
NwTemplName "vHBA_Template_B" -Order "2"

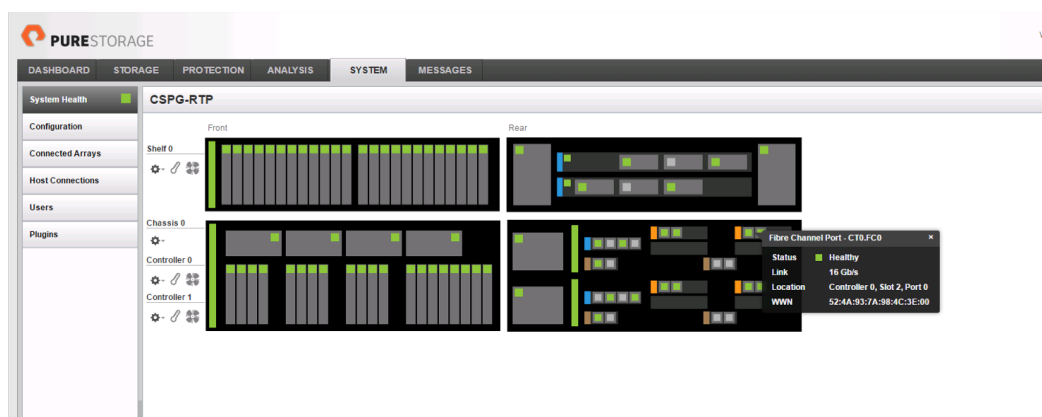
$mo_3_1 = $mo_3 | Add-UcsVhbaInterface -ModifyPresent -Name "default"

