



Cisco Learning Product

Data Center Unified Computing Implementation

Version 4.0

<https://t.me/learningnets>

Data Center Unified Computing Implementation

Version 4.0

Lab Guide

Text Part Number: 97-3023-01



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 of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED "AS IS." CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.

Table of Contents

Lab Guide	1
Overview	1
Outline	1
Lab 1-0: Access the Lab Equipment	2
Activity Objective	2
Visual Objective	2
Required Resources	2
Lab 1-0 Resource Sheet	2
Task 1: Install the Cisco AnyConnect SSL VPN Client	3
Task 2: Connect to Your Student PC Desktop	4
Lab 3-1: Initial Cisco UCS C-Series Configuration	5
Activity Objective	5
Visual Objective	5
Required Resources	5
Lab 3-1 Initial C-Series Configuration Sheet	6
Lab 3-1 Initial C-Series Configuration Sheet (Cont.)	7
Task 1: Validate Cisco IMC BIOS Configuration	7
Task 2: Configure IPMI and SoL	10
Task 3: Use IPMITool to Access Cisco IMC Data	11
Task 4: Configure Cisco UCS C-Series BIOS for Performance and Virtualization	11
Task 5: Configure vNICs for the P81E VIC	12
Task 6: Assign WWNs to the P81E VIC	15
Task 7: Configure a Fibre Channel Boot Target	16
Task 8: Install VMware ESXi 4.1 on Fibre Channel LUN	17
Task 9: Back Up and Restore the P81E Configuration	22
Lab 5-1: Configure LAN and SAN Physical Connections	25
Activity Objective	25
Visual Objective	25
Required Resources	25
Lab 5-1 Cisco UCS Connectivity Sheet	26
Task 1: Validate VLAN Assignments	28
Task 2: Validate VSAN Assignments	29
Task 3: Validate Physical Connections from IOMs to Fabric Interconnects	29
Task 4: Validate Physical SAN Connectivity from the Fabric Interconnects to the MDS Switches	30
Task 5: Validate Physical Connections from Fabric Interconnects to the Northbound L3 Switch	32
Task 6: Validate that the Northbound L3 Switch Is Trunking All Required VLANs	33
Lab 6-1: Configure Identity and Resource Pools	34
Activity Objective	34
Visual Objective	34
Required Resources	34
Lab 6-1 Identity and Resource Pools Implementation Sheet	35
Lab 6-1 Identity and Resource Pools Implementation Sheet (Cont.)	36
Lab 6-1 Identity and Resource Pools Implementation Sheet (Cont.)	37
Task 1: Configure Pod-Specific VLANs	37
Task 2: Configure UUID Prefix and Suffix Pools	38
Task 3: Configure MAC Pools	40
Task 4: Configure WWNN Pools	42
Task 5: Configure WWPN Pools	44
Task 6: Configure Server Pool Qualification Policy	46
Task 7: Validate QoS, Configure Adapter, Scrub, and QoS Policies	50

Lab 6-2: Create Mobile Service Profiles from Updating Templates	53
Activity Objective	53
Visual Objective	53
Required Resources	53
Lab 6-2 Mobile Service Profiles Implementation Sheet	54
Task 1: Create vNIC and vHBA Templates for Your Organization	55
Task 2: Create a Service Profile Template for Your Organization	57
Task 3: Create a Service Profile from the Updating Template	62
Task 4: Add IPMI Policy to Updating Template	63
Task 5: Install VMware ESXi 4.1 on Fibre Channel LUN	66
Lab 7-1: Create a Data-Center Cluster in VMware vCenter	70
Activity Objective	70
Visual Objective	70
Required Resources	70
Lab 7-1: Create a Data-Center Cluster in VMware vCenter Implementation Sheet	71
Task 1: Import the vCenter VM	72
Task 2: Add Port Profile for vCenter Networking and Attach to vCenter	73
Task 3: Start the vCenter VM and Validate Services	74
Task 4: Create a New Data Center and Add ESXi Hosts and VMs	75
Task 5: Configure vSwitch and Test vMotion	77
Lab 7-2: Install a Cisco Nexus 1000V VSM	80
Activity Objective	80
Visual Objective	80
Required Resources	80
Lab 7-2 Implementation Sheet	81
Task 1: Configure vSwitch with Control, Packet, and Management VLANs	82
Task 2: Deploy VSM from .ova File	83
Task 3: Configure the Primary VSM	84
Lab 7-3: Configure Port Profiles	87
Activity Objective	87
Visual Objective	87
Required Resources	87
Task 1: Configure VLANs and Uplink Port Profile in the VSM	88
Task 2: Configure Control, Management, and Packet vEthernet Port Profiles	89
Task 3: Configure vMotion, vmTraffic vEthernet Port Profiles	90
Task 4: Add ESXi Hosts to the DVS	91
Task 5: Migrate Windows 2008 VM from vSwitch to DVS	93
Task 6: Create an ACL Port Profile	93
Lab 8-1: Configure RBAC	95
Activity Objective	95
Visual Objective	95
Required Resources	95
Lab 8-1 Cisco UCS RBAC Implementation Sheet	96
Lab 8-1 Cisco UCS RBAC Implementation Sheet (Cont.)	97
Lab 8-1 Cisco UCS RBAC Implementation Sheet (Cont.)	98
Task 1: Create Locales for Your Pod	99
Task 2: Create Custom Roles to Apply to Pod Users	100
Task 3: Create Local User Accounts	101
Task 4: Test Locale Restrictions	103
Task 5: Define Global LDAP Properties (for Active Directory)	104
Task 6: Define an LDAP Server (for Active Directory)	105
Task 7: Test LDAP Authentication and Role Mapping	106

Lab 8-2: Back up and Import Cisco UCS Manager Configuration Data	108
Activity Objective	108
Visual Objective	108
Required Resources	108
Lab 8-2 Cisco UCS Backup-Import Implementation Sheet	109
Task 1: Create Pod-Specific Firmware Packages	110
Task 2: Create and Execute an All-Configuration Backup	112
Task 3: Delete a Firmware Policy and Restore with an Import Job	114
Task 4: Demonstrate Using an Import Job with the Replace Action	116
Lab 8-3: Reporting in the Cisco Unified Computing System	119
Activity Objective	119
Visual Objective	119
Required Resources	119
Lab 8-3 Cisco Unified Computing System Reporting Implementation Sheet	120
Task 1: Generate and Observe Major Alarms and Recovery	121
Task 2: Disable Local Console Logging	122
Task 3: Configure Syslog	123
Task 4: Configure Smart Call Home	124
Task 5: Configure and Test SNMPv3	132
Lab A-1: Initial Cisco UCS B-Series Configuration	136
Activity Objective	136
Visual Objective	136
Task 1: Complete Cisco UCS 6100 Initial Configuration	136
Task 2: Configure Server Ports to Allow Chassis Discovery	140
Task 3: Configure Uplink Ports to Northbound Communications	143
Task 4: Configure IP Communication to Cisco IMC	146
Lab Reference Guide	148

Lab Guide

Overview

This guide presents instructions and other information concerning the lab activities for this course.

Outline

This guide includes these activities:

- Lab 1-0: Access the Lab Equipment
- Lab 3-1: Initial Cisco UCS C-Series Configuration
- Lab 5-1: Configure LAN and SAN Physical Connections
- Lab 6-1: Configure Identity and Resource Pools
- Lab 6-2: Create Mobile Service Profiles from Updating Templates
- Lab 7-1: Create a Data-Center Cluster in VMware Center
- Lab 7-2: Install a Cisco Nexus 1000V VSM
- Lab 7-3: Configure Port Profiles
- Lab 8-1: Configure RBAC
- Lab 8-2: Back up and Import Cisco UCS Manager Configuration Data
- Lab 8-3: Reporting in the Cisco Unified Computing System
- Lab A-1: Initial Cisco UCS B-Series Configuration
- Lab Reference Guide

Lab 1-0: Access the Lab Equipment

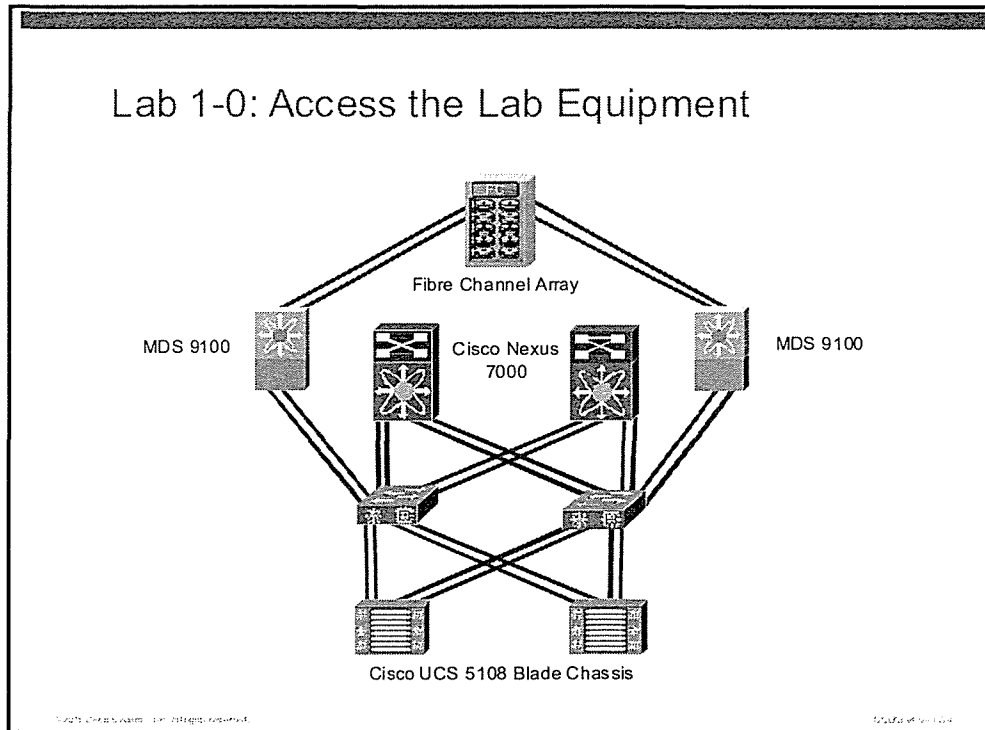
Complete this lab activity to practice what you learned in the related lesson.

Activity Objective

In this activity, you will learn the lab topology and the method to access lab equipment remotely.

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required to complete this activity:

- Student PC
- Lab resource sheet

Lab 1-0 Resource Sheet

The purpose of this document is to provide login credentials to access the remote lab components.

Task 1 AnyConnect Logins

Pod	Username	Password
1	dcdevpod1	devfeb211
2	dcdevpod2	devfeb212
3	dcdevpod3	devfeb213
4	dcdevpod4	devfeb214
5	dcdevpod5	devfeb215
6	dcdevpod6	devfeb216

Task 2 Student PC Logins

Pod	RDP Desktop	Username	Password
1	192.168.70.41	administrator	cisco123
2	192.168.70.42	administrator	cisco123
3	192.168.70.43	administrator	cisco123
4	192.168.70.44	administrator	cisco123
5	192.168.70.45	administrator	cisco123
6	192.168.70.46	administrator	cisco123

Task 1: Install the Cisco AnyConnect SSL VPN Client

In this task, you will install the SSL VPN Client that is necessary to connect to the remote lab environment.

Activity Procedure

Complete these steps:

- Step 1** Open a web browser and connect to <https://64.100.8.195/dcdev>.
- Step 2** At the DCDEV SSL VPN Portal, enter the username and password that are assigned to your pod.
- Step 3** At the Welcome screen, click the **Continue** button to accept the ASE SSL VPN User License Agreement.
- Step 4** From the DCDEV SSL VPN Portal homepage, click the **Start AnyConnect** link.
- Step 5** Click **Yes** on all security warning dialog boxes.
- Step 6** Answer **Yes** to the User Account Control dialog box that asks whether you want to install an application from an untrusted source.
- Step 7** You should be automatically connected with AnyConnect. If the AnyConnect installation fails, contact your instructor.

Task 2: Connect to Your Student PC Desktop

In this task, you will use Microsoft RDP to connect to your pod student PC.

Activity Procedure

Complete these steps:

- Step 1** From the classroom computer, launch the RDP client and connect to the pod-specific IP address that you recorded on the Lab Resource Sheet.
- Step 2** Log in by using the credentials on the Resource Sheet. Contact your instructor if you have difficulty logging in.

Activity Verification

You have completed this activity when you have achieved these goals:

- You have installed the Cisco AnyConnect SSL VPN Client and connected to the remote lab environment.
- You have made a successful connection to your student desktop.

Lab 3-1: Initial Cisco UCS C-Series Configuration

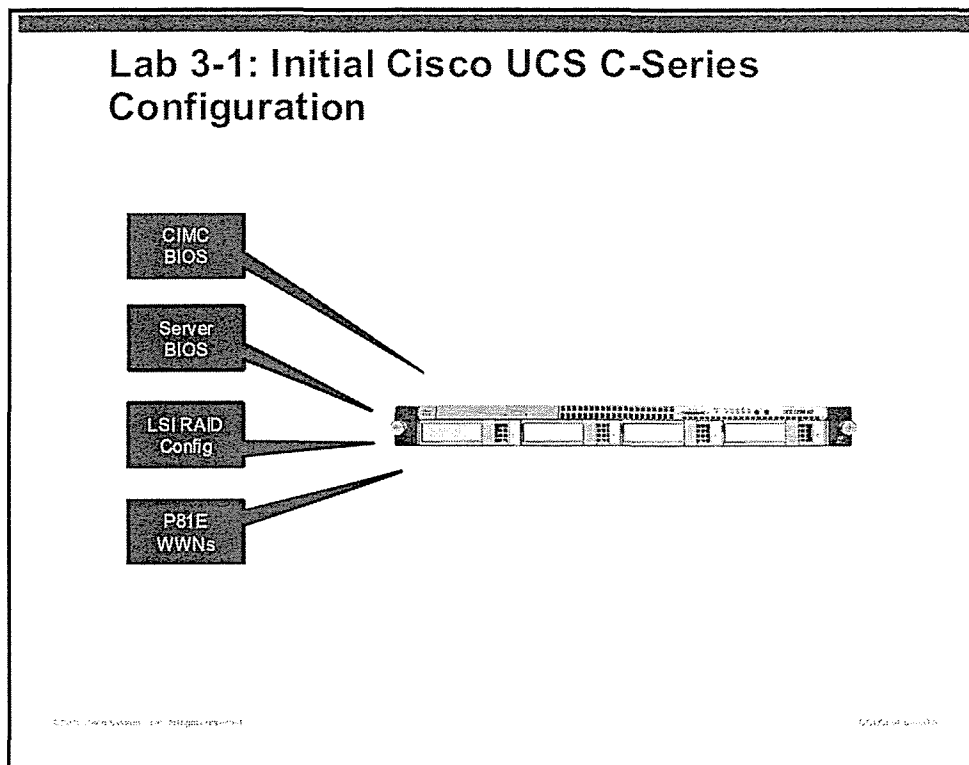
Complete this lab activity to practice what you learned in the related lesson.

Activity Objective

In this activity, you will perform initial configuration of the Cisco UCS C Series, including Cisco IMC, IPMI, and SoL. You will also install and boot VMware ESXi from SAN and create a RAID array with local disks.

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required to complete this activity:

- Student PC
- Lab reference guide

Lab 3-1 Initial C-Series Configuration Sheet

The purpose of this document is to provide implementers with the data necessary to address the P81E VIC for LAN and SAN communication.

C-Series MAC, WWNN, and WWPN Addresses

Pod	MAC Address	WWNN	WWPN
1	00:25:B5:30:00:00	20:00:00:25:B5:30:30:01	20:00:00:25:B5:40:40:00
	00:25:B5:30:00:01		20:00:00:25:B5:40:40:01
2	00:25:B5:30:00:02	20:00:00:25:B5:30:30:02	20:00:00:25:B5:40:40:02
	00:25:B5:30:00:03		20:00:00:25:B5:40:40:03
3	00:25:B5:30:00:04	20:00:00:25:B5:30:30:03	20:00:00:25:B5:40:40:04
	00:25:B5:30:00:05		20:00:00:25:B5:40:40:05
4	00:25:B5:30:00:06	20:00:00:25:B5:30:30:04	20:00:00:25:B5:40:40:06
	00:25:B5:30:00:07		20:00:00:25:B5:40:40:07
5	00:25:B5:30:00:08	20:00:00:25:B5:30:30:05	20:00:00:25:B5:40:40:08
	00:25:B5:30:00:09		20:00:00:25:B5:40:40:09
6	00:25:B5:30:00:0A	20:00:00:25:B5:30:30:06	20:00:00:25:B5:40:40:0A
	00:25:B5:30:00:0B		20:00:00:25:B5:40:40:0B

C-Series Boot Target Addresses

Pod	FC Int.	Boot Target WWPN	LUN
1	fc0	50:06:01:60:3b:a0:07:c9	0
	fc1	50:06:01:68:3b:a0:07:c9	0
2	fc0	50:06:01:60:3b:a0:07:c9	0
	fc1	50:06:01:68:3b:a0:07:c9	0
3	fc0	50:06:01:60:3b:a0:07:c9	0
	fc1	50:06:01:68:3b:a0:07:c9	0
4	fc0	50:06:01:60:3b:a0:08:ed	0
	fc1	50:06:01:68:3b:a0:08:ed	0
5	fc0	50:06:01:60:3b:a0:08:ed	0
	fc1	50:06:01:68:3b:a0:08:ed	0
6	fc0	50:06:01:60:3b:a0:08:ed	0
	fc1	50:06:01:68:3b:a0:08:ed	0

Lab 3-1 Initial C-Series Configuration Sheet (Cont.)

VSANs

vHBA Name	VSAN Number	Default VLAN (FCoE VLAN)
fc0	11	1011
fc1	12	1012

VMware ESXi Configuration

Pod	Hostname	IP Address/Mask	Gateway	VLAN
1	p1-c-esx-dc	192.168.110.41 /24	192.168.110.1	110
2	p2-c-esx-dc	192.168.110.42 /24	192.168.110.1	110
3	p3-c-esx-dc	192.168.110.43 /24	192.168.110.1	110
4	p4-c-esx-dc	192.168.110.44 /24	192.168.110.1	110
5	p5-c-esx-dc	192.168.110.45 /24	192.168.110.1	110
6	p6-c-esx-dc	192.168.110.46 /24	192.168.110.1	110

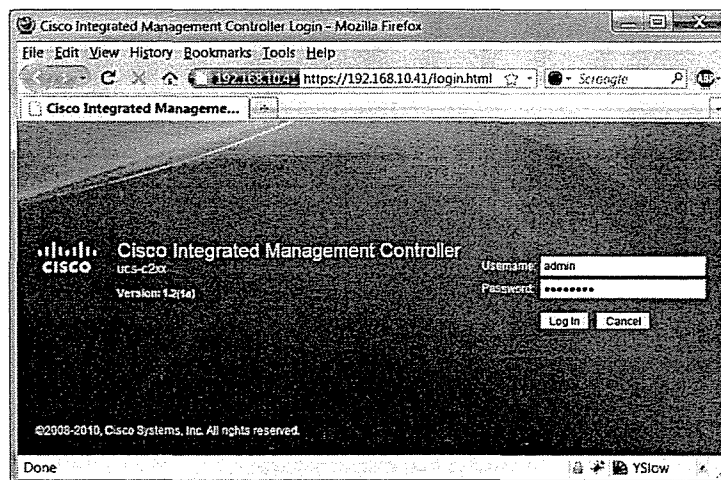
Task 1: Validate Cisco IMC BIOS Configuration

In this task, you will use the KVM console to enter the Cisco IMC BIOS and validate the configuration.

Activity Procedure

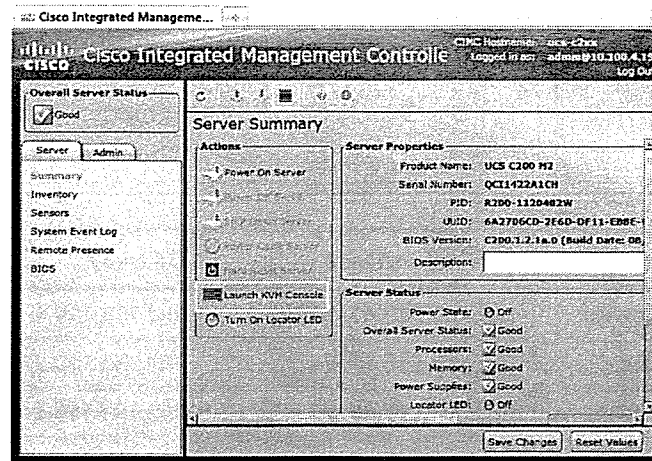
Complete these steps:

- Step 1** Browse to the Cisco IMC IP address of the C200 in your pod.
`http://192.168.10.4P` (where “P” is your pod number)
- Step 2** Log in to the Cisco IMC by using the credentials admin and NXos12345.



Step 3 From the summary page, click the **Launch KVM Console** link or the small **keyboard** icon directly above the words Server Summary.

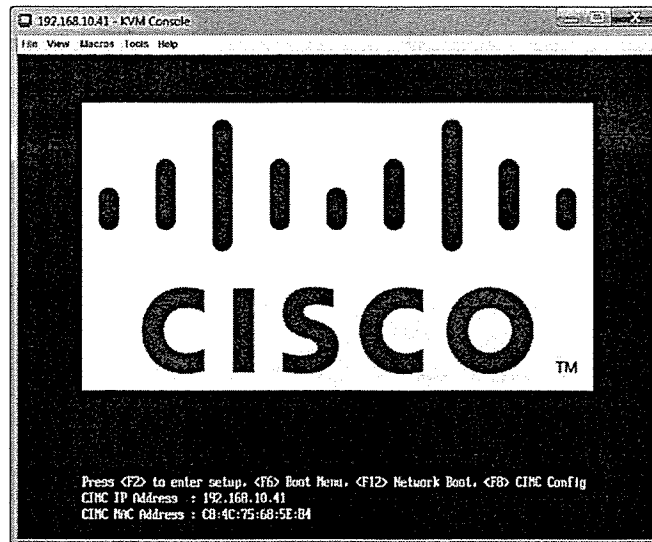
Note The advantage of the small keyboard icon is that it is visible from any screen in the Cisco Integrated Management Controller interface.



Step 4 Click **OK** to open the Java VM that the KVM runs inside. You should see a green background with a No Signal indication in yellow text. This indication displays when the server is powered down. If you see anything other than No Signal, click the **Power Off Server** link in the Actions area above the Launch KVM Console link.

Step 5 From the Cisco Integrated Management Controller summary screen, click the **Power On Server** link in the Actions area of the screen. Click **OK** when prompted to confirm powering on the server. Switch to the KVM console window and observe the server booting.

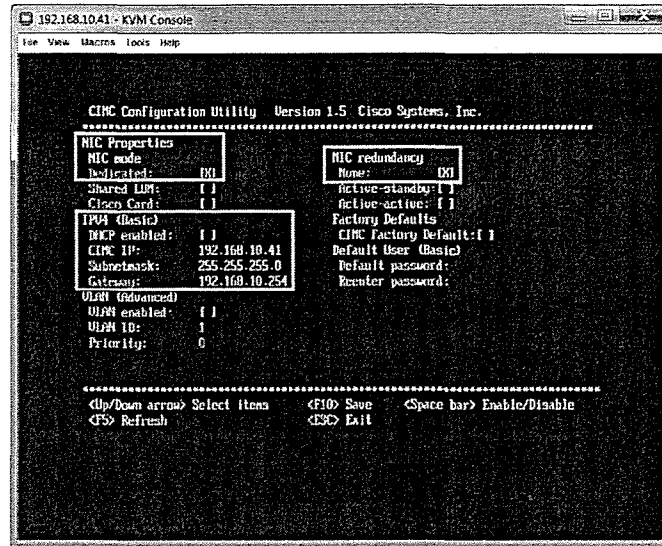
Step 6 When the Cisco BIOS banner appears, press **F8** to enter the Cisco IMC BIOS configuration.



Step 7 Validate the following settings:

- NIC mode is set to Dedicated.
- DHCP is disabled (unchecked).

- The IP address, subnet mask, and gateway match the lab reference guide for your pod.



Note Do not make any changes to the Cisco IMC BIOS settings.

Note To configure the Cisco IMC BIOS on a new, unconfigured server, you must plug a USB keyboard and VGA monitor directly into either the rear panel connectors or the front panel dongle.

Step 8 Press **ESC** to exit the Cisco IMC BIOS. Because there is no boot drive, click the **Power Off Server** link from the Cisco Integrated Management Controller window.

Task 2: Configure IPMI and SoL

In this task, you will use the Cisco IMC to configure IPMI and SoL.

Activity Procedure

Complete these steps:

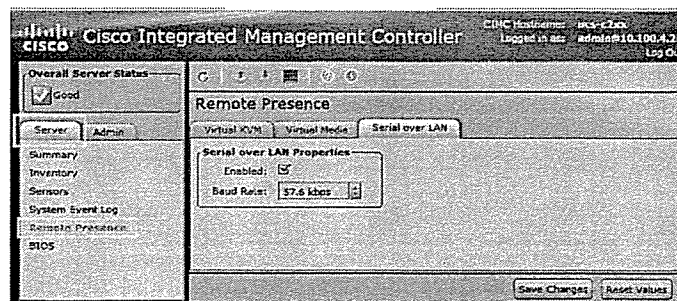
- Step 1** From the Admin tab of the Cisco Integrated Management Controller window, click the **Communications Services** link.



- Step 2** Validate that IPMI services are enabled. Most IPMI tools include the ability to encrypt IPMI management traffic. The value of the Encryption Key field must match the value that is used in your IPMI tool.

Note IPMI is enabled by default with Admin privileges and no encryption. Refer to the security policy of your organization for guidance on whether the IPMI setting should be changed or disabled altogether.

- Step 3** From the Server tab of Cisco Integrated Management Controller window, click the **Remote Presence** link.



- Step 4** In the content pane, click the **Serial over LAN** tab.
- Step 5** Check the **Enabled** check box to enable SoL.
- Step 6** Choose the serial b/s rate of the connection by using the drop-down menu.
- Step 7** Click **Save Changes**.

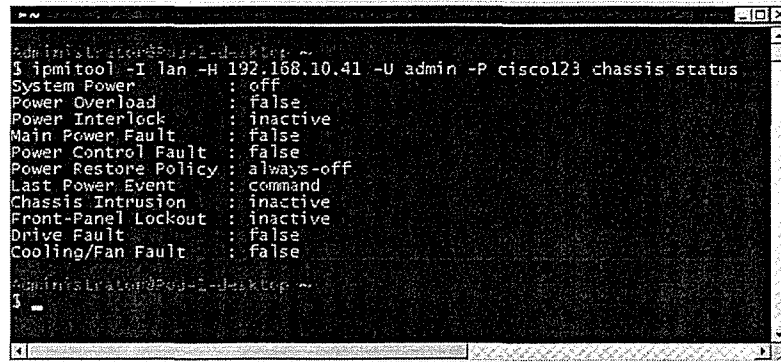
Task 3: Use IPMItool to Access Cisco IMC Data

In this task, you will use IPMItool to poll data from the Cisco IMC.

Activity Procedure

Complete these steps:

- Step 1 Log in to your pod Student PC and double-click the Cygwin application on the desktop. Cygwin allows UNIX and Linux applications to run under Windows.
- Step 2 Enter the `ipmitool -I lan -H 192.168.10.4P -U admin -P NXos12345 chassis status` command.



```
Admin@SLVatm3Pod1-Desktop ~$ ipmitool -I lan -H 192.168.10.41 -U admin -P cisco123 chassis status
System Power           : off
Power Overload          : false
Power Interlock         : inactive
Main Power Fault        : false
Power Control Fault     : false
Power Restore Policy    : always-off
Last Power Event        : command
Chassis Intrusion       : inactive
Front-Panel Lockout     : inactive
Drive Fault             : false
Cooling/Fan Fault       : false

Admin@SLVatm3Pod1-Desktop ~$
```

Task 4: Configure Cisco UCS C-Series BIOS for Performance and Virtualization

In this task, you will configure C200 BIOS settings that will increase performance for VMware ESXi.

Activity Procedure

Complete these steps:

- Step 1 Minimize your student PC window and open the Cisco Integrated Management Controller window. If you closed that window earlier, you will need to log back in.
- Step 2 Open a remote KVM console session to your server. If you performed Step 8 in Task 1, you should see a green screen indicating that the server is powered off.
- Step 3 From the Server tab of the navigation pane, make certain that the current context is the Summary. Click the **Power On Server** link.
- Step 4 When the Cisco BIOS screen appears, press **F2** to enter BIOS setup.
- Step 5 Use the right-arrow key on the keyboard to move from the **Main** tab to the **Advanced** tab in BIOS setup.
- Step 6 Use the down-arrow key to choose **Processor Configuration**, then press **Enter**.

- Step 7** Validate that all of the processor options except for Processor C3 and Coherency Support are enabled. If a value needs to be changed, press **Enter** and use the up- or down-arrow keys to make a selection. Press **Enter** to commit the value.

Current Intel(R) QPI Link Speed	Fast
Intel(R) QPI Link Frequency	4.8 GT/s
Enhanced Intel SpeedStep(R) Tech	[Enabled]
Processor C3	[Disabled]
Processor C6	[Enabled]
Number of Enabled Cores	[All]
Execute Disable Bit	[Enabled]
Intel(R) Virtualization Technology	[Enabled]
Intel(R) VT for Directed I/O	[Enabled]
Interrupt Remapping	[Enabled]
Coherency Support	[Disabled]
ATS Support	[Enabled]
Pass-through DMA Support	[Enabled]
Direct Cache Access (DCA)	[Enabled]

- Step 8** Press **ESC** to return to the **Advanced** tab.
- Step 9** Use the right-arrow key to choose the **Boot Options** tab and press **Enter**.
- Step 10** If you made changes to any of the BIOS settings, press **F10** to save and exit.
- Step 11** From the Cisco IMC, power down the server.

Task 5: Configure vNICs for the P81E VIC

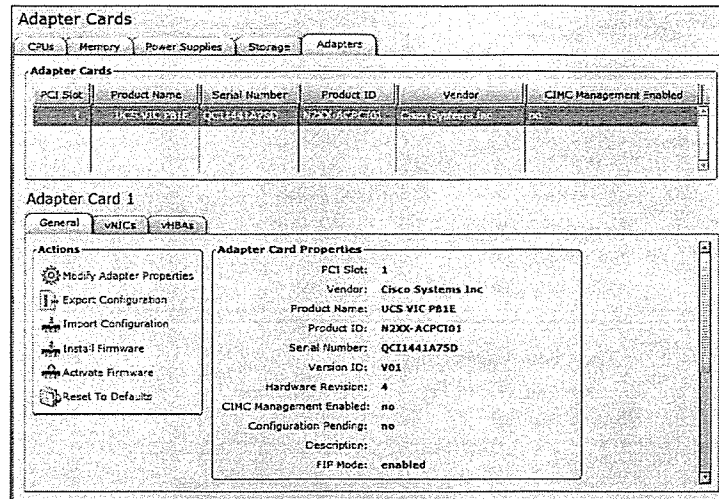
In this task, you will create vNIC definitions for the P81E VIC.

Activity Procedure

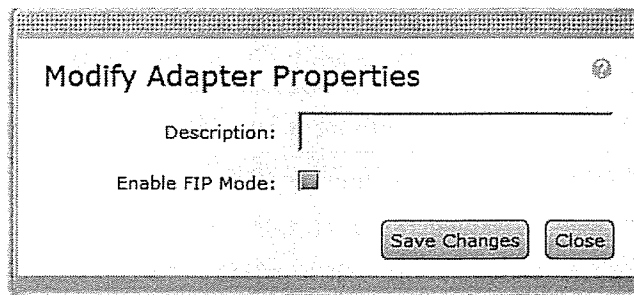
Complete these steps:

- Step 1** Minimize your student PC window and open the Cisco Integrated Management Controller window.
- Step 2** Power on the server. If the server is powered down, you will not be able to configure the P81E VIC.
- Step 3** From the Server tab in the navigation pane, click the **Inventory** link.
- Step 4** In the content pane, choose the **Adapters** tab.

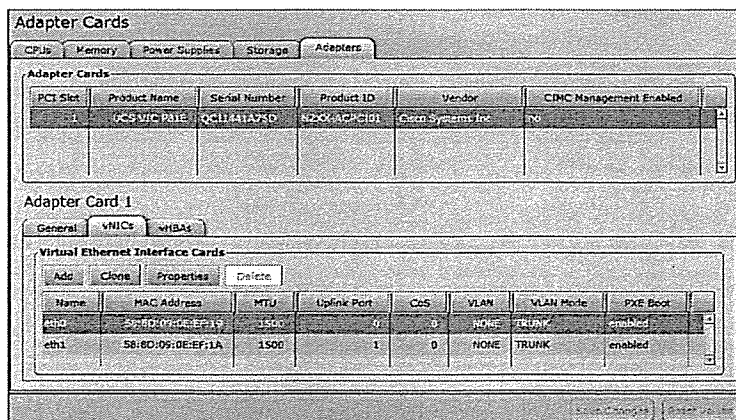
- Step 5** The General subtab displays information about installed NICs. It also displays part numbers and administrative status of the installed network adapters.



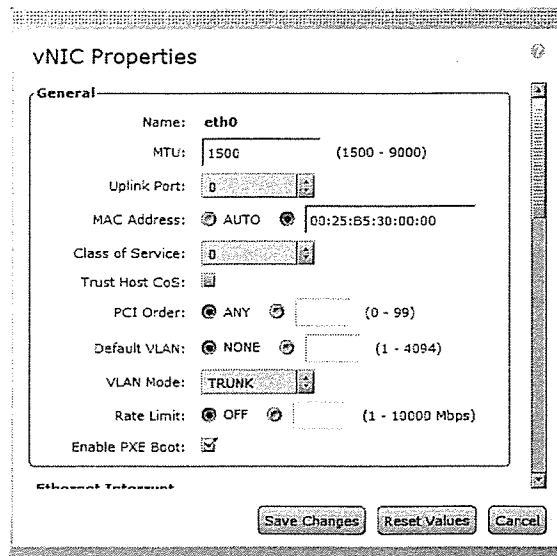
- Step 6** In the Actions panel under the General tab, click the **Modify Adapter Properties** link. Uncheck the **Enable FIP Mode** check box and then click the **Save Changes** button.



- Step 7** Click the vNICs subtab and choose **eth0**, and then click **Properties** to configure the adapter.



Step 8 Use the lab configuration sheet to add your pod-specific MAC address.



The image shows the 'vNIC Properties' dialog box for the 'eth0' interface. The 'General' tab is selected. The 'Name' is 'eth0'. The 'MTU' is set to '1500' (range 1500 - 9000). The 'Uplink Port' is '0'. The 'MAC Address' is set to '00:25:B5:30:00:00' (with 'AUTO' selected). The 'Class of Service' is '0'. The 'Trust Host CoS' checkbox is unchecked. The 'PCI Order' is 'ANY' (range 0 - 99). The 'Default VLAN' is 'NONE' (range 1 - 4094). The 'VLAN Mode' is 'TRUNK'. The 'Rate Limit' is 'OFF' (range 1 - 10000 Mbps). The 'Enable PXE Boot' checkbox is checked. At the bottom, there are three buttons: 'Save Changes', 'Reset Values', and 'Cancel'.

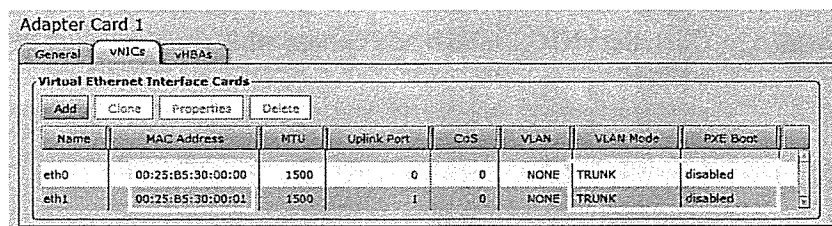
Step 9 The example that is shown illustrates changing the MAC address for eth0 on pod 1. Be certain to use your pod-specific MAC addresses that was assigned on the lab configuration sheet.

Step 10 Validate that **VLAN Mode** is set to Trunk, and disable **Enable PXE Boot** by unchecking the check box. The other default settings should be changed only to align with IT policy or to meet operating system-specific requirements.

Step 11 Click **Save Changes** to commit the changes.

Step 12 Repeat Steps 6 through 9 on interface **eth1**.

Step 13 Validate the changes in the vNICs section of the content pane.



The image shows the 'Adapter Card 1' configuration window, specifically the 'vNICs' tab. It displays a table of 'Virtual Ethernet Interface Cards'. The table has columns for Name, MAC Address, MTU, Uplink Port, CoS, VLAN, VLAN Mode, and PXE Boot. There are two entries: 'eth0' and 'eth1'. The 'eth0' entry has a MAC Address of '00:25:B5:30:00:00', MTU of '1500', Uplink Port of '0', CoS of '0', VLAN of 'NONE', VLAN Mode of 'TRUNK', and PXE Boot of 'disabled'. The 'eth1' entry has a MAC Address of '00:25:B5:30:00:01', MTU of '1500', Uplink Port of '1', CoS of '0', VLAN of 'NONE', VLAN Mode of 'TRUNK', and PXE Boot of 'disabled'.

Name	MAC Address	MTU	Uplink Port	CoS	VLAN	VLAN Mode	PXE Boot
eth0	00:25:B5:30:00:00	1500	0	0	NONE	TRUNK	disabled
eth1	00:25:B5:30:00:01	1500	1	0	NONE	TRUNK	disabled

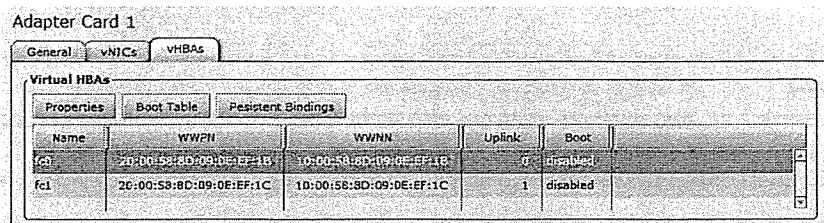
Task 6: Assign WWNs to the P81E VIC

In this task, you will assign locally administered WWNs to the VIC.

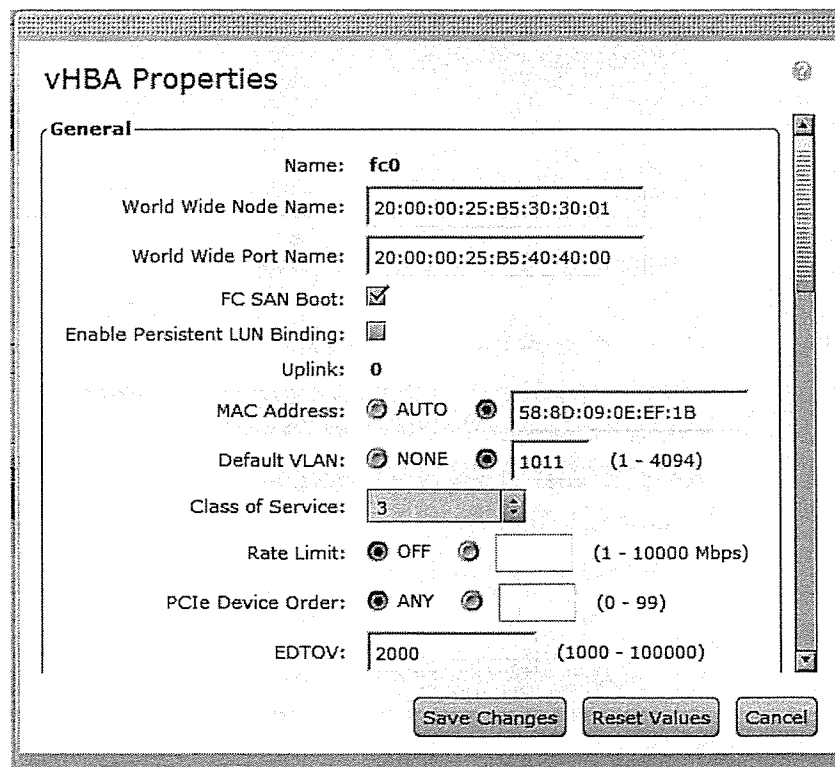
Activity Procedure

Complete these steps:

- Step 1** Click the **vHBAs** subtab and choose **interface fc0**.

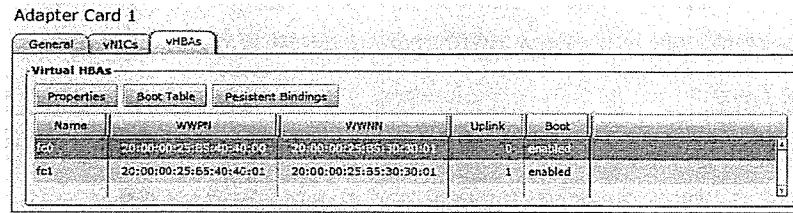


- Step 2** Click **Properties** to configure the Fibre Channel interface.
- Step 3** Refer to the Configuration sheet and change the pod-specific WWNN and WWPN addresses. If these addresses are misconfigured, SAN boot will fail.
- Step 4** Click the **FC SAN Boot** check box to enable SAN boot on this interface.
- Step 5** The other default settings should be changed only to align with IT policy or to meet operating system-specific requirements.
- Step 6** Click **Save Changes** to commit the change.



- Step 7** Repeat Steps 1 through 6 on interface **fc1** to configure the interface with your pod-specific WWNs.

Step 8 Validate the changes in the vHBA section of the content pane.



Note A single WWNN represents the P81E CNA, but each vHBA port requires a unique WWPN. The example uses the WWNs for pod 1 (Boston). Refer to the configuration sheet if you are not in pod 1.

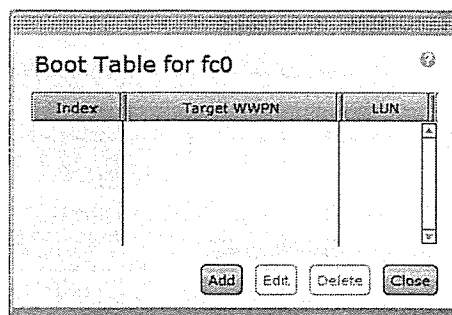
Task 7: Configure a Fibre Channel Boot Target

In this task, you will configure the SAN boot target and verify the boot order.

Activity Procedure

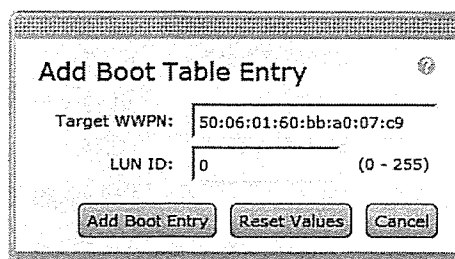
Complete these steps:

Step 1 Choose **interface fc0** and then click **Boot Table**.

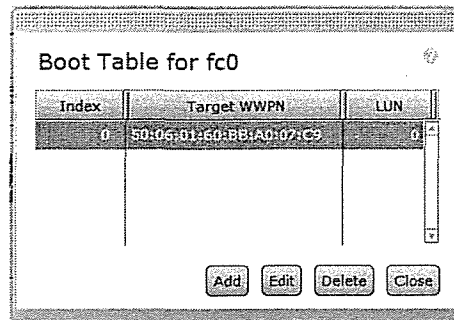


Step 2 Click **Add** to add a SAN boot target.

Step 3 Using values from the configuration sheet, enter the pod-specific boot target WWPN and LUN ID, and then click **Add Boot Entry** to commit the change.



Step 4 The new boot entry should appear in the Boot Table for interface fc0.



Step 5 Click **Close** to finish.

Step 6 Repeat Steps 1 through 5 for interface **fc1**, using the WWPN value and LUN ID for the secondary boot target as indicated in the configuration sheet.

Step 7 From the **Server** tab in the **Navigation** pane, click the **Summary** link.

Step 8 In the **Content** pane, choose the **Power Off Server** link and then click the **OK** button in the pop-up dialog box.

Task 8: Install VMware ESXi 4.1 on Fibre Channel LUN

In this task, you will validate your SAN configuration by installing and SAN-booting VMware ESXi 4.1.

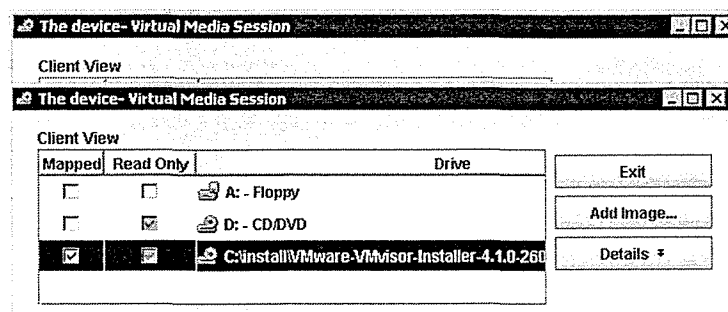
Activity Procedure

Complete these steps:

Step 1 Open a KVM window.

Step 2 From the KVM console, click the **Tools** menu and choose **Launch Virtual Media**.

Step 3 When the Virtual Media dialog box opens, click **Add Image**. Navigate to **c:\install** and choose the file **VMware-VMvisor-Installer-4.1.0.update1-348481.x86_64.iso**.