Complete-UcsTransaction
```

Create Boot Policies

This procedure defines the primary and secondary boot targets for each fabric side (fabrics A and B). These targets are the worldwide names (WWNs) that need to be collected from the first adapter of each controller on the Pure Storage FlashArray//M. They are visible on the System Health tab in the System section of the Pure Storage web portal (Figure 6).

Figure 6. System View on the System Health Tab



Find the FC0 adapters for each controller in the System view and record the values to be used for the primary and secondary targets. In the sample environment described in this document, these appear as the first ports on the right side of each controller in Figure 6 (see Table 1).

Table 1. Fabric A Boot Targets for the FlashArray//M

	Port Name	Target Role	WWN and WWPN Sample Environment	WWN and WWPN Customer Environment
FlashArray//M Controller 0	CT0.FC0	Primary	52:4a:93:7a:98:4c:3e:00	
FlashArray//M Controller 1	CT1.FC0	Secondary	52:4a:93:7a:98:4c:3e:10	

In the same System view, find the FC1 adapters for each controller and record the values to be used for the primary and secondary targets. In the sample environment described in this document, these appear as the second ports on the right side of each controller shown in Figure 6 (see Table 2).

Table 2. Fabric B Boot Targets for the FlashArray//M

	Port Name	Target Role	WWN and WWPN Sample Environment	WWN and WWPN Customer Environment
FlashArray//M Controller 0	CT0.FC1	Primary	52:4a:93:7a:98:4c:3e:01	
FlashArray//M Controller 1	CT1.FC1	Secondary	52:4a:93:7a:98:4c:3e:11	

To create boot policies for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click Boot Policies.
4. Select Create Boot Policy.
5. Enter **Boot-FC-A** as the name of the boot policy.
6. Optional: Enter a description for the boot policy.

Note: Do not select the Reboot on Boot Order Change checkbox.

7. Keep the Reboot on Boot Order Change option unselected.
8. From the Local Devices drop-down menu, select Add Remote CD/DVD.
9. From the vHBAs drop-down menu, select Add SAN Boot.
10. In the Add SAN Boot dialog box, enter **Fabric-A** in the vHBA field.