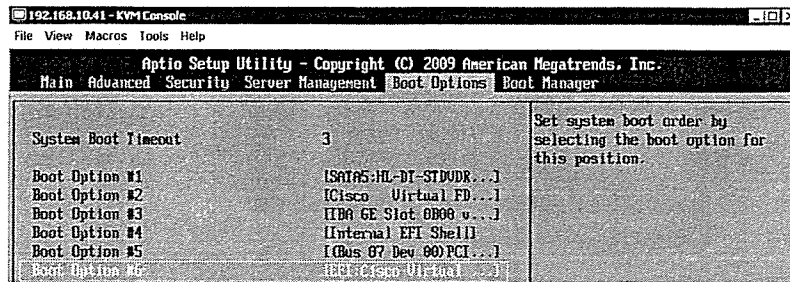


Step 4 When the new virtual device appears, click the check box under the **Mapped** column. The ISO file will now appear as a physical DVD to the server.

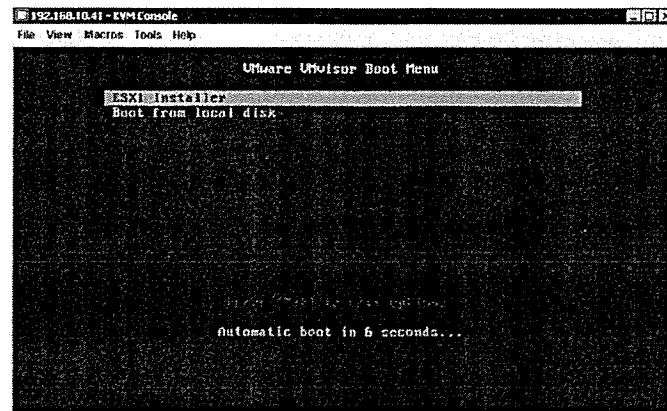
Step 5 From the Cisco IMC, click the **Power On Server** link to boot the server.

Step 6 When the Cisco BIOS screen appears, press **F2** to enter BIOS setup.

- Step 7** Use the right-arrow key to choose the **Boot Option** tab in BIOS setup. Notice that virtual media has been inserted into the boot order. If there is a risk of another device with a higher boot priority loading first, use the up- or down-arrow key to choose a priority where the virtual CD/DVD drive should be installed.



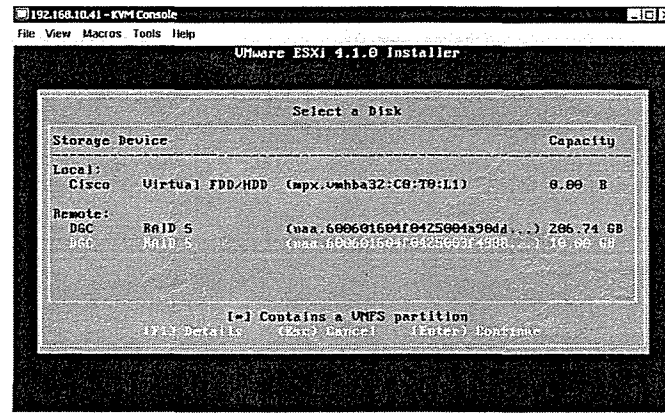
- Step 8** Press **F10** to save and exit.
- Step 9** When the Cisco BIOS screen appears, press the **Esc** key to enable viewing POST messages.
- Step 10** In about 2 minutes, the VMware ESXi boot menu will appear. Either wait 6 seconds for the installer to load automatically, or press the **Enter** key.



- Step 11** It will take about 2 minutes for the installer to load. Press the **Enter** key to begin installation.
- Step 12** On the EULA page, press the **F11** key to proceed.

Step 13 At the Select a Disk screen, choose the 10 GB LUN.

Note If you do not see the 200 GB and 10 GB LUNs, alert your instructor.



Note The 200 GB LUN is VMFS shared storage for vMotion. Do not choose the 200 GB LUN.

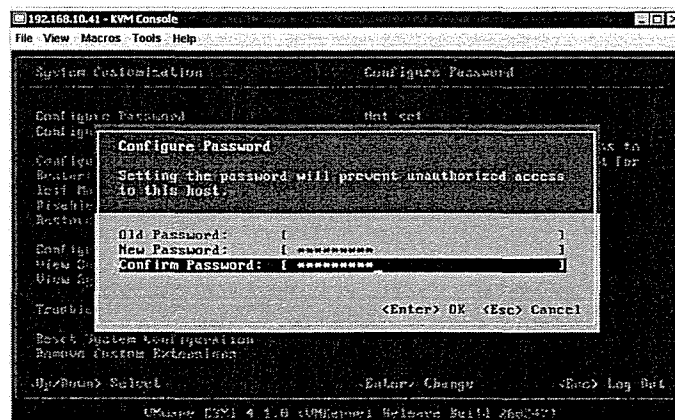
Step 14 At the Confirm Install screen, press the **Enter** key.

Step 15 When the installation is complete, the installer prompts you to press the Enter key and remove installation media. The KVM Virtual Media automatically unmaps the ESXi ISO image.

Step 16 In about 3 minutes, you should see the hypervisor loading. When the ESXi home screen appears, press the **F2** to begin configuring the hypervisor.

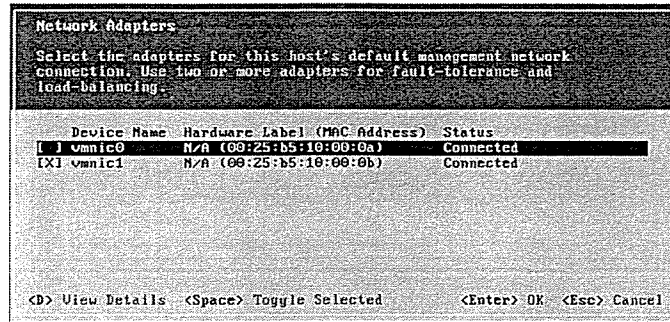
Step 17 At the authentication screen, press the **Enter** key. The password is initially null for the root user.

Step 18 The Change Password element is selected by default on the **System Configuration** screen. Press the **Enter** key to change the default password. Enter **Qwer12345** in the **New Password** and **Confirm Password** fields, and then press the **Enter** key. This action returns you to the System Configuration screen.

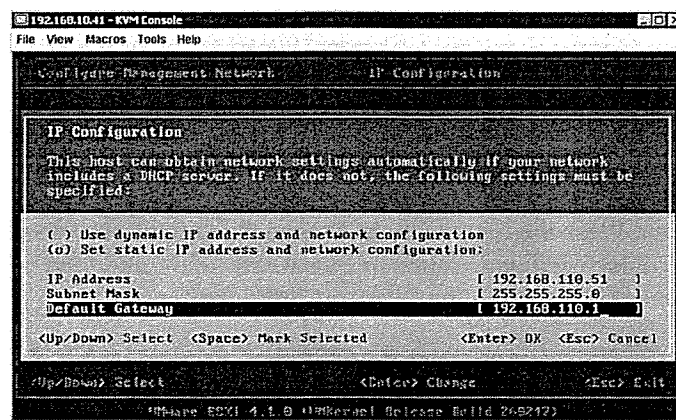


Step 19 Press the down-arrow key to choose the **Configure Management Network** element and then press the **Enter** key.

- Step 20** Press the down-arrow key to choose **Network Adapters** and press the **Enter** key. Use the space bar key to choose both network adapters and then press the **Enter** key to return to System Configuration.

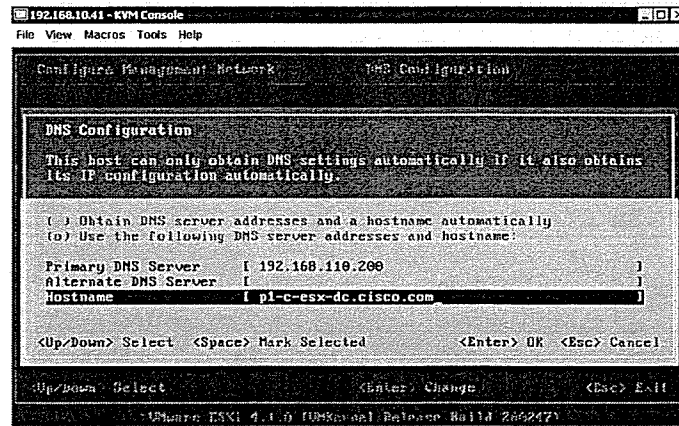


- Step 21** Press the down-arrow key to choose **VLAN (optional)** and press the **Enter** key. Enter the VLAN value from the lab configuration sheet and press the **Enter** key to return to System Configuration.
- Step 22** Press the down-arrow key to choose **IP Configuration** and press the **Enter** key.
- Step 23** Press the down-arrow key to choose **Set static IP address and network configuration:** and press the spacebar to enable it.
- Step 24** Use the lab configuration sheet to enter your pod-specific IP address, subnet mask, and default gateway, and then press the **Enter** key to return to the Configure Management Network screen.

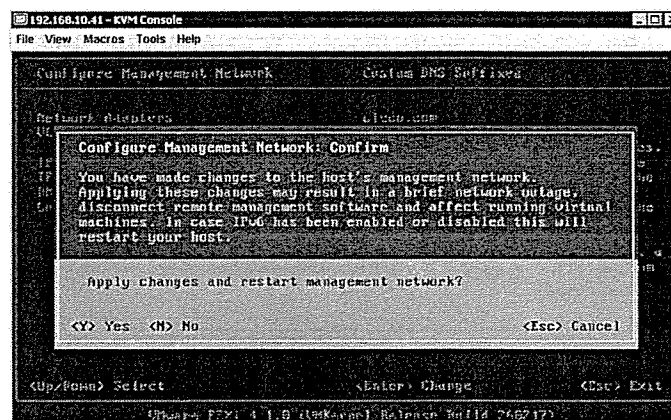


- Step 25** Press the down-arrow key to choose **DNS Configuration** and press the **Enter** key.

- Step 26** Enter **192.168.110.200** as your primary DNS server. Use the down-arrow key to choose **Hostname**. Enter the pod-specific hostname from the lab configuration sheet, and then press the **Enter** key to return to the Configure Management Network screen.

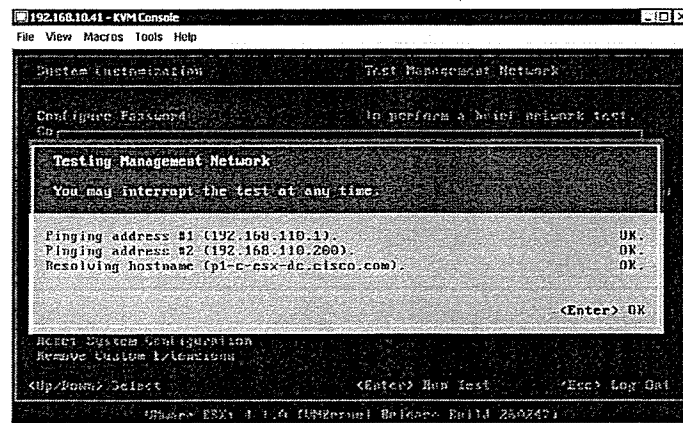


- Step 27** On the Configure Management Network screen, press the down-arrow and choose **Custom DNS Suffixes**, and then press **Enter**.
- Step 28** Press the **Esc** key to exit configuration of the management network.



- Step 29** Press the **Y** key to accept the management network configuration.
- Step 30** Press the down-arrow key to choose the **Test Management Network** element on the System Configuration screen.

- Step 31** On the Test Management Network screen, press the **Enter** key. You should see OK as the result code from pinging the default gateway, DNS server, and test resolution of the ESXi server hostname. If any of the tests fails, contact your instructor.



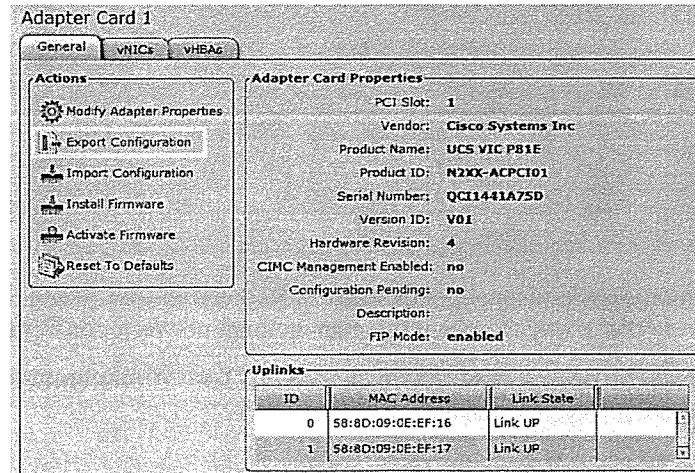
Task 9: Back Up and Restore the P81E Configuration

In this task, you will configure backup and restore for the VIC configuration.

Activity Procedure

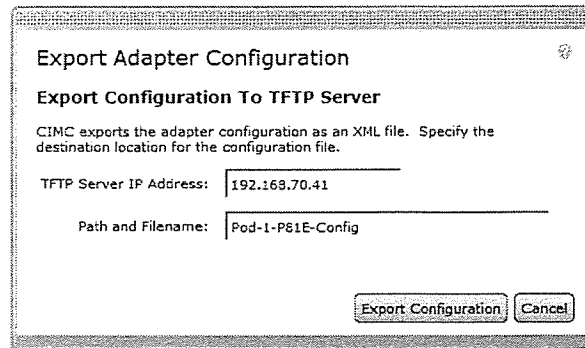
Complete these steps:

- Step 1** On your student PC, verify that 3CDaemon is running TFTP.
- Step 2** On the Adapters tab in the Inventory, choose the **General** subtab.

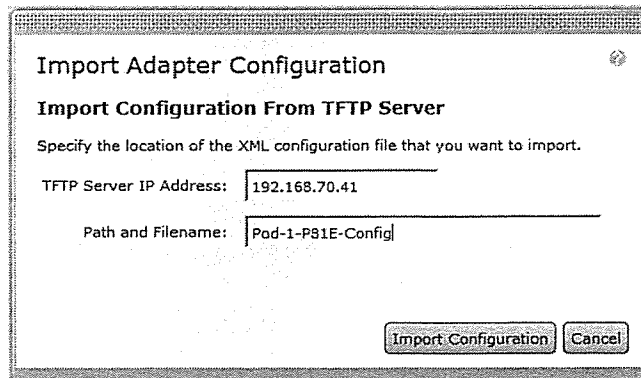


- Step 3** In the Actions section of the content pane, click the **Export Configuration** link.

- Step 4** In the pop-up window, enter the IP address of your student PC and the filename **Pod-P-P81E-Config** (where P is your pod number).



- Step 5** Click **Export Configuration** to start the transfer.
- Step 6** Another pop-up window should indicate Export Successful. Click **Finish** to complete the operation.
- Step 7** To simulate the process of recovering from a deleted or corrupted adapter profile, click the **Reset to Defaults** link in the Actions panel.
- Step 8** Click **OK** in the pop-up that asks you to verify the operation.
- Step 9** Click the **vNICs** and **vHBAs** tabs to verify that the locally administered MAC addresses, WWNs, and boot table are back at their default values.
- Step 10** Click the **Import Configuration** link in the Actions panel.
- Step 11** In the pop-up window, enter the IP address of the TFTP server and the filename for your pod.



- Step 12** Click **Import Configuration**.
- Step 13** Another pop-up window should alert you that the import was successful. Click **Finish** to complete the operation.
- Click the **vNICs** and **vHBAs** tabs and verify that the configuration was restored, based on the addresses in the lab configuration sheet.

Activity Verification

You have completed this activity when you have achieved these goals:

- You have entered the Cisco IMC BIOS and validated the settings.
- You have configured IPMI and used IPMITool to successfully poll chassis status.
- You have configured SoL support.
- You have validated server BIOS settings for virtualization in performance.
- You have configured vNICs for the P81E and assigned WWNN and WWPNS.
- You have configured SAN boot target.
- You have successfully installed, configured, and SAN booted VMware ESXi.
- You have backed up and restored the P81E configuration from a TFTP server.

Lab 5-1: Configure LAN and SAN Physical Connections

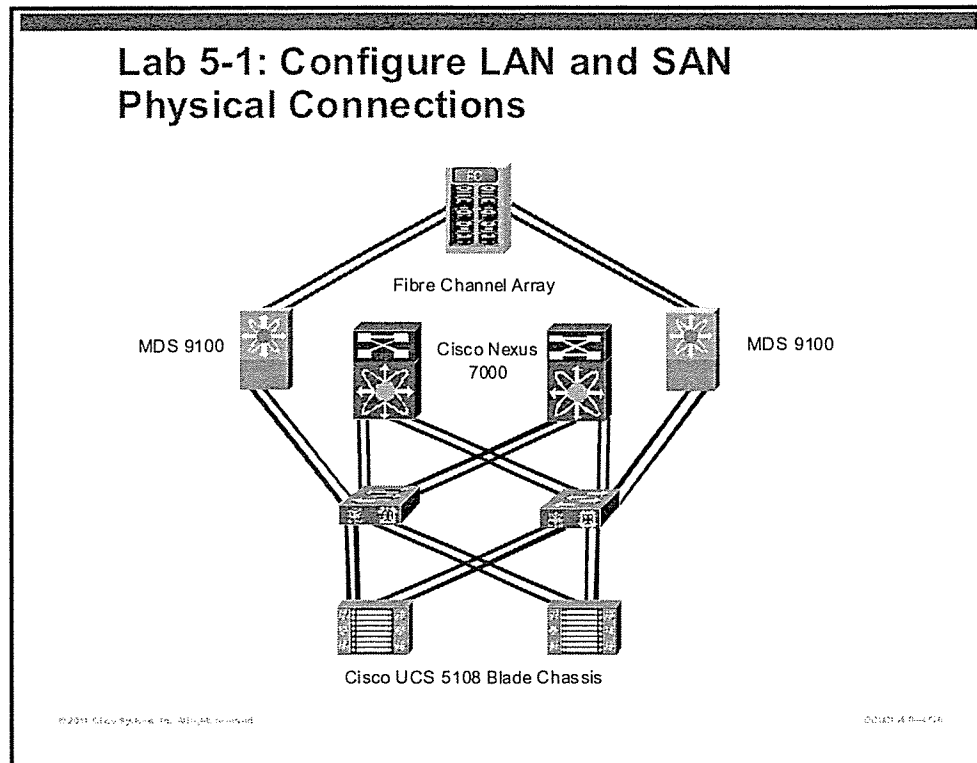
Complete this lab activity to practice what you learned in the related lesson.

Activity Objective

In this activity, you will validate LAN and SAN connectivity from the IOM to the fabric interconnect and northbound Ethernet and Fibre Channel switches.

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required to complete this activity:

- Student PC
- Lab connectivity sheet

Lab 5-1 Cisco UCS Connectivity Sheet

The purpose of this document is to provide implementers with the data that is necessary to cross-connect and validate the physical and logical connectivity for LAN and SAN communication.

VLANs

VLAN Name	VLAN Number	Connectivity
Common_Mgmt	10	A/B
default	1	A/B

VSANs

VSAN Name	VLAN Number	FCoE VLAN	Connectivity
vsan11	11	1011	A
vsan21	12	1012	B
Default	1	—	B

Southbound Connectivity

IOM 2	Fabric Interconnect A	IOM 1	Fabric Interconnect B
Fabric Port 2/1	Server Port 11	Fabric Port 1/1	Server Port 11
Fabric Port 2/2	Server Port 12	Fabric Port 1/2	Server Port 12
Fabric Port 2/3	Server Port 13	Fabric Port 1/3	Server Port 13
Fabric Port 2/4	Server Port 14	Fabric Port 1/4	Server Port 14

Northbound Connectivity

Nexus 7010 A	Fabric Interconnect	Nexus 7010 B	Fabric Interconnect
Ethernet 1/1	Uplink Port 1	Ethernet 1/1	Uplink Port 1
Ethernet 1/2	Uplink Port 2	Ethernet 1/2	Uplink Port 2
Ethernet 1/3	Uplink Port 3	Ethernet 1/3	Uplink Port 3
Ethernet 1/4	Uplink Port 4	Ethernet 1/4	Uplink Port 4
Ethernet 1/5	Uplink Port 5	Ethernet 1/5	Uplink Port 5
Ethernet 1/6	Uplink Port 6	Ethernet 1/6	Uplink Port 6
Ethernet 2/6	Uplink Port 19 (B)	Ethernet 2/6	Uplink Port 20 (B)
Ethernet 2/9	Uplink Port 19 (A)	Ethernet 2/9	Uplink Port 20 (A)

Note The Cisco Nexus 7010 devices are configured with a vPC to the fabric interconnects. Therefore, elements of the port channel appear to be misconfigured.

SAN Connectivity

MDS A	Fabric Interconnect A	MDS B	Fabric Interconnect B
fc1/3	Uplink FC Port 2/1	fc1/3	Uplink FC Port 2/1
fc1/4	Uplink FC Port 2/2	fc1/4	Uplink FC Port 2/2
fc1/5	Uplink FC Port 2/3	fc1/5	Uplink FC Port 2/3
fc1/6	Uplink FC Port 2/4	fc1/6	Uplink FC Port 2/4
fc1/7	Uplink FC Port 2/5	fc1/7	Uplink FC Port 2/5
fc1/8	Uplink FC Port 2/6	fc1/8	Uplink FC Port 2/6
fc1/9	Uplink FC Port 2/7	fc1/9	Uplink FC Port 2/7
fc1/10	Uplink FC Port 2/8	fc1/10	Uplink FC Port 2/8

Device Authentication

Device	IP Address	Username	Password
Fabric Interconnect A	192.168.10.101	admin	Qwer12345
Fabric Interconnect B	192.168.10.102	admin	Qwer12345
Fabric Cluster IP	192.168.10.200	admin	Qwer12345
MDS Fabric A	192.168.10.2	student	Qwer12345
MDS Fabric B	192.168.20.2	student	Qwer12345
Nexus 7010 A	192.168.100.1	student	Qwer12345
Nexus 7010 B	192.168.100.2	student	Qwer12345

Task 1: Validate VLAN Assignments

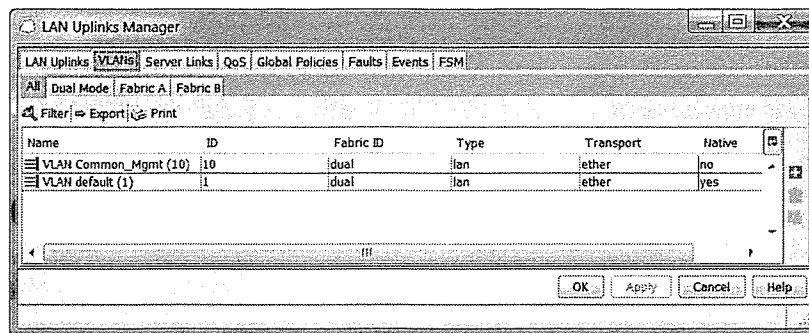
In this task, you will validate that all VLANs that are specified in the configuration sheet are present and configured for both fabrics.

Note The configuration sheet can be removed to avoid flipping back and forth in the Lab Guide.

Activity Procedure

Complete these steps:

- Step 1** Open a browser and connect to Cisco UCS Manager.
- Step 2** In the Equipment tab of the Navigation pane, click either fabric interconnect.
- Step 3** In the content pane, click the **General** tab and then click the **LAN Uplinks Manager** link.
- Step 4** In LAN Uplinks Manager, click the **VLANs** tab. Validate that all required VLANs are present.



- Step 5** Click the **Dual Mode** subtab below VLANs. This action displays the VLANs that were defined as common or global. This list should be identical to the All tab. The Fabric A and Fabric B tabs would be populated by fabric-only or fabric-specific VLANs. This Cisco UCS deployment includes only common or global VLANs.
- Step 6** Click **OK** to close the LAN Uplinks Manager.

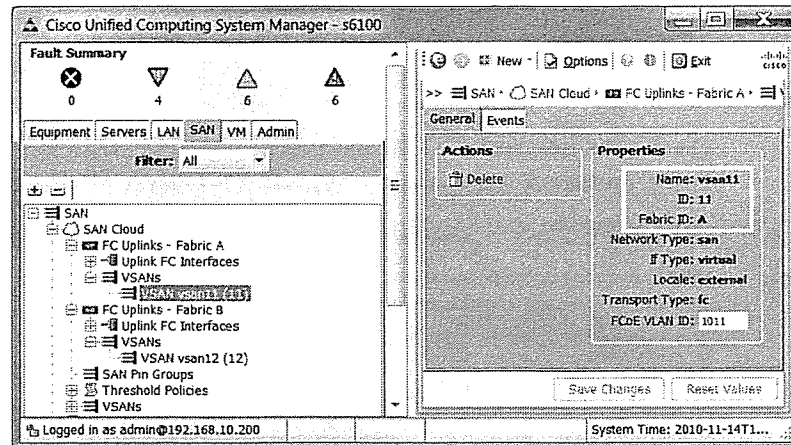
Task 2: Validate VSAN Assignments

In this task, you will validate that all VSANs that are specified in the configuration sheet are present and configured for the correct fabric.

Activity Procedure

Complete these steps:

- Step 1** On the SAN tab of the navigation pane, expand both fabric interconnects under the SAN Cloud. Then, expand the VSAN item beneath each fabric interconnect.



- Step 2** Choose VSAN 11 under fabric interconnect A. In the content pane, validate the fabric association by using the configuration sheet. Repeat this step for VSAN 12 on fabric interconnect B.

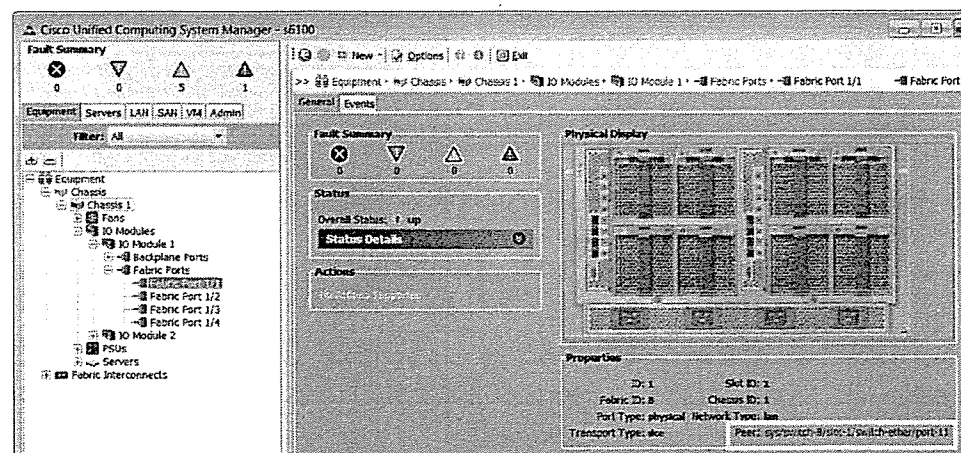
Task 3: Validate Physical Connections from IOMs to Fabric Interconnects

In this task, you will validate that all physical connections between IOMs and fabric connects are correct.

Activity Procedure

Complete these steps:

- Step 1** From the Equipment tab in Cisco UCS Manager, expand Chassis 1 > Modules > IO Module 1 > Fabric Ports.



- Step 2** Choose **Fabric Port 1/1**. In the content pane, observe the entry to the left of Peer. The example shows that IOM port 1/1 on Chassis 1 maps to fabric interconnect B port 11.
- Step 3** Repeat this process for all IOM ports and validate against the configuration sheet.

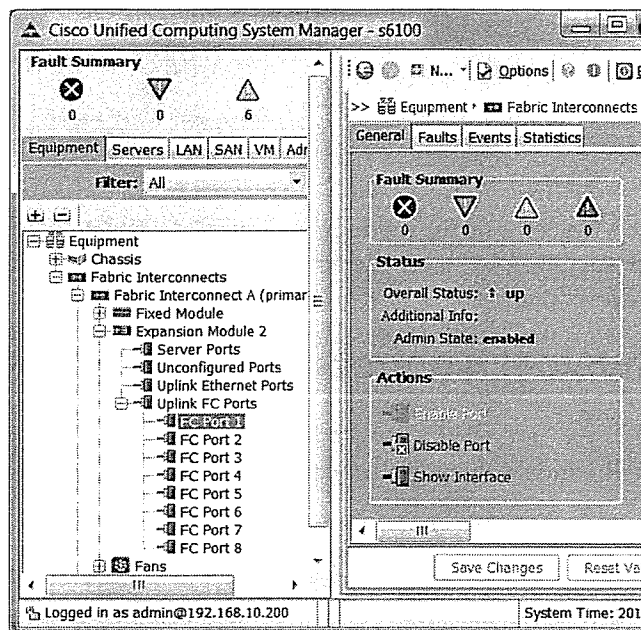
Task 4: Validate Physical SAN Connectivity from the Fabric Interconnects to the MDS Switches

In this task, you will validate physical connectivity between the fabric interconnect Fibre Channel expansion module and the MDS switch.

Activity Procedure

Complete these steps:

- Step 1** On the Equipment tab of the navigation pane in Cisco UCS Manager, expand **Fabric Interconnect A > Expansion Module 2 > Uplink FC Ports**.
- Step 2** Choose **FC Port 1**. Validate that the Overall Status indicates “up” in the content pane.



- Step 3** Refer to the configuration sheet for authentication credentials, and open an SSH session to MDS for fabric A.

Step 4 Use the **show interface brief** command. You should see this output.

```
MDS9124-1# show interface brief

fc1/3 11 F on up sw1 F 4 --
fc1/4 11 F on up sw1 F 4 --
fc1/5 11 F on up sw1 F 4 --
fc1/6 11 F on up sw1 F 4 --
fc1/7 11 F on up sw1 F 4 --
fc1/8 11 F on up sw1 F 4 --
fc1/9 11 F on up sw1 F 4 --
fc1/10 11 F on up sw1 F 4 --
```

Step 5 In Cisco UCS Manager, click the link to **Disable FC Port 1**.

Step 6 Repeat the **show interface brief** command.

Step 7 Observe that interface fc1/3 now indicates a status of **notConnected**. This status should match the port mapping that is indicated in the configuration sheet.

Step 8 Enable the port in Cisco UCS Manager.

Step 9 Repeat this process on fabric interconnect B and MDS switch B until you are satisfied that the port mappings are correct.

Note On the MDS switch, enter the **show run interface fc1/3** command. Notice that there is no description for this port. Best practice is to use the optional Description field to indicate port mapping.

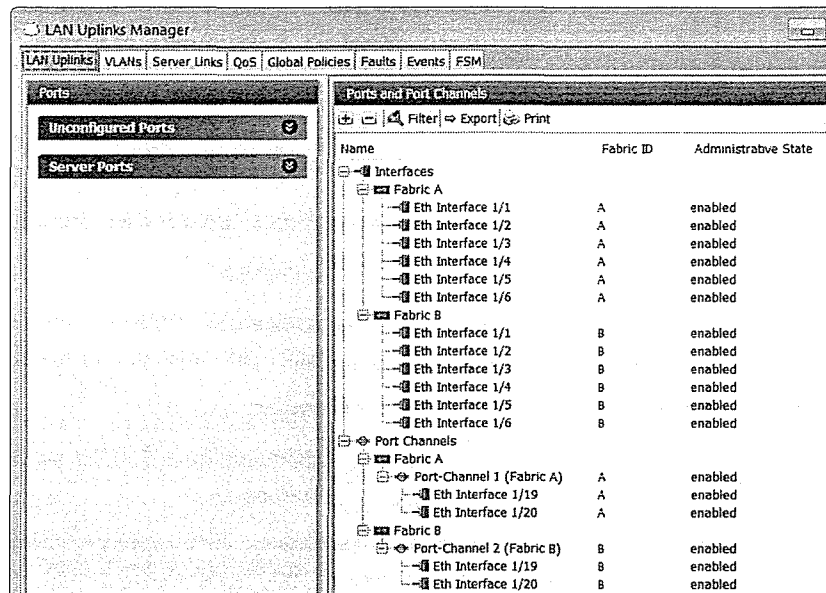
Task 5: Validate Physical Connections from Fabric Interconnects to the Northbound L3 Switch

In this task, you will validate that all physical connections between fabric interconnect A and the Cisco Nexus 7010 devices are correct.

Activity Procedure

Complete these steps:

Step 1 In Cisco UCS Manager, open the LAN Uplinks Manager.



Step 2 Using the credentials in the configuration sheet, connect by SSH to Cisco Nexus 7010 A.

Step 3 Use the **show cdp neighbor** command to display the mapping of Layer 2 neighbors.

N7010-C1# show cdp neighbor						
Device-ID	Local Intrfce	Hldtme	Capability	Platform	Port ID	
3750-1	mgmt0	179	R S I	WS-C3750G-24P	Gig1/0/3	
s6100-A(SS112520C6W)	Eth1/1	134	S I s	N10-S6100	Eth1/1	
s6100-A(SS112520C6W)	Eth1/2	121	S I s	N10-S6100	Eth1/2	
s6100-A(SS112520C6W)	Eth1/3	123	S I s	N10-S6100	Eth1/3	
s6100-A(SS112520C6W)	Eth1/4	124	S I s	N10-S6100	Eth1/4	
s6100-A(SS112520C6W)	Eth1/5	127	S I s	N10-S6100	Eth1/5	
s6100-A(SS112520C6W)	Eth1/6	131	S I s	N10-S6100	Eth1/6	
N7010-C2(TBM12234230)	Eth2/1	168	R S I s	N7K-C7010	Eth2/1	
N7010-C2(TBM12234230)	Eth2/3	179	R S I s	N7K-C7010	Eth2/3	
s6100-B(SS112520C6K)	Eth2/6	146	S I s	N10-S6100	Eth1/19	
s6100-A(SS112520C6W)	Eth2/9	128	S I s	N10-S6100	Eth1/19	
N5K1(SS1142508QC)	Eth2/10	175	S I s	N5K-C5010P-BF	Eth1/20	
NX5K2(SS11425206K)	Eth2/11	175	S I s	N5K-C5010P-BF	Eth1/20	

Step 4 Although the fabric interconnects view the topology as a single port channel to each Cisco Nexus 7010 device, a vPC is configured on both northbound switches. Both Cisco Nexus 7010 devices have one interface that is connected to each fabric interconnect.

Step 5 Verify that this output is consistent with the port mapping in the configuration sheet. Leave your SSH session open.

Task 6: Validate that the Northbound L3 Switch Is Trunking All Required VLANs

In this task, you will validate that the Cisco Nexus 7010 devices are trunking the correct VLANs for Cisco Unified Computing System.

Activity Procedure

Complete these steps:

Step 1 From the SSH session to the Cisco Nexus 7010, you can see that interfaces eth 2/6 and eth 2/9 are connected to fabric interconnects A and B.

Step 2 Run the **show interface trunk module 2** command to view the allowed VLANs.

```
N7010-C1# show interface trunk module 2

-----
Port Vlans Allowed on Trunk
-----

Eth2/3 10-179
Eth2/6 10-179
Eth2/9 10-179
```

Step 3 In the output, match the VLAN range against the configuration sheet.

Step 4 Repeat Steps 1 through 3 for Nexus 7010 B.

Note Although best practice is to limit the allowed VLAN list to the exact VLANs that are in use on the southbound switch, configuring additional VLANs for future use is common.

Activity Verification

You have completed this activity once you have validated these configurations:

- All VLAN assignments match the configuration sheet.
- All VSAN assignments match the configuration sheet.
- All IOM connections match the configuration sheet.
- All physical SAN ports from the fabric interconnects to MDS match the configuration sheet.
- All physical LAN ports from the fabric interconnects to the northbound switch match the configuration sheet.
- All required VLANs are being trunked by the northbound switch.

Lab 6-1: Configure Identity and Resource Pools

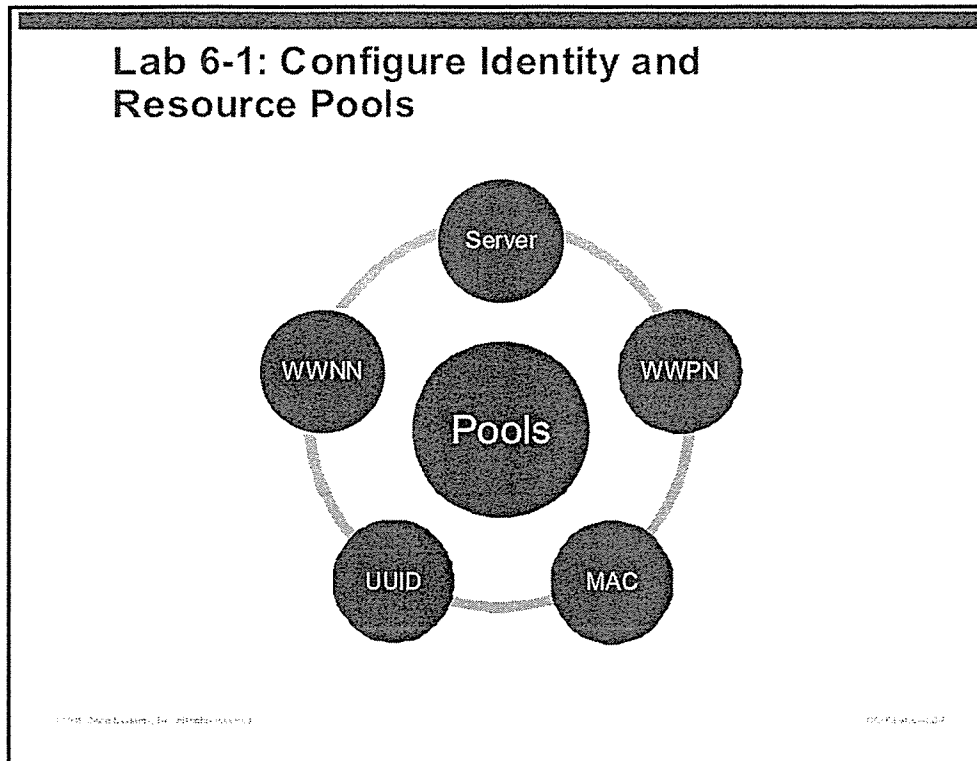
Complete this lab activity to practice what you learned in the related lesson.

Activity Objective

In this activity, you will configure identity and resource pools and policies to be consumed by service profiles in Lab 6-2.

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required to complete this activity:

- Student PC
- Lab identity and resource pools implementation sheet
- Lab reference guide

Lab 6-1 Identity and Resource Pools Implementation Sheet

Use this implementation sheet to aid in the configuration tasks in lab 6-1.

Task 1 Configure Pod-Specific VLANs

Pod	VLAN Prefix	Control	Management	Packet	vMotion	VM Traffic
1	BOS	111	110	211	311	411
2	ORD	112	110	212	312	412
3	DFW	113	110	213	313	413
4	MIA	114	110	214	314	414
5	JFK	115	110	215	315	415
6	SFO	116	110	216	316	416

Task 2 Configure UUID Prefix and Suffix Pools

Pod	Org	UUID Pool Name	UUID Prefix	UUID Suffix	Size
1	Boston	BOS_UUID	00000000-0000-1010	1010-000000000001	2
2	Chicago	ORD_UUID	00000000-0000-2020	2020-000000000001	2
3	Dallas	DFW_UUID	00000000-0000-3030	3030-000000000001	2
4	Miami	MIA_UUID	00000000-0000-4040	4040-000000000001	2
5	New-York	JFK_UUID	00000000-0000-5050	5050-000000000001	2
6	San-Francisco	SFO_UUID	00000000-0000-6060	6060-000000000001	2

Task 3 Configure MAC Pools

Pod	Org	MAC Pool Name	MAC Prefix	MAC Suffix	Size
1	Boston	BOS_MAC	00:25:B5	10:00:00	2
2	Chicago	ORD_MAC	00:25:B5	10:00:02	2
3	Dallas	DFW_MAC	00:25:B5	10:00:04	2
4	Miami	MIA_MAC	00:25:B5	10:00:06	2
5	New-York	JFK_MAC	00:25:B5	10:00:08	2
6	San-Francisco	SFO_MAC	00:25:B5	10:00:0A	2

Lab 6-1 Identity and Resource Pools Implementation Sheet (Cont.)

Task 4 Configure WWNN Pools

Pod	Org	WWNN Pool Name	WWNN Prefix	WWNN Suffix	Size
1	Boston	BOS_WWNN	20:00:00:25:B5	10:10:01	1
2	Chicago	ORD_WWNN	20:00:00:25:B5	10:10:02	1
3	Dallas	DFW_WWNN	20:00:00:25:B5	10:10:03	1
4	Miami	MIA_WWNN	20:00:00:25:B5	10:10:04	1
5	New-York	JFK_WWNN	20:00:00:25:B5	10:10:05	1
6	San-Francisco	SFO_WWNN	20:00:00:25:B5	10:10:06	1

Task 5 Configure WWPN Pool

Pod	Org	WWPN Pool Name	WWPN Prefix	WWPN Suffix	Size
1	Boston	BOS_WWPN	20:00:00:25:B5	20:20:00	2
2	Chicago	ORD_WWPN	20:00:00:25:B5	20:20:02	2
3	Dallas	DFW_WWPN	20:00:00:25:B5	20:20:04	2
4	Miami	MIA_WWPN	20:00:00:25:B5	20:20:06	2
5	New-York	JFK_WWPN	20:00:00:25:B5	20:20:08	2
6	San-Francisco	SFO_WWPN	20:00:00:25:B5	20:20:0A	2

Task 6 Configure Server Pool Qualification Policy

Pod	Org	Server Pool Name	Qualification Name	Server Pool Policy	Blade	Size
1	Boston	BOS_Server	BOS_QUAL	BOS_POLICY	1	1
2	Chicago	ORD_Server	ORD_QUAL	ORD_POLICY	2	1
3	Dallas	DFW_Server	DFW_QUAL	DFW_POLICY	3	1
4	Miami	MIA_Server	MIA_QUAL	MIA_POLICY	4	1
5	New-York	JFK_Server	JFK_QUAL	JFK_POLICY	5	1
6	San-Francisco	SFO_Server	SFO_QUAL	SFO_POLICY	6	1

Lab 6-1 Identity and Resource Pools Implementation Sheet (Cont.)

Task 7 Validate QoS, Configure Adapter, Scrub, and QoS Policies

Pod	Org	Adapter Policy Name	RSS Status	Failback Timer	Scrub Policy Name	QoS Policy Name
1	Boston	BOS_Adapter	Enabled	2	BOS_Scrub	BOS_QoS
2	Chicago	ORD_Adapter	Enabled	2	ORD_Scrub	ORD_QoS
3	Dallas	DFW_Adapter	Enabled	2	DFW_Scrub	DFW_QoS
4	Miami	MIA_Adapter	Enabled	2	MIA_Scrub	MIA_QoS
5	New-York	JFK_Adapter	Enabled	2	JFK_Scrub	JFK_QoS
6	San-Francisco	SFO_Adapter	Enabled	2	SFO_Scrub	SFO__QoS

Task 1: Configure Pod-Specific VLANs

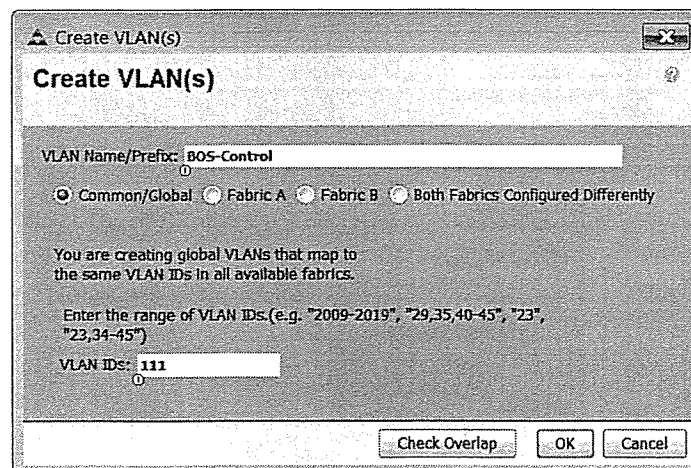
In this task, you will configure the named VLANs that are required by VMware ESXi.

Activity Procedure

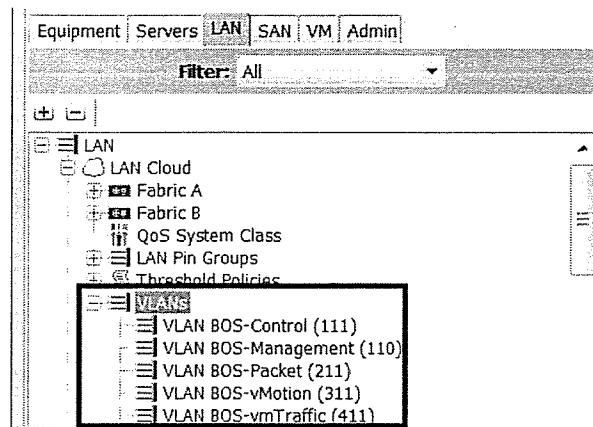
Complete these steps:

Note The examples that are used in all tasks of this lab are based on pod 1 (Boston). Be sure to use the values that are associated with your assigned pod, according to the implementation sheet.

- Step 1** In Cisco UCS Manager, choose the **LAN** tab.
- Step 2** Click the plus symbol (+) to the left of VLANs to expand the list.
- Step 3** Right-click **VLANs** and then click **Create VLAN(s)** from the drop-down list.
- Step 4** Use the resource sheet for this task and name your VLANs by using the three-letter airport code for the city of your pod (the old name for Chicago O'Hare was Orchard Field, hence ORD); for example, BOS-Control, BOS-Management, BOS-Packet.



- Step 5** Repeat Steps 3 and 4 to create your Management, Packet, vMotion, and vmTraffic VLANs. The following figure shows an example of pod 1 VLANs.