11. Confirm that Primary is selected for the Type option.

The screenshot shows the 'Create Boot Policy' dialog box in Cisco UCS Manager. The 'Name' field is populated with 'Boot-FC-A'. The 'Description' field is empty. The 'Reboot on Boot Order Change' checkbox is unchecked. The 'Enforce vNIC/vHBA/iSCSI Name' checkbox is checked. The 'Boot Mode' is set to 'Legacy'. A 'WARNINGS' section is visible. The 'Add SAN Boot' dialog box is open, showing 'vHBA' set to 'Fabric-A' and 'Type' set to 'Primary'. The 'Add SAN Boot' dialog box has 'OK' and 'Cancel' buttons.

12. Click OK to add the SAN boot initiator.
13. From the vHBA drop-down menu, select Add SAN Boot Target.
14. Enter **1** as the value for Boot Target LUN.
15. Enter the WWPN for CT0.FC0 recorded in **Error! Reference source not found..**
16. Select Primary for the SAN boot target type.

The screenshot shows the 'Create Boot Policy' dialog box. The 'Name' field is set to 'Boot-FC-A'. The 'Description' field is empty. The 'Reboot on Boot Order Change' checkbox is unchecked. The 'Enforce vNIC/vHBA/SCSI Name' checkbox is checked. The 'Boot Mode' is set to 'Legacy'. A 'WARNINGS' section is visible. The 'Add SAN Boot Target' sub-dialog is open, showing 'Boot Target LUN' as '1', 'Boot Target WWPN' as '52:4a:93:7a:98:4c:3e:00', and 'Type' as 'Primary'. The 'OK' button is highlighted in blue.

Create Boot Policy

Name : Boot-FC-A

Description :

Reboot on Boot Order Change : ☐

Enforce vNIC/vHBA/SCSI Name : ☒

Boot Mode : ☒ Legacy ☐ Uefi

WARNINGS:
The type (primary/secondary) does not indicate a boot order presence.
The effective order of boot devices within the same...
If Enforce vNIC/vHBA/SCSI Name is selected and...
If it is not selected, the vNICs/vHBAs are selected if...

+ Local Devices

+ vNICs

- vHBAs

Add SAN Boot

Add SAN Boot Target

+ iSCSI vNICs

+ CIMC Mounted vMedia

+ EFI Shell

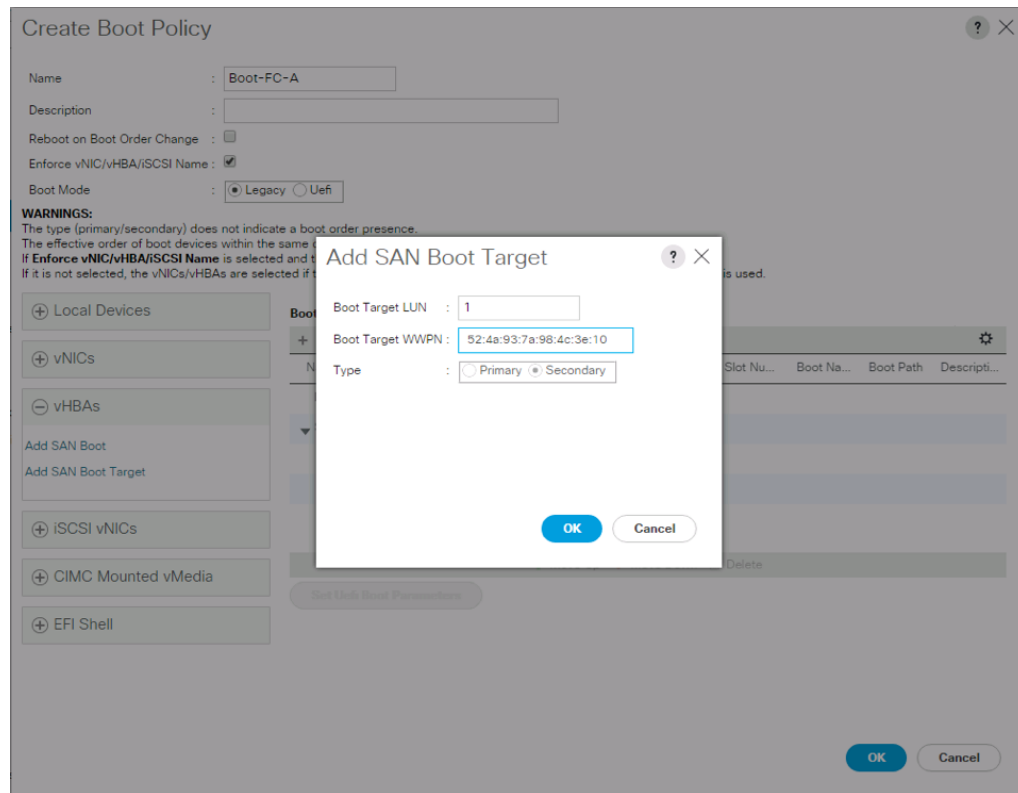
Boot Target LUN : 1

Boot Target WWPN : 52:4a:93:7a:98:4c:3e:00

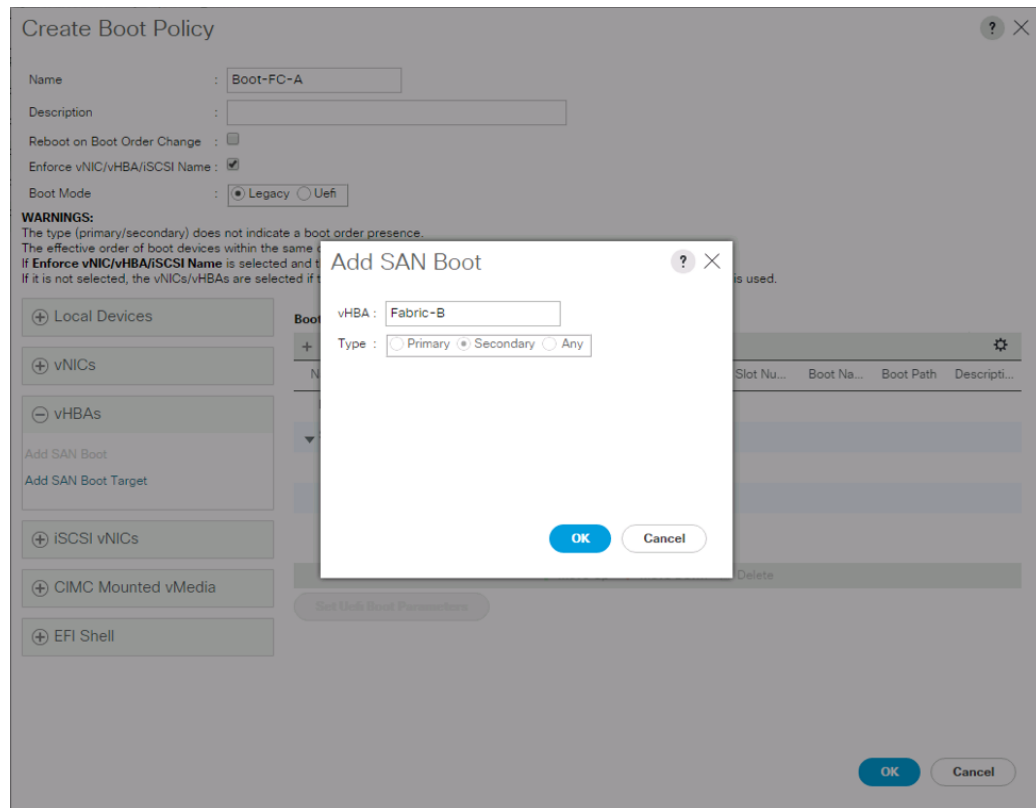
Type : ☒ Primary ☐ Secondary

OK Cancel

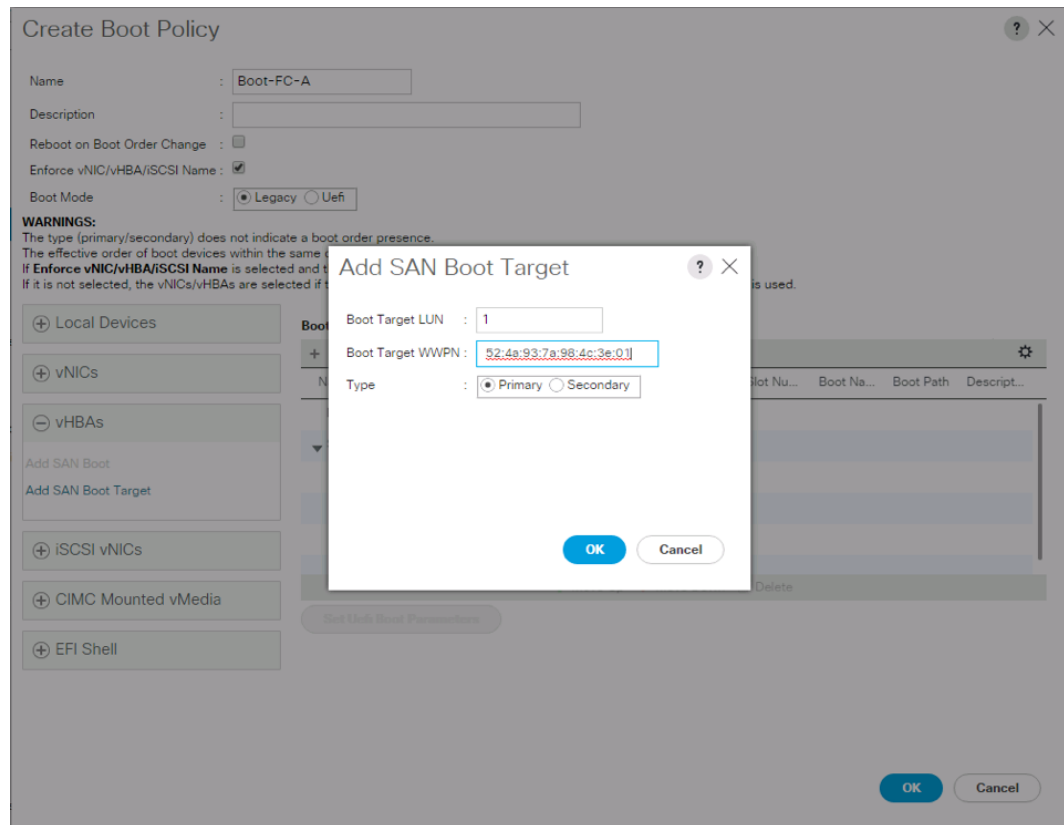
17. Click OK to add the SAN boot target.