Note Do not use the VLAN names and numbers that are called out in the figure, unless you are in pod 1 (Boston). Refer to the resource sheet for your pod-specific naming and numbering.

Task 2: Configure UUID Prefix and Suffix Pools

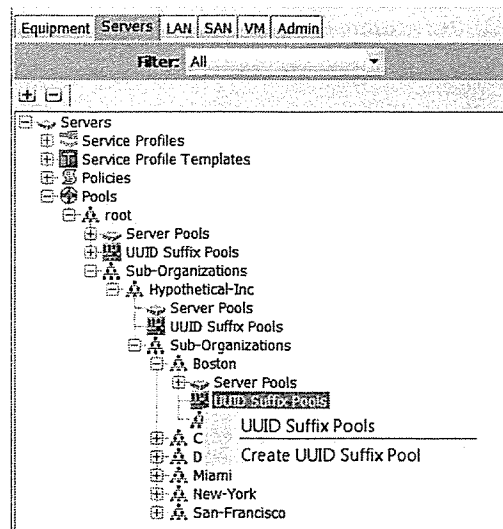
In this task, you will configure UUID pools to be consumed by service profile templates.

Activity Procedure

Complete these steps:

Note The examples that are used in all tasks of this lab are based on pod 1 (Boston). Be sure to use the values that are associated with your assigned pod, according to the implementation sheet.

- Step 1** In Cisco UCS Manager, choose the **Servers** tab.
- Step 2** Expand **Pools > Root > Sub-Organizations > Hypothetical-Inc > Sub-Organizations > Your Organization > UUID Suffix Pools**.
- Step 3** Right-click **UUID Suffix Pools** and choose **Create UUID Suffix Pool**.



-
- Create UUID Suffix Pool
- # Unified Computing System Manager
- Create UUID Suffix Pool
1. ✓ Define name and description
 2. ↪ Add UUID Blocks
- Define name and description
- Name: BOS_UUID
- Description: Boston UUID Pool
- Prefix: ☐ derived ☒ other
- 00000000-0000-1010
- < Prev Next > Finish Cancel

-
- Create UUID Suffix Pool**
1. ☒ Define name and description
 2. ☒ Add UUID Blocks
- ## Unified Computing System Manager
- ### Add UUID Blocks
- | Name | From | To |
|------|--|--------------|
| | 0000-000000000001 - 00000000-000000... | 0000-0000... |
-
- < Prev Next > Finish Cancel
- Create a Block of UUID Suffixes**
- From: 0000-000000000001 Size: 2
- OK Cancel

- | >> | Servers | Pools | root | Sub-Organizations | Hypothetical-Inc | Sub-Organizations | Boston | UUID Suffix Pools |
|--|-----------|--------------------|-------------------|-------------------|------------------|-------------------|--------|-------------------|
| UUID Suffix Pools | | | | | | | | |
| <div> <div> <div></div> <div></div> <div></div> </div> <div>Filter</div> <div>Export</div> <div>Print</div> </div> | | | | | | | | |
| Name | Pool Name | UUID Prefix | From | To | | | | |
| Pool BOS_UUID | BOS_UUID | 00000000-0000-1010 | 0000-000000000001 | 0000-000000000002 | | | | |

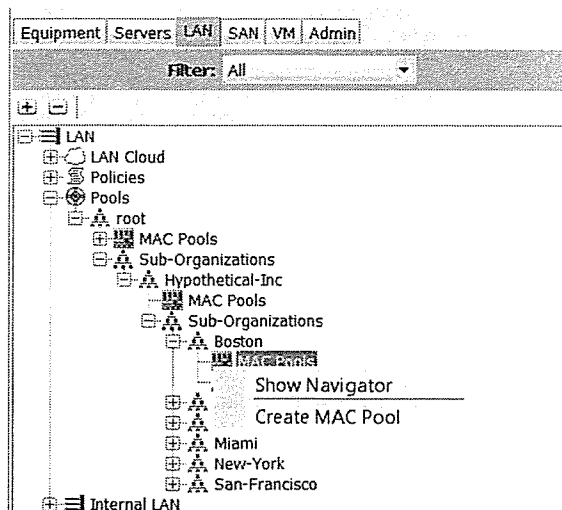
Task 3: Configure MAC Pools

In this task, you will configure MAC addresses that will be consumed by service profile templates.

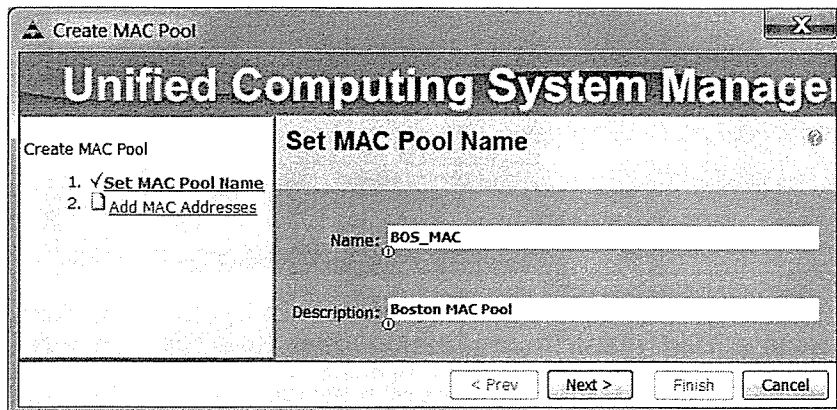
Activity Procedure

Complete these steps:

- Step 1** In Cisco UCS Manager, choose the **LAN** tab.
- Step 2** Expand **Pools > Root > Sub-Organizations > Hypothetical-Inc > Sub-Organizations > Your Organization > MAC Pools**.



- Step 3** Right-click **MAC Pools** and choose **Create MAC Pool**.
- Step 4** In the MAC Pool creation wizard, enter the name of the MAC pool, according to the implementation sheet; you can also enter an optional description.



- Step 5** Click **Next** to continue.

- Step 6** Click the plus symbol (+), enter the MAC suffix for your pod, and then click **OK**. Observe that the MAC pool wizard automatically provides the first 3 bytes of the MAC address.

Create MAC Pool

Unified Computing System Manager

Create MAC Pool

1. ✓ Set MAC Pool Name
2. ✓ Add MAC Addresses

Add MAC Addresses

Name	From	To
[00:25:85:10:00:00 - 00:25:85:10:00:01]	00:25:85:10:00:00	00:25:85:10:00:01

Add Delete

< Prev Next > Finish Cancel

Create a Block of MAC Addresses

First MAC Address: 00:25:85:10:00:00 Size: 2

OK Cancel

- Step 7** Click **Finish** to complete the wizard.
- Step 8** Expand the new MAC pool to view the details of the newly created pool.

>> LAN Pools root Sub-Organizations Hypothetical-Inc Sub-Organizations Boston MAC Pools

MAC Pools

Filter Export Print

Name	Size	Assigned
MAC POOL BOS_MAC	2	0
[00:25:85:10:00:00 - 00:25:85:10:00:01]		

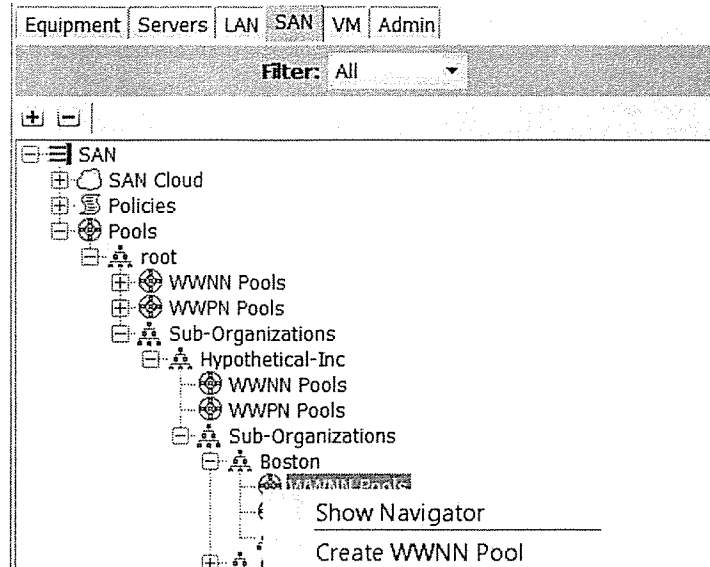
Task 4: Configure WWNN Pools

In this task, you will configure WWNNs that will be consumed by service profile templates.

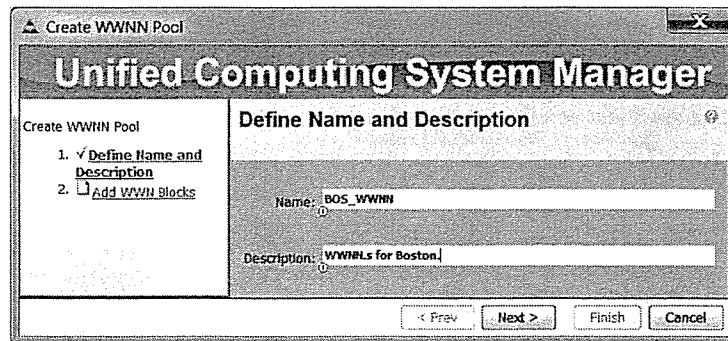
Activity Procedure

Complete these steps:

- Step 1 In Cisco UCS Manager, choose the **SAN** tab.
- Step 2 Expand **Pools > Root > Sub-Organizations > Hypothetical-Inc > Sub-Organizations > Your Organization > WWNN Pools**.
- Step 3 Right-click **WWNN Pools** and choose **Create WWNN Pool**.

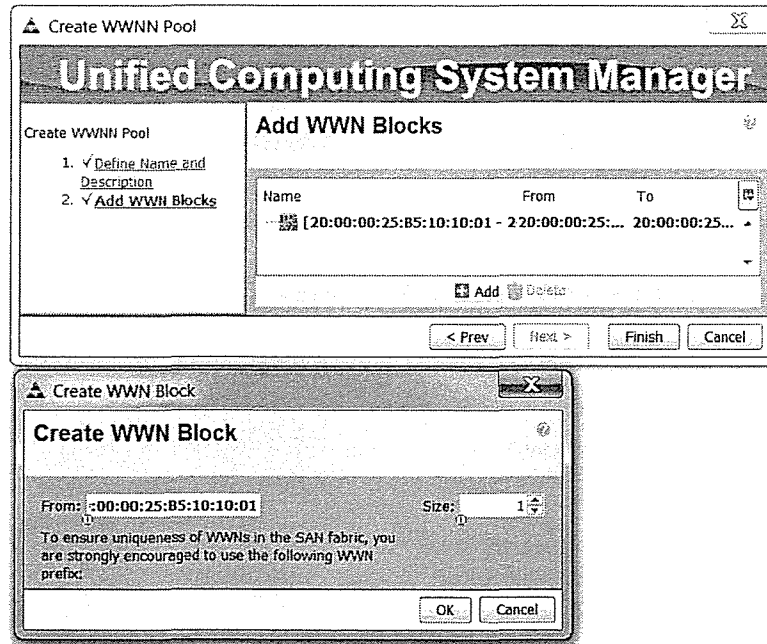


- Step 4 In the WWNN pool creation wizard, enter the name of the WWNN pool, according to the implementation sheet; you can also enter an optional description.



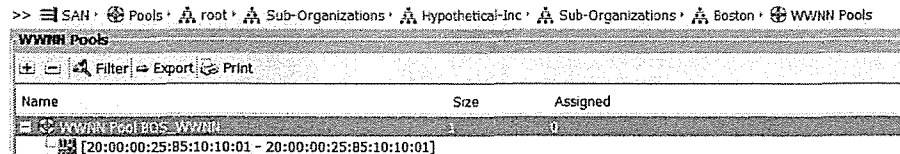
- Step 5 Click **Next** to continue.

- Step 6** Click the plus symbol (+), enter the WWNN Suffix for your pod, and then click **OK**. Observe that the WWNN pool wizard automatically provides the first 5 bytes of the WWNN address.



- Step 7** Click **Finish** to complete the wizard.

- Step 8** Expand the new WWNN pool to view the details of the newly created pool.



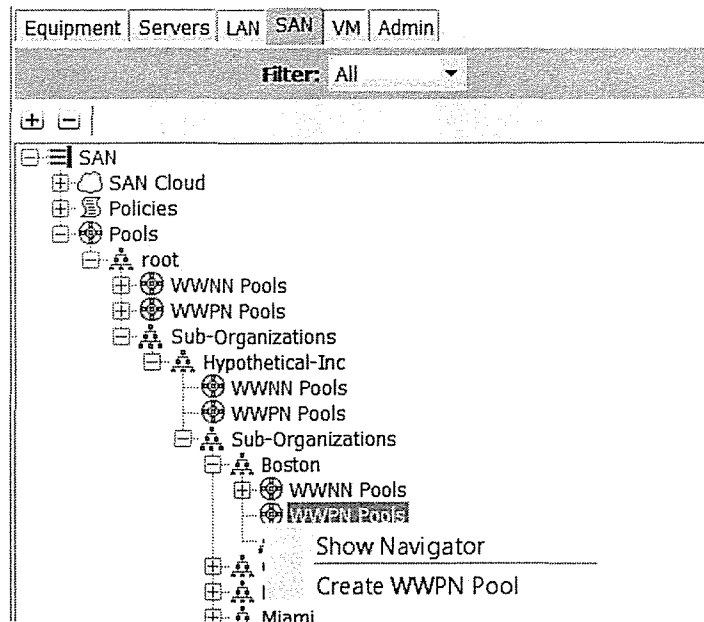
Task 5: Configure WWPN Pools

In this task, you will configure WWPNs that will be consumed by service profile templates.

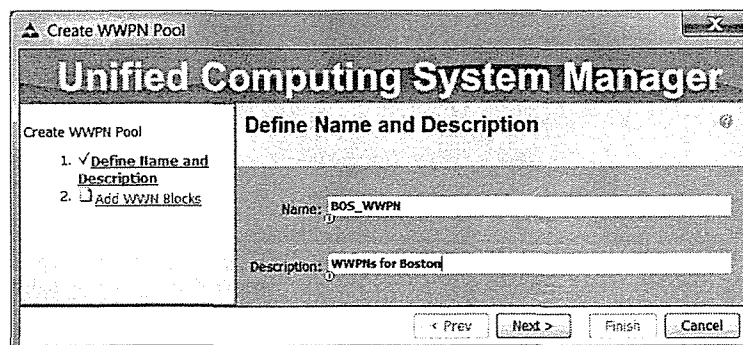
Activity Procedure

Complete these steps:

- Step 1 In Cisco UCS Manager, choose the SAN tab.
- Step 2 Expand **Pools > Root > Sub-Organizations > Hypothetical-Inc > Sub-Organizations > Your Organization > WWPN Pools**.
- Step 3 Right-click **WWPN Pools** and choose **Create WWPN Pool**.

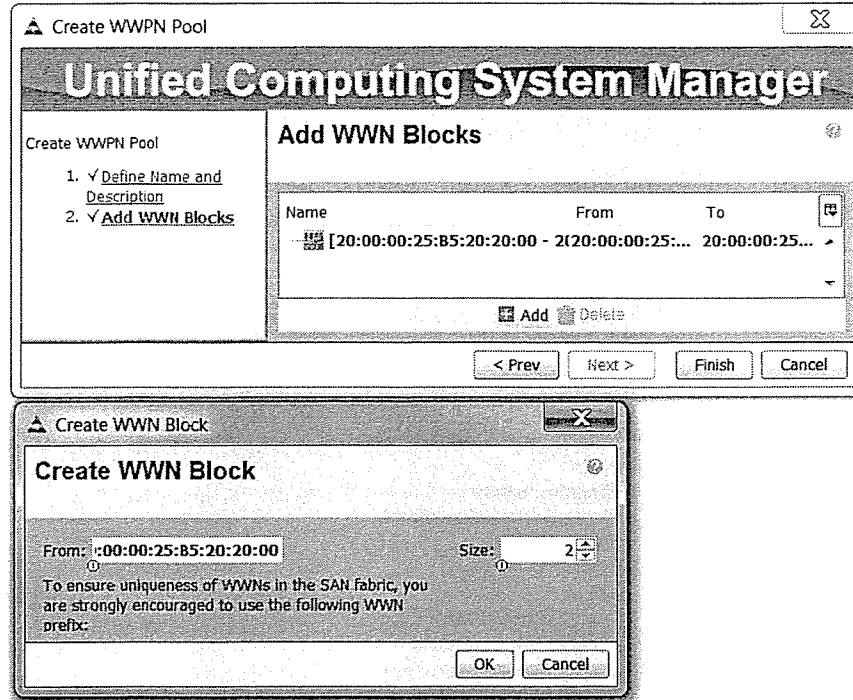


- Step 4 In the WWPN pool creation wizard, enter the name of the WWPN pool, according to the implementation sheet; you can also enter an optional description.



- Step 5 Click **Next** to continue.

- Step 6** Click the plus symbol (+) and enter the WWPN suffix for your pod. Click **OK**. Observe that the WWPN pool wizard automatically provides the first 5 bytes of the WWPN address.



- Step 7** Click **Finish** to complete the wizard.
- Step 8** Expand the new WWPN pool to view the details of the newly created pool.

>> SAN > Pools > root > Sub-Organizations > Hypothetical-Inc > Sub-Organizations > Boston > WWPN Pools

WWPN Pools

Filter Export Print

Name	Size	Assigned
WWPN Pool BOS- WWPN	2	0
[20:00:00:25:85:20:20:00 - 20:00:00:25:85:20:20:01]		

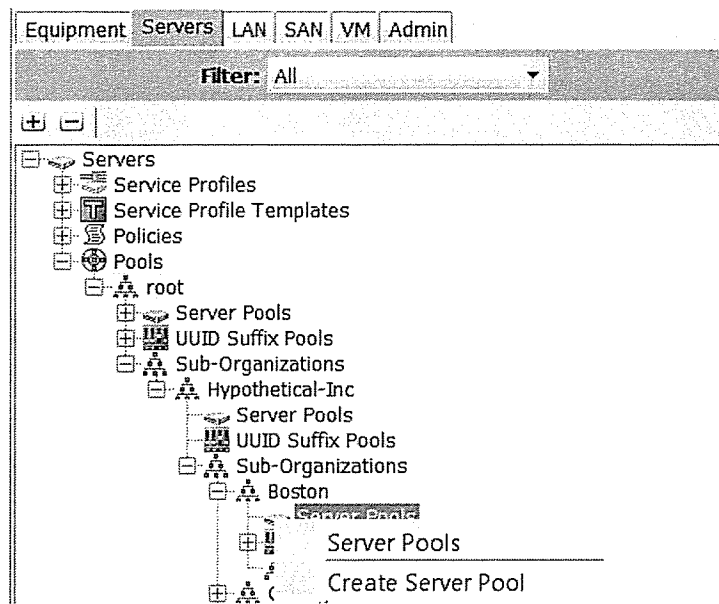
Task 6: Configure Server Pool Qualification Policy

In this task, you will configure and test a server pool qualification policy to automatically populate a server pool with your assigned blade server.

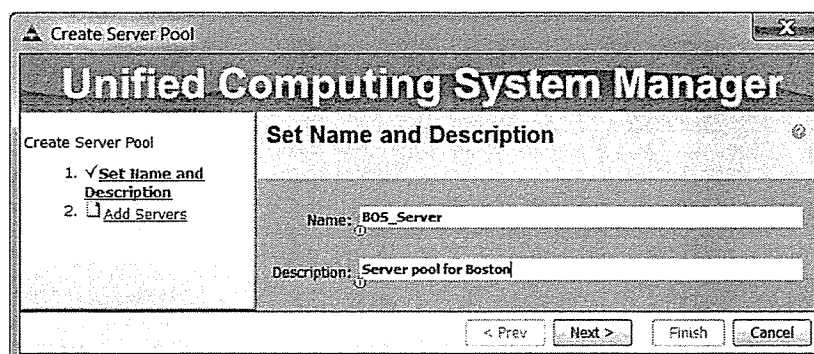
Activity Procedure

Complete these steps:

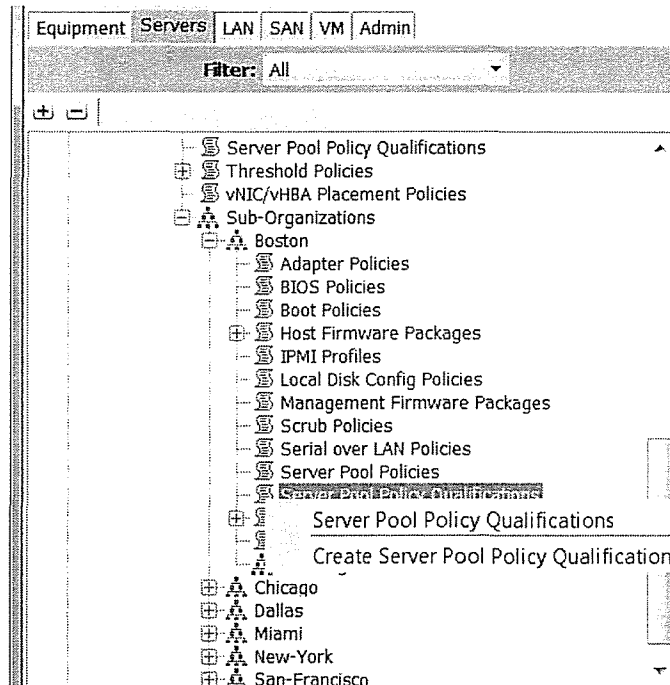
- Step 1 In Cisco UCS Manager, choose the **Servers** tab.
- Step 2 Expand **Pools > Root > Sub-Organizations > Hypothetical-Inc > Sub-Organizations > Your Organization > Server Pools**.
- Step 3 Right-click **Server Pools** and choose **Create Server Pool**.



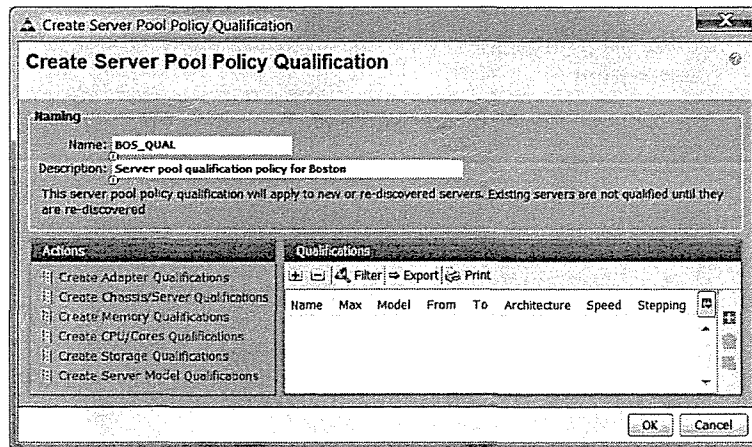
- Step 4 In the Server pool creation wizard, enter the name of the server pool, according to the implementation sheet; you can also enter an optional description.



- Step 5 Click **Next** to continue.
- Step 6 Click **Finish** to complete the wizard.
- Step 7 In the Servers tab, expand **Policies > Root > Sub-Organizations > Hypothetical-Inc > Sub-Organizations > Your Organization > Server Pool Policy Qualifications**.
- Step 8 Right-click **Server Pool Policy Qualifications** and choose **Create Server Pool Policy Qualification**.

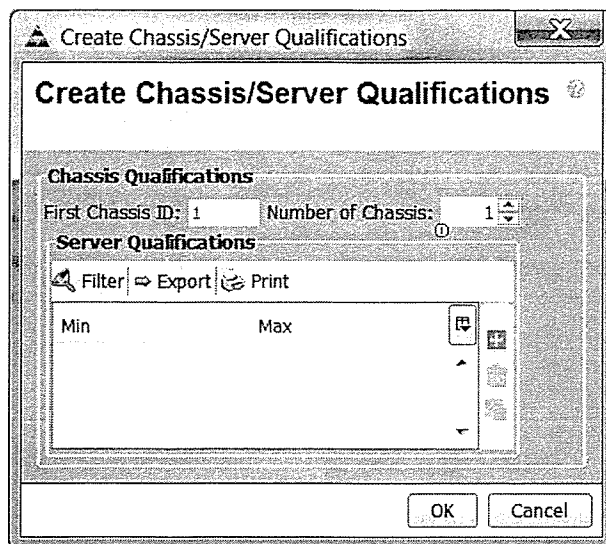


- Step 9** In the Server Pool Policy Qualification creation wizard, enter the name of the server pool qualification policy, according to the implementation sheet; you can also enter an optional description.

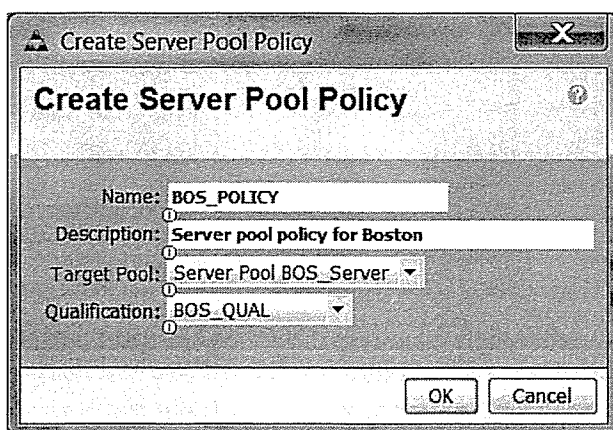


- Step 10** In the Actions panel, click the Create Chassis/Server Qualifications link.

- Step 11** If there were multiple chassis in this Cisco Unified Computing System, you could choose which chassis to begin the selection and how many chassis the selection could span. Click the plus symbol (+) to choose the blade that is assigned to your pod, according to the implementation sheet.



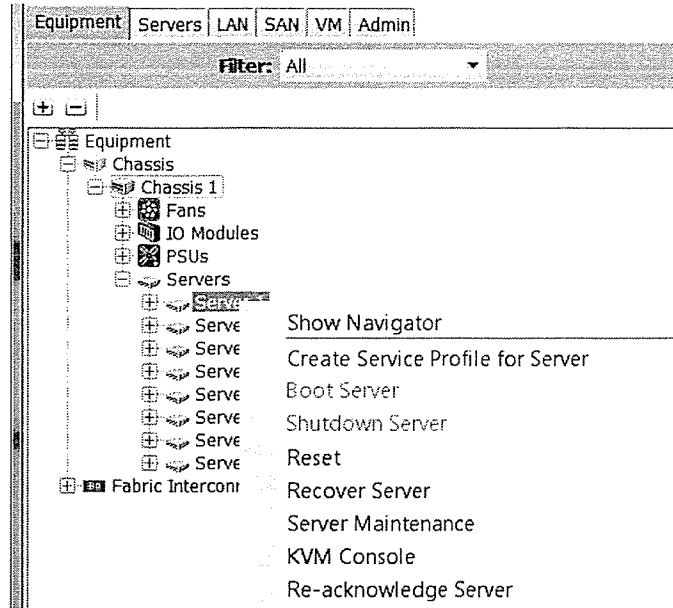
- Step 12** The **First Slot ID** value corresponds to the blade number from the implementation sheet.
- Step 13** Click **Finish Stage** and then **Finish** to add your blade to the selection criteria.
- Step 14** In the Create Server Pool Policy Qualification window, your blade appears in the Qualifications panel.
- Step 15** Click **OK** to finish the qualification policy.
- Step 16** From the navigation pane, right-click **Server Pool Policies** and choose **Create Server Pool Policy**.
- Step 17** Enter the policy name from the implementation sheet; you can also enter an optional description.
- Step 18** Choose your Target Pool and Qualification from the drop-down list and then click **OK** to finish.



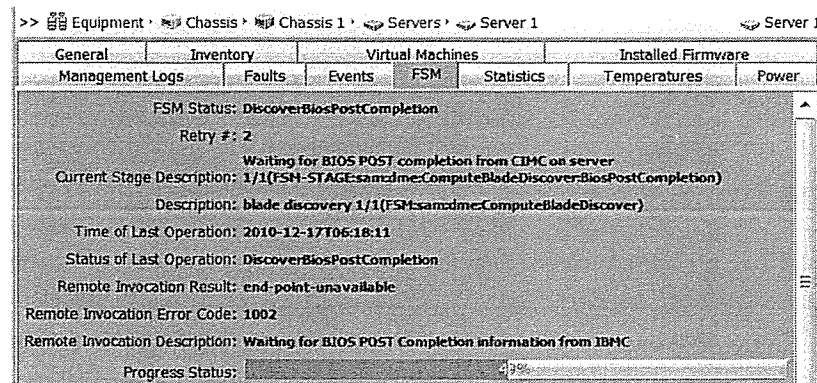
Note Because pool qualification policies are evaluated only when a server is initially or later acknowledged by the chassis, you must reacknowledge your blade.

- Step 19** Choose the **Equipment** tab in Cisco UCS Manager.
- Step 20** Expand **Equipment > Chassis > Chassis 1 > Servers**.

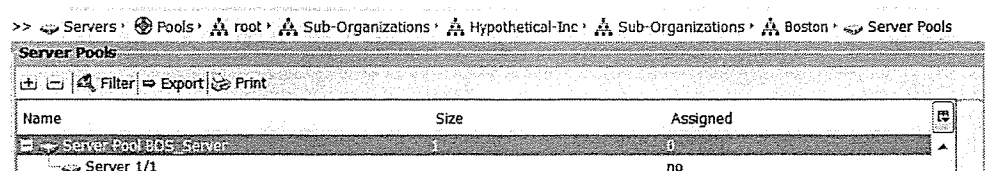
- Step 21** Right-click your assigned server and choose **Re-acknowledge Server** from the pop-up menu. Click **Yes** to confirm that you want to reacknowledge the server.



- Step 22** Click the **FSM** tab in the content pane to observe Cisco UCS Manager adding the server into inventory.



- Step 23** When the FSM status reaches 100 percent, return to the Servers tab in the navigation pane and expand **Pools > Root > Sub-Organizations > Hypothetical-Inc > Sub-Organizations > Your Organization > Server Pools**.
- Step 24** In the content pane, expand your server pool. Assuming that the qualification policy is configured correctly, you should see your assigned server as a member of the pool.



Task 7: Validate QoS, Configure Adapter, Scrub, and QoS Policies

In this task, you will verify that global QoS allows Ethernet jumbo frames. You will configure adapter, scrub, and QoS policies.

Activity Procedure

Complete these steps:

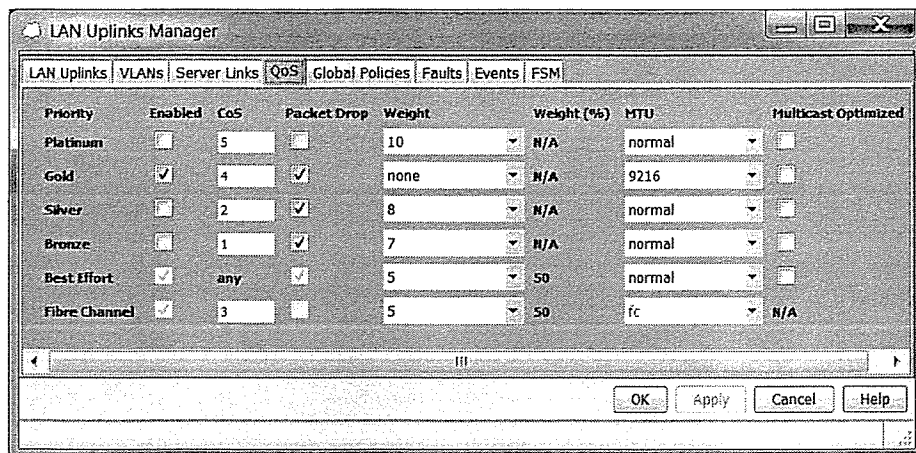
Step 1 In Cisco UCS Manager, choose the **Equipment** tab and expand **Equipment > Fabric Interconnects > Fabric Interconnect A**.

Step 2 In the content pane, click the **LAN Uplinks Manager** link.

Step 3 Choose the **QoS** tab.

Note Because QoS is a global setting that applies to both fabric interconnects, the QoS setting was preconfigured for you. The Gold QoS Priority is disabled by default.

Step 4 Verify that the Gold Priority is enabled, Packet Drop is checked, Weight is none, and MTU is 9216.

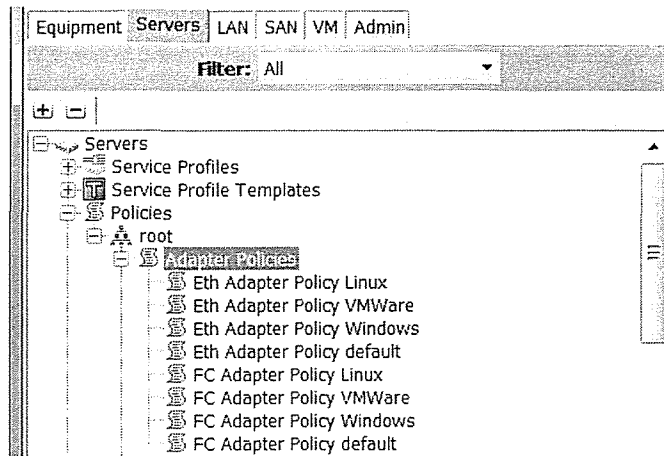


Step 5 Click **OK** to close the LAN Uplinks Manager.

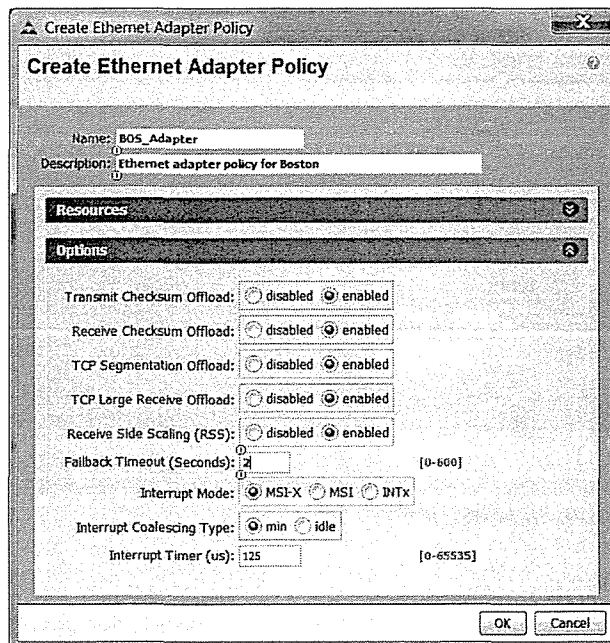
Step 6 In the Servers tab, expand **Policies > Root > Adapter Policies**.

Note Observe that there are six default adapter policies that can be applied to a service profile. These policies define adapter settings that are generally desirable for Linux, Windows, and VMware. If a service profile does not explicitly choose an adapter policy, then the default adapter policy is applied to that service profile. Adapter policies for Ethernet and Fibre Channel are individually configurable.

Note Because these policies are created at the root level of the organizational hierarchy, they can be consumed by service profiles in any suborganization.

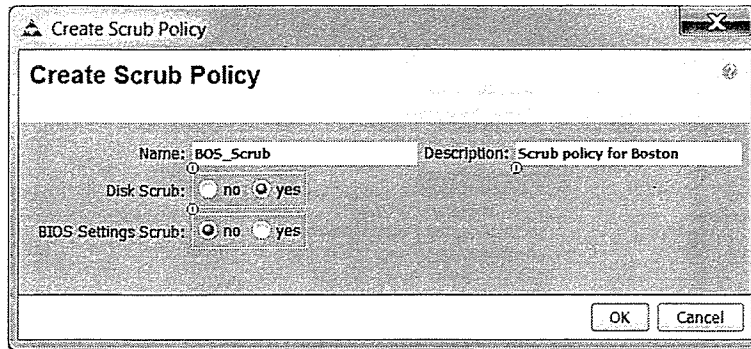


- Step 7** In the Servers tab, expand **Policies > Root > Sub-Organizations > Hypothetical-Inc > Sub-Organizations > Your Organization > Adapter Policies**.
- Step 8** Right-click **Adapter Policies** in your organization and choose **Create Ethernet Adapter Policy**.
- Step 9** Click the **enabled** radio button for Receive Side Scaling (RSS) and set the Failback Timer to 2 seconds.



- Step 10** Click **OK** to save your new adapter policy.
- Step 11** The QoS setting and adapter policy will be selected in the service profile template that you create in Lab 6-2. Any service policies that are created from the template will inherit the QoS setting and adapter policy.
- Step 12** While still under the policies of your organization in the navigation window, right-click **Scrub Policies** and choose **Create Scrub Policy** from the pop-up menu.
- Step 13** Name the scrub policy, according to the lab implementation sheet.
- Step 14** Choose the **Yes** radio button for Disk Scrub.

Step 15 Click **OK** to save the new policy.

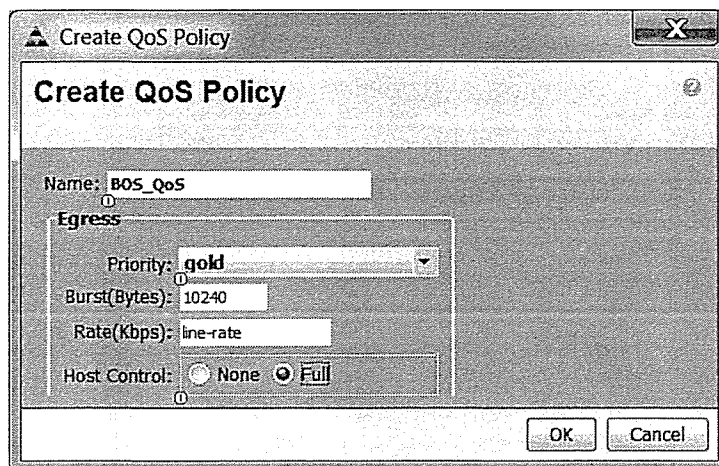


Step 16 In the LAN tab, expand **Policies > Root > Sub-Organizations > Hypothetical-Inc > Sub-Organizations > Your Organization > QoS Policies**.

Step 17 Right-click **QoS Policies** in your organization and choose **Create QoS Policy**.

Step 18 Use the lab implementation sheet to determine the policy name.

Step 19 Choose **gold** from the Priority drop-down menu. Click the **Full** radio button for Host Control.



Step 20 Click **OK** to save the policy.

Activity Verification

You have completed this activity when you have achieved these goals:

- You have created your pod-specific VLANs
- You have created your assigned UUID pool with two UUIDs.
- You have created your assigned MAC pool with two MAC addresses.
- You have created your assigned WWNN pool with one WWNN.
- You have created your assigned WWPN pool with two WWPN.
- You have created and tested a server pool qualification policy.
- You have validated QoS settings and configured adapter, scrub, and QoS policies.

Lab 6-2: Create Mobile Service Profiles from Updating Templates

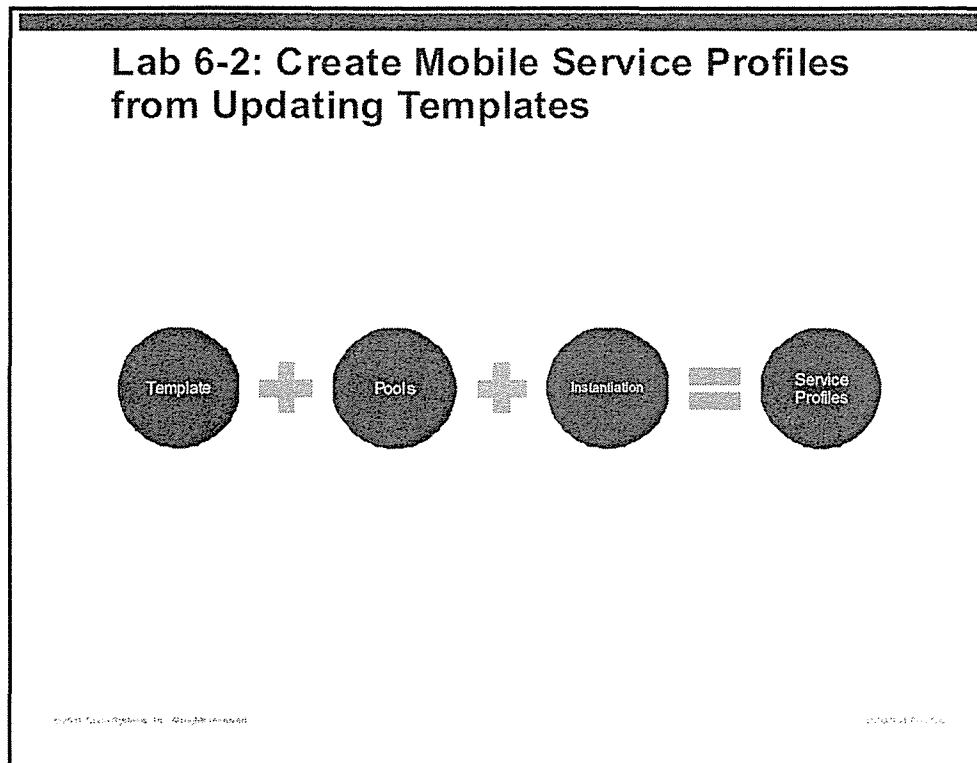
Complete this lab activity to practice what you learned in the related lesson.

Activity Objective

In this activity, you will configure service profile templates to generate service profiles from the templates. All service profiles will use servers and identities that are pulled from pools.

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required to complete this activity:

- Student PC
- Lab implementation sheet
- Lab reference guide

Lab 6-2 Mobile Service Profiles Implementation Sheet

Use this implementation sheet to aid in the configuration tasks in Lab 6-2.

Task 1 Create vNIC and vHBA Templates for Your Organization

Pod	Org	vNIC-A Name	vNIC-B Name	vHBA-A Name	vHBA-B Name
1	Boston	BOS_vNIC-A	BOS_vNIC-B	BOS_vHBA-A	BOS_vHBA-B
2	Chicago	ORD_vNIC-A	ORD_vNIC-B	ORD_vHBA-A	ORD_vHBA-B
3	Dallas	DFW_vNIC-A	DFW_vNIC-B	DFW_vHBA-A	DFW_vHBA-B
4	Miami	MIA_vNIC-A	MIA_vNIC-B	MIA_vHBA-A	MIA_vHBA-B
5	New-York	JFK_vNIC-A	JFK_vNIC-B	JFK_vHBA-A	JFK_vHBA-B
6	San-Francisco	SFO_vNIC-A	SFO_vNIC-B	SFO_vHBA-A	SFO_vHBA-B

Task 2 Create a Service Profile Template for Your Organization

Pod	Org	Template	Boot WWPN Pri	Boot WWPN Sec	LUN
1	Boston	BOS_Template	50:06:01:60:3b:a0:07:c9	50:06:01:68:3b:a0:07:c9	0
2	Chicago	ORD_Template	50:06:01:60:3b:a0:07:c9	50:06:01:68:3b:a0:07:c9	0
3	Dallas	DFW_Template	50:06:01:60:3b:a0:07:c9	50:06:01:68:3b:a0:07:c9	0
4	Miami	MIA_Template	50:06:01:60:3b:a0:08:ed	50:06:01:68:3b:a0:08:ed	0
5	New-York	JFK_Template	50:06:01:60:3b:a0:08:ed	50:06:01:68:3b:a0:08:ed	0
6	San-Francisco	SFO_Template	50:06:01:60:3b:a0:08:ed	50:06:01:68:3b:a0:08:ed	0

Task 4 Create IPMI Policy

Pod	Policy Name	IPMI Username	IPMI Password
1	BOS_IPMI	BOS_IPMI	Qwer12345
2	ORD_IPMI	ORD_IPMI	Qwer12345
3	DFW_IPMI	DFW_IPMI	Qwer12345
4	MIA_IPMI	MIA_IPMI	Qwer12345
5	JFK_IPMI	JFK_IPMI	Qwer12345
6	SFO_IPMI	SFO_IPMI	Qwer12345

Task 3 Create a Service Profile from the Updating Template

Pod	Org	Service Profile Prefix	Number
1	Boston	BOS_SP	1
2	Chicago	ORD_SP	1
3	Dallas	DFW_SP	1
4	Miami	MIA_SP	1
5	New-York	JFK_SP	1
6	San-Francisco	SFO_SP	1

Task 4 Install VMware ESXi 4.1 on Fibre Channel LUN

Pod	ESXi Hostname	IP Address	Gateway	VLAN
1	p1-b-esx-dc.cisco.com	192.168.110.21/24	192.168.110.1	110
2	p2-b-esx-dc	192.168.110.22/24	192.168.110.1	110
3	p3-b-esx-dc	192.168.110.23/24	192.168.110.1	110
4	p4-b-esx-dc	192.168.110.24/24	192.168.110.1	110
5	p5-b-esx-dc	192.168.110.25/24	192.168.110.1	110
6	p6-b-esx-dc	192.168.110.26/24	192.168.110.1	110

Task 1: Create vNIC and vHBA Templates for Your Organization

In this task, you will configure updating vNIC and vHBA templates that leverages the pooled resources, identities, and policies that you created in Lab 6-1.

Activity Procedure

Complete these steps:

- Step 1** In Cisco UCS Manager, choose the **LAN** tab and expand **Policies > Root > Sub-Organizations > Hypothetical-Inc > Sub-Organizations > Your Organization**.
- Step 2** Right-click **vNIC Templates** and choose **Create vNIC Template**.
- Step 3** Name the template, based on the vNIC-A name in the resource sheet.
- Step 4** Choose the **Fabric A** radio button.
- Step 5** Check the **Enable Failover** check box.
- Step 6** Set the Template Type to **Updating Template**.
- Step 7** Choose the five pod-specific Control, Management, Packet, vMotion and vmTraffic VLANs that you created in Lab 6-1.
- Step 8** Choose your pod-specific MAC Pool and QoS Policy from the drop-down menus.