18. From the vHBA drop-down menu, select Add SAN Boot Target.
19. Enter **1** as the value for Boot Target LUN.
20. Enter the WWPN for CT1.FC0 recorded in **Error! Reference source not found..**



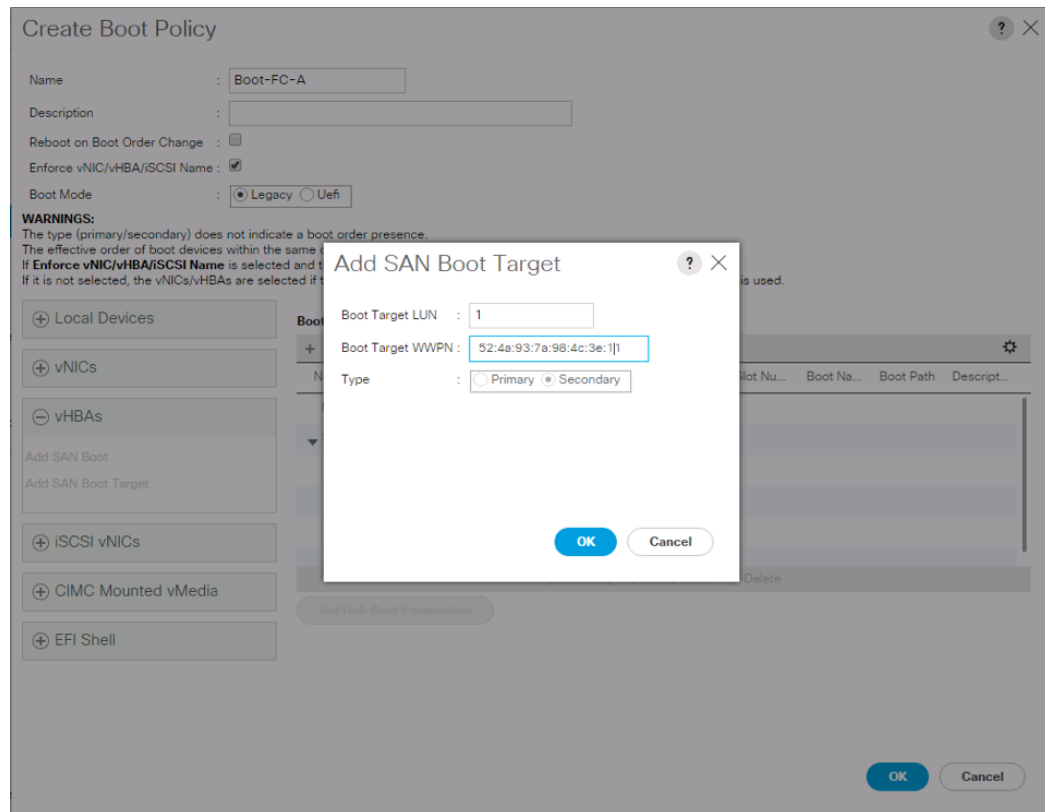
21. Click OK to add the SAN boot target.
22. From the vHBA drop-down menu, select Add SAN Boot.
23. In the Add SAN Boot dialog box, enter **Fabric-B** in the vHBA box.
24. Verify that the SAN boot type is automatically set to Secondary and that the Type option is unavailable.



25. Click OK to add the SAN boot initiator.
26. From the vHBA drop-down menu, select Add SAN Boot Target.
27. Enter **1** as the value for Boot Target LUN.
28. Enter the WWPN for CT0.FC1 recorded in **Error! Reference source not found.**
29. Select Primary for the SAN boot target type.



30. Click OK to add the SAN boot target.
31. From the vHBA drop-down menu, select Add SAN Boot Target.
32. Enter **1** as the value for Boot Target LUN.
33. Enter the WWPN for CT1.FC1 recorded in **Error! Reference source not found.**



34. Click OK to add the SAN boot target.
35. Expand CIMC Mounted Media and select Add CIMC Mounted CD/DVD.

Create Boot Policy

Name

: Boot-FC-A

Description

:

Reboot on Boot Order Change

:

☐

Enforce vNIC/vHBA/iSCSI Name

:

☒

Boot Mode

:

Legacy

Uefi

WARNINGS:

The type (primary/secondary) does not indicate a boot order presence.

The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.

If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.

If it is not selected, the vNICs/vHBAs are selected if they exist, otherwise the vNIC/vHBA with the lowest PCIe bus scan order is used.

Local Devices

vNICs

vHBAs

Add SAN Boot

Add SAN Boot Target

iSCSI vNICs

CIMC Mounted vMedia

EFI Shell

Boot Order

Advanced Filter

Export

Print

Name	Order	Type	WWN
Remote CD/DVD	1		
San	2		
SAN Primary		Primary	
SAN Secondary		Secondary	
SAN Target Primary		Primary	52:4A:93:7A:98:4C:3E:01
SAN Target Secondary		Secondary	52:4A:93:7A:98:4C:3E:11

Move Up

Move Down

Delete

Set Uefi Boot Parameters

OK

Cancel

36. Click OK. Then click OK again to create the boot policy.

PowerTool cmdlet Steps: Create Boot Policies

```
Start-UcsTransaction
$mo = Get-UcsOrg -Level root | Add-UcsBootPolicy -Name "Boot-FC-A"
$mo_1 = $mo | Add-UcsLsbootVirtualMedia -Access "read-only-remote" -LunId "0" -
Order 1
$mo_2 = $mo | Add-UcsLsbootSan -Order 2
$mo_2_1 = $mo_2 | Add-UcsLsbootSanCatSanImage -Type "primary" -VnicName "Fabric-
A"
$mo_2_1_1 = $mo_2_1 | Add-UcsLsbootSanCatSanImagePath -Lun "1" -Type "primary" -
Wwn "52:4A:93:7A:98:4C:3E:00"
$mo_2_1_2 = $mo_2_1 | Add-UcsLsbootSanCatSanImagePath -Lun "1" -Type "secondary"
-Wwn "52:4A:93:7A:98:4C:3E:10"
$mo_2_2 = $mo_2 | Add-UcsLsbootSanCatSanImage -Type "secondary" -VnicName
"Fabric-B"
$mo_2_2_1 = $mo_2_2 | Add-UcsLsbootSanCatSanImagePath -Lun "1" -Type "primary" -
Wwn "52:4A:93:7A:98:4C:3E:01"
$mo_2_2_2 = $mo_2_2 | Add-UcsLsbootSanCatSanImagePath -Lun "1" -Type "secondary"
-Wwn "52:4A:93:7A:98:4C:3E:11"
$mo_3 = $mo | Add-UcsLsbootVirtualMedia -Access "read-only-remote-cimc" -LunId
"0" -Order 3
Complete-UcsTransaction
```

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Page 79 of 89

Create a Service Profile Template

In this procedure, you create one service profile template for infrastructure ESXi hosts for fabric A boot.

To create the service profile template, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root.
3. Right-click root.
4. Select Create Service Profile Template to open the Create Service Profile Template wizard.
5. Enter **VM-Host-Infra-A** as the name of the service profile template. This service profile template is configured to boot from FlashArray//M controller 1 on fabric A.
6. Select the Updating Template option.
7. Under UUID, select UUID_Pool as the UUID pool.

Create Service Profile Template

You must enter a name for the service profile template and specify the template type. You can also specify how a UUID will be assigned to this template and enter a description.

Name :

The template will be created in the following organization. Its name must be unique within this organization.
Where : **org-root**

The template will be created in the following organization. Its name must be unique within this organization.
Type : ☐ Initial Template ☒ Updating Template

Specify how the UUID will be assigned to the server associated with the service generated by this template.
UUID

UUID Assignment:

The UUID will be assigned from the selected pool.
The available/total UUIDs are displayed after the pool name.

Optionally enter a description for the profile. The description can contain information about when and where the service profile should be used.

< Prev Next > Finish Cancel

8. Click Next.

Configure Storage Provisioning

1. If you have servers with no physical disks, click the Local Disk Configuration Policy tab and select the SAN-Boot Local Storage Policy. Otherwise, select the default Local Storage Policy.

Create Service Profile Template

Optionally specify or create a Storage Profile, and select a local disk configuration policy.

Specific Storage Profile Storage Profile Policy **Local Disk Configuration Policy**

Local Storage: SAN-Boot

Create Local Storage Policy

Select Local Storage Policy to use

- Create a Specific Storage Policy
- Storage Policies
- SAN-Boot**
- default

Mode : **No Local Storage**

Protect Configuration : **Yes**

If **Protect Configuration** is set, the local disk configuration is preserved if the service profile is disassociated with the server. In that case, a configuration error will be raised when a new service profile is associated with that server if the local disk configuration in that profile is different.

FlexFlash : **Disable**

FlexFlash State : **Disable**

If **FlexFlash State** is disabled, SD cards will become unavailable immediately. Please ensure SD cards are not in use before disabling the FlexFlash State.

FlexFlash RAID Reporting State : **Disable**

< Prev Next > **Finish** Cancel

2. Click Next.

Configure Networking Options

1. Keep the default setting for Dynamic vNIC Connection Policy.
2. Select the Use Connectivity Policy option to configure the LAN connectivity.
3. Select Infra-LAN-Policy from the LAN Connectivity Policy pull-down menu.

Create Service Profile Template

Optionally specify LAN configuration information.

Dynamic vNIC Connection Policy: Select a Policy to use (no Dynamic vNIC Policy by default)

[Create Dynamic vNIC Connection Policy](#)

How would you like to configure LAN connectivity?

☐ Simple ☐ Expert ☐ No vNICs ☒ Use Connectivity Policy

LAN Connectivity Policy: <not set> [Create LAN Connectivity Policy](#)

Initiator Name: <not set>

Initiator Name Assignment: Domain Policies

Infra-LAN-Policy

[Create IQN Suffix Pool](#)

WARNING: The selected pool does not contain any available entities. You can select it, but it is recommended that you add entities to it.

[< Prev](#) [Next >](#) [Finish](#) [Cancel](#)

4. Click Next.

Configure Storage Options

1. Select the Use Connectivity Policy option for the “How would you like to configure SAN connectivity?” field.
2. Select the Infra-SAN-Policy option from the SAN Connectivity Policy pull-down menu.

Create Service Profile Template