Step 9 Click the **OK** button to complete the wizard.

Create vNIC Template

Name: BOS_vNIC-A

Description:

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

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, it will be overwritten.

Template Type: ☐ Initial Template ☐ Updating Template

Select	Name	Native VLAN
☒	BOS-Control	
☒	BOS-Management	
☒	BOS-Packet	
☒	BOS-Motion	

Create VLAN

MTU: 1500

MAC Pool: BOS_MAC

QoS Policy: BOS_QoS

OK Cancel

- Step 10 Repeat Steps 2 through 9 to create the vNIC-B template. This time, choose the **Fabric B** radio button.
- Step 11 In Cisco UCS Manager, choose the SAN tab and expand **Policies > Root > Sub-Organizations > Hypothetical-Inc > Sub-Organizations > Your Organization**.
- Step 12 Right-click **vHBA Templates** and choose **Create vHBA Template**.
- Step 13 Name the template, based on the vHBA-A name in the resource sheet.
- Step 14 Choose the **Fabric A** radio button.
- Step 15 Set the Template Type to **Updating Template**.
- Step 16 Choose **VSAN 11** from the Select VSAN drop-down list.
- Step 17 Choose your pod-specific WWPN Pool from the drop-down menu.
- Step 18 Click the **OK** button to complete the wizard.

Create vHBA Template

Name: BOS-vHBA-A

Description:

Fabric ID: ☐ A ☐ B

Select VSAN: vsan11

Template Type: ☐ Initial Template ☒ Updating Template

Max Data Field Size: 2048

WWPN Pool: BOS_WWPN

OK Cancel

- Step 19 Repeat steps 12 through 18 to create the vHBA template for Fabric B. Fabric B uses VSAN 12.

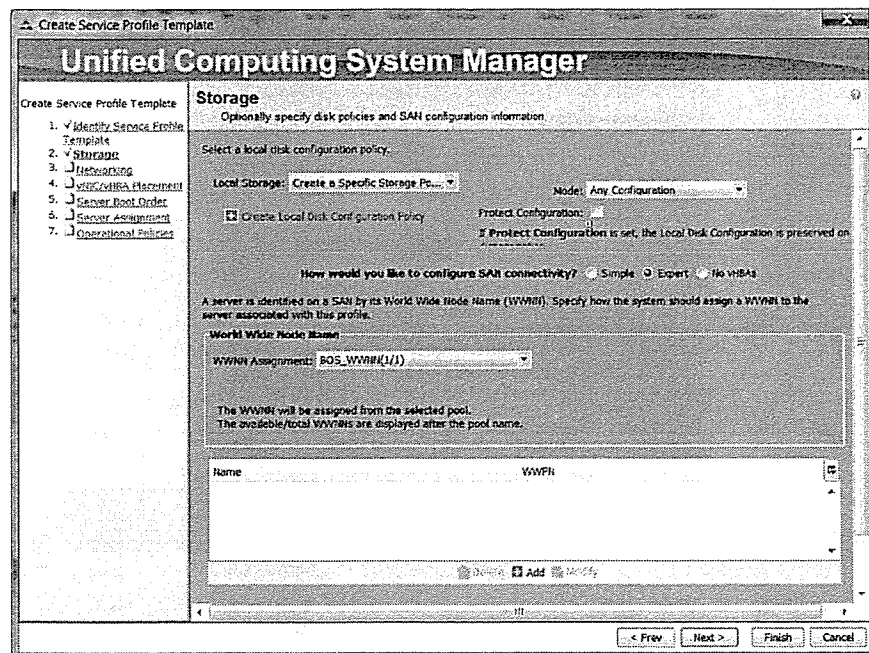
Task 2: Create a Service Profile Template for Your Organization

In this task, you will configure an updating service profile template that leverages the pooled resources and identities that you created in Lab 6-1.

Activity Procedure

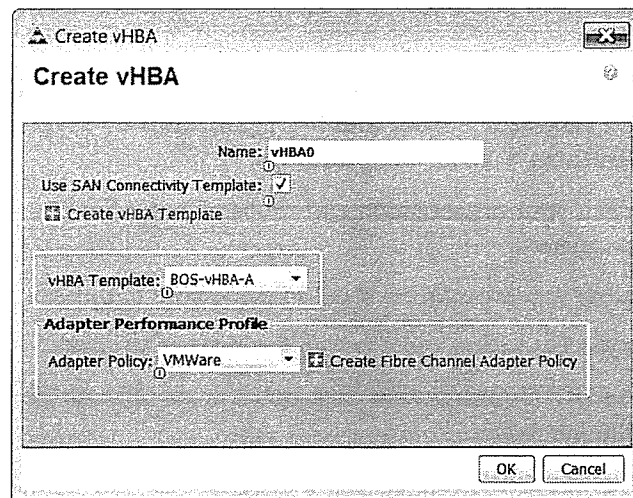
Complete these steps:

- Step 1** In Cisco UCS Manager, choose the **Servers** tab and expand **Servers > Service Profile Templates > Root > Sub-Organizations > Hypothetical-Inc > Sub-Organizations > Your Organization**.
- Step 2** Right-click your organization and choose **Create Service Profile Template** from the pop-up menu.
- Step 3** Use the lab implementation sheet to name your template.
- Step 4** Choose the **Updating** radio button for Type of template.
- Step 5** From the UUID Assignment drop-down menu, choose the UUID pool that you created in lab 6-1.
- Step 6** Click **Next** to continue.
- Step 7** From the Local Storage drop-down menu, choose **Create a Specific Storage Policy**.
- Step 8** Uncheck the **Protect Configuration** check box. If this step is skipped, service profile association might fail.
- Step 9** Choose the **Expert** radio button for configuring SAN connectivity.
- Step 10** In the World Wide Node Name drop-down menu, choose the WWNN pool that you created in Lab 6-1.

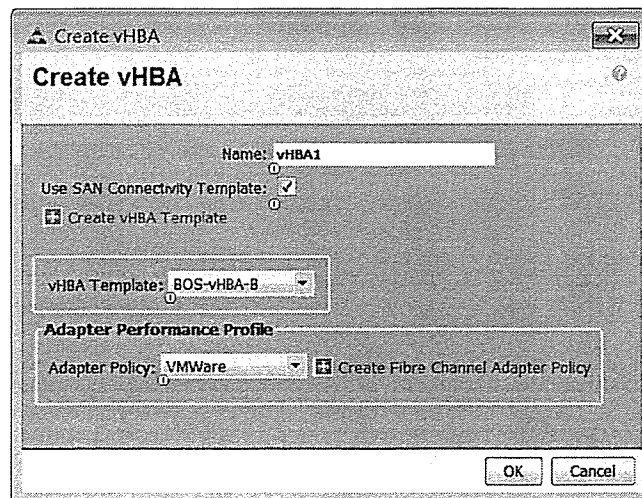


- Step 11** Click the plus symbol (+) to create the vHBA for fabric A.
- Step 12** Name the first vHBA **vHBA0**.

- Step 13** Check the **Use SAN Connectivity Template** check box and choose your pod-specific vHBA template for fabric A.
- Step 14** Choose **VMWare** from the Adapter Policy drop-down menu.
- Step 15** Click **OK** to save the vHBA definition.

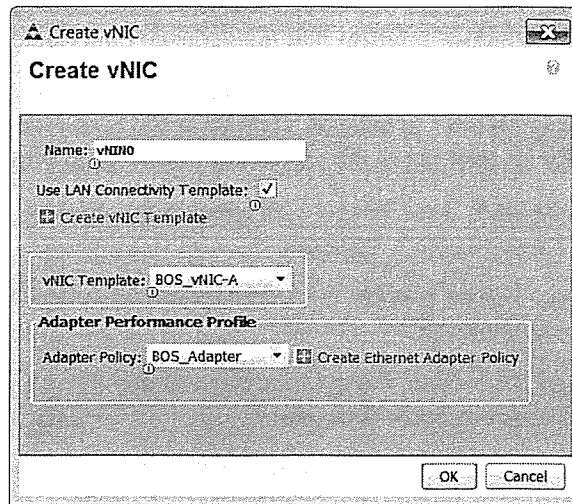


- Step 16** Click the plus symbol (+) to create the vHBA for fabric B.
- Step 17** Name the second vHBA **vHBA1**.
- Step 18** Click the **Use SAN Connectivity Template** check box and choose your pod-specific vHBA template for fabric B.
- Step 19** Choose **VMWare** from the **Adapter Policy** drop-down menu.
- Step 20** Click **OK** to save the vHBA definition.

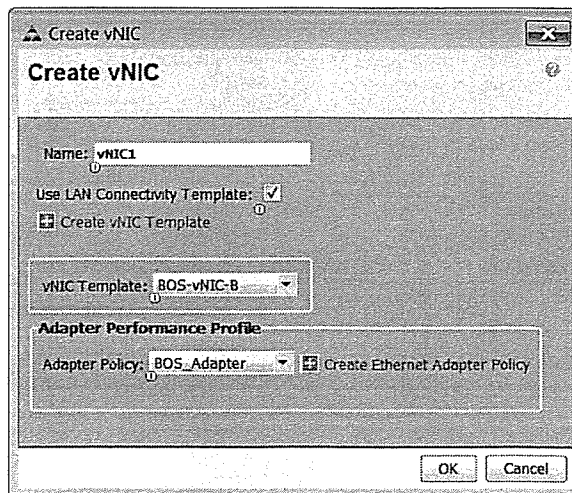


- Step 21** Click **Next** to continue.
- Step 22** Leave the Dynamic vNIC policy at default.
- Step 23** Choose the **Expert** radio button to configure networking.
- Step 24** Click the plus symbol (+) to create the first vNIC.
- Step 25** Name the vNIC **vNIC0**.

- Step 26 Check the **Use LAN Connectivity Template** check box.
- Step 27 Choose the pod-specific **vNIC Template** from the drop-down menu.
- Step 28 Choose the pod-specific **Adapter Policy** from the drop-down menu.

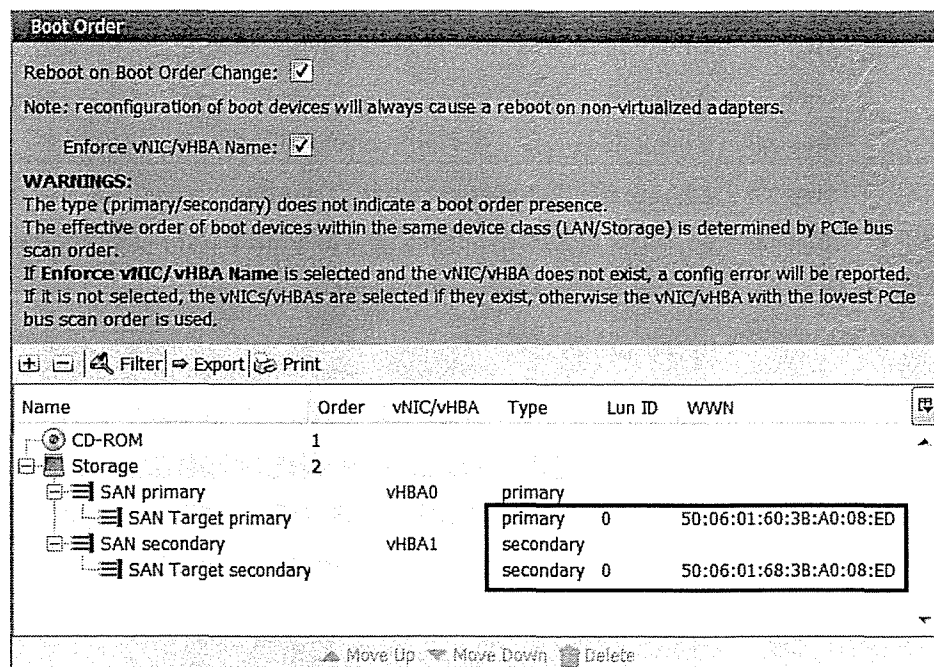


- Step 29 Click **OK** to commit the configuration.
- Step 30 Click the plus symbol (+) to create the second vNIC.
- Step 31 Name the vNIC **vNIC1**.
- Step 32 Check the **Use LAN Connectivity Template** check box.
- Step 33 Choose the pod-specific **vNIC Template** from the drop-down menu.
- Step 34 Choose the pod-specific **Adapter Policy** from the drop-down menu.



- Step 35 Click **OK** to commit the configuration.
- Step 36 Click **Next** to continue.
- Step 37 On the vNIC/vHBA Placement screen, accept the defaults and click **Next** to continue.
- Step 38 From the Boot Policy drop-down menu, choose **Create Specific Boot Policy**.
- Step 39 Check the check box to the right of **Reboot on Boot Order Change**.

- Step 40** Check the check box to the right of **Enforce vNIC/vHBA Name**.
- Step 41** In the Local Devices panel, click **Add CD-ROM** to put it at the top of the boot order.
- Step 42** In the vHBAs panel, click and drag **vHBA0** beneath the CD-ROM in the boot order.
- Step 43** In the pop-up window, confirm that the Primary radio button is selected, and then click **OK**.
- Step 44** Click and drag **vHBA1** to beneath vHBA0 in the boot order. vHBA1 will automatically be selected as the secondary. There is no pop-up menu.
- Step 45** Click the **Add SAN Boot Target** link beneath the vHBAs panel and choose **Add SAN Boot Target to SAN Primary**.
- Step 46** Enter the Boot Target WWPN Pri and LUN ID, according to the lab implementation sheet, and then click **OK**.
- Step 47** Click the **Add SAN Boot Target** link beneath the vHBAs panel and choose **Add SAN Boot Target to SAN Secondary**.
- Step 48** Enter the Boot Target WWPN Sec and LUN ID, according to the lab implementation sheet, click the **Secondary** radio button, and then click **OK**.
- Step 49** Your boot order should appear similar to the figure.



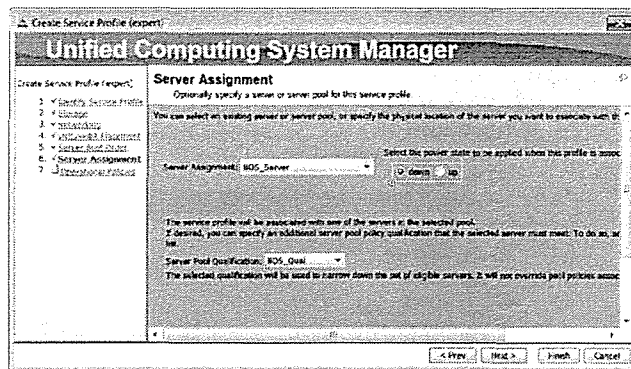
Note The boot target WWPNs and LUN IDs are pod-specific. Enter these values carefully.

Step 50 Click **Next** to continue.

Step 51 On the Server Assignment screen, choose your server pool from the Pool Assignment drop-down list.

Step 52 Choose your server qualification policy from the Server Pool Qualification drop-down list.

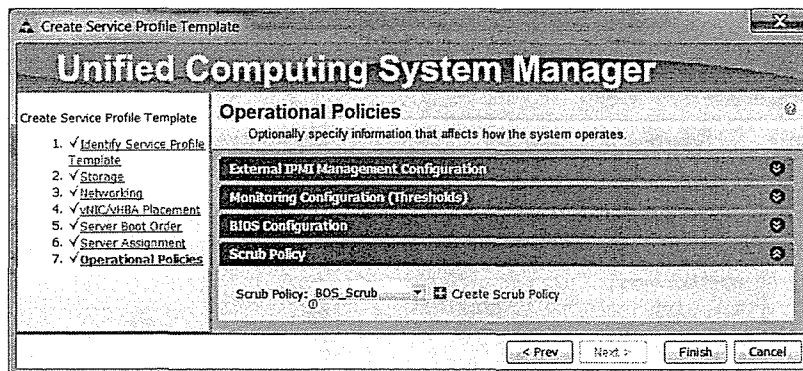
Step 53 Set the power state radio button to **Down**.



Step 54 Click **Next** to continue.

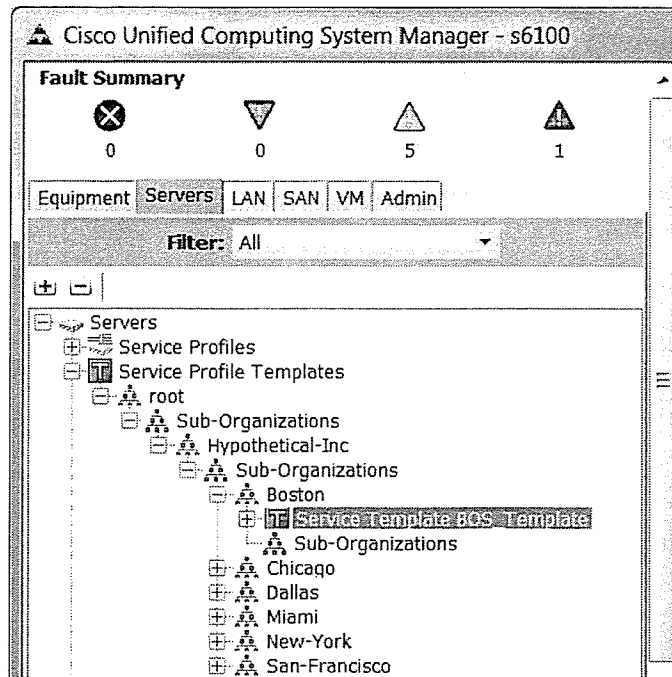
Step 55 In the Operational Policies screen, click the double down-arrow icon to expand Scrub Policy.

Step 56 Choose your scrub policy from the drop-down list.



Step 57 Click **Finish** to complete your service profile template.

Step 58 Your completed service profile template will appear beneath your organization.



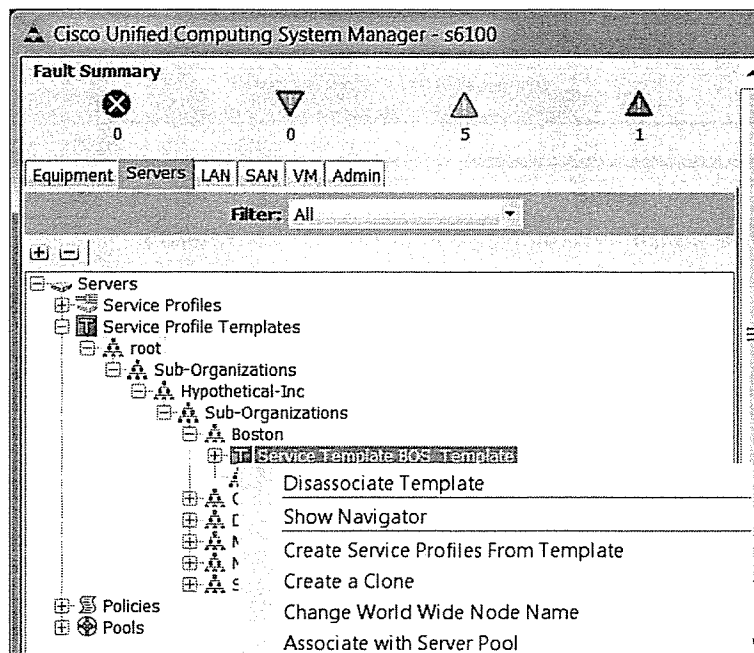
Task 3: Create a Service Profile from the Updating Template

In this task, you will spawn a service profile from the service profile template that you created in Task 1.

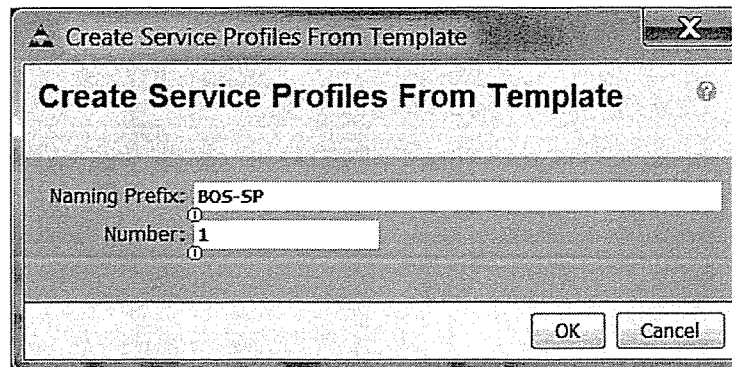
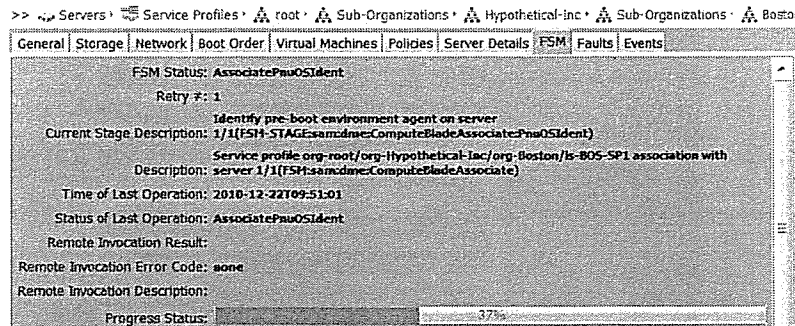
Activity Procedure

Complete these steps:

Step 1 Right-click your service profile template and choose **Create Service Profiles From Template**.



- Step 2 In the pop-up box, enter the name from the lab implementation sheet.
- Step 3 Click **OK** to generate the new service profile.
- Step 4 On the Servers tab, expand **Servers > Service Profiles > Root > Sub-Organizations > Hypothetical-Inc > Sub-Organizations > Your Organization**.
- Step 5 Click the service profile name in the navigation pane. In the content pane, click the **FSM** tab.
- Step 6 Observe the process of service profile association. This process should take about 5 minutes to reach 100 percent.



- Step 7 In the content pane, click the **General** tab, and validate your server indicates power-off in the Status area.

Task 4: Add IPMI Policy to Updating Template

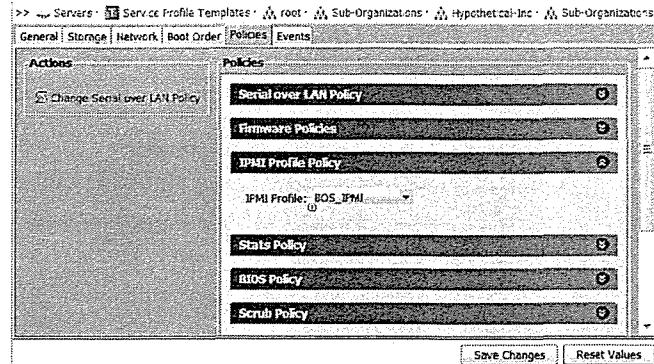
In this task, you will add an IPMI policy to your service profile template and observe the policy as it is pushed out to your service policy.

Activity Procedure

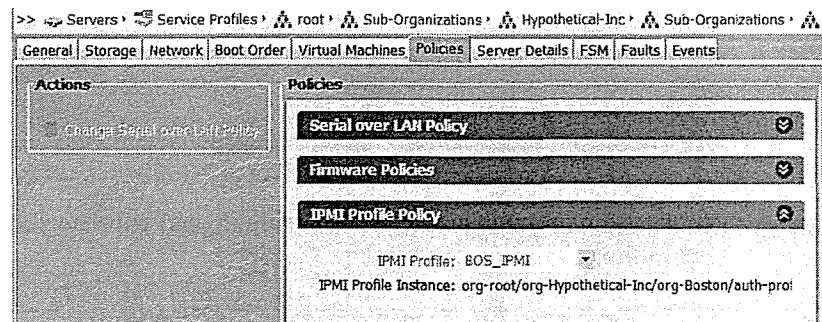
Complete these steps:

- Step 1 On the Servers tab, expand **Servers > Policies > Root > Sub-Organizations > Hypothetical-Inc > Sub-Organizations > Your Organization**.
- Step 2 Right-click the **IPMI Profiles** element and choose **Create IPMI Profile**.
- Step 3 Use the implementation sheet to name the new IPMI profile.
- Step 4 Click the plus symbol (+) and create a new user and password that are based on the implementation sheet.

- Step 5** Click **OK** to save the new IPMI profile for your organization.
- Step 6** On the **Servers** tab, expand **Servers > Service Profile Templates > Root > Sub-Organizations > Hypothetical-Inc > Sub-Organizations > Your Organization**.
- Step 7** Click your service profile template name in the navigation pane.
- Step 8** In the content pane, click the **Policies** tab.
- Step 9** Click the double down-arrow icon to the right of **IPMI Profile Policy** and choose your newly created profile from the drop-down list.
- Step 10** Click **Save Changes** to commit the configuration change to the service profile template.



- Step 11** On the **Servers** tab, expand **Servers > Service Profiles > Root > Sub-Organizations > Hypothetical-Inc > Sub-Organizations > Your Organization**.
- Step 12** Click the name of your service profile.
- Step 13** In the content pane, click the **Policies** tab and expand the **IPMI Profile Policy**. Observe that the template updated your service profile.



- Step 14** To determine the IP address that is assigned to the Cisco IMC of your server, click the **Admin** tab in the navigation pane.
- Step 15** From the Filter drop-down menu, choose **Communications Management**.
- Step 16** Click **Management IP Pool** in the navigation pane.
- Step 17** In the content pane, find the IP address that is assigned to your blade server.

>> Communication Management Management IP Pool (ext-mgmt) Management IP Pool (ext-mgmt)

General IP Addresses IP Blocks Events

Filter Export Print

IP Address	Assigned To
192.168.10.51	sys/chassis-1/blade-8/mgmt/ipv4-pooled-addr
192.168.10.52	sys/chassis-1/blade-7/mgmt/ipv4-pooled-addr
192.168.10.53	sys/chassis-1/blade-6/mgmt/ipv4-pooled-addr
192.168.10.54	sys/chassis-1/blade-5/mgmt/ipv4-pooled-addr
192.168.10.55	sys/chassis-1/blade-4/mgmt/ipv4-pooled-addr
192.168.10.56	sys/chassis-1/blade-3/mgmt/ipv4-pooled-addr
192.168.10.57	sys/chassis-1/blade-1/mgmt/ipv4-pooled-addr
192.168.10.58	sys/chassis-1/blade-2/mgmt/ipv4-pooled-addr

Step 18 On your student PC, double-click the Cygwin icon on the desktop.

Step 19 Enter the command `ipmitool -I lan -H 192.168.10.57 -U BOS_IPMI -P QWER12345 chassis status`.

Note The example is based on pod 1 (Boston). To correctly execute this command, replace the IP address in the command with the management IP address from Step 17.

Step 20 Notice that the command returned an error. The user was granted insufficient privileges in the IPMI profile.

```
Administrator@Pod-1-desktop ~
$ ipmitool -I lan -H 192.168.10.57 -U BOS_IPMI -P QWER12345 chassis status
Activate Session error: Requested privilege level exceeds limit
Error: Unable to establish LAN session
Error sending Chassis Status command

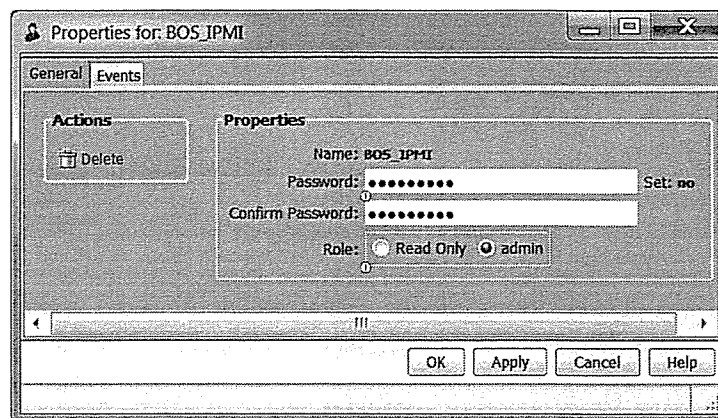
Administrator@Pod-1-desktop ~
$
```

Step 21 In the Servers tab, expand **Servers > Policies > Root > Sub-Organizations > Hypothetical-Inc > Sub-Organizations > Your Organization**.

Step 22 Click your IPMI profile in the navigation pane. In the content pane, choose your IPMI user and then click **Modify** (just beneath the trash icon).

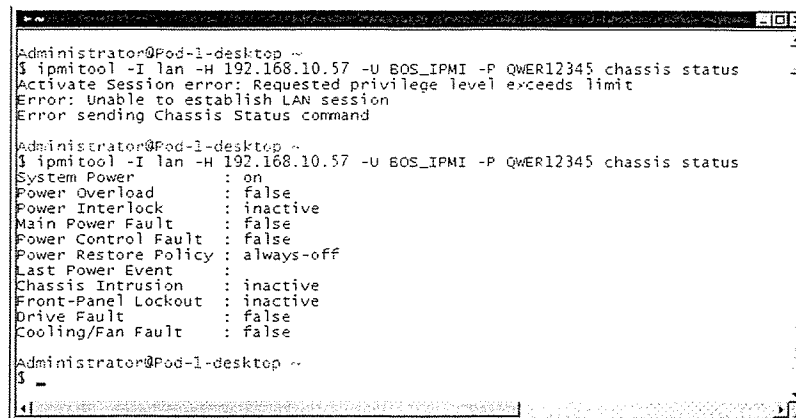
Step 23 Change the Role radio button to **admin** and re-enter the password **QWER12345**.

Step 24 Click **Apply** and then click **OK** to commit the change.



Step 25 Retry the `ipmitool` command on your student PC. This time the command should work correctly.

Note The IPMI policy updated the template, which in turn dynamically updated any service profiles that were created from that template. Updating templates can greatly reduce administrative overhead that is associated with adding or modifying a policy on many service profiles.



```
Administrator@Pod-1-desktop ~  
$ ipmitool -I lan -H 192.168.10.57 -U BOS_IPMI -P QWER12345 chassis status  
Activate Session error: Requested privilege level exceeds limit  
Error: Unable to establish LAN session  
Error sending Chassis Status command  
  
Administrator@Pod-1-desktop ~  
$ ipmitool -I lan -H 192.168.10.57 -U BOS_IPMI -P QWER12345 chassis status  
System Power : on  
Power Overload : false  
Power Interlock : inactive  
Main Power Fault : false  
Power Control Fault : false  
Power Restore Policy : always-off  
Last Power Event :  
Chassis Intrusion : inactive  
Front-Panel Lockout : inactive  
Drive Fault : false  
Cooling/Fan Fault : false  
  
Administrator@Pod-1-desktop ~  
$
```

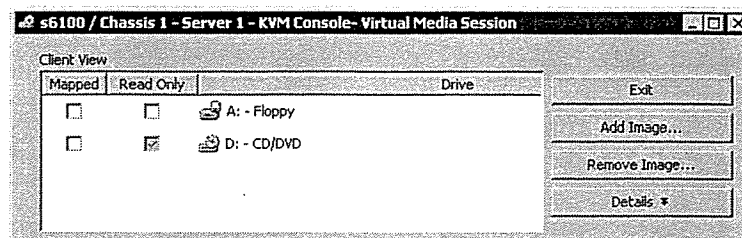
Task 5: Install VMware ESXi 4.1 on Fibre Channel LUN

In this task, you will validate your Service Profile configuration by installing and SAN booting VMware ESXi 4.1.

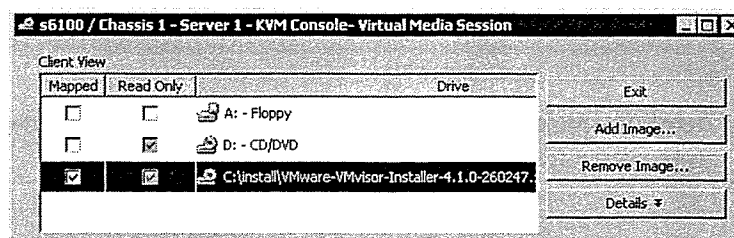
Activity Procedure

Complete these steps:

- Step 1** On the Servers tab in the Navigation pane, click your service profile.
- Step 2** Click the **KVM Console** link to open a KVM window.
- Step 3** In the KVM console, click the **Tools** menu and choose **Launch Virtual Media**.
- Step 4** When the Virtual Media dialog box opens, click the **Add Image** button. Navigate to **c:\install** and choose the file **VMware-VMvisor-Installer-4.1.0.update1-348481.x86_64.iso**.

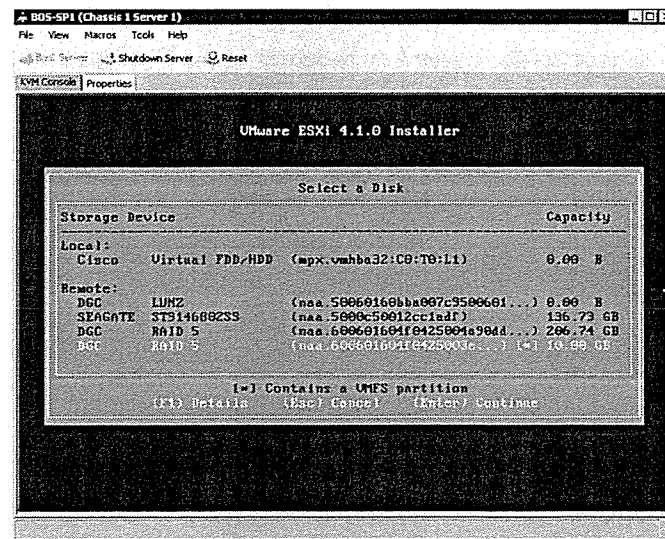


- Step 5** When the new virtual device appears, click the check box under the **Mapped** column. The ISO file now appears as a physical DVD to the server.



- Step 6** In the Actions panel of the UCS manager content pane, click the **Boot Server** link to boot the server.
- Step 7** When the Cisco BIOS screen appears, press the **Esc** key to enable viewing POST messages.
- Step 8** In about 2 minutes, the VMware ESXi boot menu will appear. Either wait 6 seconds for the installer to load automatically, or press the **Enter** key.
- Step 9** The installer will take about 2 minutes to load. Press the **Enter** key to begin installation.
- Step 10** On the EULA page, press the **F11** key to proceed.
- Step 11** At the Select a Disk screen, choose the 10 GB LUN. There might be an existing partition on the 10 GB LUN from a previous install. Press the **Enter** key to confirm overwriting the existing partition.

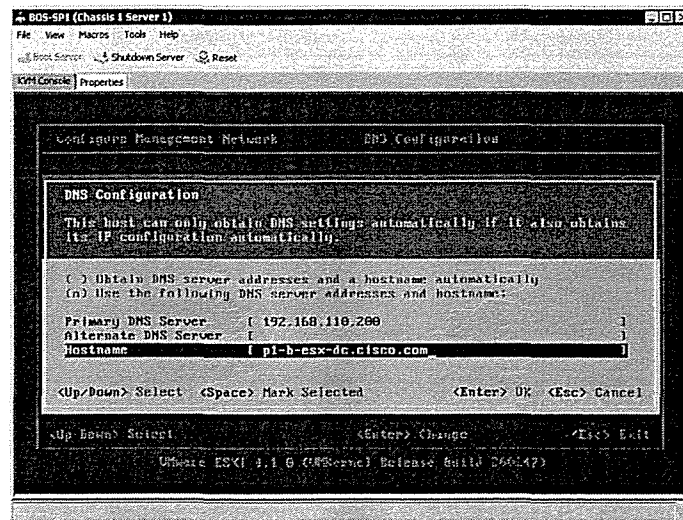
Note If you do not see the 206 GB and 10 GB LUNs, alert your instructor.



Note The 206 GB LUN is VMFS shared storage for vMotion. Do not choose the 206 GB LUN.

- Step 12** At the Confirm Install screen, press the **F11** key.
- Step 13** When the installation is complete, the installer prompts you to press the **Enter** key and remove installation media. The KVM Virtual Media automatically unmaps the ESXi ISO image.
- Step 14** In about 3 minutes, you should see the hypervisor loading. When the ESXi home screen appears, press **F2** to begin configuring the hypervisor.
- Step 15** At the authentication screen, press the **Enter** key. The password is initially null for the root user.
- Step 16** The Change Password element is selected on the System Configuration screen.
- Step 17** Press the **Enter** key to change the default password. Enter **Qwer12345** in the New Password and Confirm Password fields and then press the **Enter** key. This action will return you to the System Configuration screen

- Step 18** Press the down-arrow key to choose the **Configure Management Network** element and then press the **Enter** key.
- Step 19** Press the down-arrow key to choose **Network Adapters** and press the **Enter** key. Use the spacebar to choose both network adapters and then press the **Enter** key to return to System Configuration.
- Step 20** Press the down-arrow key to choose **VLAN (optional)** and press the **Enter** key. Enter the VLAN value from the lab configuration sheet and press the **Enter** key to return to System Configuration.
- Step 21** Press the down-arrow key to choose **IP Configuration** and press the **Enter** key.
- Step 22** Press the down-arrow key to choose **Set Static IP Address and Network Configuration** and press the spacebar to enable that option.
- Step 23** Use the lab configuration sheet to enter your pod-specific IP address, subnet mask, and default gateway, and then press the **Enter** key to return to the Configure Management Network screen.
- Step 24** Press the down-arrow key to choose **DNS Configuration** and press the **Enter** key.
- Step 25** Enter **192.168.110.200** as your primary DNS server. Use the down-arrow key to choose Hostname. Enter the pod-specific hostname from the lab configuration sheet, and then press the **Enter** key to return to the Configure Management Network screen.



- Step 26** Press the **Esc** key to exit configuration of the management network.
- Step 27** Press the **Y** key to accept the management network configuration.
- Step 28** Press the down-arrow key to choose the **Test Management Network** element on the System Configuration screen.
- Step 29** On the Test Management Network screen, press the **Enter** key. You should see OK as the result code from pinging the default gateway, DNS server, and test resolution of the ESXi server hostname. If any of the tests fails, contact your instructor.

Activity Verification

You have completed this activity when you have achieved these goals:

- You have created a service profile template that is based on pools that were created under the pod that is assigned to your organization.

- You have generated a service profile from an updating template and observed the association process.
- You have added an IPMI policy to your template and observed that the policy was dynamically added to the service profile.
- You have installed, SAN booted, and configured VMware ESXi.

Lab 7-1: Create a Data-Center Cluster in VMware vCenter

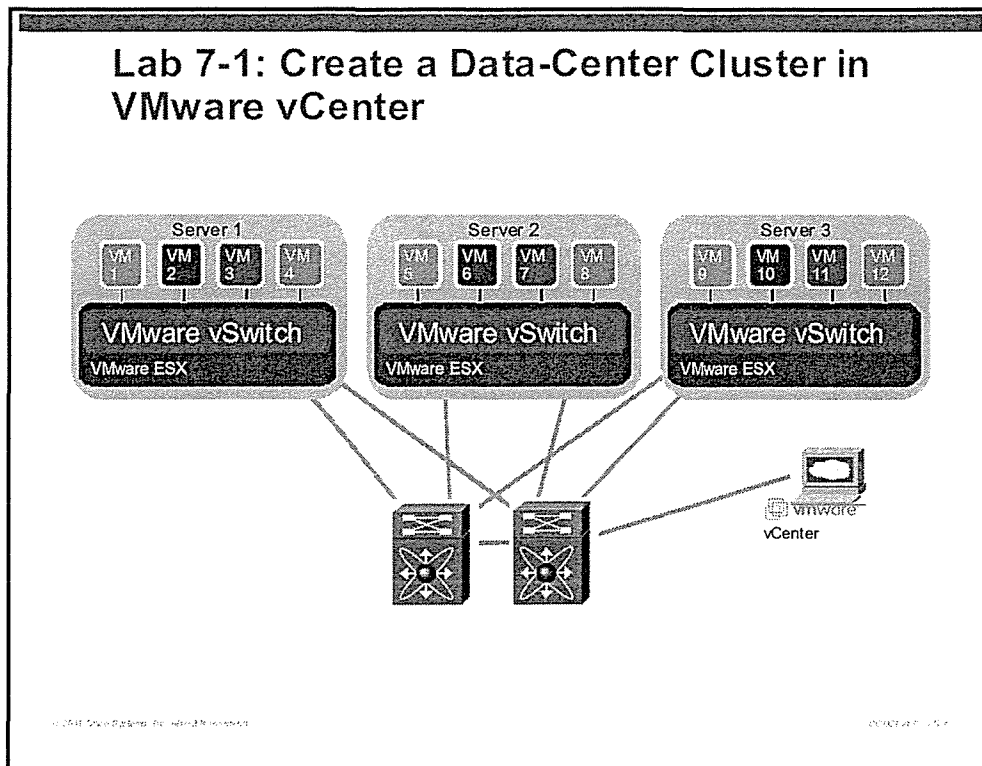
Complete this lab activity to practice what you learned in the related lesson.

Activity Objective

In this activity, you will build a data-center cluster in vCenter to prepare for the installation of Cisco Nexus 1000V in Lab 7-2.

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required to complete this activity:

- Student PC
- Lab resource sheet
- Lab reference guide

Lab 7-1: Create a Data-Center Cluster in VMware vCenter Implementation Sheet

Use this implementation sheet to aid in the configuration tasks in Lab 7-1.

Task 1 Attach to B200 ESXi Server and Import VMs

Pod	ESXi Host	Service Profile	vCenter VM	Windows 2008 VM
1	p1-b-esx-dc	BOS-SP1	vCenter-1	Win2008-1
2	p2-b-esx-dc	ORD-SP1	vCenter-2	Win2008-2
3	p3-b-esx-dc	DFW-SP1	vCenter-3	Win2008-3
4	p4-b-esx-dc	MIA-SP1	vCenter-4	Win2008-4
5	p5-b-esx-dc	JFK-SP1	vCenter-5	Win2008-5
6	p6-b-esx-dc	SFO-SP1	vCenter-6	Win2008-6

Tasks 2 and 3 Create VMware Data Centers with Two ESXi Servers

Pod	Data Center	vCenter Server	B200 Host	C200 Host
1	DC-1	vCenter-1	p1-b-esx-dc	p1-c-esx-dc
2	DC-2	vCenter-2	p2-b-esx-dc	p2-c-esx-dc
3	DC-3	vCenter-3	p3-b-esx-dc	p3-c-esx-dc
4	DC-4	vCenter-4	p4-b-esx-dc	p4-c-esx-dc
5	DC-5	vCenter-5	p5-b-esx-dc	p5-c-esx-dc
6	DC-6	vCenter-6	p6-b-esx-dc	p6-c-esx-dc

Task 5 Configure vSwitch and Test vMotion

Pod	Data Center	MGMT	vMotion	vmTraffic	Windows 2008
1	DC-1	110	311	411	192.168.41.10/24
2	DC-2	110	312	412	192.168.42.10/24
3	DC-3	110	313	413	192.168.43.10/24
4	DC-4	110	314	414	192.168.44.10/24
5	DC-5	110	315	415	192.168.45.10/24
6	DC-6	110	316	416	192.168.46.10/24

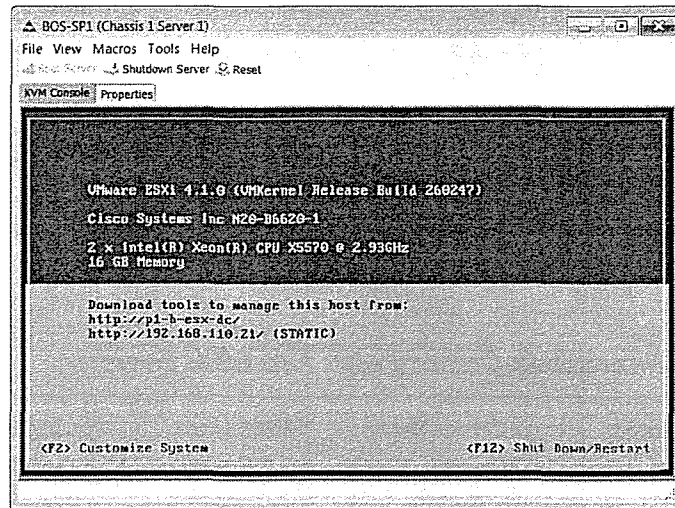
Task 1: Import the vCenter VM

In this task, you will import a vCenter VM into your B-200 ESXi host.

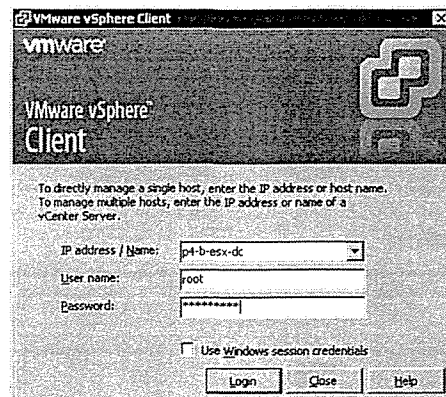
Activity Procedure

Complete these steps:

- Step 1** In Cisco UCS Manager, choose the service profile for your pod, as listed in the implementation sheet.
- Step 2** In the Content pane, click the **Boot Server** link.
- Step 3** Click the **KVM Console** link and wait until you see that ESXi has fully booted.



- Step 4** From your student PC desktop, double-click the **VMware vSphere Client** and connect to your B200 hostname, as indicated in the implementation sheet. Authenticate with user **root** and password **Qwer12345**.



- Step 5** If you receive a certificate warning, click the **Install the Certificate** check box, and then click the **Ignore** button.
- Step 6** Click the **OK** button to ignore the Evaluation License warning.
- Step 7** In the Content pane, choose the **Configuration** tab.
- Step 8** In the Hardware panel, click the **Storage** link.

- Step 9 In the Datastores list, right-click the **VM_Storage** datastore and choose **Browse Datastore**.
- Step 10 Click your pod-specific vCenter VM. In the file listing to the right, right-click the .vmx file and choose **Add to Inventory**.
- Step 11 When the Add to Inventory wizard appears, click the **Next** button to accept the default name.
- Step 12 On the Resource Pool screen, click the **Next** button to choose your ESXi server host.