Optionally specify disk policies and SAN configuration information.

How would you like to configure SAN connectivity?

☐ Simple ☐ Expert ☐ No vHBAs ☒ Use Connectivity Policy

SAN Connectivity Policy: <not set> [Create SAN Connectivity Policy](#)

<not set>

Domain Policies

Infra-SAN-Policy

[< Prev](#) [Next >](#) [Finish](#) [Cancel](#)

3. Click Next.

Configure Zoning Options

1. Do not set any zoning options.
2. Click Next.

Configure vNIC/HBA Placement

1. In the Select Placement list, leave the placement policy set to Let System Perform Placement.
2. Click Next.

Configure vMedia Policy

1. From the vMedia Policy pull-down menu, select ESXi-6.0U2-HTTP.

The screenshot shows the 'Create Service Profile Template' wizard. On the left, a vertical list of steps is shown, with step 7, 'vMedia Policy', highlighted in blue. The main content area is titled 'Create Service Profile Template' and contains a section for 'vMedia Policy'. A dropdown menu is open, showing the following options: 'Select vMedia Policy to use', 'Create a Specific vMedia Policy', 'vMedia Policies', and 'ESXi-6.0U2-HTTP'. The 'ESXi-6.0U2-HTTP' option is highlighted in blue. At the bottom right, there are four buttons: '< Prev', 'Next >', 'Finish' (highlighted in blue), and 'Cancel'.

2. Click Next.

Configure Server Boot Order

1. Select Boot-FC-A for Boot Policy.

Create Service Profile Template

Optionally specify the boot policy for this service profile template.

Select a boot policy.

Boot Policy: **Boot-FC-A** [Create Boot Policy](#)

Name: **Select Boot Policy to use**

Description: **Create a Specific Boot Policy**

Reboot: **Boot Policies**

Enforce: **Boot-FC-A**

Boot Mode: **Boot-FC-no-Media**

WARNING
The type of boot order presence. The effect of the boot order is determined by the device class (LAN/Storage/SCSI) is determined by PCIe bus scan order. If the vNIC/vHBA/SCSI does not exist, a config error will be reported. If they exist, otherwise the vNIC/vHBA with the lowest PCIe bus scan order is used.

Boot Order: **default**

Boot Order: **diag**

Boot Order: **utility**

Name	Order	vNIC/vHBA...	Type	WWN	LUN Name	Slot Num...	Boot Name	Boot Path	Description
Remot...	1								
San	2								
CIMC ...	3								

[Create iSCSI vNIC](#) [Set iSCSI Boot Parameters](#) [Set UEFI Boot Parameters](#)

[< Prev](#) [Next >](#) [Finish](#) [Cancel](#)

2. Click Next to continue to the next section.

Configure Maintenance Policy

1. Change Maintenance Policy to default.

Create Service Profile Template

Specify how disruptive changes such as reboots, network interruptions, and firmware upgrades should be applied to the server associated with this service profile.

Maintenance Policy

Select a maintenance policy to include with this service profile or create a new maintenance policy that will be accessible to all service profiles.

Maintenance Policy: **Select (no policy used by default)** [Create Maintenance Policy](#)

Name: **Select (no policy used by default)**

Description: **Domain Policies**

default

No maintenance policy is selected by default. The service profile will immediately reboot when disruptive changes are applied.

Name	Order	vNIC/vHBA...	Type	WWN	LUN Name	Slot Num...	Boot Name	Boot Path	Description
------	-------	--------------	------	-----	----------	-------------	-----------	-----------	-------------

[< Prev](#) [Next >](#) [Finish](#) [Cancel](#)

2. Click Next.

Configure Server Assignment

1. In the Pool Assignment list, select Infra_Pool.
2. Optional: Select a server pool qualification policy.
3. Select Down as the power state to be applied when the profile is associated with the server.
4. Select UCS-Broadwell for Server Pool Qualification.
5. Leave the Firmware Management setting at the bottom of the page as is. The default setting from the Host Firmware list will be used.

Create Service Profile Template

Optionally specify a server pool for this service profile template.

You can select a server pool you want to associate with this service profile template.

Pool Assignment: **Infra_Pool** [Create Server Pool](#)

Select the power state to be applied when this profile is associated with the server.

☒ Up ☐ Down

The service profile template will be associated with one of the servers in the selected pool. If desired, you can specify an additional server pool policy qualification that the selected server must meet. To do so, select the qualification from the list.

Server Pool Qualification: **<not set>**

Restrict Migration: **<not set>**

Server Pool Qualification Dropdown:

- Domain Policies
- UCS-Broadwell**
- all-chassis

Firmware Management (Server, Adapter)

[< Prev](#) [Next >](#) [Finish](#) [Cancel](#)

6. Click Next.

Configure Operational Policies

1. In the BIOS Policy list, select VM-Host-Infra.
2. Expand Power Control Policy Configuration and select No-Power-Cap in the Power Control Policy list.

Complete the Template

1. Click Finish to create the service profile template.
2. Click OK in the confirmation message.

PowerTool cmdlet Steps: Create a Service Profile Template