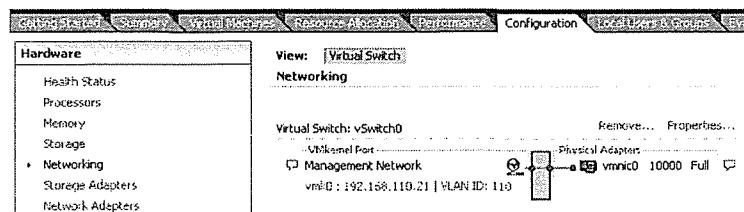
Task 2: Add Port Profile for vCenter Networking and Attach to vCenter

In this task, you will create and bind a port profile to allow external communications to your vCenter server.

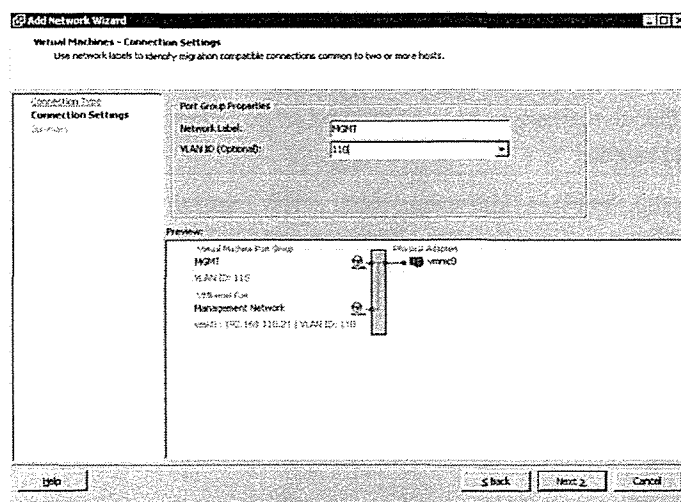
Activity Procedure

Complete these steps:

- Step 1 Choose your B-Series ESXi host in the vSphere Client Navigation pane.
- Step 2 In the Content pane, choose the **Configuration** tab.
- Step 3 In the Hardware panel, click the **Networking** link.

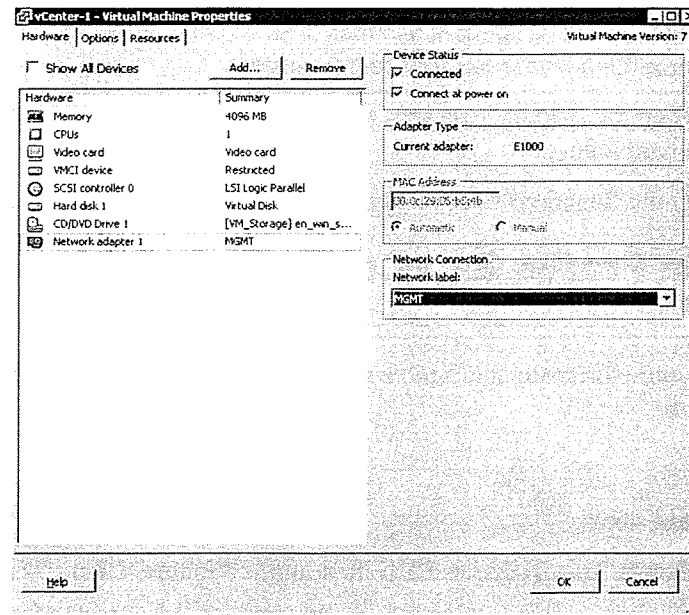


- Step 4 Click the blue **Properties** link to edit the vSwitch. In the vSwitch0 Properties window, click the **Add** button.
- Step 5 At the Connection Type screen, click the **Next** button to leave the Connection Type as Virtual Machine.
- Step 6 All pods should enter **MGMT** in the Network Label field and **VLAN 110** in the VLAN ID field, and then click the **Next** button.



- Step 7 On the final screen of the wizard, review the changes you made and then click the **Finish** button.

Step 8 Right-click your B-Series ESXi host and choose **Edit Settings**.



Step 9 Click **Network Adapter 1** and choose **MGMT** from the drop-down menu, and then click the **OK** button.

Task 3: Start the vCenter VM and Validate Services

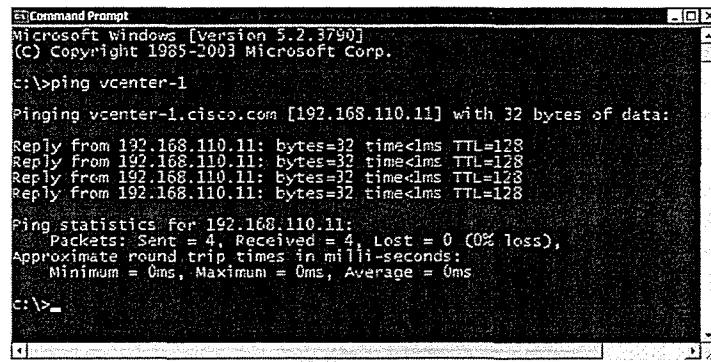
In this task, you will import and power on your vCenter VM on your B-200 ESXi host.

Activity Procedure

Complete these steps:

- Step 1** Right-click the vCenter VM and choose **Power > Power On**.
- Step 2** In the Content pane, click the **Console** tab to observe the VM booting.
- Step 3** Click in the console window and press **Ctrl-Alt-Insert** to bring up the login window.
- Step 4** Login as **administrator** with password **Qwer12345**.
- Step 5** On the vCenter desktop, right-click **My Computer** and then click **Manage**.
- Step 6** Click the plus symbol (+) to the left of **Services and Applications**, and then click **Services**.
- Step 7** In the Services list to the right, verify that the **VMware vCenter Update Manager**, **VMware VirtualCenter Management Webservices**, and **VMware VirtualCenter Server** services are running. If not, you might need to manually start them.
- Step 8** Close the vSphere client. You will now interact primarily with the vCenter server.

- Step 9** From your student PC desktop, ping your vCenter server.



```
Microsoft Windows [version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

c:\>ping vcenter-1

Pinging vcenter-1.cisco.com [192.168.110.11] with 32 bytes of data:

Reply from 192.168.110.11: bytes=32 time<1ms TTL=128
Reply from 192.168.110.11: bytes=32 time<1ms TTL=128
Reply from 192.168.110.11: bytes=32 time<1ms TTL=128
Reply from 192.168.110.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.110.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

c:\>
```

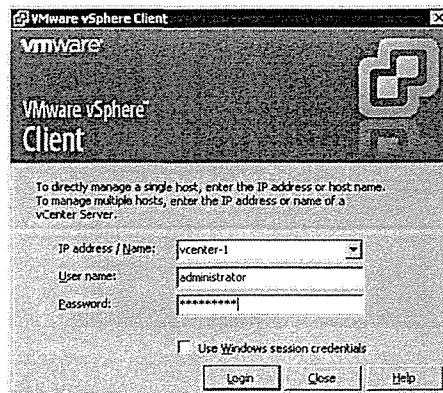
Task 4: Create a New Data Center and Add ESXi Hosts and VMs

In this task, you will create a new data center in vCenter and import your ESXi hosts and Windows 2008 VM.

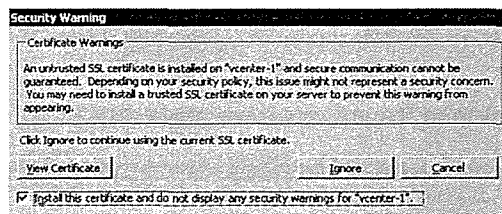
Activity Procedure

Complete these steps:

- Step 1** From your student PC desktop, double-click the **VMware vSphere Client** and connect to your pod-specific vCenter hostname, as indicated in the implementation sheet. Authenticate with user **administrator** and password **Qwer12345**.

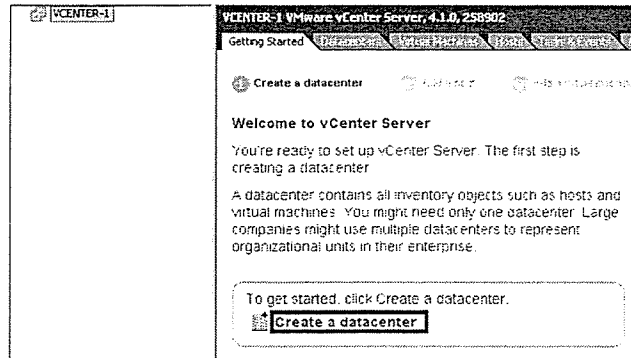


In the Security Warning dialog box, click the **Install the Certificate and Do Not Display Any Security Warnings** check box to install the certificate, and then click the **Ignore** button to continue.



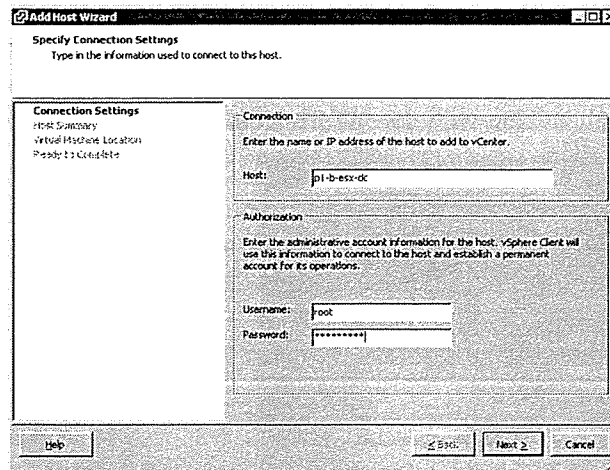
- Step 2** Click the **OK** button on the Evaluation License warning.
- Step 3** In the Getting Started tab of the vCenter content pane, click the **Create Datacenter** link.

Step 4 Name your data center, based on the lab implementation sheet.



Step 5 Click the new data center in the vCenter navigation pane, and then click the **Add a Host** link in the content pane.

Step 6 Enter the pod-specific hostname of your B-Series ESXi host, user **root** and password **Qwer12345**.



Step 7 Click the **Yes** button in the Security Alert dialog box to accept, and then click the **Next** button.

Step 8 On the Host Information screen, verify that the hostname being imported is correct, and then click the **Next** button.

Step 9 At the Assign License screen, click the **Next** button to continue using the evaluation license.

Step 10 Click the **Next** button to leave Lockdown mode disabled.

Step 11 Click the **Next** button to install the ESXi host in your data center, and then click the **Finish** button to complete the host wizard.

Step 12 You should now see your host under your data center and the vCenter VM should be visible under the ESXi host.

Step 13 Repeat Steps 5 through 12 to import your C-Series ESXi host. Refer to the lab implementation sheet to enter the hostname.

Step 14 When the C-Series host is added, choose it in the navigation pane under your data center.

- Step 15 In the content pane, choose the **Configuration** tab.
- Step 16 In the Hardware panel, click the **Storage** link.
- Step 17 In the Datastores list, right-click the blue **Refresh** link in the upper-right portion of the screen.
- Step 18 The VM_Storage datastore should now be visible.
- Step 19 In the Datastores list, right-click the **VM_Storage** datastore and choose **Browse Datastore**.
- Step 20 Click your pod-specific Windows 2008 VM. In the file listing to the right, right-click the **.vmk** file and choose **Add to Inventory**.
- Step 21 When the Add to Inventory wizard appears, click the **Next** button to accept the default name.
- Step 22 On the Host/Cluster screen, choose your C-Series ESXi host and then click the **Next** button to continue.
- Step 23 At the Ready to Complete screen, click the **Finish** button to add your vCenter server to the VM inventory of your ESXi host.

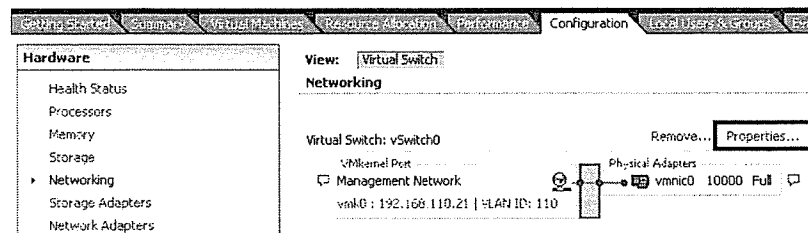
Task 5: Configure vSwitch and Test vMotion

In this task, you will create port profiles to enable networking in the virtual switch and test vMotion.

Activity Procedure

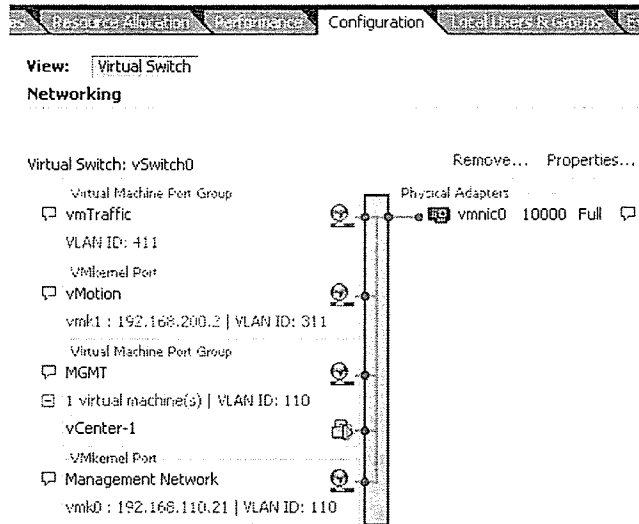
Complete these steps:

- Step 1 Choose your B-Series ESXi host in the navigation pane.
- Step 2 In the content pane, choose the **Configuration** tab.
- Step 3 In the Hardware panel, click the **Networking** link.
- Step 4 Click the blue **Properties** link to edit the vSwitch.

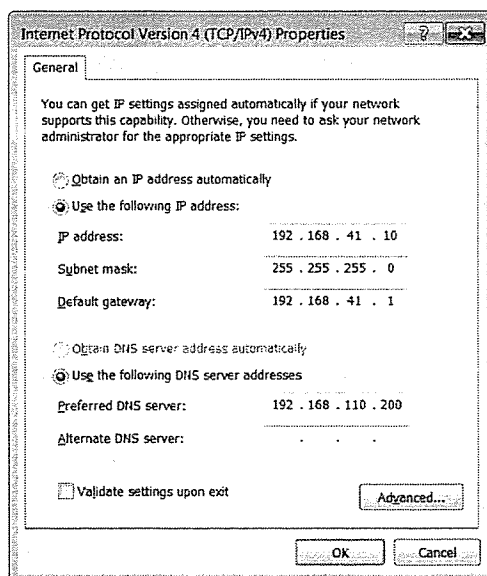


- Step 5 In the vSwitch0 properties window, click the **Add** button to add a new port profile. For the vmTraffic VLAN, choose **Virtual Machine** as the Connection Type.
- Step 6 Add port profiles for the vmTraffic and MGMT VLANs, according to the lab implementation sheet for Task 5.
- Step 7 For the vMotion port profile, be sure to use the vmKernel Connection Type and check the **Use this port group for vMotion** check box.
- Step 8 In the vmKernel – IP Settings window, all pods should use 192.168.200.2/255.255.255.0 and edit the default gateway to 192.168.200.1.

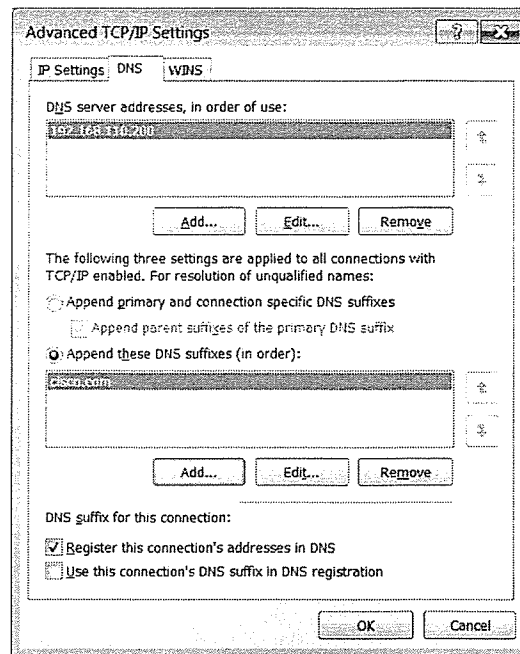
- Step 9** Repeat Steps 1 through 8 for your C-Series ESXi host. In the vmKernel – IP Settings window, all pods should use 192.168.200.3/255.255.255.0 and edit the default gateway to 192.168.200.1.
- Step 10** Your vSwitch0 configuration should closely match this figure.



- Step 11** In the vCenter navigation pane, right-click your Windows 2008 VM and choose **Edit Settings**.
- Step 12** Choose **Network Adapter 1**, then choose **vmTraffic** from the Network Connection drop-down menu, and then click the **OK** button.
- Step 13** Power on your Windows 2008 server VM.
- Step 14** Click the **Console** tab in the vCenter content pane and observe the boot process.
- Step 15** Press **Ctrl-Alt-Insert** to access the login screen. Authenticate as **administrator** with password **Qwer12345**.
- Step 16** Using the Task 5 table in the lab implementation sheet, configure the pod-specific IP address and subnet mask on your Windows 2008 server. Use .1 on your vmTraffic subnet as the default gateway. All pods should use 192.168.110.200 as the DNS server address.



- Step 17** Click the **Advanced** button.
- Step 18** Click the **Add** button to append cisco.com as a DNS suffix so that you do not have to enter an FQDN for name resolution.



- Step 19** Click the **OK** button to commit the DNS suffix configuration.
- Step 20** Click the **OK** button on the TCP/IP settings window to commit the IP configuration.
- Step 21** Open a DOS window and ping your default gateway.
- Step 22** Right-click your Windows 2008 VM in the vCenter client and choose **Migrate** from the drop-down menu.
- Step 23** In the Select Migration Type screen, choose the **Change Host** radio button and then click the **Next** button.
- Step 24** In the Select Destination screen, choose the second ESX host and then click the **Next** button.
- Step 25** In the vMotion Priority screen, accept the default "**High Priority (recommended)**" radio button and then click the **Next** button.
- Step 26** In the Ready to Complete screen, review the information and then click the **Finish** button.

Activity Verification

You have completed this activity when you have achieved these goals:

- You have successfully imported the vCenter VM into your Cisco UCS B-Series ESXi host.
- You have configured a port profile to support external communications for vCenter.
- You have powered on vCenter VM and validated services.
- You have configured a new data center and added both ESXi hosts.
- You have configured vSwitch on both hosts and tested vMotion.

Lab 7-2: Install a Cisco Nexus 1000V VSM

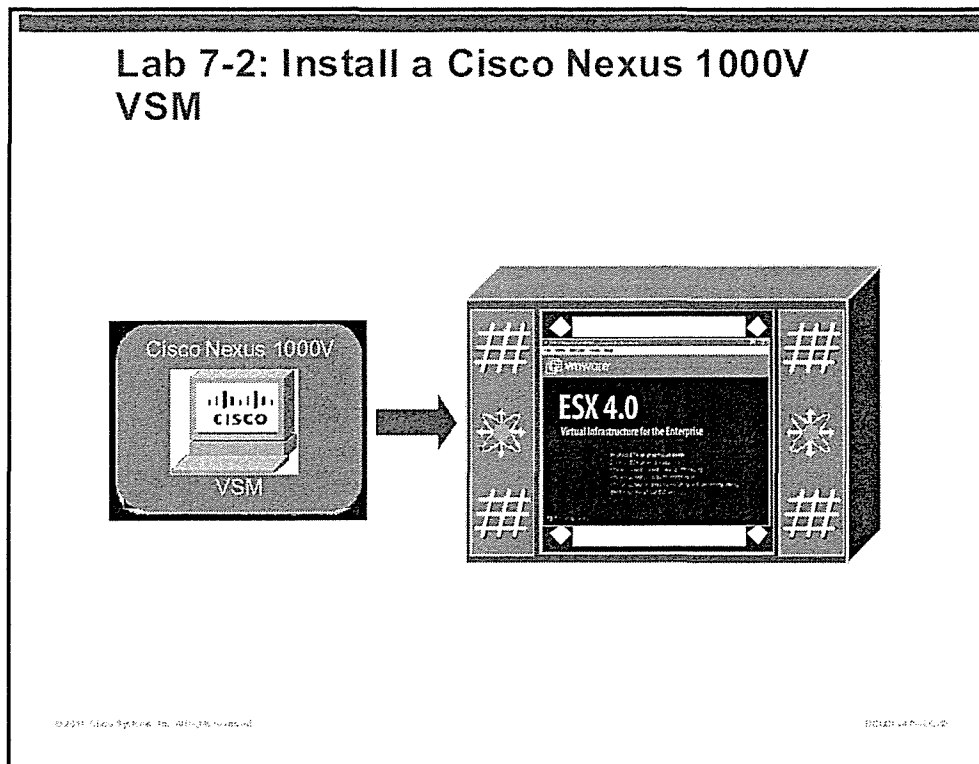
Complete this lab activity to practice what you learned in the related lesson.

Activity Objective

In this activity, you will install and configure a Cisco Nexus 1000V VSM on your C200 server.

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required to complete this activity:

- Student PC
- Lab reference guide

Lab 7-2 Implementation Sheet

Task 1 Configure vSwitch and Test vMotion

Pod	Data Center	control	management	packet
1	DC-1	111	110	211
2	DC-2	112	110	212
3	DC-3	113	110	213
4	DC-4	114	110	214
5	DC-5	115	110	215
6	DC-6	116	110	216

Task 2 Deploy VSM from .OVA File

Pod	VSM Name	VSM IP	control	management	packet
1	VSM-1	192.168.110.31	111	110	211
2	VSM-2	192.168.110.32	112	110	212
3	VSM-3	192.168.110.33	113	110	213
4	VSM-4	192.168.110.34	114	110	214
5	VSM-5	192.168.110.35	115	110	215
6	VSM-6	192.168.110.36	116	110	216

Task 3: Configure the Primary VSM

Pod	Switch Name	Admin Password	VSM Domain ID	Native VLAN
1	Nexus1000-1	Qwer12345	1	1
2	Nexus1000-2	Qwer12345	2	1
3	Nexus1000-3	Qwer12345	3	1
4	Nexus1000-4	Qwer12345	4	1
5	Nexus1000-5	Qwer12345	5	1
6	Nexus1000-6	Qwer12345	6	1

Task 1: Configure vSwitch with Control, Packet, and Management VLANs

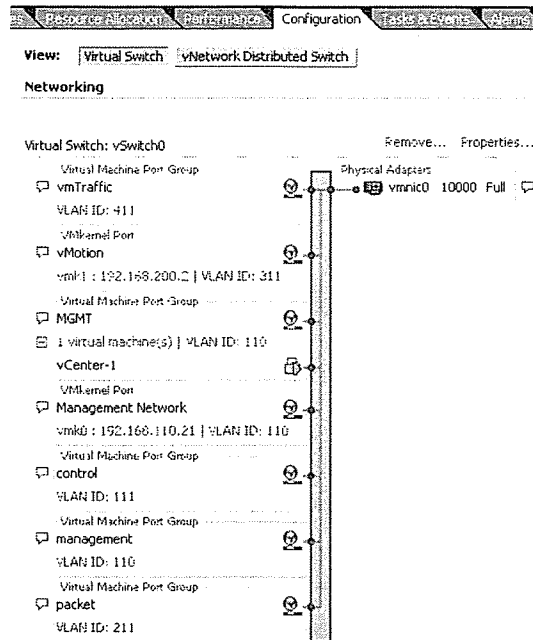
In this task, you will create port profiles in the vSwitch to support the VSM until the DVS is created.

Activity Procedure

Complete these steps:

- Step 1** In the vCenter navigation pane, highlight your first B-Series ESXi server.
- Step 2** In the content pane, click the **Configuration** tab.
- Step 3** In the Hardware section of the content pane, click the **Networking** link.
- Step 4** In the Virtual Switch view, click the **Properties** link for **vSwitch0**.
- Step 5** In the vSwitch0 Properties window, click the **Add** button.
- Step 6** In the Add Network Wizard window, click the **Next** button to leave the Connection Type as Virtual Machine.
- Step 7** Enter **control** in the Network Label text field of the Port Group.
- Step 8** In the VLAN ID field, enter the pod-specific VLAN according to the lab implementation sheet, and then click the **Next** button.
- Step 9** Review the settings, and then click the **Finish** button.
- Step 10** Repeat Steps 6 through 9 for the management port group. Make sure to use the correct VLAN ID from the implementation sheet.
- Step 11** Repeat Steps 6 through 9 for the packet port group. Make sure to use the correct VLAN ID from the implementation sheet.
- Step 12** Repeat Steps 2 through 12 for your C-Series ESXi server. Be careful to use the same names and VLAN IDs as you did for your first ESX server.
- Step 13** Your vSwitch0 configuration should closely match the following figure.

- Step 14** Notice that control, packet, and management are listed in that order. This order is very important for correct operation.



- Step 15** Click the Close button in the vSwitch0 Properties window.

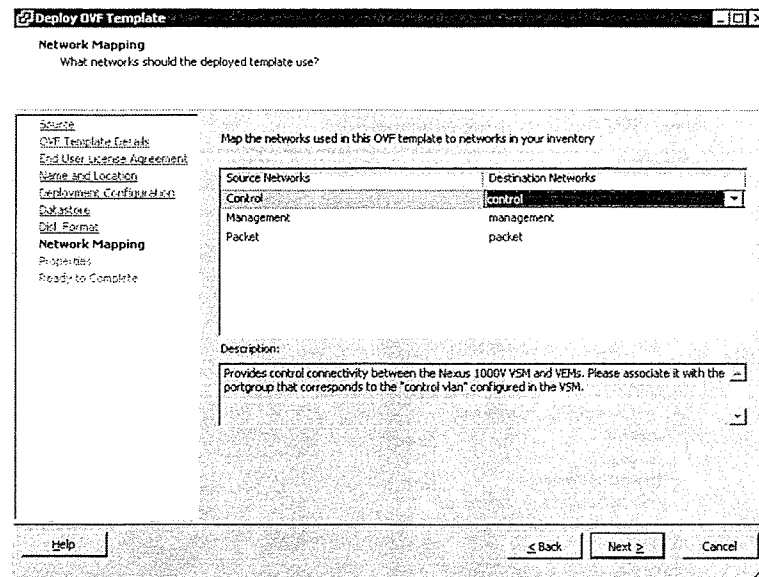
Task 2: Deploy VSM from .ova File

In this task, you will install the VSM VM from an .ova file on your student PC.

Activity Procedure

Complete these steps:

- Step 1** From the File menu of vCenter, choose **Deploy OVF Template**.
- Step 2** In the Source screen of the Deployment Wizard, click the **Browse** button and browse to c:\install\Nexus1000v.4.2.1.SV1.4\VSM\Install on the student PC.
- Step 3** Choose the nexus-1000v.4.2.1.SV1.4.ova and then click the **Next** button.
- Step 4** In the OVF Template Details window, click the **Next** button.
- Step 5** In the End User License Agreement window, click the **Accept** button and then click the **Next** button.
- Step 6** In the Name and Location window, change the name of the VSM VM to the name that is listed in the implementation sheet for Task 2, and then click the **Next** button.
- Step 7** In the Deployment Configuration window, choose **Nexus 1000v Installer** from the Configuration drop-down list and then click the **Next** button.
- Step 8** In the Datastore window, choose the **VM_Storage** datastore and then click the **Next** button.
- Step 9** At the Disk Format screen, click the **Next** button to accept the default thick provisioned disk.
- Step 10** In the Network Mapping window, choose the appropriate destination networks from the drop-down list under Destination Networks.
- Step 11** Choose **control** for the Control source network, **management** for Management, and **packet** for Packet, and then click the **Next** button.



- Step 12** Enter your pod number as the VSM Domain ID.
- Step 13** In the Properties window, enter the password **Qwer12345** for the VSM and the VSM IP address that are assigned to your group (refer to the implementation sheet). All pods will use a subnet mask of 255.255.255.0 and a default gateway of 192.168.1.10.1. Click the **Next** button.
- Step 14** In the Ready to Complete window, verify your settings. Click the **Back** button to make any changes or click the **Finish** button to start the VSM deployment.
- Step 15** The deployment should only take a few minutes to complete. Click the **Close** button when the deployment is finished.

Task 3: Configure the Primary VSM

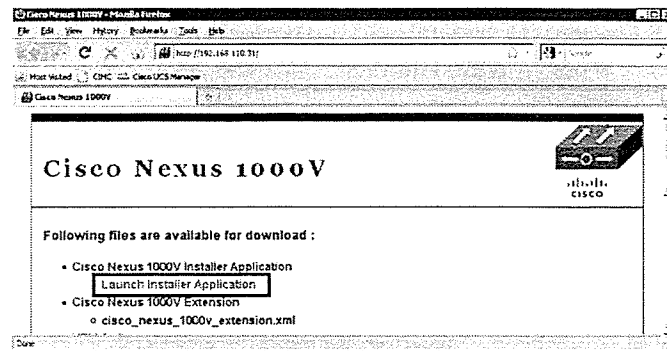
In this task, you will configure the primary VSM.

Activity Procedure

Complete these steps:

- Step 1** From vCenter, power on the VSM VM.
- Step 2** From the vCenter content pane, click the **Console** tab and wait until you see the login prompt. Do not log in here.
- Step 3** From the student PC desktop, launch Firefox and browse to the IP address that you assigned to your VSM.

Step 4 Click the **Launch Installer Application** link in your browser.



Step 5 Accept any security warnings that you might get to run the application.

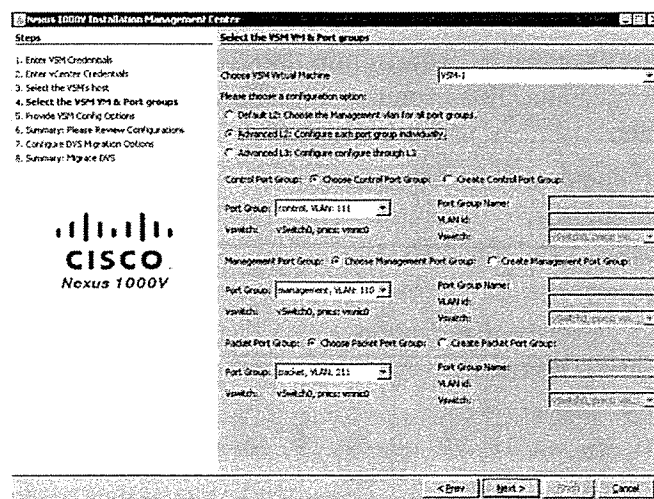
Step 6 In the Enter VSM Credentials screen of the management center wizard, enter your VSM admin password (**Qwer12345**) in the **VSM Password** text field and then click the **Next** button.

Step 7 In the Enter vCenter Credentials screen of the Cisco Nexus 1000V configuration wizard, enter the IP address, username, and password for your vCenter server and then click the **Next** button. Leave the port field unchanged.

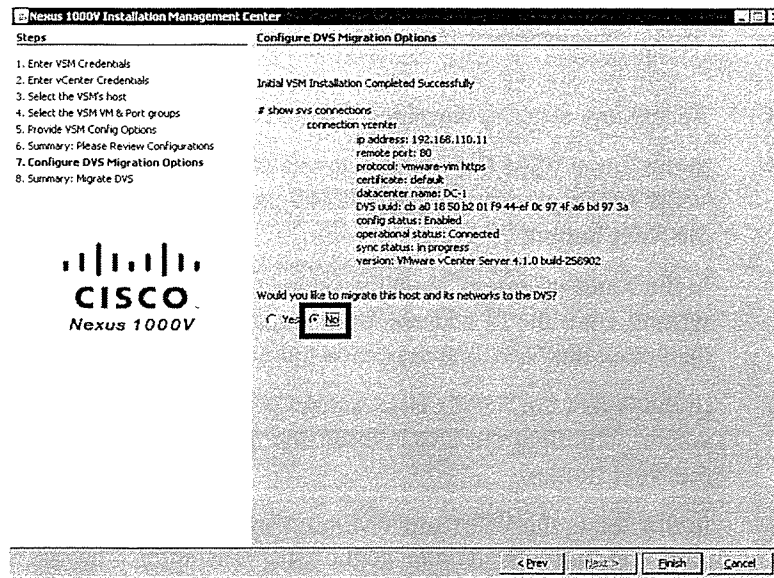
Step 8 In the Select the VSM's Host screen of the Cisco Nexus 1000V configuration wizard, highlight the ESXi server that is currently hosting the VSM and then click the **Next** button.

Step 9 In the Select the VSM and VM Port Groups screen of the Cisco Nexus 1000V configuration wizard, choose the VSM VM in the Choose VSM Virtual Machine drop-down list.

Step 10 Click the **Advanced L2** radio button and choose the appropriate port groups for the control, management, and packet port groups. This is a very important step, so take your time and consult your instructor if you have any questions. Click the **Next** button to continue.



- Step 11** In the Provide VSM Config Options screen of the Cisco Nexus 1000V configuration wizard, you will enter pod-specific values for the Switch Name, Admin password, SVS Domain ID, and native VLAN fields, according to the lab implementation sheet:. When you are finished, click the **Next** button.
- Step 12** The configuration wizard then deploys your selected configuration options to the VSM VM and validates the configuration. This process can take as much as 10 minutes.
- Step 13** In the Configure DVS Migration Options screen, choose the **No** radio button and then click the **Finish** button.



- Step 14** In the Summary screen, click the **Close** button.
- Step 15** To verify that the Cisco Nexus 1000V DVS object was created in vCenter, click the **Home > Inventory** link at the top of your vCenter GUI and select **Inventory > Networking**.
- Step 16** Use Putty to SSH to your VSM.
- Step 17** On the VSM, log in as the admin user with a password of **Qwer12345** and run the **show svcs connections** command to display the connection between the VSM and vCenter.

```
Nexus1000-1# show svcs connections
```

```
connection vcenter:
```

```
ip address: 192.168.110.11
remote port: 80
protocol: vmware-vim https
certificate: default
datacenter name: DC-1
DVS uuid: cb a0 18 50 b2 01 f9 44-ef 0c 97 4f a6 bd 97 3a
config status: Enabled
operational status: Connected
sync status: Complete
version: VMware vCenter Server 4.1.0 build-258902
```

Lab 7-3: Configure Port Profiles

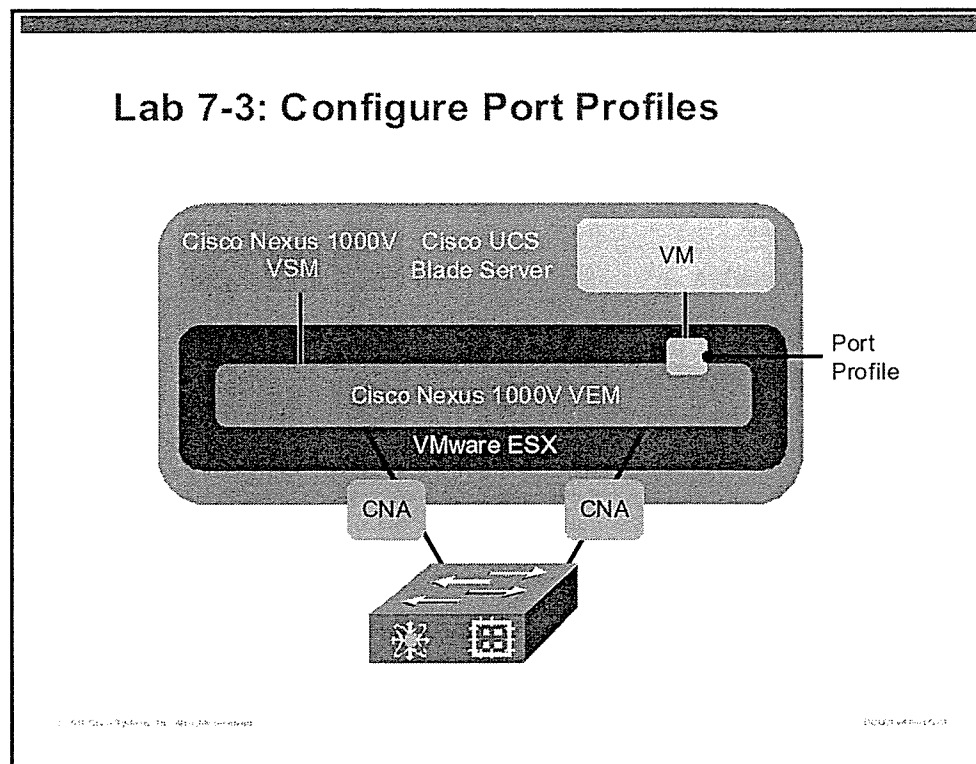
Complete this lab activity to practice what you learned in the related lesson.

Activity Objective

In this activity, you will configure port profiles on the VSM and publish them as port groups to vCenter.

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required to complete this activity:

- Student PC
- Lab reference guide

Task 1: Configure VLANs and Uplink Port Profile in the VSM

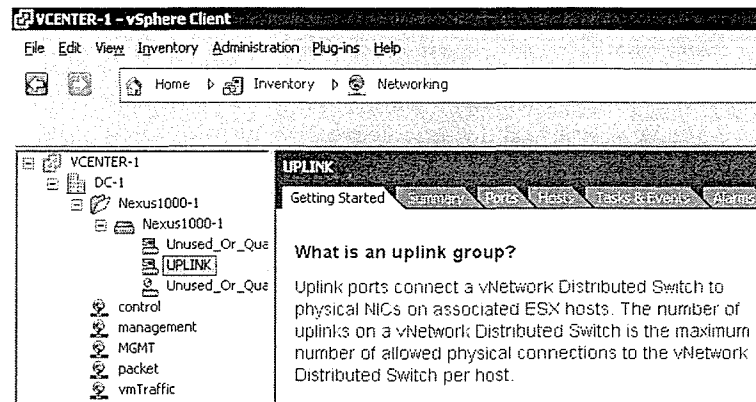
In this task, you will configure VLANs and an uplink port profile on the VSM.

Activity Procedure

Complete these steps:

- Step 1** From your Putty session, enter the following commands to declare the control, management, packet, vm-traffic, and vmotion VLANs in the VSM. Replace “P” with your pod number. The names are not required, but make the configuration easier to read.
- ```
configure
vlan 11P
name control
vlan 11P
name management
vlan 21P
name packet
vlan 31P
name vMotion
vlan 41P
name vmTraffic
exit
```
- Step 2** Enter the following commands in the VSM console to create the uplink port profile. Use your pod number in place of “P” in the VLAN numbers.
- ```
port-profile type ethernet UPLINK
switchport mode trunk
switchport trunk allowed vlan 110, 11P, 21P, 31P, 41P
switchport trunk native vlan 1
no shutdown
system vlan 110, 11P, 21P
vmware port-group
state enabled
```
- Step 3** Enter the following command in the VSM console to save your running configuration:
- ```
copy run start
```

- Step 4** Verify that the uplink port profile was pushed to vCenter, by going to the Home > Inventory > Networking view and selecting your DVS. You should see the profiles that you created in the Networks tab.



## Task 2: Configure Control, Management, and Packet vEthernet Port Profiles

In this task, you will configure the control, management, and packet port profiles that are required for proper VSM-to-VEM communications.

### Activity Procedure

Complete these steps:

- Step 1** Use the following commands to create a port profile that is called **control** on your VSM.

---

**Note** In the following steps, replace "P" with your pod number.

---

```
configure
port-profile type vethernet control
vmware port-group
switchport mode access
switchport access vlan 11P
no shutdown
system vlan 11P
state enabled
```

- Step 2** Use the following commands to create a port profile that is called **management**.

```
configure
port-profile type vethernet management
vmware port-group
switchport mode access
switchport access vlan 110
no shutdown
system vlan 110
```

- state enabled**
- Step 3** Use the following commands to create a port profile that is called **packet**.
- ```
configure
port-profile type vethernet packet
vmware port-group
switchport mode access
switchport access vlan 21P
no shutdown
system vlan 21P
state enabled
```

Task 3: Configure vMotion, vmTraffic vEthernet Port Profiles

In this task, you will configure the port profiles that are required for vMotion and VM connectivity.

Activity Procedure

Complete these steps:

- Step 1** Use the following commands to create a port profile that is called **vmotion**.

Note In the following steps, replace "P" with your pod number.

- ```
port-profile type vethernet vMotion
vmware port-group
switchport mode access
switchport access vlan 31P
no shutdown
state enabled
```
- Step 2** Use the following commands to create a port profile that is called **vm-traffic**.
- ```
port-profile type vethernet vmTraffic
vmware port-group
switchport mode access
switchport access vlan 41P
no shutdown
state enabled
end
```
- Step 3** Copy the running configuration to the startup configuration:
- ```
copy run start
```

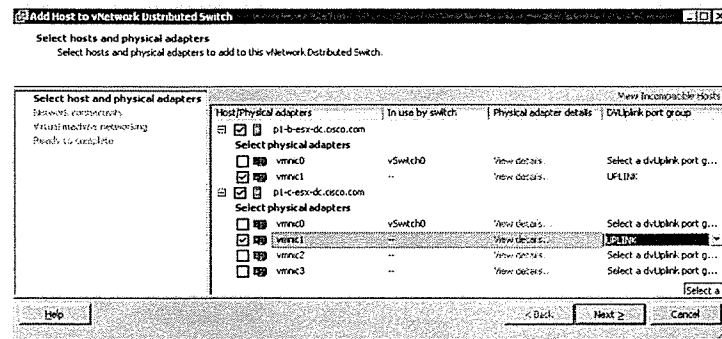
## Task 4: Add ESXi Hosts to the DVS

In this task, you will configure the ESXi hosts to use the DVS instead of the vSwitch.

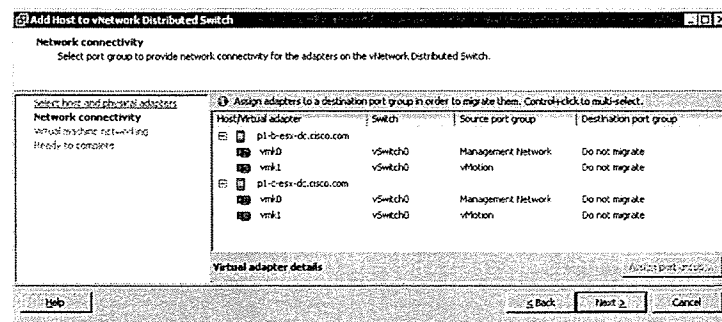
### Activity Procedure

Complete these steps:

- Step 1** In vCenter, click the **PlugIns** menu and choose **Manage Plugins**.
- Step 2** In the Available Plugins section, click the blue link to the right of VMware Update Manager Plugin and then follow the wizard to install the plug-in.
- Step 3** Do not install the Cisco Nexus 1000V plug-in. That plug-in will generate errors and is not necessary.
- Step 4** On your vCenter server, navigate to the VSM definition **Home > Inventory > Networking**.
- Step 5** Right-click your VSM (Nexus1000-X) in the content pane and choose **Add Host**.
- Step 6** In the Select Host and Physical Adapters screen of the wizard, click the check box next to your B-Series and C-Series ESXi servers.
- Step 7** Choose the check box next to the adapter that corresponds to vmnic1, and then choose **Uplink** from the DVUplink port group drop-down list.



- Step 8** Click the **Next** button.
- Step 9** At the Network Connectivity screen, click the **Next** button, without changing any options. You should not migrate the virtual adapters that are connected to vSwitch0.
- Step 10** At the Virtual Machine Networking screen, click the **Next** button to leave DVS port profile assignment for later in the lab.



- Step 11** On the Virtual Machine Networking screen, click the **Next** button to leave that task for later.
- Step 12** Click the **Finish** button to complete the wizard.
- Step 13** Verify that your hosts have been added by clicking the **Hosts** tab in the content pane.
- Step 14** Log in to your VSM console and use the **show module** command to verify that the VEMs installed properly. Note that the VUM might take a few minutes to install the VEMs.
- Step 15** When installed, the VEMs should report into the VSM as modules on your Cisco Nexus 1000V switch.

```
Nexus1000-1# show module
```

| Mod | Ports | Module-Type               | Model      | Status   |
|-----|-------|---------------------------|------------|----------|
| 1   | 0     | Virtual Supervisor Module | Nexus1000V | active * |
| 3   | 248   | Virtual Ethernet Module   | NA         | ok       |
| 4   | 248   | Virtual Ethernet Module   | NA         | ok       |

| Mod | Sw           | Hw                                          |
|-----|--------------|---------------------------------------------|
| 1   | 4.2(1)SV1(4) | 0.0                                         |
| 3   | 4.2(1)SV1(4) | VMware ESXi 4.1.0 Releasebuild-260247 (2.0) |
| 4   | 4.2(1)SV1(4) | VMware ESXi 4.1.0 Releasebuild-260247 (2.0) |

| Mod | MAC-Address(es)                        | Serial-Num |
|-----|----------------------------------------|------------|
| 1   | 00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8 | NA         |
| 3   | 02-00-0c-00-03-00 to 02-00-0c-00-03-80 | NA         |
| 4   | 02-00-0c-00-04-00 to 02-00-0c-00-04-80 | NA         |

| Mod | Server-IP      | Server-UUID                          | Server-Name           |
|-----|----------------|--------------------------------------|-----------------------|
| 1   | 192.168.110.31 | NA                                   | NA                    |
| 3   | 192.168.110.21 | 00000000-0000-1010-0000-000000000002 | p1-b-esx-dc.cisco.com |
| 4   | 192.168.110.51 | cd06276a-6d2e-11df-beeb-c84c75685e84 | p1-c-esx-dc.cisco.com |

\* this terminal session

## Task 5: Migrate Windows 2008 VM from vSwitch to DVS

In this task, you will configure your Windows 2008 host to use the Cisco Nexus 1000V DVS.