```
Start-UcsTransaction

$mo = Get-UcsOrg -Level root | Add-UcsServiceProfile -BiosProfileName "VM-Host-Infra" -BootPolicyName "Boot-FC-A" -IdentPoolName "UUID_Pool" -LocalDiskPolicyName "SAN-Boot" -MaintPolicyName "default" -Name "VM-Host-Infra-A" -PowerPolicyName "No-Power-Cap" -Type "updating-template" -VmediaPolicyName "ESXi-6.0U2-HTTP"

$mo_1 = $mo | Add-UcsVnicConnDef -ModifyPresent -LanConnPolicyName "Infra-LAN-Policy" -SanConnPolicyName "Infra-SAN-Policy"

$mo_2 = $mo | Add-UcsVnic -AdaptorProfileName "" -Addr "derived" -AdminCdnName "" -AdminHostPort "ANY" -AdminVcon "any" -CdnPropInSync "yes" -CdnSource "vnic-name" -IdentPoolName "" -Mtu 1500 -Name "03-vMotion-B" -NwCtrlPolicyName "" -NwTemplateName "" -Order "4" -PinToGroupName "" -QosPolicyName "" -StatsPolicyName "default" -SwitchId "A"

$mo_3 = $mo | Add-UcsVnic -AdaptorProfileName "" -Addr "derived" -AdminCdnName "" -AdminHostPort "ANY" -AdminVcon "any" -CdnPropInSync "yes" -CdnSource "vnic-name" -IdentPoolName "" -Mtu 1500 -Name "02-vMotion-A" -NwCtrlPolicyName "" -NwTemplateName "" -Order "3" -PinToGroupName "" -QosPolicyName "" -StatsPolicyName "default" -SwitchId "A"

$mo_4 = $mo | Add-UcsVnic -AdaptorProfileName "" -Addr "derived" -AdminCdnName "" -AdminHostPort "ANY" -AdminVcon "any" -CdnPropInSync "yes" -CdnSource "vnic-name" -IdentPoolName "" -Mtu 1500 -Name "01-Mgmt-B" -NwCtrlPolicyName "" -NwTemplateName ""
```

```

"" -Order "2" -PinToGroupName "" -QosPolicyName "" -StatsPolicyName "default" -
SwitchId "A"

$mo_5 = $mo | Add-UcsVnic -AdaptorProfileName "" -Addr "derived" -AdminCdnName ""
-AdminHostPort "ANY" -AdminVcon "any" -CdnPropInSync "yes" -CdnSource "vnic-name"
-IdentPoolName "" -Mtu 1500 -Name "00-Mgmt-A" -NwCtrlPolicyName "" -NwTemplName
"" -Order "1" -PinToGroupName "" -QosPolicyName "" -StatsPolicyName "default" -
SwitchId "A"

$mo_6 = $mo | Add-UcsVnic -AdaptorProfileName "" -Addr "derived" -AdminCdnName ""
-AdminHostPort "ANY" -AdminVcon "any" -CdnPropInSync "yes" -CdnSource "vnic-name"
-IdentPoolName "" -Mtu 1500 -Name "05-App-B" -NwCtrlPolicyName "" -NwTemplName ""
-Order "6" -PinToGroupName "" -QosPolicyName "" -StatsPolicyName "default" -
SwitchId "A"

$mo_7 = $mo | Add-UcsVnic -AdaptorProfileName "" -Addr "derived" -AdminCdnName ""
-AdminHostPort "ANY" -AdminVcon "any" -CdnPropInSync "yes" -CdnSource "vnic-name"
-IdentPoolName "" -Mtu 1500 -Name "04-App-A" -NwCtrlPolicyName "" -NwTemplName ""
-Order "5" -PinToGroupName "" -QosPolicyName "" -StatsPolicyName "default" -
SwitchId "A"

$mo_8 = $mo | Add-UcsVnicFcNode -ModifyPresent -Addr "pool-derived" -
IdentPoolName "node-default"

$mo_9 = $mo | Add-UcsVhba -AdaptorProfileName "" -Addr "derived" -AdminCdnName ""
-AdminHostPort "ANY" -AdminVcon "any" -CdnPropInSync "yes" -CdnSource "vnic-name"
-IdentPoolName "" -MaxDataFieldSize 2048 -Name "Fabric-A" -NwTemplName "" -Order
"7" -PersBind "disabled" -PersBindClear "no" -PinToGroupName "" -QosPolicyName ""
-StatsPolicyName "default" -SwitchId "A"