### Activity Procedure

Complete these steps:

- Step 1** In your vCenter server, choose your Windows 2008 host in the navigation pane and then click the **Console** tab in the content pane.

## Task 6: Create an ACL Port Profile

In this task, you will configure an IP ACL that will be inherited by another port profile.

### Activity Procedure

Complete these steps:

- Step 1** Create an IP ACL named NO-SPOOF in a port profile that is called VM-ACL, that prevents hosts from using TCP source ports lower than 1024, and that allows the host to use IP addresses only on its assigned subnet for TCP, UDP, and IP.

---

**Note** The example below uses the IP vmTraffic subnet for pod 1. Be sure to use the correct subnet for your pod.

---

```
Nexus1000-1# configure
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Nexus1000-1(config)# port-profile VM-ACL
```

```
Nexus1000-1(config-port-prof)# ip access-list NO-SPOOF
```

```
Nexus1000-1(config-acl)# permit tcp 192.168.4P.0/24 gt 1023 any
```

```
Nexus1000-1(config-acl)# permit udp 192.168.4P.0/24 any
```

```
Nexus1000-1(config-acl)# permit ip 192.168.4P.0/24 any
```

```
Nexus1000-1(config-acl)# exit
```

```
Nexus1000-1(config)# port-profile VM-ACL
```

```
Nexus1000-1(config-port-prof)# state enabled
```

```
Nexus1000-1(config-port-prof)#
```

- Step 2** Next, configure your vmTraffic port profile to inherit the ACL port profile.

```
Nexus1000-1(config)# port-profile vmTraffic
```

```
Nexus1000-1(config-port-prof)# inherit port-profile VM-ACL
```

```
Nexus1000-1(config-port-prof)# exit
```

- Step 3** Save your VSM configuration.

```
Nexus1000-1(config)# copy run start
```

**Step 4** Verify that the ACL is inherited by the vmTraffic port profile.

```
Nexus1000-1(config)# show port-profile name vmTraffic
```

```
port-profile vmTraffic
 type: Vethernet
 description:
 status: enabled
 max-ports: 32
 inherit: VM-ACL
 config attributes:
 switchport mode access
 switchport access vlan 41P
 no shutdown
 evaluated config attributes:
 switchport mode access
 switchport access vlan 41P
 no shutdown
 assigned interfaces:
 port-group: vmTraffic
 system vlans: none
 capability l3control: no
 capability iscsi-multipath: no
 port-profile role: none
 port-binding: static
```

# Lab 8-1: Configure RBAC

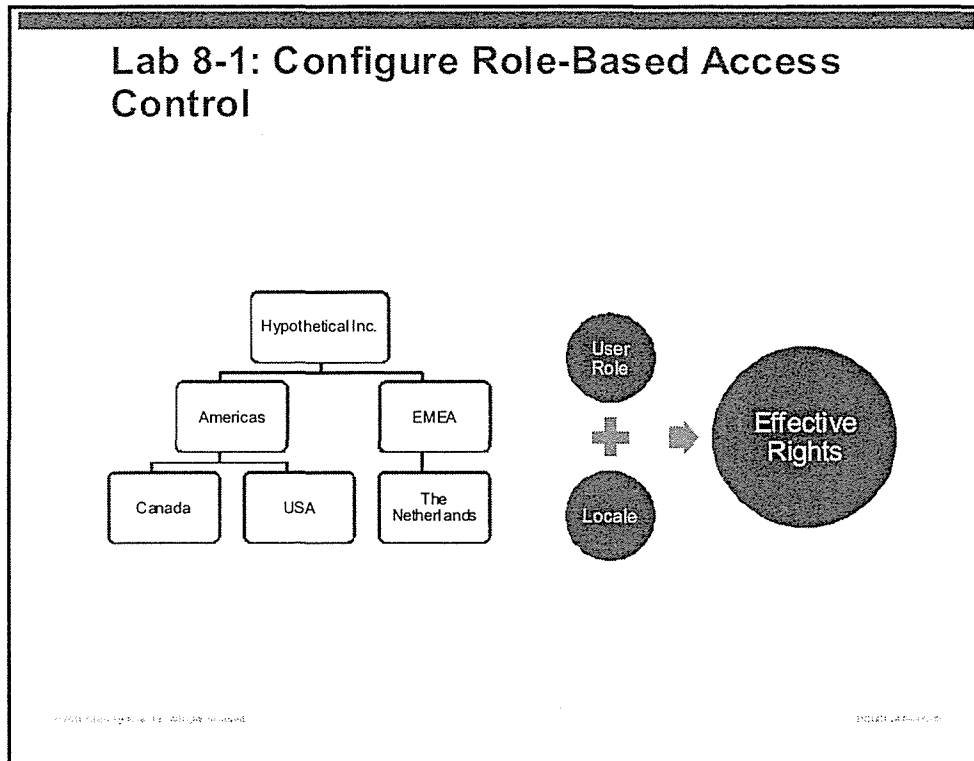
Complete this lab activity to practice what you learned in the related lesson.

## Activity Objective

In this activity, you will configure locales and users, and assign roles to restrict access control to Cisco UCS Manager.

## Visual Objective

The figure illustrates what you will accomplish in this activity.



## Required Resources

These are the resources and equipment that are required to complete this activity:

- Student PC
- Lab implementation sheet
- Lab reference guide

## Lab 8-1 Cisco UCS RBAC Implementation Sheet

The purpose of this sheet is to provide a reference to create the organizational structure and locales for Hypothetical, Inc., a fictional company.

Create these organizations and the associated locales specific to your pod.

| Pod          | Level     | Organization     | Locale |
|--------------|-----------|------------------|--------|
|              | Top Level | root             | —      |
| Prepopulated | Level 1   | Hypothetical-Inc | —      |
| 1            | Level 2   | Boston           | BOS    |
| 2            | Level 2   | Chicago          | ORD    |
| 3            | Level 2   | Dallas           | DFW    |
| 4            | Level 2   | Miami            | MIA    |
| 5            | Level 2   | New-York         | JFK    |
| 6            | Level 2   | San-Francisco    | SFO    |

## Lab 8-1 Cisco UCS RBAC Implementation Sheet (Cont.)

Use this table to create pod-specific custom roles with the appropriate privileges.

| Pod | Custom Role | Privileges                                   |
|-----|-------------|----------------------------------------------|
| 1   | BOS-Admin   | All except admin, AAA, fault, and operations |
| 1   | BOS-LAN-SAN | All ext-lan-*, ext-san-*                     |
| 1   | BOS-SERVER  | All service-profile-*                        |
| 2   | ORD-Admin   | All except admin, AAA, fault, and operations |
| 2   | ORD-LAN-SAN | All ext-lan-*, ext-san-*                     |
| 2   | ORD-SERVER  | All service-profile-*                        |
| 3   | DFW-Admin   | All except admin, AAA, fault, and operations |
| 3   | DFW-LAN-SAN | All ext-lan-*, ext-san-*                     |
| 3   | DFW-SERVER  | All service-profile-*                        |
| 4   | MIA-Admin   | All except admin, AAA, fault, and operations |
| 4   | MIA-LAN-SAN | All ext-lan-*, ext-san-*                     |
| 4   | MIA-SERVER  | All service-profile-*                        |
| 5   | JFK-Admin   | All except admin, AAA, fault, and operations |
| 5   | JFK-LAN-SAN | All ext-lan-*, ext-san-*                     |
| 5   | JFK-SERVER  | All service-profile-*                        |
| 6   | SFO-Admin   | All except Admin.                            |
| 6   | SFO-LAN-SAN | All ext-lan-*, ext-san-*                     |
| 6   | SFO-SERVER  | All service-profile-*                        |

### LDAP Server Parameters

| Pod | LDAP Host    | Order   | Bind DN                          | Key      |
|-----|--------------|---------|----------------------------------|----------|
| 1   | p1.cisco.com | default | CN=ldap;CN=users;DC=cisco;DC=com | cisco123 |
| 2   | p2.cisco.com | default | CN=ldap;CN=users;DC=cisco;DC=com | cisco123 |
| 3   | p3.cisco.com | default | CN=ldap;CN=users;DC=cisco;DC=com | cisco123 |
| 4   | p4.cisco.com | default | CN=ldap;CN=users;DC=cisco;DC=com | cisco123 |
| 5   | p5.cisco.com | default | CN=ldap;CN=users;DC=cisco;DC=com | cisco123 |
| 6   | p6.cisco.com | default | CN=ldap;CN=users;DC=cisco;DC=com | cisco123 |

## Lab 8-1 Cisco UCS RBAC Implementation Sheet (Cont.)

Use this table to create pod-specific users and assign the correct custom role. Bind a pod-specific locale to restrict the scope of user rights.

| Pod | User        | Password  | Role        | Locale |
|-----|-------------|-----------|-------------|--------|
| 1   | bos-admin   | NXos12345 | BOS-Admin   | BOS    |
| 1   | bos-lan-san | NXos12345 | BOS-LAN-SAN | BOS    |
| 1   | bos-server  | NXos12345 | BOS-SERVER  | BOS    |
| 2   | ord-admin   | NXos12345 | ORD-Admin   | ORD    |
| 2   | ord-lan-san | NXos12345 | ORD-LAN-SAN | ORD    |
| 2   | ord-server  | NXos12345 | ORD-SERVER  | ORD    |
| 3   | dew-admin   | NXos12345 | DFW-Admin   | DFW    |
| 3   | dfw-lan-san | NXos12345 | DFW-LAN-SAN | DFW    |
| 3   | dfw-server  | NXos12345 | DFW-SERVER  | DFW    |
| 4   | mia-admin   | NXos12345 | MIA-Admin   | MIA    |
| 4   | mia-lan-san | NXos12345 | MIA-LAN-SAN | MIA    |
| 4   | mia-server  | NXos12345 | MIA-SERVER  | MIA    |
| 5   | jfk-admin   | NXos12345 | JFK-Admin   | JFK    |
| 5   | jfk-lan-san | NXos12345 | JFK-LAN-SAN | JFK    |
| 5   | jfk-server  | NXos12345 | JFK-SERVER  | JFK    |
| 6   | sfo-admin   | NXos12345 | SFO-Admin   | SFO    |
| 6   | sfo-lan-san | NXos12345 | SFO-LAN-SAN | SFO    |
| 6   | sfo-server  | NXos12345 | SFO-SERVER  | SFO    |

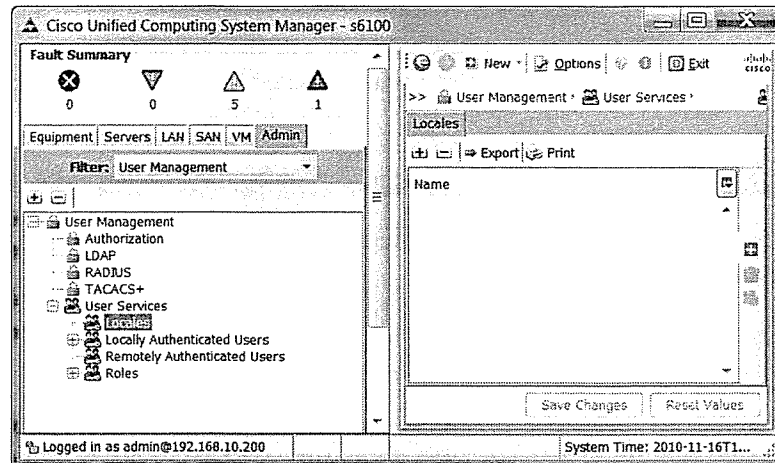
# Task 1: Create Locales for Your Pod

In this task, you will create pod-specific organizations that are based on the Cisco UCS RBAC implementation sheet.

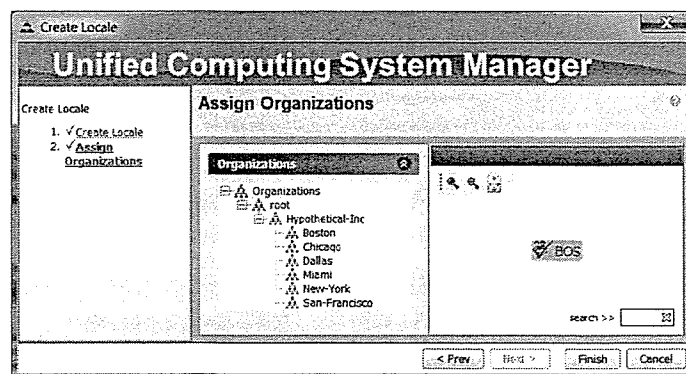
## Activity Procedure

Complete these steps:

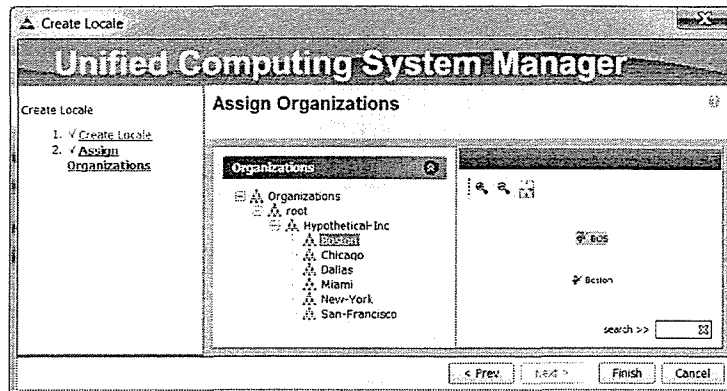
- Step 1 Click the **Admin** tab in Cisco UCS Manager. Choose **User Management** from the Filter drop-down menu.
- Step 2 In the navigation pane, expand **User Services** and then click **Locales**. In the content pane, click the plus symbol (+) to start the Create Locale wizard.



- Step 3 Refer to the Cisco UCS RBAC implementation sheet for the name of the locale for your pod. In this example, pod 1 is used to illustrate the process.
- Step 4 When the Create Locale wizard begins, enter the name of the locale for your pod. Locale names can be 1 to 16 characters long and cannot include spaces, punctuation, or most special characters. Click **Next** to proceed.
- Step 5 Click the double-down arrow icon to the right of **Organizations** to display available organizations.



- Step 6** Click and drag your organization to the right and drop it beneath the name of the locale. If the organization does not appear, click the redraw icon to the right of the magnifying glasses.



- Step 7** When your organization appears under the new locale, click **Finish** to close the wizard.

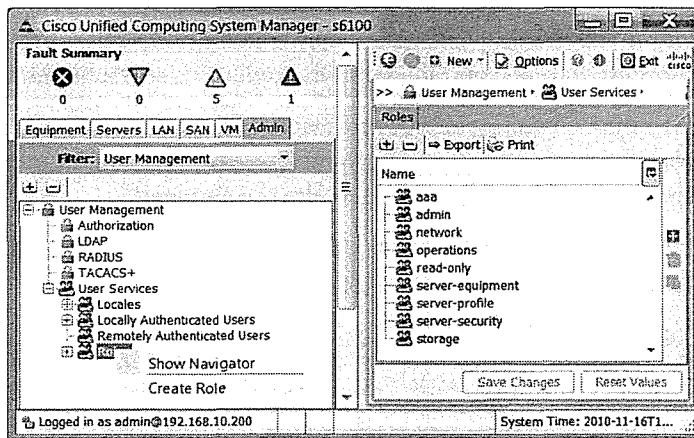
## Task 2: Create Custom Roles to Apply to Pod Users

In this task, you will create pod-specific custom roles that are based on the Cisco UCS RBAC implementation sheet.

### Activity Procedure

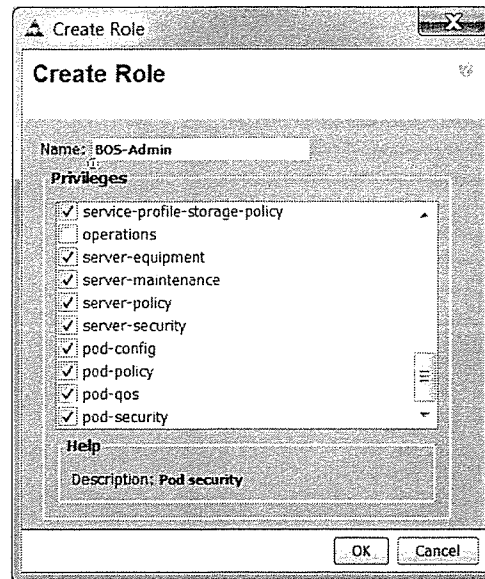
Complete these steps:

- Step 1** Scroll down in the navigation window to Roles. Right-click **Roles** and choose **Create Role**.



- Step 2** Refer to the Cisco UCS RBAC implementation sheet for the role names and specific privileges to be assigned to custom roles for your pod.
- Step 3** As an example, pod 1 will create an admin role that is called BOS-Admin and assign all privileges except AAA, admin, fault, and operations.

**Step 4** When the privileges are set, click **OK** to close the Create Role wizard.



**Step 5** The new role will appear in the role listing.

**Step 6** Repeat this process until Admin, LAN-SAN, and SERVER roles are created for your pod.

## Task 3: Create Local User Accounts

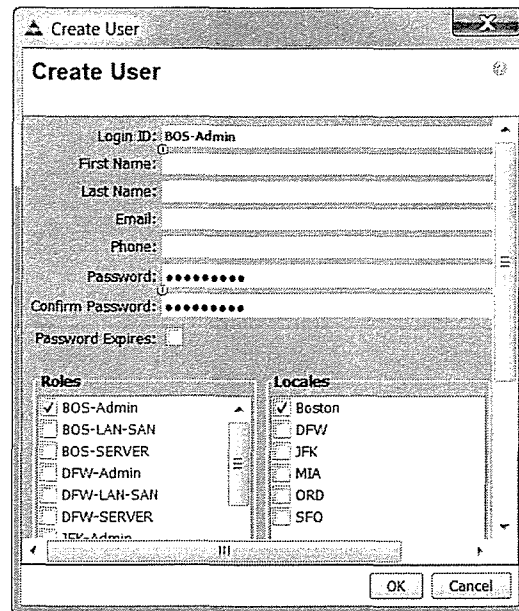
In this task, you will create pod-specific users that are based on the Cisco UCS RBAC implementation sheet.

### Activity Procedure

Complete these steps:

**Step 1** In the Admin tab, right-click **Locally Authenticated Users**. Choose **Create User**.

- Step 2** When the Create User wizard appears, enter the name of the new user and password. Choose the appropriate role and locale.



The 'Create User' dialog box contains the following fields and options:

- Login ID:** BOS-Admin
- First Name:** [Empty]
- Last Name:** [Empty]
- Email:** [Empty]
- Phone:** [Empty]
- Password:** [Masked with dots]
- Confirm Password:** [Masked with dots]
- Password Expires:** [Empty]
- Roles:**
  - ☒ BOS-Admin
  - ☐ BOS-LAN-SAN
  - ☐ BOS-SERVER
  - ☐ DFW-Admin
  - ☐ DFW-LAN-SAN
  - ☐ DFW-SERVER
  - ☐ JFK-Admin
- Locales:**
  - ☒ Boston
  - ☐ DFW
  - ☐ JFK
  - ☐ MIA
  - ☐ ORD
  - ☐ SFO

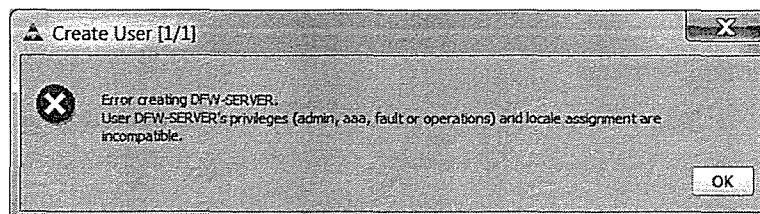
Buttons: OK, Cancel

- Step 3** Click **OK** to close the user wizard.
- Step 4** Repeat until the three users for your pod are created.

---

**Note** If the error dialog box appears after clicking OK, go back to the role that is associated with the user. Be certain you have not assigned the AAA, admin, fault, or operations privileges to the user. Those four privileges are applied systemwide and cannot be restricted by a locale.

---



## Task 4: Test Locale Restrictions

In this task, you will validate that the locale assignment restricts user rights to a given organization.

### Activity Procedure

Complete these steps:

**Step 1** Log out of Cisco UCS Manager and log in with your pod-specific admin account (for example, BOS-Admin).

---

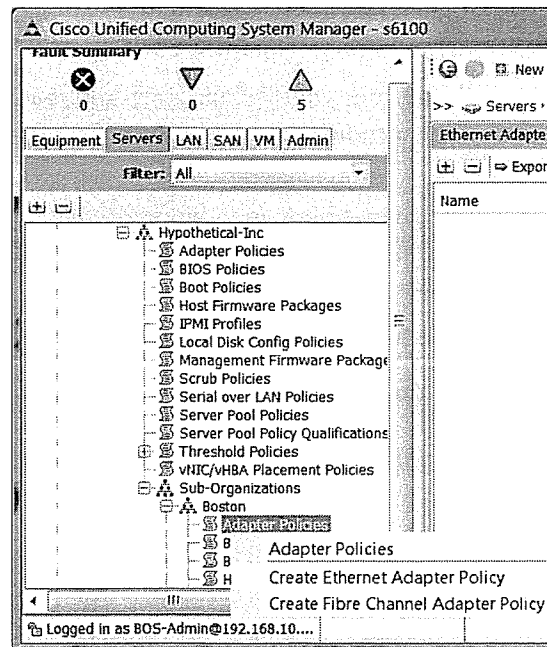
**Note** Usernames and passwords are case sensitive.

---

**Step 2** Choose the **Servers** tab from the navigation pane and expand **Policies**.

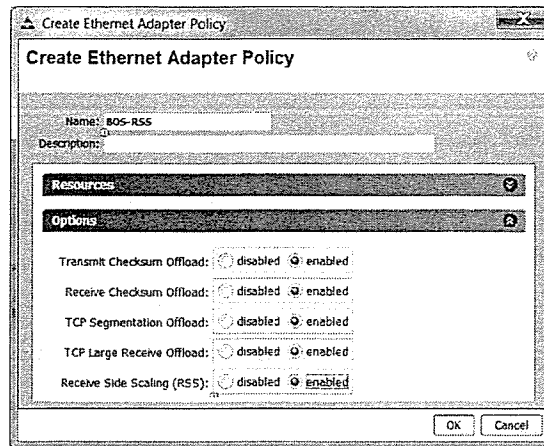
**Step 3** Expand **Root > Sub-Organizations > Hypothetical-Inc > Sub-Organizations > YOUR Organization**.

**Step 4** In the organization that is associated with your login, create a new adapter policy. Right-click **Adapter Policies** and select **Create Ethernet Adapter Policy**.



**Step 5** Name the policy with your three-letter locale and RSS (for example, BOS-RSS).

**Step 6** Under Options, enable **Receive Side Scaling (RSS)**.



**Step 7** Click **OK** to save the new policy.

**Step 8** Scroll down to explore other organizations. Click in the organization of any other pod and attempt to create an adapter policy. You should not be able to create, modify, or delete an object that is created in another organization because your rights are restricted to your locale. The option will be grayed-out.

**Step 9** Go back to the **Admin** tab, edit your Admin user, and remove the locale by unchecking the box. You can now exercise your rights anywhere in the organization hierarchy.

**Step 10** Add all of the locales to your Admin user and verify that you can now create objects in all organizations under Hypothetical-Inc. Verify that you do not have rights to create objects in Hypothetical-Inc. or root.

**Step 11** Restore your Admin user to be restricted to your locale only.

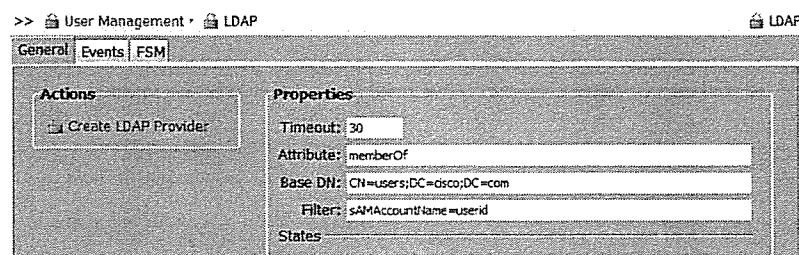
## Task 5: Define Global LDAP Properties (for Active Directory)

In this task, you will validate global LDAP properties that define how to parse usernames and perform attribute mapping.

### Activity Procedure

Complete these steps:

**Step 1** From the Admin tab, choose **User Management** from the filter drop-down list and then click **LDAP**. In the content pane, observe the configured elements in the Properties panel.



**Step 2** The Properties panel lists global defaults that apply to all configured LDAP servers. The Attribute field is used to match an LDAP attribute to a role defined in Cisco UCS Manager. The attribute memberOf queries the LDAP server for Active Directory group membership. The Base DN determines where in the LDAP tree to query for authentication requests. The Filter field lists the LDAP attribute that corresponds with the user ID. The Attribute and Filter fields are case sensitive.

---

**Note** The examples that are shown are specific to Active Directory. If your organization uses a Linux-based LDAP server, then the Attribute and Filter fields will be different. Consult your LDAP administrator for the proper data.

---

---

**Note** As many as 16 LDAP servers can be defined, but only one is active. All secondary LDAP servers act as standby authentication servers.

---

## Task 6: Define an LDAP Server (for Active Directory)

In this task, you will configure your student PC as an LDAP external authentication provider.

---

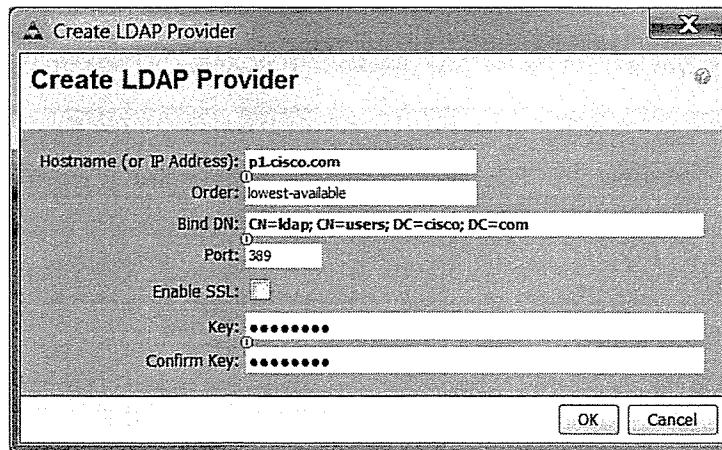
**Note** The preconfigured LDAP server in Cisco UCS Manager will service the actual authentication requests. The steps that are performed in this task are provided to familiarize you with the process of defining an LDAP server.

---

### Activity Procedure

Complete these steps:

- Step 1** In the Actions panel of the content pane, click the **Create LDAP Provider** link.
- Step 2** In the pop-up window, use the Cisco UCS RBAC implementation sheet to populate the fields that define your pod-specific LDAP server elements.



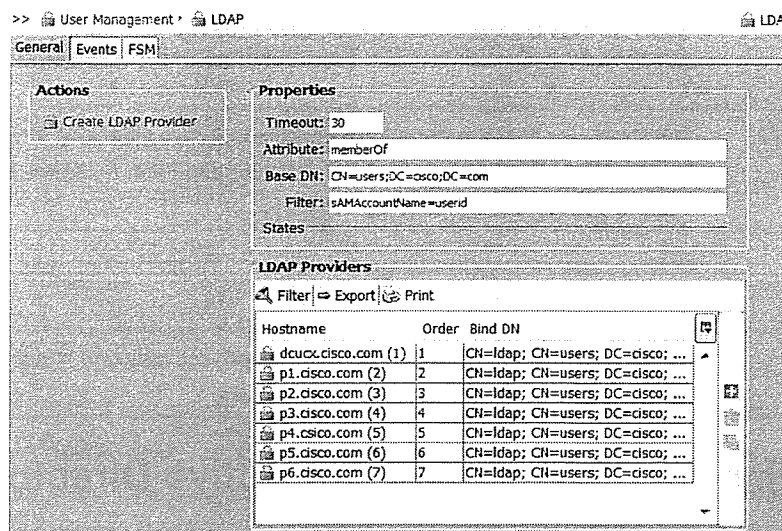
- Step 3** Click **OK** to save your new LDAP server definition.

---

**Note** The CN=ldap in the Bind DN is the username that logs into Active Directory with sufficient privileges to proxy the authentication request and return an attribute for role mapping.

---

- Step 4** After all LDAP servers are defined, the display should appear similar to the figure. If the LDAP servers are not in numerical priority order, click any other element in the navigation pane and then click the **LDAP** link again.



- Step 5** In the navigation pane, click the **Authorization** element under User Management. In the content pane, observe that two categories can be configured for external authorization: Console and Default. Console refers to the serial DB-9 connector on the fabric interconnect. Default refers to any remote access, including HTTPS or SSH. The role policy for remote users includes two selections that determine how to manage role mapping if the username that is supplied for authentication does not match the LDAP database. If no-login is selected, then authentication will always fail. If assign-default-role is selected, then the user will be authenticated with read-only privileges. Best practice is to deny access to users who lack authentication credentials.

## Task 7: Test LDAP Authentication and Role Mapping

In this task, you will configure your student PC as an LDAP external authentication provider.

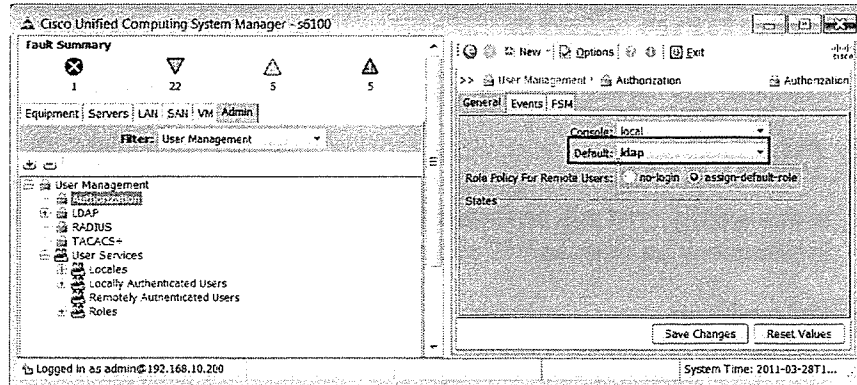
|             |                                                                                                                                                                                                                            |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Note</b> | The preconfigured LDAP server in Cisco UCS Manager will service the actual authentication requests. The steps that are performed in this task are provided to familiarize you with the process of defining an LDAP server. |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Activity Procedure

Complete these steps:

- Step 1** In the navigation pane, select **Authorization** under User Management.

- Step 2** In the content pane, select ldap from the Default: category and then click **Save Changes**.



- Step 3** Log out of UCS Manager.
- Step 4** Log in to UCS Manager with your pod-specific admin user (for example, bos-admin).
- Step 5** Click the Servers tab in the navigation pane and locate your service profile.
- Step 6** Select your service profile from the navigation pane and then click the **General** tab in the content pane.
- Step 7** Click the **Reset UUID** link in the Actions area. If the link is clickable, role mapping succeeded.

## Activity Verification

You have completed this activity when you have achieved these goals:

- You have created all pod-specific organizations
- You have created all required pod-specific locales.
- You have created all required pod-specific custom roles.
- You have created all required pod-specific users with custom roles and locales.
- You have validated locale restrictions.
- You have validated the settings of the LDAP server.
- You have tested LDAP attribute-to-role mapping.

# Lab 8-2: Back up and Import Cisco UCS Manager Configuration Data

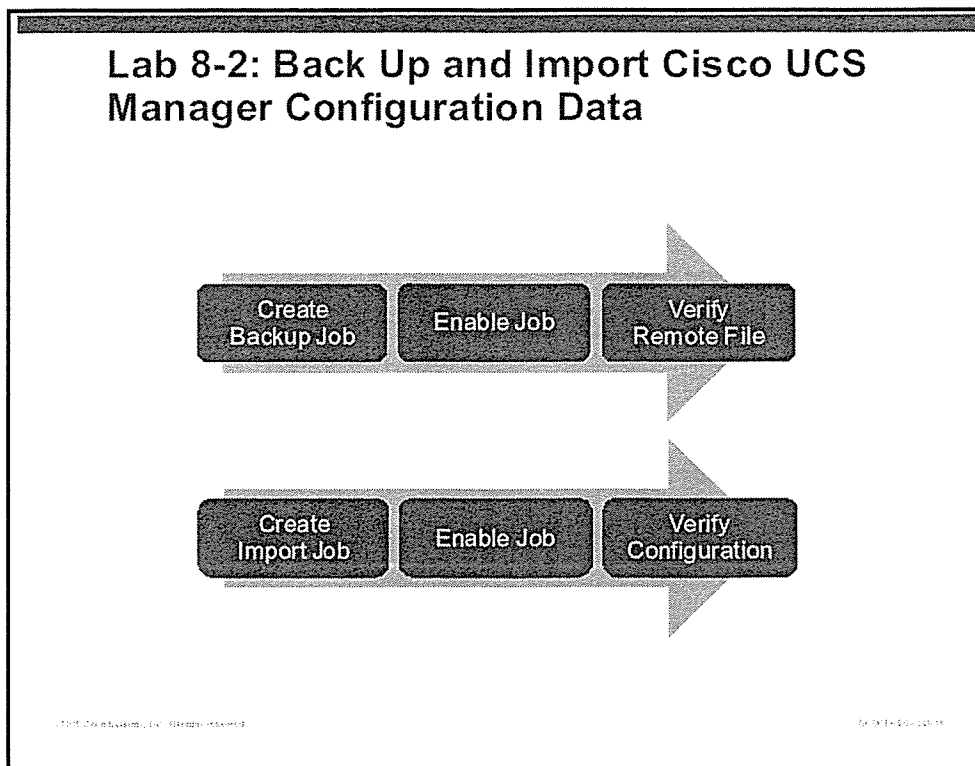
Complete this lab activity to practice what you learned in the related lesson.

## Activity Objective

In this activity, you will perform a backup operation, delete configuration data, and restore an import operation from an FTP server.

## Visual Objective

The figure illustrates what you will accomplish in this activity.



## Required Resources

These are the resources and equipment that are required to complete this activity:

- Student PC
- Cisco UCS backup-import implementation sheet

## Lab 8-2 Cisco UCS Backup-Import Implementation Sheet

Use this table to create pod-specific firmware packages to test backup, and differentiate between a replace and merge operation for import jobs.

| Pod | Pkg Name | Backup Server | Backup File   | User      | Password |
|-----|----------|---------------|---------------|-----------|----------|
| 1   | bos-mezz | 192.168.70.41 | Boston        | anonymous | cisco    |
| 1   | bos-raid |               |               | anonymous | cisco    |
| 1   | bos-bios |               |               | anonymous | cisco    |
| 2   | ord-mezz | 192.168.70.42 | Chicago       | anonymous | cisco    |
| 2   | ord-raid |               |               | anonymous | cisco    |
| 2   | ord-bios |               |               | anonymous | cisco    |
| 3   | dfw-mezz | 192.168.70.43 | Dallas        | anonymous | cisco    |
| 3   | dfw-raid |               |               | anonymous | cisco    |
| 3   | dfw-bios |               |               | anonymous | cisco    |
| 4   | mia-mezz | 192.168.70.44 | Miami         | anonymous | cisco    |
| 4   | mia-raid |               |               | anonymous | cisco    |
| 4   | mia-bios |               |               | anonymous | cisco    |
| 5   | jfk-mezz | 192.168.70.45 | New_York      | anonymous | cisco    |
| 5   | jfk-raid |               |               | anonymous | cisco    |
| 5   | jfk-bios |               |               | anonymous | cisco    |
| 6   | sfo-mezz | 192.168.70.46 | San_Francisco | anonymous | cisco    |
| 6   | sfo-raid |               |               | anonymous | cisco    |
| 6   | sfo-bios |               |               | anonymous | cisco    |

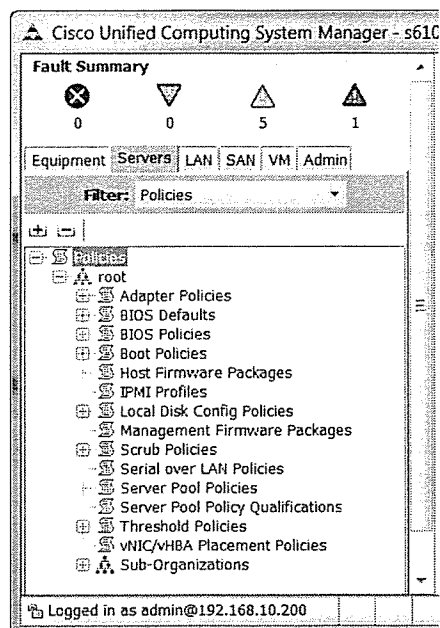
# Task 1: Create Pod-Specific Firmware Packages

In this task, you will use the Cisco UCS backup-import implementation sheet to create firmware packages.

## Activity Procedure

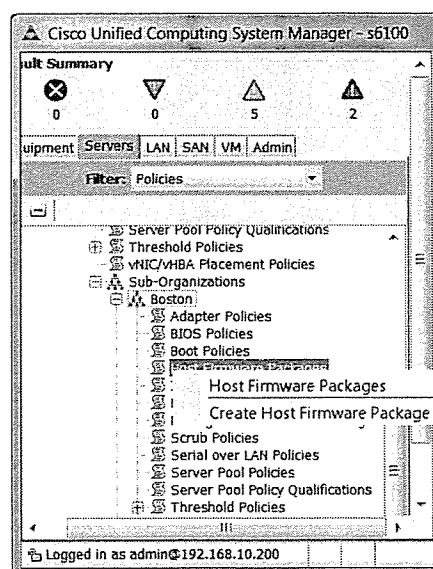
Complete these steps:

- Step 1** In the Servers tab in the navigation pane, choose **Policies** from the Filter drop-down list.

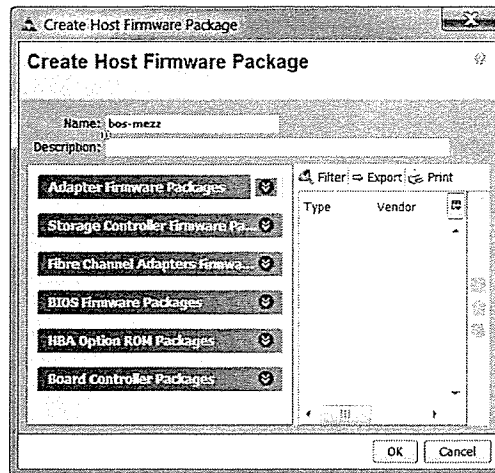


- Step 2** Expand **Root > Sub-Organizations > Hypothetical-Inc > Sub-Organizations** to expose the organization for your pod. Expand your organization.

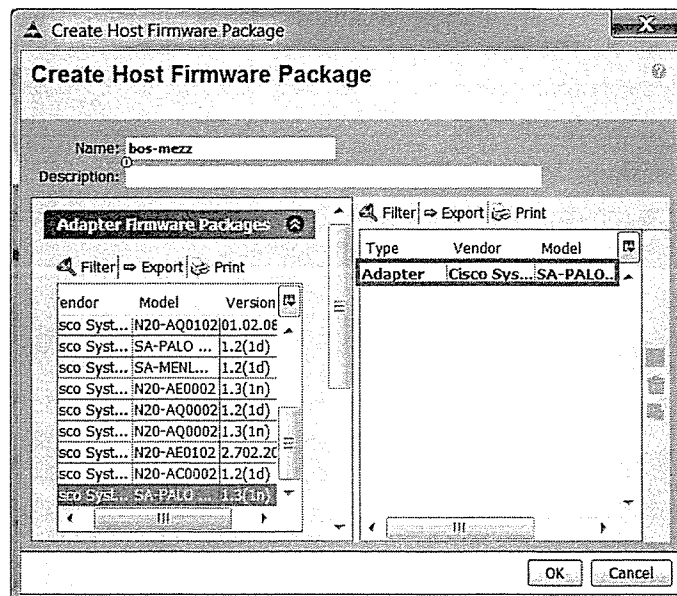
- Step 3** Right-click **Host Firmware Packages** and choose **Create Host Firmware Package** to start the wizard.



- Step 4** Name the firmware package, according to the Cisco UCS Backup-Import implementation sheet.
- Step 5** Click the double-down arrow icon to the right of **Adapter Firmware Packages** in the package list.

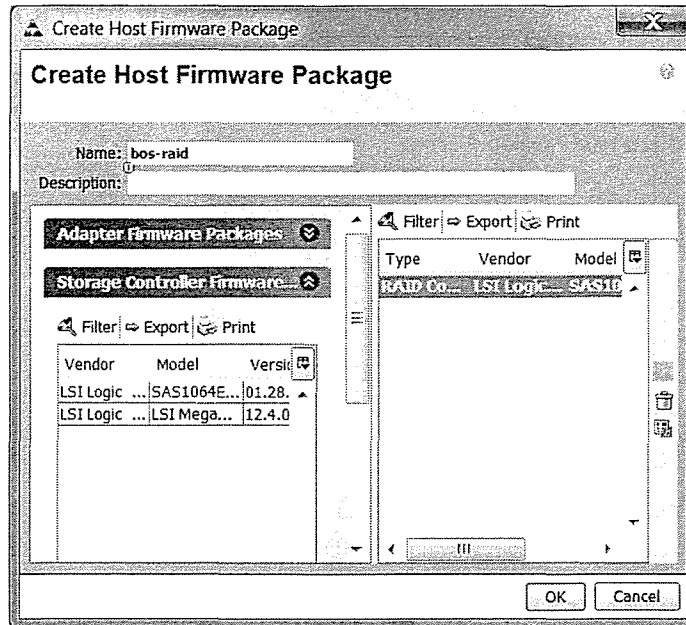


- Step 6** Scroll down the adapter list and choose **SA-PALO** adapter version 1.3(1n). Drag that driver to the empty firmware list on the right.

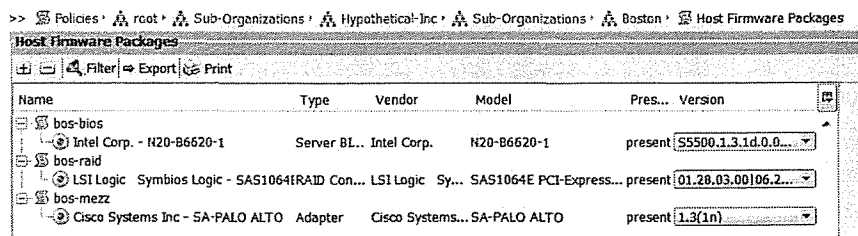


- Step 7** Click **OK** to finish creating the firmware package.
- Step 8** Right-click **Host Firmware Packages** and choose **Create Host Firmware Package**. The next firmware package is for the RAID adapter. Use the Cisco UCS backup-import implementation sheet to name the new package.
- Step 9** Click the double down-arrow icon to the right of **Storage Controller Firmware Packages** to expand the list of available RAID firmware.

- Step 10** Click and drag the **LSI SAS1064E** firmware to the empty list on the right. Click **OK** to finish the firmware package.



- Step 11** Right-click **Host Firmware Packages** and choose **Create Host Firmware Package**. The next firmware package is for the server BIOS. Use the Cisco UCS backup-import implementation sheet to name the new package.
- Step 12** Click the double down-arrow icon to the right of the **BIOS Firmware Packages** to expand the list of available BIOS firmware.
- Step 13** Click and drag the **N20-B6620-1** version 1.3 firmware to the empty list on the right. Click **OK** to finish the firmware package.



## Task 2: Create and Execute an All-Configuration Backup

In this task, you will use the Cisco UCS backup-import implementation sheet to create a backup job.

### Activity Procedure

Complete these steps:

- Step 1** On the student PC desktop, launch 3CDAemon.
- Step 2** Log out of Cisco UCS Manager and log back in as **admin** user. The pod-specific admin accounts cannot create backup jobs.
- Step 3** Choose the **Admin** tab in the navigation pane. Then click the **All** icon at the top of the Admin hierarchy. Click the **Backup** link in the content pane.

- Step 4** When the backup wizard appears, delete any existing backup jobs by choosing the job and then clicking the trash icon. Click **Apply Changes** to commit the delete operation.
- Step 5** Click the **Create Backup Operation** link in the upper-left corner of the backup window.
- Step 6** In the new window, set Admin State to **Enabled**. Set Type to **All configuration**.

**Create Backup Operation**

Admin State: ☒ enabled ☐ disabled

Type: ☐ Full state ☒ All configuration ☐ System configuration ☐ Logical configuration

Preserve Identities: ☐

If preserve identities is selected, vHBAs WWPNs, vNICs MACs, WWPNs and UUIDs that are derived from pools are preserved during a backup.  
If not selected, the identities will be reassigned after a restore

Protocol: ☒ FTP ☐ TFTP ☐ SCP ☐ SFTP

Hostname: 192.168.70.41

Remote File: Boston

User: anonymous

Password: \*\*\*\*\*

OK Cancel

- Step 7** Set the remaining values to match the Cisco UCS backup-import implementation sheet for your pod. Please note that the values in the figure apply only to the Boston pod. Click **OK** to save and execute the backup job.
- Step 8** Choose your backup job from the list. If your FTP server is set up correctly, the backup job is likely complete.
- Step 9** Towards the bottom of the window, click the double down-arrow icon to expand FSM Details.

Progress Status: 100% Completed

**FSM Details**

Retry #: 0

Current Stage Description:  
Description:

Time of Last Operation: 2010-11-18T15:20:59

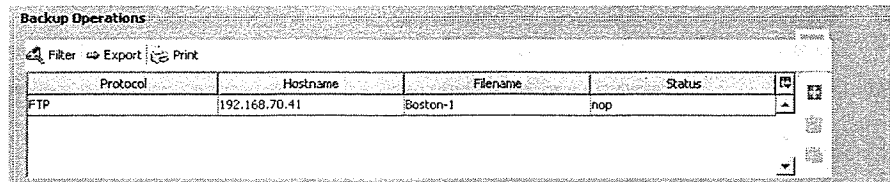
Status of Last Operation: backupSuccess

Remote Invocation Result:  
Remote Invocation Error Code: none

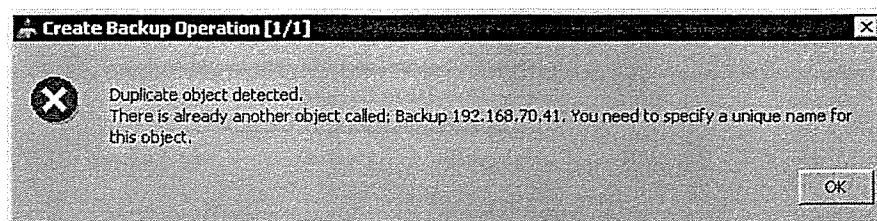
Remote Invocation Description:

- Step 10** The Status of Last Operation should be backupSuccess. If any other status message appears, the backup has failed and you will need to determine why.
- Step 11** When a backup job runs, its administrative state is set to disabled. Click the radio button to enable the backup job. In the example, there is already a backup job on the remote file system called Boston. Set the backup name to **Boston-1** and re-enter the FTP password. Click **Apply** to start the new backup job.

- Step 12** This saved job can be reused to create new backup jobs with new filenames on the remote file system.
- Step 13** Now, click the plus symbol (+) at the far right of the Backup Operations portion of the window.



- Step 14** In the job creation screen, set the administrative state to **Enabled**, and set the backup type to **All configuration**. Enter a filename for the backup job on the remote file system. Enter the IP address, username, and password for the remote FTP server.
- Step 15** Click **Apply** to execute the backup job. The error dialog box that is shown will appear.




---

**Note** Backup jobs are uniquely identified by either the IP address or FQDN of the destination host. If you need to create more than one backup job to the same destination, create DNS A-Record aliases for the IP address.

---

## Task 3: Delete a Firmware Policy and Restore with an Import Job

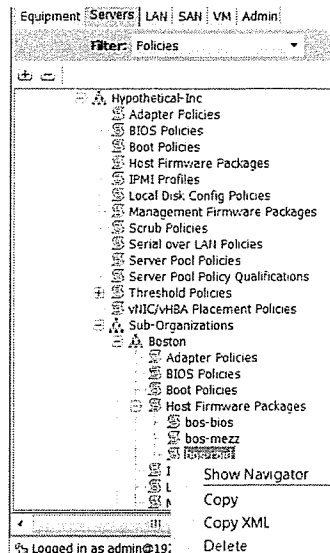
In this task, you will restore a firmware policy from an import job.

### Activity Procedure

Complete these steps:

- Step 1** On the student PC desktop, verify that 3CDaemon is running.

**Step 2** From Cisco UCS Manager, delete your pod-specific RAID firmware package.

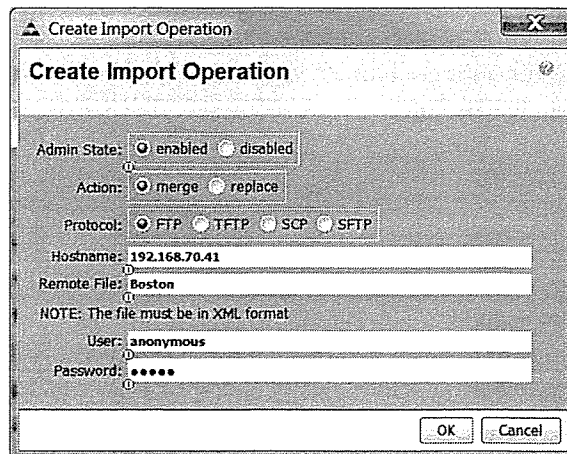


**Step 3** Click the **Admin** tab in the navigation window and choose the filter **All** from the drop-down menu.

**Step 4** In the content pane, click the **Import Configuration** link to open the import jobs.

**Step 5** Click the **Create Import Operation** link to create a new import job.

**Step 6** In the Create Import Operation dialog box, set the Admin State of the import job to Enabled. Set the Action to Merge, and enter the name of your pod-specific backup filename, IP address, username, and password. The Boston pod is used in the example.



**Step 7** Click **OK** to execute the import job.

**Step 8** Click the double down-arrow icon to the right of FSM Details to monitor the progress of the import job. It should take less than 30 seconds to complete. The Status of the Last Operation should indicate importSuccess, as shown in the example.

| FSM Details                    |                     |
|--------------------------------|---------------------|
| Retry #:                       | 0                   |
| Current Stage Description:     |                     |
| Description:                   |                     |
| Time of Last Operation:        | 2010-11-23T07:18:51 |
| Status of Last Operation:      | importSuccess       |
| Remote Invocation Result:      |                     |
| Remote Invocation Error Code:  | none                |
| Remote Invocation Description: |                     |

**Step 9** Switch to the **Server** tab and navigate to your **Host Firmware** tab policies. Verify that your pod-specific RAID policy has been restored.

**Note** A merge operation will fill in elements of the configuration that have been deleted since the time of the last backup. If an object in the Cisco UCS Manager configuration exists with the same name as an object in an import job, that object is not restored.

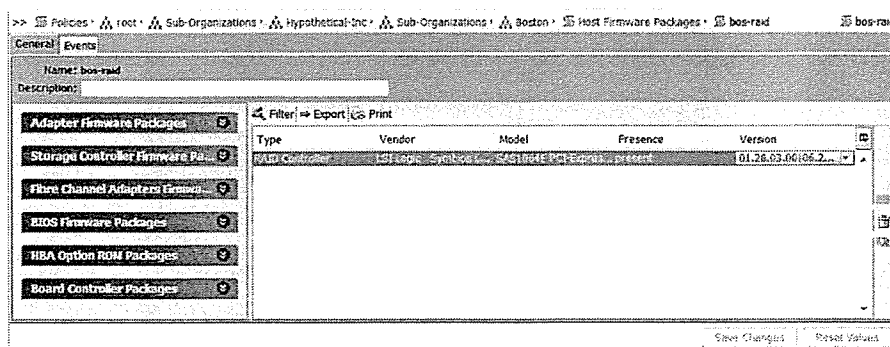
## Task 4: Demonstrate Using an Import Job with the Replace Action

In this task, you will restore a firmware policy using the replace action to demonstrate the differences between merge and replace.

### Activity Procedure

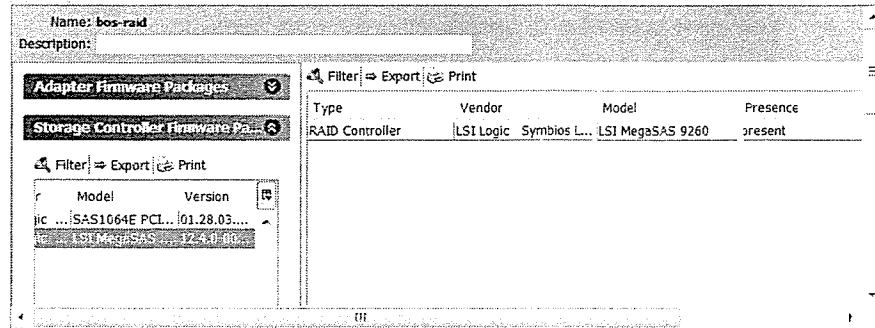
Complete these steps:

- Step 1** From the Server tab in Cisco UCS Manager, navigate to your pod-specific RAID firmware policy.
- Step 2** Click the **LSI firmware** element, and then click the trash icon to delete that firmware from the package.

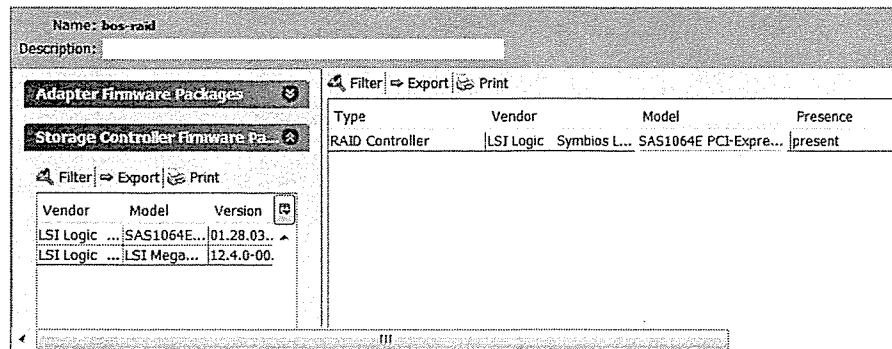


**Step 3** Click **Save Changes** to commit the change.

- Step 4** Click the double down-arrow icon to the right of Storage Controller Firmware Packages, to reveal the available RAID firmware packages.



- Step 5** Click and drag the **LSI MegaSAS** firmware package into the white space on the right.
- Step 6** Click **Save Changes** to commit the change.
- Step 7** Choose the **Admin** tab and then click the **All** link at the top of the Admin hierarchy.
- Step 8** In the content window, click the **Import Configuration** link.
- Step 9** In the import jobs window, click the import job that you created previously.
- Step 10** Click the radio button to make this a Replace operation.
- Step 11** Set the admin state to Enabled, and enter a password for the FTP server. Click **Apply** to start the import job.
- Step 12** In less than 30 seconds, the job should finish with a status of importSuccess.
- Step 13** Return to the Server tab and navigate to your pod-specific firmware packages.
- Step 14** Click the **RAID** firmware package and examine the contents. Notice that the LSI MegaSAS firmware package was replaced with the original LSI SAS1064E package.



**Note** Unlike the merge operation, a replace operation will overwrite any existing objects in a Cisco UCS Manager configuration with an object of the same name and all of its inherent properties from the import job. The danger with the replace operation is that if objects have been modified since the last backup, those changes will be lost. However, in the event of malicious or accidental changes to the Cisco UCS Manager database, a replace action ensures return to a known good baseline.

## Activity Verification

You have completed this activity when you have achieved these goals:

- You have created pod-specific firmware packages.
- You have executed an all-configuration backup job.
- You have deleted a firmware package and restored it with an import job.
- You have demonstrated the important differences between a merge and a replace action in an import job.

# Lab 8-3: Reporting in the Cisco Unified Computing System

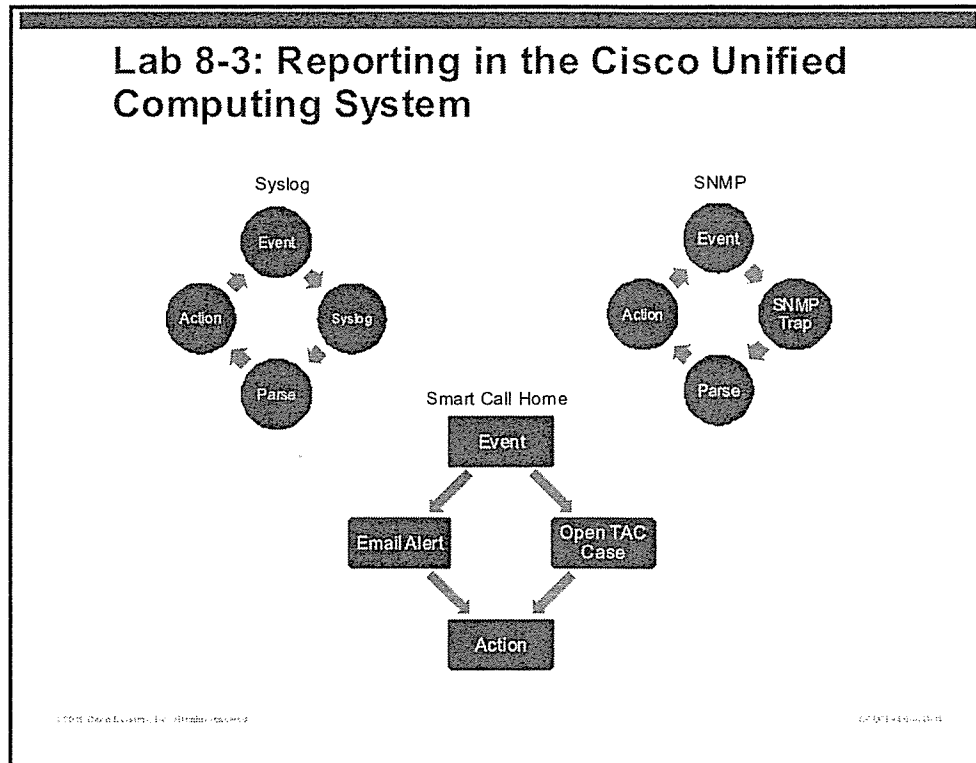
Complete this lab activity to practice what you learned in the related lesson.

## Activity Objective

In this activity, you will configure and test syslog, Smart Call Home, and SNMPv3.

## Visual Objective

The figure illustrates what you will accomplish in this activity.



## Required Resources

These are the resources and equipment that are required to complete this activity:

- Student PC
- Cisco UCS reporting implementation sheet

## Lab 8-3 Cisco Unified Computing System Reporting Implementation Sheet

Use this implementation sheet to aid in the configuration tasks in Lab 6-3.

### Task 1 Generate and Observe Major Alarms and Recovery

| Pod | Interconnect | Server Port |
|-----|--------------|-------------|
| 1   | Fabric A     | Port 1      |
| 2   | Fabric A     | Port 2      |
| 3   | Fabric A     | Port 3      |
| 4   | Fabric B     | Port 1      |
| 5   | Fabric B     | Port 2      |
| 6   | Fabric B     | Port 3      |

### Task 3 Configure Syslog

| Pod | Server   | Level       | Hostname      | Facility |
|-----|----------|-------------|---------------|----------|
| 1   | Server 1 | Warning     | 192.168.70.41 | local7   |
| 3   | Server 2 | Information | 192.168.70.43 | local7   |
| 5   | Server 3 | Debug       | 192.168.70.45 | local7   |

### Task 6 Configure SNMPv3

| Pod | Username | Hash Algorithm | AES | Password  | Privacy Password |
|-----|----------|----------------|-----|-----------|------------------|
| 1   | p1-snmp  | SHA            | Yes | QWER12345 | ASDF12345        |
| 2   | p1-snmp  | SHA            | Yes | QWER12345 | ASDF12345        |
| 3   | p1-snmp  | SHA            | Yes | QWER12345 | ASDF12345        |
| 4   | p1-snmp  | SHA            | Yes | QWER12345 | ASDF12345        |
| 5   | p1-snmp  | SHA            | Yes | QWER12345 | ASDF12345        |
| 6   | p1-snmp  | SHA            | Yes | QWER12345 | ASDF12345        |

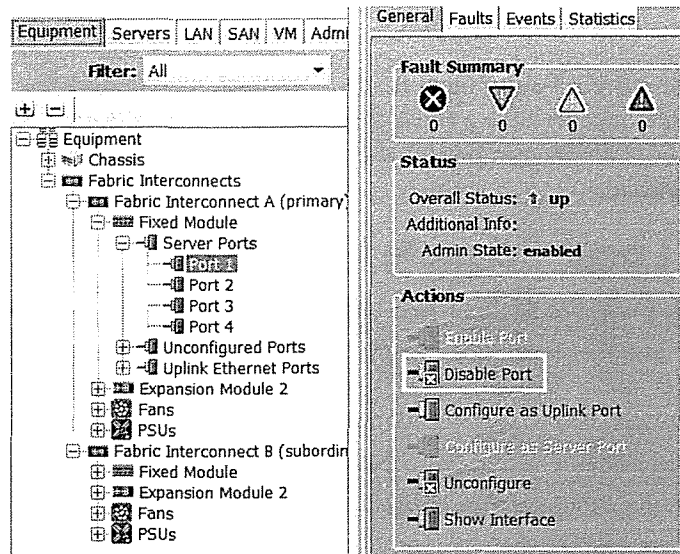
# Task 1: Generate and Observe Major Alarms and Recovery

In this task, you will shut down IOM interfaces to generate major alarms.

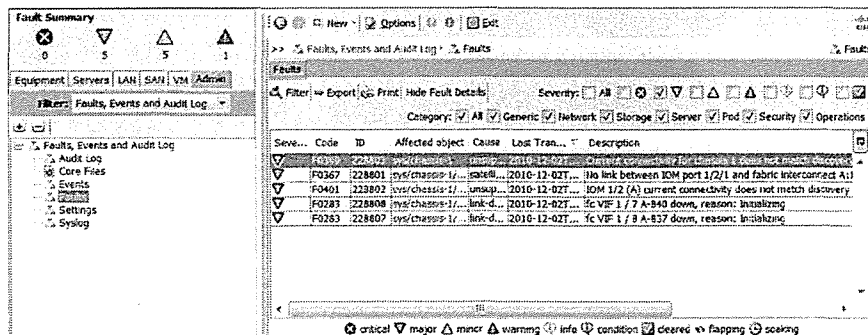
## Activity Procedure

Complete these steps:

- Step 1** On the Equipment tab in Cisco UCS Manager, navigate to the fabric interconnect that is specified in the Cisco UCS reporting implementation sheet.
- Step 2** Expand **Fixed Module > Server Ports**.
- Step 3** Click the server port that is assigned to your pod. In the content window, click the **Disable Port** link in the Actions panel.



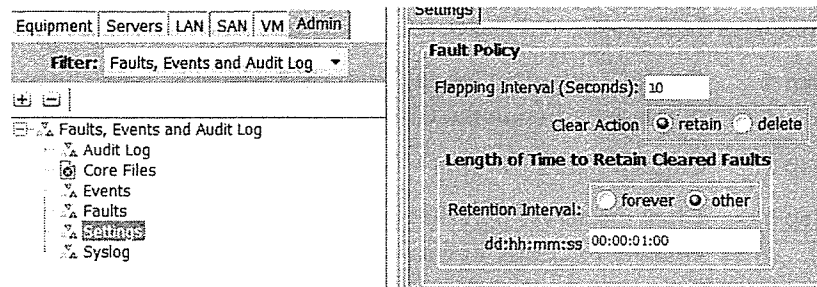
- Step 4** Click the **Admin** tab and choose **Faults, Events and Audit Log** from the Filter drop-down menu.



- Step 5** When the first pod disables its assigned server port on the fabric interconnect, the chassis generates a series of alarms. Expand the interface to full screen to view the greatest detail.
- Step 6** After viewing alarms, go back to the fabric interconnect to which you are assigned and enable the port that you disabled.

- Step 7** Return to the Faults, Events and Audit Log section in the Admin tab. Watch as alarms are cleared and disappear from the faults screen.

What controls how long an alarm remains in the fault window and whether it should be stored? Click the **Settings** element in the Admin tab.



- Step 8** The current Fault Policy is set to delete cleared faults after 1 minute. The fabric interconnects have a finite amount of persistent storage. Best practice is not to choose a retention period of Forever because of the risk of filling up the logging partition.

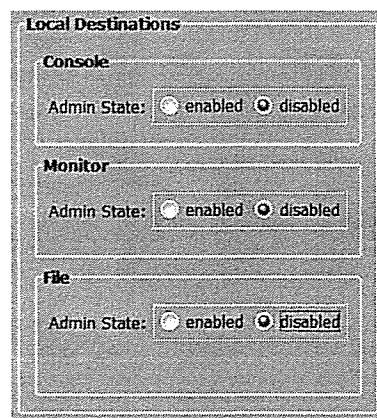
## Task 2: Disable Local Console Logging

In this task, you will verify that Cisco UCS Manager is not logging to the CLI or local flash file system.

### Activity Procedure

Complete these steps:

- Step 1** On the Admin tab in the navigation pane, choose the **Syslog** element.
- Step 2** In the content pane, verify that the Admin State of Console, Monitor, and File logging are set to Disabled.



- Step 3** Selectively enable each of the Local Destinations and observe the options. The Console option (if enabled) determines the level of logging messages that are sent to the Cisco UCS Manager CLI interface. The Monitor option (if enabled) determines the level of logging messages that can be sent over an SSH connection. The File option (if enabled) determines the logging level of messages that are sent to a file in the local flash file system. The administrator also has control over the size of this local buffer.

|             |                                                                                                                                                                                                                                                                                                                                                                         |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Note</b> | Because of the potentially high rate of logging messages that can be generated by the fabric interconnects, it is a best practice to leave Console and File logging disabled. Each character that is sent to the serial console generates an interrupt. If the rate is high enough, access to the serial console can be lost until the fabric interconnect is rebooted. |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Task 3: Configure Syslog

In this task, you will configure Cisco UCS Manager to output logging messages to syslog servers for persistent archival storage of logging data.

### Activity Procedure

Complete these steps:

- Step 1** Cisco UCS Manager supports a maximum of three destinations for syslog. As such, three pods will configure syslog and the other three will observe. Refer to the Cisco UCS Reporting implementation sheet to determine which three pods will configure syslog. If your pod is selected to configure syslog, open a remote desktop session to your student PC.
- Step 2** Double-click the **3CDaemon** icon on the desktop. In the left side of the 3CDaemon window, click the **Syslog Server** tab.
- Step 3** For the three pods that are selected to configure syslog, click the **Enabled** radio button to the right of Admin State. Refer to the Cisco UCS reporting implementation sheet for the data to configure syslog output to your student PC.
- Step 4** Click **Save Changes** to commit your syslog configuration.
- Step 5** When all three pods have finished configuring syslog, the content pane for Remote Destinations should match the figure.

The screenshot displays the 'Remote Destinations' configuration window. It contains three sections, one for each server:

- Server 1:** Admin State: ☒ enabled ☐ disabled; Level: information; Hostname (or IP Address): 192.168.70.41; Facility: local7.
- Server 2:** Admin State: ☒ enabled ☐ disabled; Level: information; Hostname (or IP Address): 192.168.70.43; Facility: local7.
- Server 3:** Admin State: ☒ enabled ☐ disabled; Level: information; Hostname (or IP Address): 192.168.70.43; Facility: local7.

- Step 6** Now that syslog is configured, return to Task 1 and perform Steps 1 through 6 to disable and re-enable server ports to the IOMs.
- Step 7** Alarms should appear in your syslog window.

---

**Note** Syslog is the preferred method of archiving Cisco UCS Manager logging data. The number and capacity of syslog servers in use, as well as the backup regimen and retention period for log data, is dictated by IT policy and regulatory compliance requirements.

---

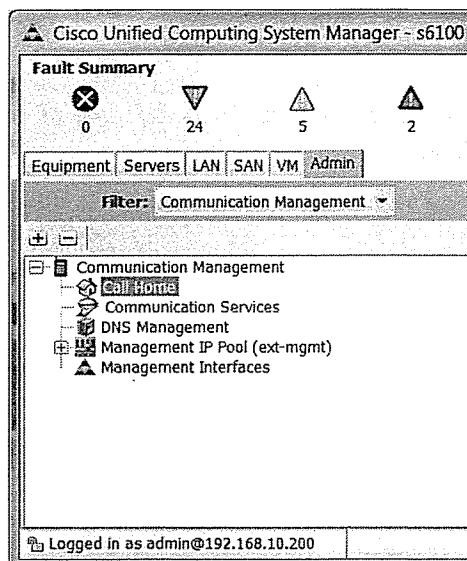
## Task 4: Configure Smart Call Home

In this task, you will configure Smart Call Home and create profiles.

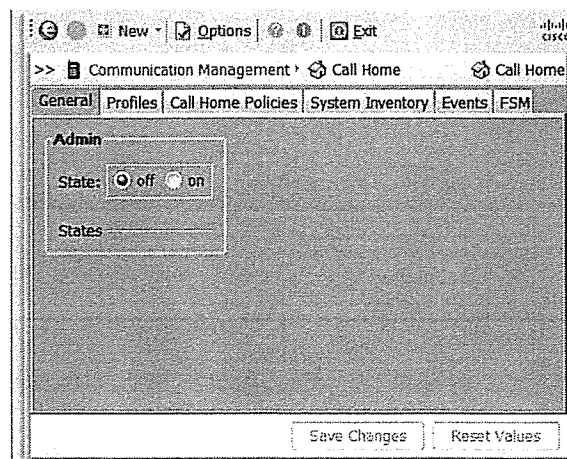
### Activity Procedure

Complete these steps:

- Step 1** Log into Cisco UCS Manager if necessary.
- Step 2** Choose the **Admin** tab in the navigation pane. It may be helpful to change the Filter field to Communication Management for the following steps. Choose the **Call Home** icon.



- Step 3** In the content pane, confirm that Admin State is off.



---

**Note** It is possible that Admin State will be on if another student has enabled it and saved the configuration. If this is the case, skip the next step.

---

**Step 4** Change the Admin State to **On**.

The screenshot shows the 'Call Home' configuration window in Cisco UCS Expert. The 'Admin' section has the following settings:

- State: ☒ off ☒ **on**
- Switch Priority: debugging
- Throttling: ☐ off ☒ on
- States: (empty)

Experiment with various values in the Contact Information fields. Are any fields required? Are any formats enforced?

The screenshot shows the 'Contact Information' section of the 'Call Home' configuration window. The fields are filled with the following example data:

- Contact: James Casaletto
- Phone: +1-408-555-1212
- Email: ucs-expert@cisico.com
- Address: 170 W Tasman Drive, San Jose, CA 95134

---

**Note** All fields in Contact Information are required. Only the Phone and Email fields enforce any format checking. The Phone value must use the international format, beginning with the plus symbol (+) and followed by a country code. The Email field uses standard email format.

---

**Step 5** Experiment with various values in the Ids fields. Are any fields required? Are any formats enforced?

The screenshot shows the 'Ids' configuration window with three empty text input fields:

- Customer ID:
- Contract ID:
- Site ID:

---

**Note** All ID fields are optional. These values will be included in any Call Home messages.

---

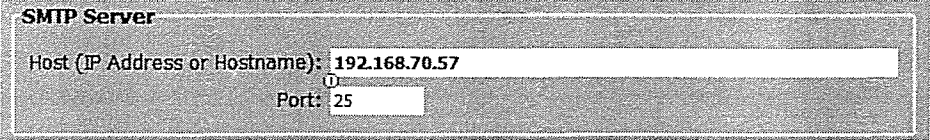
- Step 6** Experiment with various values in the Email Addresses fields. Are any fields required? Are any formats enforced?



The 'Email Addresses' configuration window shows two text input fields. The 'From' field is populated with 'ucs-system@localhost.com' and the 'Reply To' field is populated with 'ucs-expert@cisco.com'. Both fields have a small circular icon with a lowercase 'i' to their left, indicating an information or help tooltip.

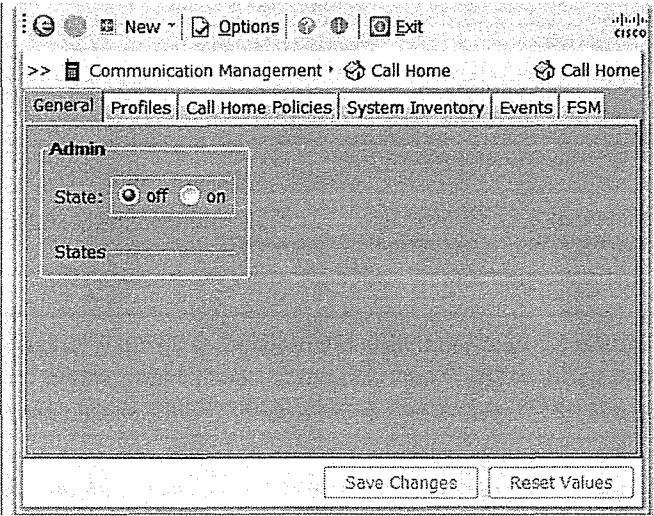
**Note** The Email Addresses fields are used to populate the email headers of Call Home messages. They should be descriptive of the system from which the messages are generated, but do not necessarily need to be valid addresses. Ideally, the Reply To value should be a real, monitored email address to catch any rejected Call Home messages.

- Step 7** Review the options that are available in the SMTP Server section.



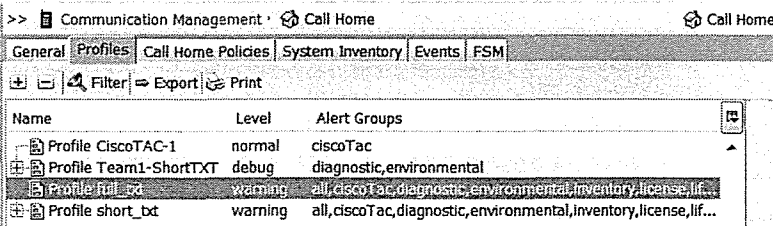
The 'SMTP Server' configuration window shows two text input fields. The 'Host (IP Address or Hostname)' field is populated with '192.168.70.57' and the 'Port' field is populated with '25'. Both fields have a small circular icon with a lowercase 'i' to their left, indicating an information or help tooltip.

- Step 8** Do not save the Call Home configuration. Because the lab is a shared environment, each student will review but not save the settings. Return the Admin State to Off.



The 'Call Home Admin' configuration window shows a 'State' section with two radio buttons: 'off' (selected) and 'on'. Below the radio buttons is a 'States' section with a text input field. At the bottom of the window are two buttons: 'Save Changes' and 'Reset Values'.

- Step 9** In the content pane, choose the **Profiles** tab, and then click **Profile full\_txt**.

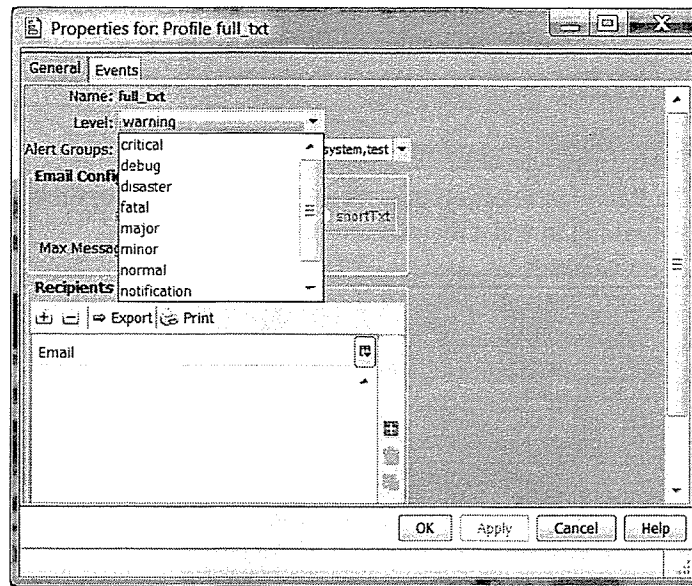


The 'Call Home Profiles' configuration window shows a table of profiles. The 'full\_txt' profile is selected. The table has three columns: Name, Level, and Alert Groups.

| Name                   | Level   | Alert Groups                                                   |
|------------------------|---------|----------------------------------------------------------------|
| Profile CiscoTAC-1     | normal  | ciscoTac                                                       |
| Profile Team1-ShortTXT | debug   | diagnostic,environmental                                       |
| Profile full_txt       | warning | all,ciscoTac,diagnostic,environmental,inventory,license,lif... |
| Profile short_txt      | warning | all,ciscoTac,diagnostic,environmental,inventory,license,lif... |

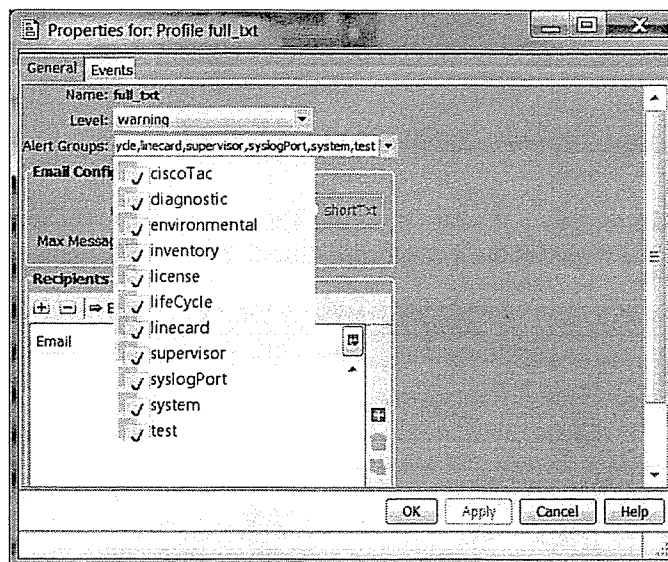
- Step 10** Right-click the **full\_txt** profile and choose **Show Navigator**.

- Step 11** Take a moment to review the message levels available. This setting dictates that all messages of the selected level and above (meaning more severe) will be sent to recipients of this profile.

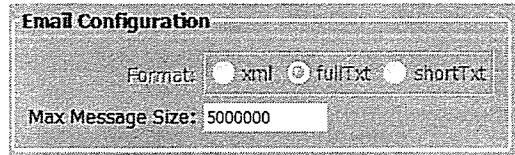


**Note** The levels in this field are listed alphabetically, not by severity. Severity order from least severe to most severe is debug, notification, normal, warning, minor, major, critical, fatal, and disaster.

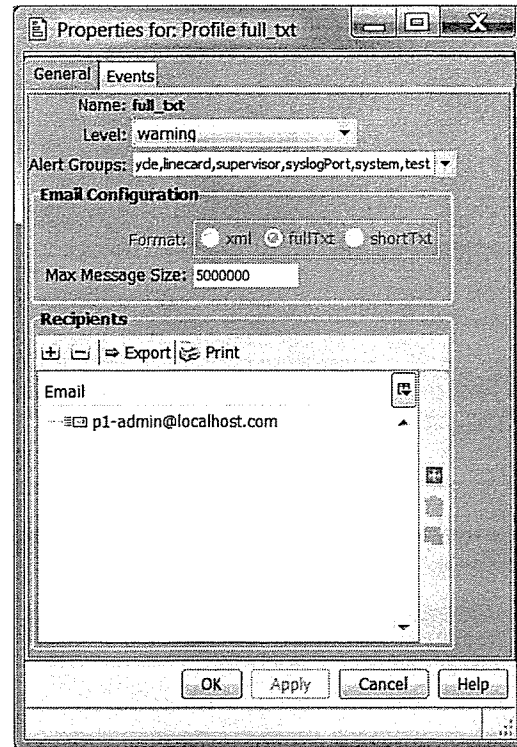
- Step 12** Take a moment to review the Alert Groups that are available. This setting dictates which category of messages will trigger this profile.



- Step 13** Review the Email Configuration section. This section allows you to choose the format of messages that are sent to recipients of this profile. You can also set a maximum message size (in bytes). Any data above this size will be truncated.



- Step 14** The Recipients section may already have users from other teams. Click the plus symbol (+) to add a recipient to this profile.

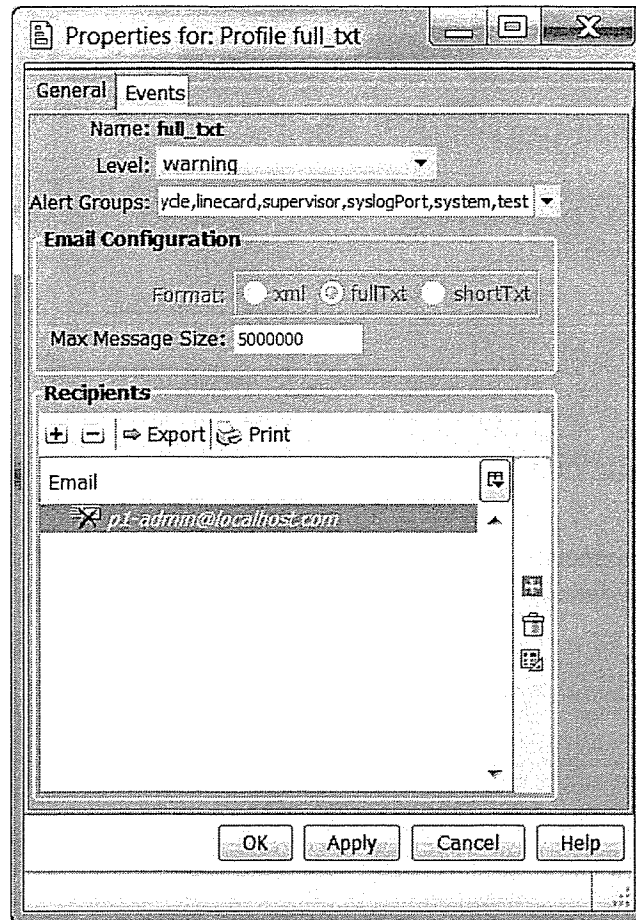


- Step 15** Add a recipient of your choosing. The address that you specify does not matter as long as it passes the syntax checking of Cisco UCS Manager.



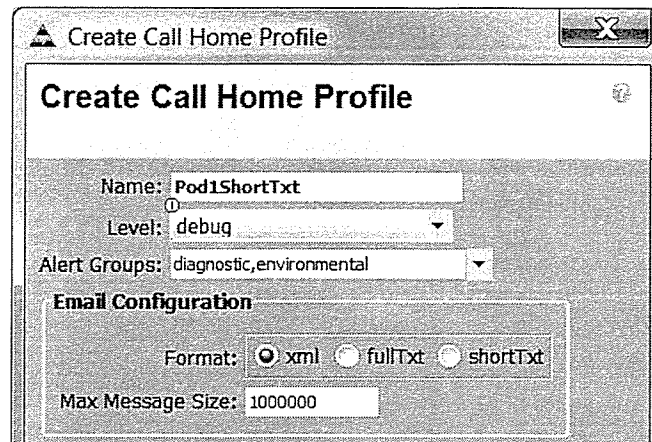
- Step 16** Click **OK** to confirm creation of the recipient.
- Step 17** Delete the recipient that you created. Highlight the recipient that you created and then click the trash icon.
- Step 18** Click **Yes** to delete the recipient.

- Step 19** Note that the recipient is not immediately removed from the list. The recipient line in the table will be grayed out and italicized, indicating that it will be removed.



- Step 20** Click **Apply** and then **OK** to complete removal of the user and to close the properties window.
- Step 21** Click the plus symbol (+) in the Profiles tab to add a new Call Home profile.
- Step 22** From the pop-up selection, click **Create Call Home Profile**.

- Step 23** Name your profile **PodXShortTxt**, where *X* is your team number. Set the Level and Alert Groups fields to any values that you wish. Set Format to **shortTxt** and leave the Max Message Size value at the default.



**Create Call Home Profile**

Name:

Level:

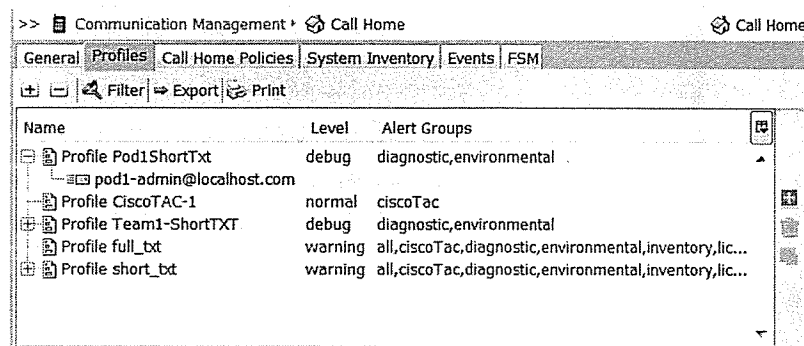
Alert Groups:

**Email Configuration**

Format: ☒ xml ☐ fullTxt ☐ shortTxt

Max Message Size:

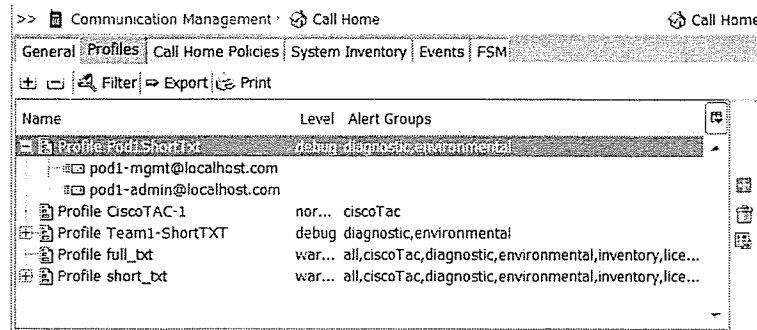
- Step 24** Add an email recipient. Click the plus symbol (+) and enter **podX-admin@localhost.com**, and then click **OK** to save your Call Home profile.
- Step 25** Click **OK** to confirm creation of your profile.
- Step 26** Expand your profile icon and verify that the recipient that you configured is listed.



| Name                     | Level   | Alert Groups                                           |
|--------------------------|---------|--------------------------------------------------------|
| Profile Pod1ShortTxt     | debug   | diagnostic,environmental                               |
| pod1-admin@localhost.com |         |                                                        |
| Profile CiscoTAC-1       | normal  | ciscoTac                                               |
| Profile Team1-ShortTXT   | debug   | diagnostic,environmental                               |
| Profile full_txt         | warning | all,ciscoTac,diagnostic,environmental,inventory,lic... |
| Profile short_txt        | warning | all,ciscoTac,diagnostic,environmental,inventory,lic... |

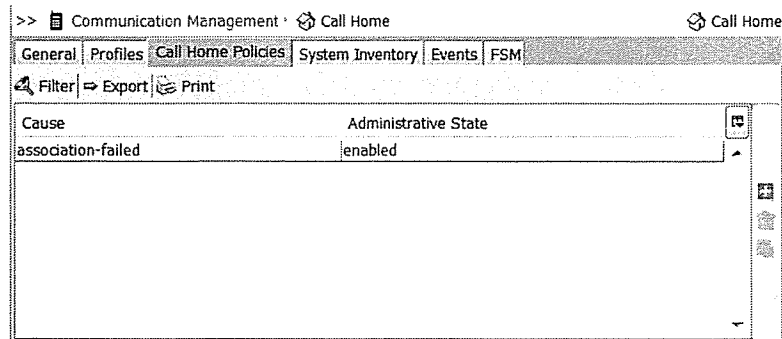
- Step 27** You might need to add additional email recipients at a future date. Right-click your profile icon and choose **Recipient**.
- Step 28** Enter **podX-mgmt@localhost.com**, and then click **OK** to save your Call Home profile.
- Step 29** Click **OK** to confirm addition of the recipient.

**Step 30** Verify that both recipients now appear under the profile icon of your team.



**Step 31** In the content pane, click the **Call Home Policies** tab.

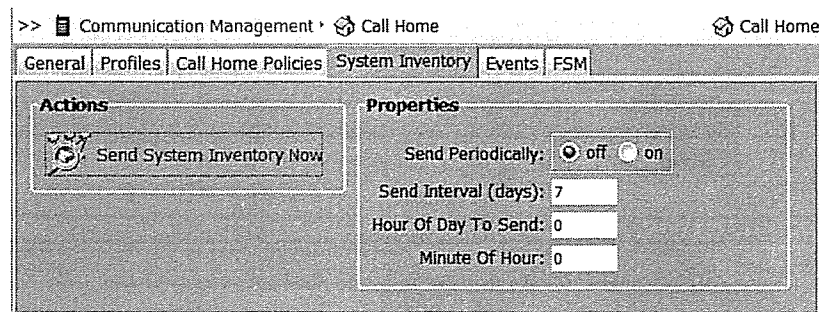
**Step 32** Click the plus symbol (+) to add a new Call Home Policy.



**Step 33** Explore the options for creating a new Call Home Policy. When you have reviewed the options available, click **Cancel**. Only one of each policy can be created. Because the lab is a shared environment, if multiple teams attempt to create the same policy, errors will occur.

**Step 34** If you receive a warning regarding committed changes, click **Yes** to confirm discarding the changes.

**Step 35** In the content pane, choose the **System Inventory** tab. Spend a few moments reviewing the configuration options for System Inventory.



**Note** Automatically sending the system inventory on a regular basis can help an organization keep track of a changing Cisco Unified Computing System deployment. It is also useful for service organizations to track additions or subtractions from customer environments for warranty or service purposes. When this feature is enabled, the system inventory is sent to any Call Home recipients in profiles that have selected the Inventory alert group.

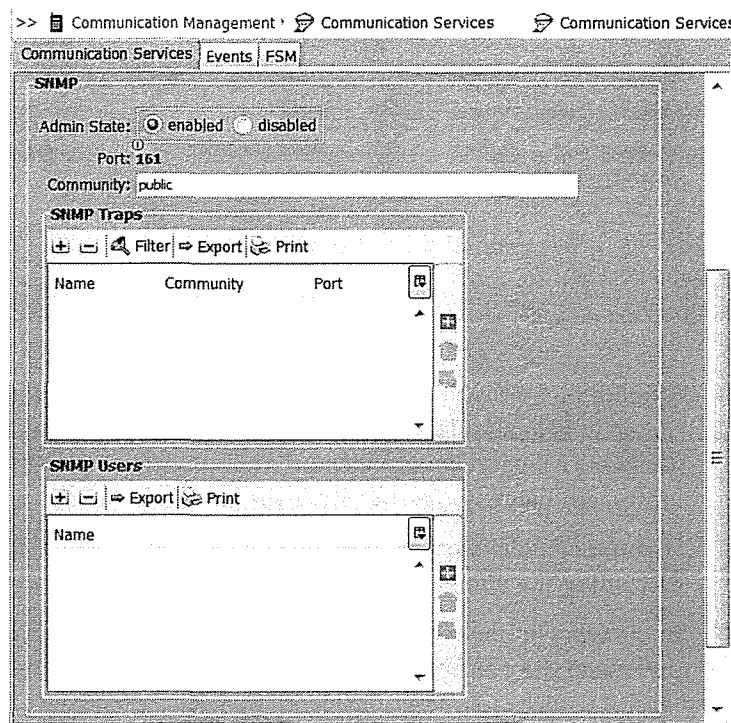
## Task 5: Configure and Test SNMPv3

In this task, you will configure and test SNMP to the Cisco UCS Fabric Interconnects.