$mo_10 = $mo | Add-UcsVhba -AdaptorProfileName "" -Addr "derived" -AdminCdnName
"" -AdminHostPort "ANY" -AdminVcon "any" -CdnPropInSync "yes" -CdnSource "vnic-
name" -IdentPoolName "" -MaxDataFieldSize 2048 -Name "Fabric-B" -NwTemplName "" -
Order "8" -PersBind "disabled" -PersBindClear "no" -PinToGroupName "" -
QosPolicyName "" -StatsPolicyName "default" -SwitchId "A"

$mo_11 = $mo | Add-UcsFabricVCon -ModifyPresent -Fabric "NONE" -Id "1" -InstType
"auto" -Placement "physical" -Select "all" -Share "shared" -Transport
"ethernet","fc"

$mo_12 = $mo | Add-UcsFabricVCon -ModifyPresent -Fabric "NONE" -Id "2" -InstType
"auto" -Placement "physical" -Select "all" -Share "shared" -Transport
"ethernet","fc"

$mo_13 = $mo | Add-UcsFabricVCon -ModifyPresent -Fabric "NONE" -Id "3" -InstType
"auto" -Placement "physical" -Select "all" -Share "shared" -Transport
"ethernet","fc"

$mo_14 = $mo | Add-UcsFabricVCon -ModifyPresent -Fabric "NONE" -Id "4" -InstType
"auto" -Placement "physical" -Select "all" -Share "shared" -Transport
"ethernet","fc"

$mo_15 = $mo | Set-UcsServerPower -State "admin-up"

$mo_16 = $mo | Add-UcsServerPoolAssignment -ModifyPresent -Name "Infra_Pool" -
Qualifier "UCS-Broadwell" -RestrictMigration "no"

Complete-UcsTransaction

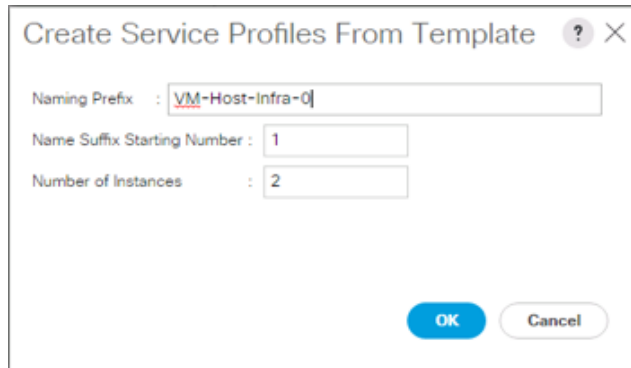
```

Create Service Profiles

To create service profiles from the service profile template, complete the following steps:

1. Connect to the Cisco UCS 6332-16UP Fabric Interconnect through Cisco UCS Manager and click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root > Service Template VM-Host-Prod-Fabric-A.
3. Right-click VM-Host-Infra-Fabric-A and select Create Service Profiles from Template.
4. Enter **VM-Host-Infra-0** as the service profile prefix.

5. Leave Name Suffix Starting Number set to 1.
6. Leave Number of Instances set to 2.
7. Click OK to create the service profiles.



8. Click OK in the confirmation message to provision two FlashStack service profiles.

PowerTool cmdlet Steps: Create Service Profiles

```
Get-UcsOrg -Level root | Get-UcsServiceProfile -Name "VM-Host-Infra-A" -LimitScope | Add-  
UcsServiceProfileFromTemplate -NewName @("VM-Host-Infra-01","VM-Host-Infra-02") -  
DestinationOrg "org-root"
```

Conclusion

Cisco UCS PowerTool cmdlets provide powerful options for configuring and implementing Cisco UCS using the XML API that Cisco UCS has incorporated from its creation. By using the PowerTool cmdlets, you can configure the Cisco UCS solution for FlashStack VSI much more quickly than with the Cisco UCS Manager GUI. You can also quickly find PowerTool cmdlet syntax by interacting with the GUI.

For More Information

For additional information, see the following:

- FlashStack Virtual Server Infrastructure Design Guide for VMware vSphere 6.0 U2:
http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/ucs_flashstack_vsi_vm6_designs.html
- FlashStack Virtual Server Infrastructure Deployment Guide for VMware vSphere 6.0 U2:
http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/ucs_flashstack_vsi_vm6.html
- Cisco UCS Manager: <http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-manager/index.html>
- Cisco UCS PowerTool documentation:
http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/msft_tools/powertools/ucs_powertool_book/2x/b_Cisco_UCSM_PowerTool_UG_Release_2x/b_Cisco_UCSM_PowerTool_UG_Release_2x_chapter_0_0.html
- Cisco UCS PowerTool download:
<https://software.cisco.com/download/release.html?i=y&mdfid=286305108&softwareid=284574017&release=2.1.1>



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA

C11-738575-00 02/17