### Activity Procedure

Complete these steps:

- Step 1** In Cisco UCS Manager, choose the **Admin** tab and filter on **Communication Management**.
- Step 2** Click the **Communication Services** element in the navigation pane.
- Step 3** In the content pane, scroll down to the SNMP panel and then click the **Enabled** radio button.



- Step 4** The default SNMP community string is public. This community string is used for SNMPv1 and SNMPv2c, but it must be set to some value even if only SNMPv3 is employed.

---

**Note** Because SNMPv1 and SNMPv2c send the community string in plaintext and offer no authentication or payload encryption, best practice is to use only SNMPv3. Because there is currently no option to disable SNMPv2, set a 32-character random hexadecimal value for the community string.

---

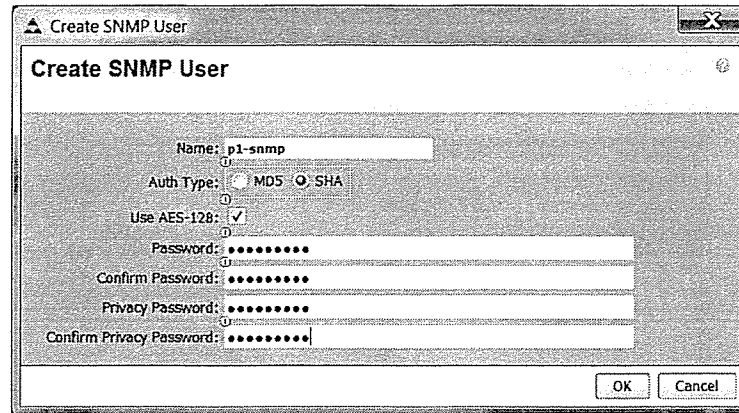
---

**Note** Because the administrative state of SNMP and the value for the community string are global settings, only one pod at a time can modify these values.

---

- Step 5** To enable SNMPv3, click the plus symbol (+) to the right of the SNMP Users panel in the content pane.

- Step 6** Refer to the Cisco UCS Reporting implementation sheet for the data that is required to build the user for your pod. The example that is shown is for pod 1.



---

**Note** SNMPv3 offers two levels of protection for accessing SNMP MIB data from the devices. On Cisco devices, they are commonly referred to as Auth and Priv, which are short for Authentication and Privacy. The Auth property (when enforced) requires user authentication to access MIB data. The Priv property requires encryption of the SNMP payload. Best practice is to employ Authentication and Privacy for maximum protection against unauthorized MIB access and eavesdropping attacks.

---

---

**Note** The Auth Type field determines the selection of cryptographic hash used to obfuscate SNMP user passwords as they pass through the network. MD5 offer a 128-bit message digest and SHA offers 160 bits. It is a best practice to use SHA.

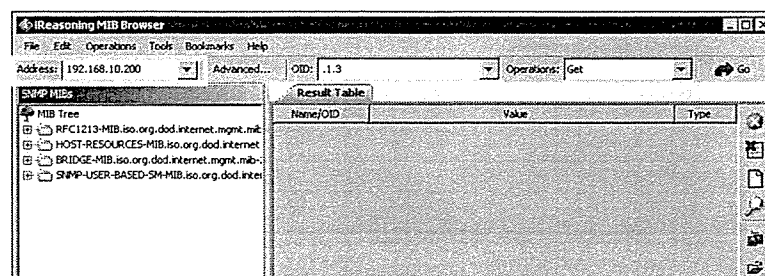
---

---

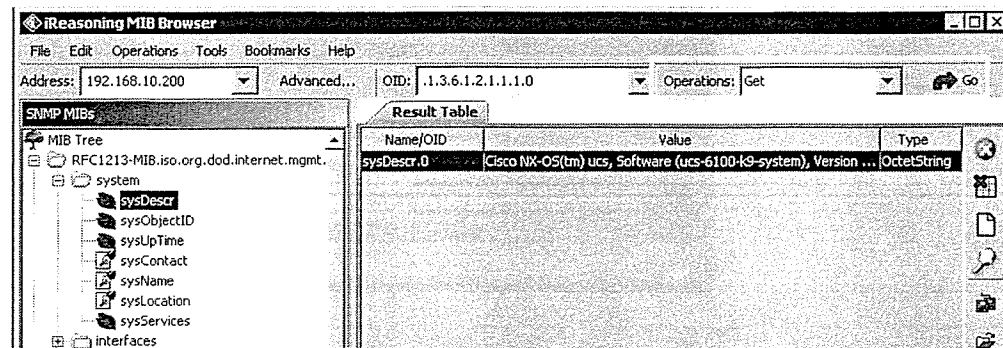
**Note** If the Use AES-128 box is checked, a Privacy Password must be set. This enables SNMP packet payload encryption.

---

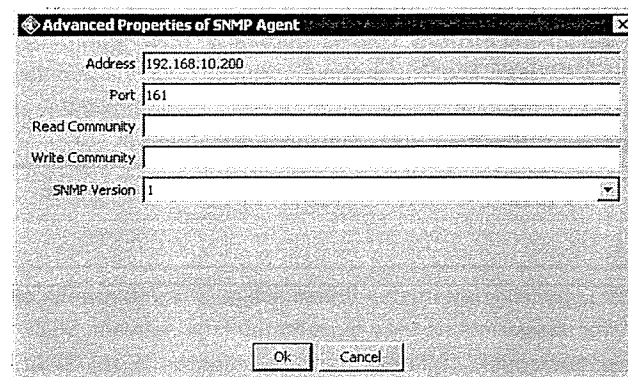
- Step 7** Click **OK** to complete the SNMP user creation.
- Step 8** Click **Save Changes** to commit the SNMP user configuration.
- Step 9** On the student PC, open My Computer from the desktop and run the c:\install\snmp\setup.exe program to install the MIB browser.
- Step 10** Double-click the **MIB Browser** icon on the desktop.
- Step 11** In the Address field, enter the IP address of the Cisco UCS Manager cluster (192.168.10.200).



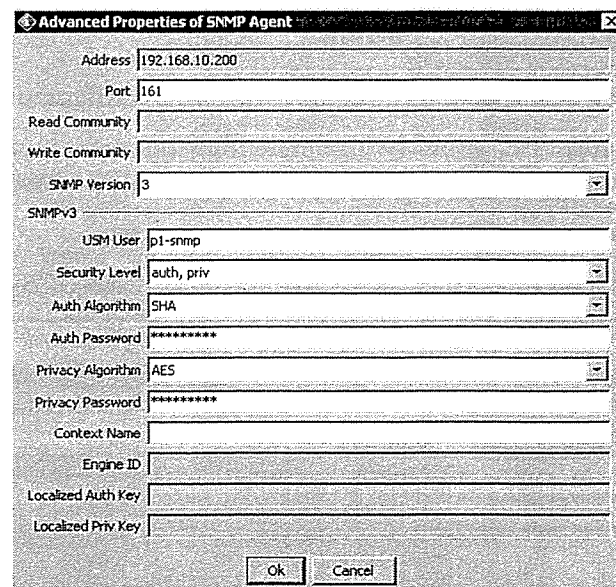
- Step 12** Under the SNMP MIB Tree, expand RFC1213-MIB by clicking the plus symbol (+).
- Step 13** Expand the **System** folder and choose **sysDescr**.
- Step 14** Be sure that **Get** is selected in the Operations field, and then click **Go**. This will use the default SNMP community string (public) to pull information, like the **show version** command does in Cisco NX-OS.



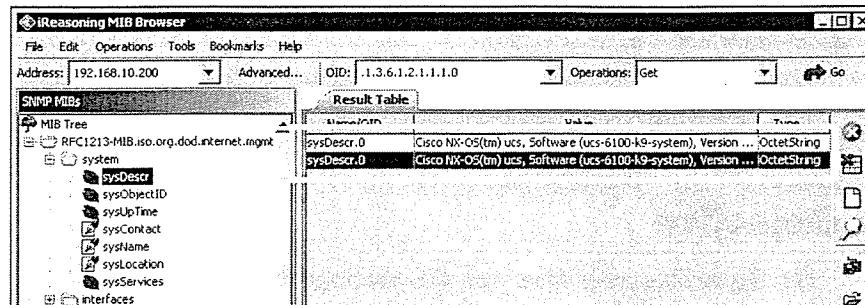
- Step 15** Click **Advanced** to the right of the Address field.



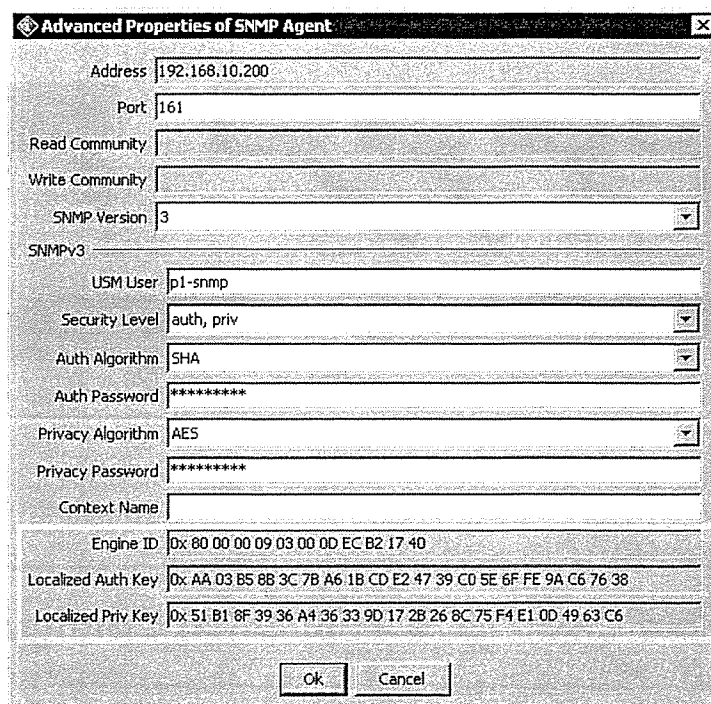
- Step 16** Choose **SNMP Version 3** from the drop-down menu. The Advanced Properties page will expand to include SNMPv3 attributes. Enter your SNMPv3 credentials exactly like you did in Cisco UCS Manager SNMP User. The Context Name field remains blank.



- Step 17** Click **OK** to save the profile.
- Step 18** From the main MIB browser screen, click **Go** to test the new settings.
- Step 19** A second line with the sysDescr information should appear.



- Step 20** Click **Advanced** again and observe that hashed values now appear in the Localized Auth Key and Localized Priv Key fields. The Engine ID uniquely identifies the fabric interconnect.



- Step 21** Click **OK** to close the Advanced Properties dialog box and the MIB Browser.
- Step 22** As a bonus exercise, observe the differences in SNMP packet payload, by using Wireshark.

## Activity Verification

You have completed this activity when you have achieved these goals:

- You have generated and recovered from major alarms.
- You have disabled unnecessary local logging functions.
- You have configured syslog destinations and verified that messages reach the server.
- You have explored the configuration of the Smart Call Home feature.

# Lab A-1: Initial Cisco UCS B-Series Configuration

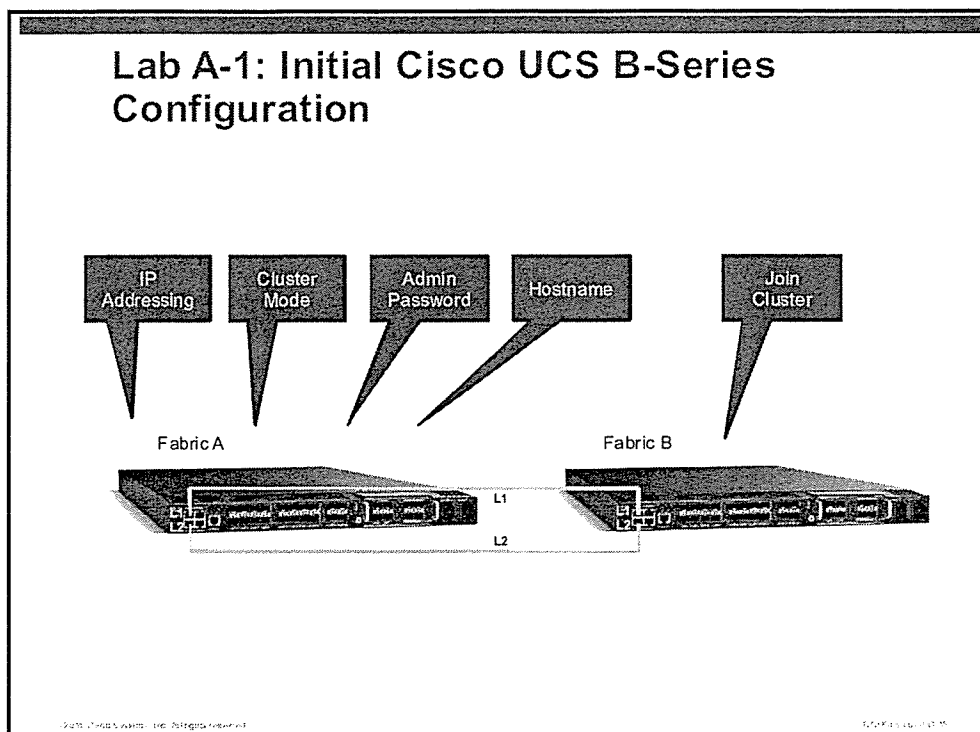
Complete this lab activity to practice what you learned in the related lesson.

## Activity Objective

In this activity, the student is presented with a guided demonstration to illustrate initial setup of the Cisco 6100 Series fabric interconnects. This appendix is a useful reference during installations.

## Visual Objective

The figure illustrates what you will accomplish in this activity.



## Task 1: Complete Cisco UCS 6100 Initial Configuration

In this task, you will complete the initial configuration of a Cisco UCS 6100 Fabric Interconnect and establish a cluster relationship between two Cisco UCS 6100 Fabric Interconnects.

### Activity Procedure

Complete these steps:

**Step 1** Choose the console method of initial configuration.

System is coming up ... Please wait ...

nohup: appending output to 'nohup.out'

---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of the system. Only minimal configuration including IP connectivity to the Fabric interconnect and its clustering mode is performed through these steps.

Type Ctrl-C at any time to abort configuration and reboot system.

To back track or make modifications to already entered values, complete input till end of section and answer no when prompted to apply configuration.

Enter the configuration method. (console/gui) ? **console**

**Step 2** Specify that you will be setting up the system manually (as opposed to restoring from a backup) and set the admin password.

Enter the setup mode; setup newly or restore from backup.  
(setup/restore) ? **setup**

You have chosen to setup a new Fabric interconnect. Continue?  
(y/n): **y**

Enter the password for "admin": **cisco12345**  
Confirm the password for "admin": **cisco12345**

**Step 3** Set the cluster configuration options. For the first switch, use "A." For the second switch, use "B."

---

**Note** The system name will apply to both nodes—the fabric designator (A or B) will be appended to form the hostname.

---

Do you want to create a new cluster on this Fabric interconnect (select 'no' for standalone setup or if you want this switch to be added to an existing cluster)? (yes/no) [n]:  
**y**

Enter the switch fabric (A/B) []: **A**  
Enter the system name: **s6100**

**Step 4** Set the management IP configuration options. Each fabric interconnect has a unique IP address as well as a shared cluster address.

Physical Switch Mgmt0 IPv4 address : **192.168.10.101**

Physical Switch Mgmt0 IPv4 netmask : **255.255.255.0**

IPv4 address of the default gateway : **192.168.10.254**

Cluster IPv4 address : **192.168.10.200**

Configure the DNS Server IPv4 address? (yes/no) [n]: **n**

Configure the default domain name? (yes/no) [n]: **n**

**Step 5** Confirm the configuration information and apply it.

Following configurations will be applied:

Switch Fabric=A

System Name=s6100

Physical Switch Mgmt0 IP Address=192.168.10.101

```
Physical Switch Mgmt0 IP Netmask=255.255.255.0
Default Gateway=192.168.10.254
```

```
Cluster Enabled=yes
Cluster IP Address=192.168.10.200
```

```
Apply and save the configuration (select 'no' if you want to
re-enter)? (yes/no): yes
```

```
Applying configuration. Please wait.
```

**Step 6** Log in to the switch and view the cluster status.

```
s6100-A login: admin
Password: cisco12345
Cisco UCS 6100 Series Fabric Interconnect
```

```
TAC support: http://www.cisco.com/tac
```

```
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
```

```
...
```

```
s6100-A# show cluster state
Cluster Id: 0x2ebe725040b711de-0x92a7000decb21744
```

```
A: UP, ELECTION IN PROGRESS, (Management services: UP)
B: UNRESPONSIVE, INAPPLICABLE, (Management services:
UNRESPONSIVE)
```

```
HA NOT READY:
No chassis configured
WARNING: Failover cannot start, chassis configuration is
incomplete
```

**Step 7** Complete the initial configuration on fabric interconnect B. When starting, that fabric interconnect should detect the presence of the cluster.

```
System is coming up ... Please wait ...
nohup: appending output to 'nohup.out'
```

```
---- Basic System Configuration Dialog ----
```

```
This setup utility will guide you through the basic
configuration of the system. Only minimal configuration
including IP connectivity to the Fabric interconnect and its
clustering mode is performed through these steps.
```

```
Type Ctrl-C at any time to abort configuration and reboot
system.
```

```
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.
```

```
Enter the configuration method. (console/gui) ? console
```

Installer has detected the presence of a peer Fabric interconnect. This Fabric interconnect will be added to the cluster. Continue (y/n) ? **y**

**Step 8** Provide the admin password to the first switch and the local unique IP address for this fabric interconnect. All of the other configuration options will be replicated from the first switch.

```
Enter the admin password of the peer Fabric interconnect:
Connecting to peer Fabric interconnect... done
Retrieving config from peer Fabric interconnect... done
Peer Fabric interconnect Mgmt0 IP Address: 192.168.10.101
Peer Fabric interconnect Mgmt0 IP Netmask: 255.255.255.0
Cluster IP address : 192.168.10.200
Physical Switch Mgmt0 IPv4 address : 192.168.10.102
Apply and save the configuration (select 'no' if you want to
re-enter)? (yes/no): yes
```

**Step 9** Log in and display the cluster status.

```
s6100-B login: admin
Password: cisco12345
Cisco UCS 6100 Series Fabric Interconnect
```

```
TAC support: http://www.cisco.com/tac
```

```
Copyright (c) 2010, Cisco Systems, Inc. All rights reserved.
```

```
...
```

```
s6100-B# show cluster state
Cluster Id: 0x2ebe725040b711de-0x92a7000decb21744
```

```
B: UP, SUBORDINATE
```

```
A: UP, PRIMARY
```

```
HA NOT READY:
```

```
No chassis configured
```

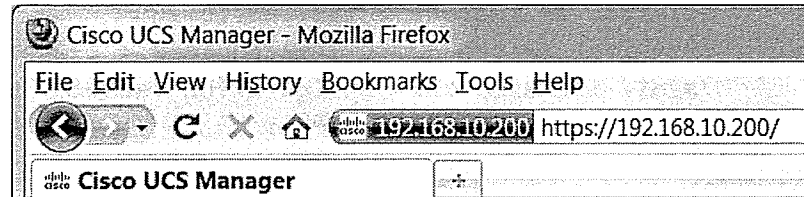
## Task 2: Configure Server Ports to Allow Chassis Discovery

In this task, you will configure four of the fixed 10 GB ports as server ports that connect to the IOM on the chassis.

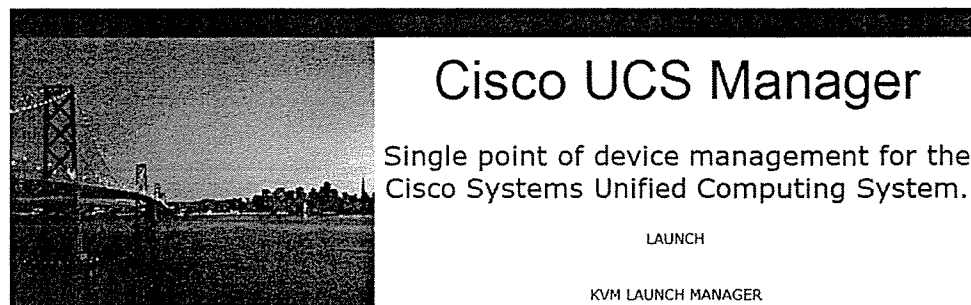
### Activity Procedure

Complete these steps:

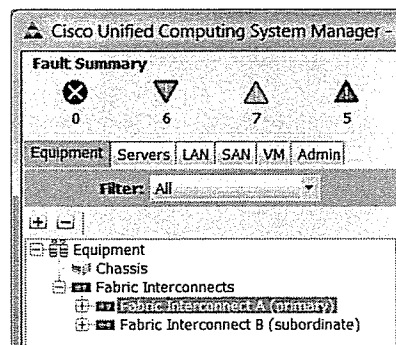
- Step 1** Log in to the Cisco UCS Manager GUI to complete the initial configuration. Direct a web browser to the cluster IP address that was specified in the earlier task.
- Step 2** Click the **Launch** link to start the Cisco UCS Manager application.



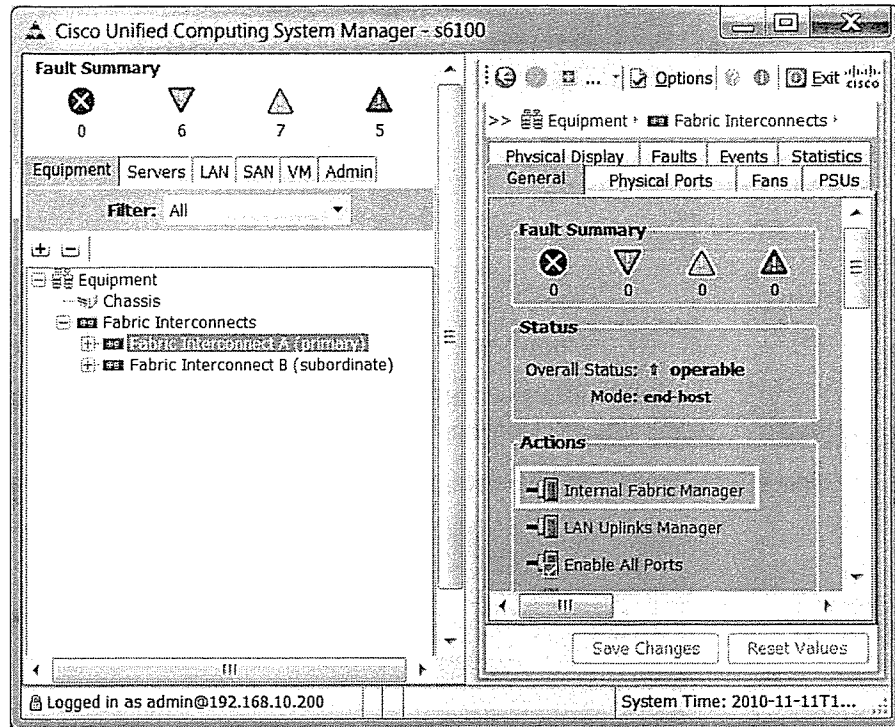
**Note** It is normal to receive a security error in your browser. The root certificate of Cisco UCS Manager is a self-signed certificate and is not in the root certificate store of your browser.



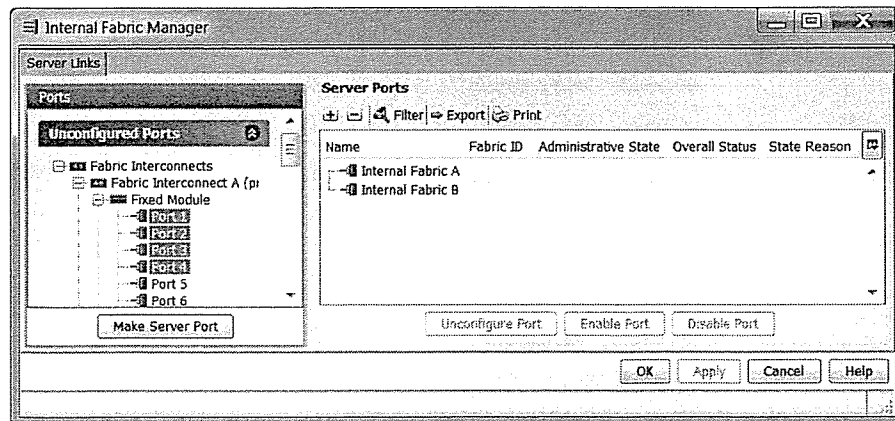
- Step 3** Log in by using the username **admin** and the password **cisco12345**, entered during the setup wizard.
- Step 4** Note that in the Equipment tab, both fabric interconnects are visible, with no chassis. Recall that the default state of all interfaces on the fabric interconnects is the unconfigured state.



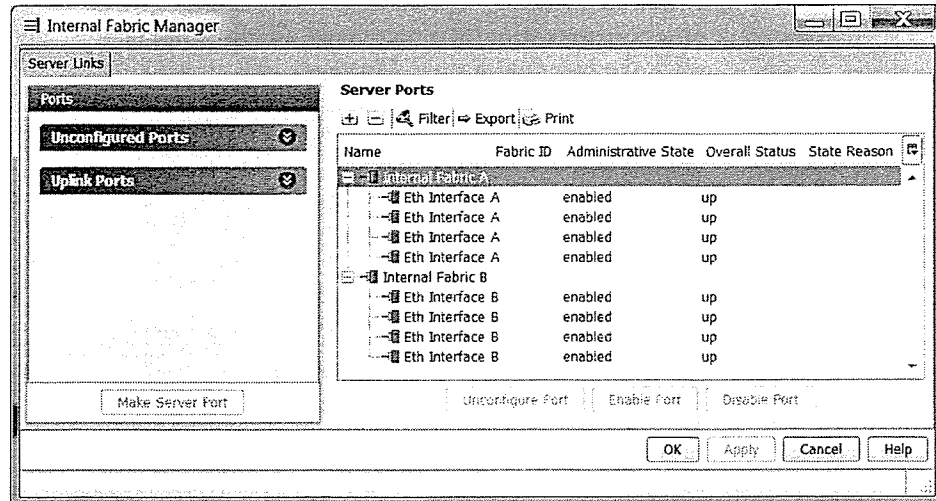
- Step 5** Before the chassis is manageable and the cluster becomes fully operational, each fabric interconnect must have at least one active link to the chassis. Expand **Fabric Interconnect A** in the Equipment tab of the navigation pane. In the content pane, click the **Internal Fabric Manager** link.



- Step 6** Click the double down-arrow to expand the list of unconfigured ports. Choose ports 1 through 4 by pressing **Ctrl** while clicking each port in turn. Click **Make Server Port**. Scroll down the list to fabric interconnect B and make ports 1 through 4 server ports.

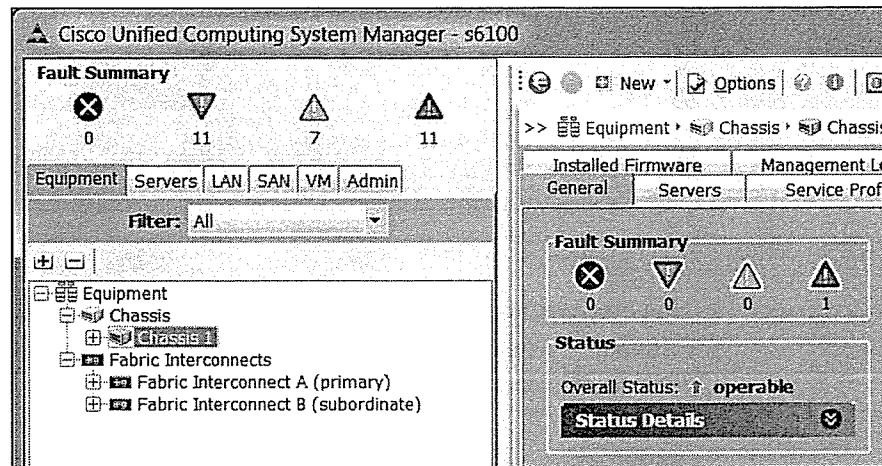


Step 7 Ports 1 through 4 and fabric interconnects A and B now appear as server ports.



Step 8 Click OK to close the Internal Fabric Manager.

Step 9 Chassis 1 has been discovered and is now visible in the Equipment tab.



Step 10 Return to the CLI and check the cluster status again. It might take as much as 30 seconds before the CLI reports that the cluster is operational.

```
s6100-A# show cluster state
```

```
Cluster Id: 0x2ebe725040b711de-0x92a7000decb21744
```

```
A: UP, PRIMARY
```

```
B: UP, SUBORDINATE
```

```
HA NOT READY:
```

```
No chassis configured
```

```
s6100-A# show cluster state
```

```
Cluster Id: 0xdc25b7d840bb11de-0xba02000decb21744
```

```
A: UP, PRIMARY
```

```
B: UP, SUBORDINATE
```

```
HA READY
```

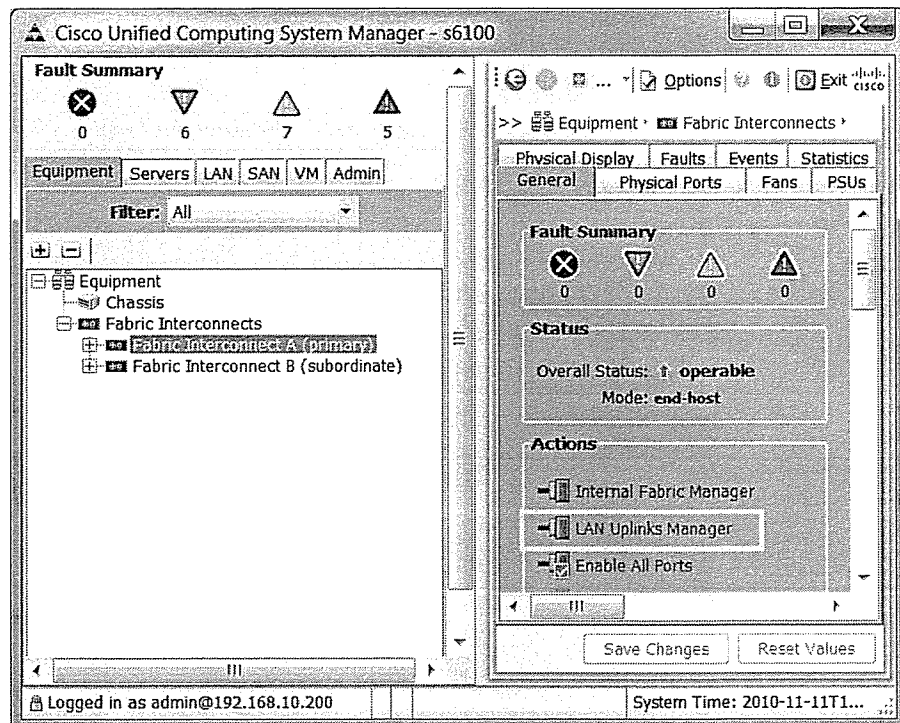
## Task 3: Configure Uplink Ports to Northbound Communications

In this task, you will configure two port channels to provide a communication path from the fabric interconnects to the aggregation and core layers of the data center network. This is often referred to as northbound communication. Communication from the fabric interconnects to the IOMs is referred to as southbound.

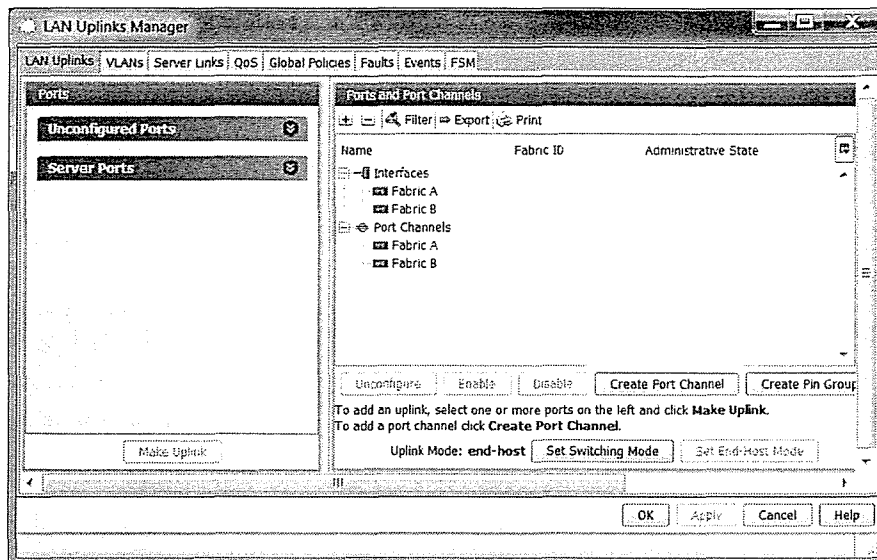
### Activity Procedure

Complete these steps:

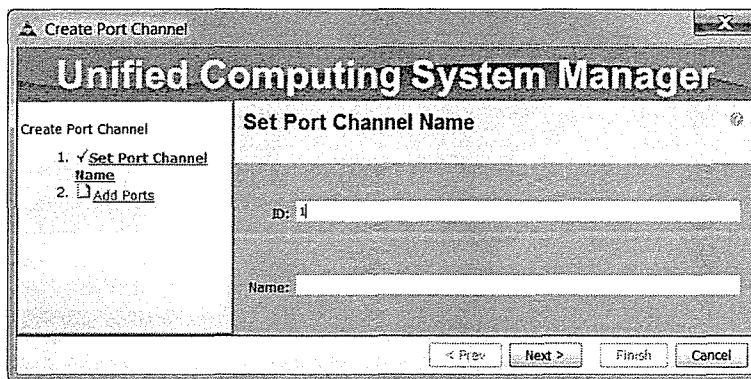
- Step 1** Configuring uplink ports is similar to configuring server ports. Choose either fabric interconnect in the Equipment tab of the navigation pane. Click the **LAN Uplinks Manager** link.



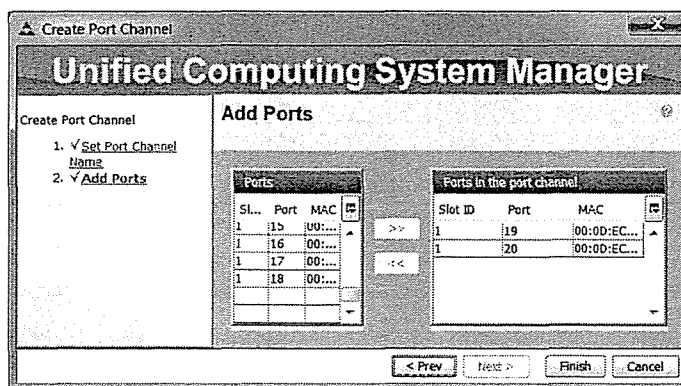
- Step 2** Instead of creating individual links, create a two-interface port channel on each fabric interconnect. Click **Create Port Channel** to begin the wizard. You are presented with the choice of Fabric A or Fabric B. Choose **Fabric A** to create the first port channel on Fabric A.



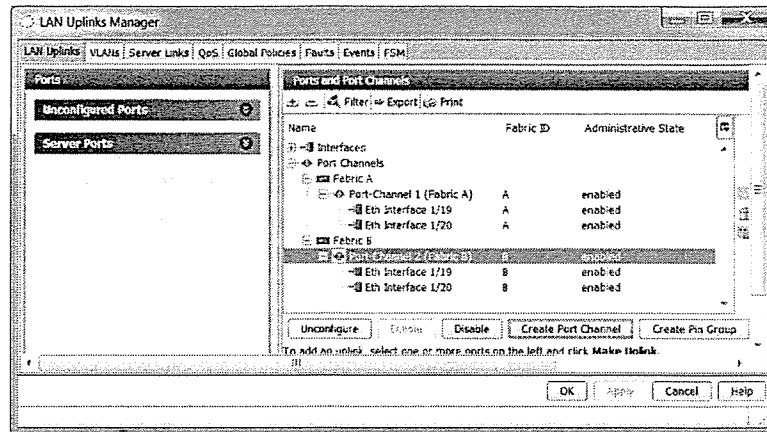
- Step 3** On the first screen of the port channel creation wizard, enter a port channel ID of 1, and then click **Next**.



- Step 4** Press **Ctrl** and choose ports 19 and 20 from the port list. Click **>>** to add the ports to the port channel. Click **Finish** to end the wizard. Repeat these steps to create a port channel with ports 19 and 20 on Fabric B.



- Step 5** Your port channels should appear in the LAN Uplinks Manager. Choose each port channel and then click **Enable** to complete the process.



- Step 6** Click **OK** to close the LAN Uplinks Manager.

## Task 4: Configure IP Communication to Cisco IMC

In this task, you will configure a pool of IP addresses that will be assigned to the Cisco IMC on each server blade.

---

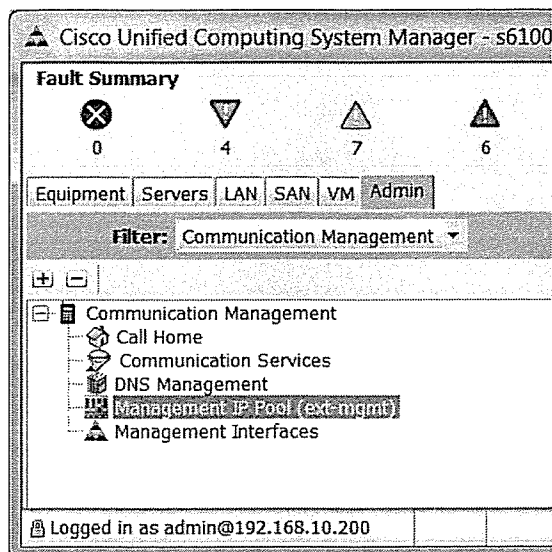
**Note** To avoid confusion when using the term Cisco IMC, it is important to consider the context in which it is used. In the context of Cisco UCS C-Series Rack-Mount Servers, Cisco IMC refers to the configuration user interface. In the context of Cisco UCS B-Series devices, Cisco IMC refers to the chip on the server motherboard that provides access to KVM, IPMI, and SoL services. In earlier versions of the documentation, the Cisco IMC was called the BMC.

---

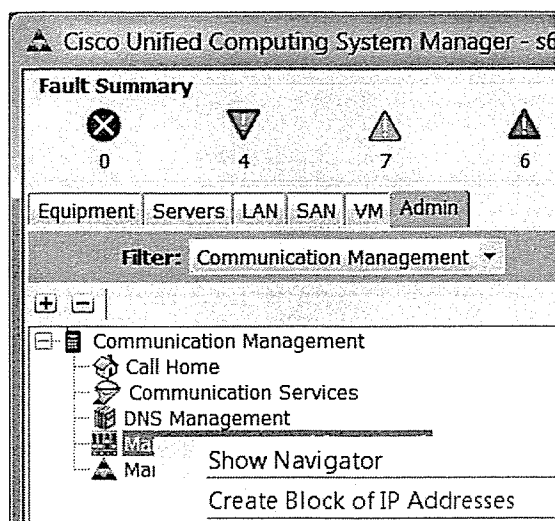
### Activity Procedure

Complete these steps:

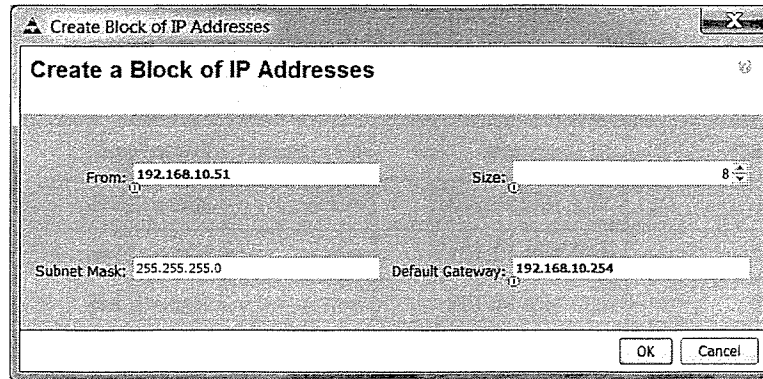
- Step 1** Navigate to the **Admin** tab and choose the **Communications Management** filter from the drop-down list. Choose the **Management IP Pool** icon.



- Step 2** Right-click **Management IP Pool** and choose **Create Block of IP Addresses**.

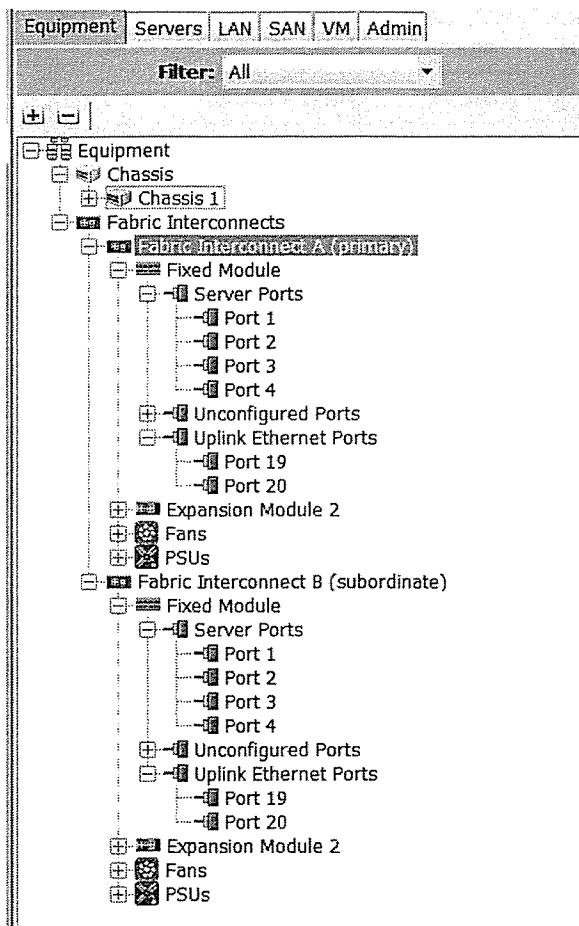


**Step 3** Create a block of eight addresses starting at 192.168.10.51 and then click **OK**.



## Activity Verification

When you complete this activity, your network topology should be like the following:



# Lab Reference Guide

This section contains a listing of device addresses and authentication credentials.

## Infrastructure

| Device | IP Address     | Username | Password  |
|--------|----------------|----------|-----------|
| UCSM   | 192.168.10.200 | admin    | NXos12345 |
| 6120-A | 192.168.10.101 | admin    | NXos12345 |
| 6120-B | 192.168.10.102 | admin    | NXos12345 |
| 5010-A | 192.168.10.91  | student  | NXos12345 |
| 5010-B | 192.168.10.92  | student  | NXos12345 |
| MDS-1  | 192.168.110.26 | student  | NXos12345 |
| MDS-2  | 192.168.110.51 | student  | NXos12345 |
| 7010-A | 192.168.100.1  | student  | NXos12345 |
| 7010-B | 192.168.100.2  | student  | NXos12345 |
| CIMC-1 | 192.168.10.41  | admin    | NXos12345 |
| CIMC-2 | 192.168.10.42  | admin    | NXos12345 |
| CIMC-3 | 192.168.10.43  | admin    | NXos12345 |
| CIMC-4 | 192.168.10.44  | admin    | NXos12345 |
| CIMC-5 | 192.168.10.45  | admin    | NXos12345 |
| CIMC-6 | 192.168.10.46  | admin    | NXos12345 |

## Remote Desktops

| Device       | IP Address    | Username      | Password |
|--------------|---------------|---------------|----------|
| Student PC 1 | 192.168.70.41 | administrator | cisco123 |
| Student PC 2 | 192.168.70.42 | administrator | cisco123 |
| Student PC 3 | 192.168.70.43 | administrator | cisco123 |
| Student PC 4 | 192.168.70.44 | administrator | cisco123 |
| Student PC 4 | 192.168.70.45 | administrator | cisco123 |
| Student PC 5 | 192.168.70.46 | administrator | cisco123 |

## ESXi Servers

| Device | Hostname    | IP Address     | Username | Password  |
|--------|-------------|----------------|----------|-----------|
| B200   | p1-b-esx-dc | 192.168.110.21 | root     | Qwer12345 |
| B200   | p2-b-esx-dc | 192.168.110.22 | root     | Qwer12345 |
| B200   | p3-b-esx-dc | 192.168.110.23 | root     | Qwer12345 |
| B200   | p4-b-esx-dc | 192.168.110.24 | root     | Qwer12345 |
| B200   | p5-b-esx-dc | 192.168.110.25 | root     | Qwer12345 |
| B200   | p6-b-esx-dc | 192.168.110.26 | root     | Qwer12345 |
| C200   | p1-c-esx-dc | 192.168.110.51 | root     | Qwer12345 |
| C200   | p2-c-esx-dc | 192.168.110.52 | root     | Qwer12345 |
| C200   | p3-c-esx-dc | 192.168.110.53 | root     | Qwer12345 |
| C200   | p4-c-esx-dc | 192.168.110.54 | root     | Qwer12345 |
| C200   | p5-c-esx-dc | 192.168.110.55 | root     | Qwer12345 |
| C200   | p6-c-esx-dc | 192.168.110.56 | root     | Qwer12345 |

