Cisco Data Center Unified Computing Implementation (DCUCI) Lab Guide

L5519C-001
Nov 2011

Global Knowledge®

Cisco Data Center Unified Computing Implementation (DCUCI) Lab Guide

L5519C-001
Nov 2011

Table of Contents

DCUCI

Lab Guide

Overview

This guide includes these activities:

- Lab 2-1 - Exploring UCS Hardware
- Lab 3-1 - Upgrading Cisco UCS Components
- Lab 6-1 - Creating Simple Service Profiles
- Lab 6-2 - Configuring Resource Pools
- Lab 6-3 - Creating Mobile Service Profiles
- Lab 7-1 - Testing High Availability
- Lab 7-2 - Backing Up and Importing Configuration Data
- Lab 7-3 – Reporting
- Lab 9 – Virtualization TBD

Naming Conventions for UCS Lab Setup

VSAN Assignment

Team Number	VSAN ID	VSAN Name	UCS Fabric	FCoE VLAN	SAN Boot Target WWN
Odd -1,3,5,7	11	VSAN11	A	1011	50:0a:09:81:98:4a:91:fd
Even - 2,4,6,8	12	VSAN12	B	1012	50:0a:09:82:98:4a:91:fd

WWPN Assignment

Pod	Linux	ESXi
Pod1	20:00:00:25:B5:0A:01:02	20:00:00:25:B5:0A:01:03
PodX	20:00:00:25:B5:0Y:0X:02	20:00:00:25:B5:0Y:0X:03

where X your team number

and Y is A for odd and B for even team numbers

WWNN Assignment

Pod	Linux	ESXi
Pod1	20:00:01:25:B5:0A:01:02	20:00:01:25:B5:0A:01:03
PodX	20:00:01:25:B5:0Y:0X:02	20:00:01:25:B5:0Y:0X:03

where X is your team number

and Y is A for odd and B for even team numbers

MAC Assignment

Pod	Linux	ESXi
Pod1	00:25:b5:00:01:02	00:25:b5:00:01:03
PodX	00:25:b5:00:0X:02	00:25:b5:00:0X:03

UUID Assignment

Pod	Linux	ESXi
Pod1	1000-000000000002	1000-000000000003
PodX	X000-000000000002	X000-000000000003

Lab 2-1: Exploring Cisco Unified Computing System Hardware

Complete this lab exercise to examine the Cisco Unified Computing System hardware components and practice what you learned in the related module.

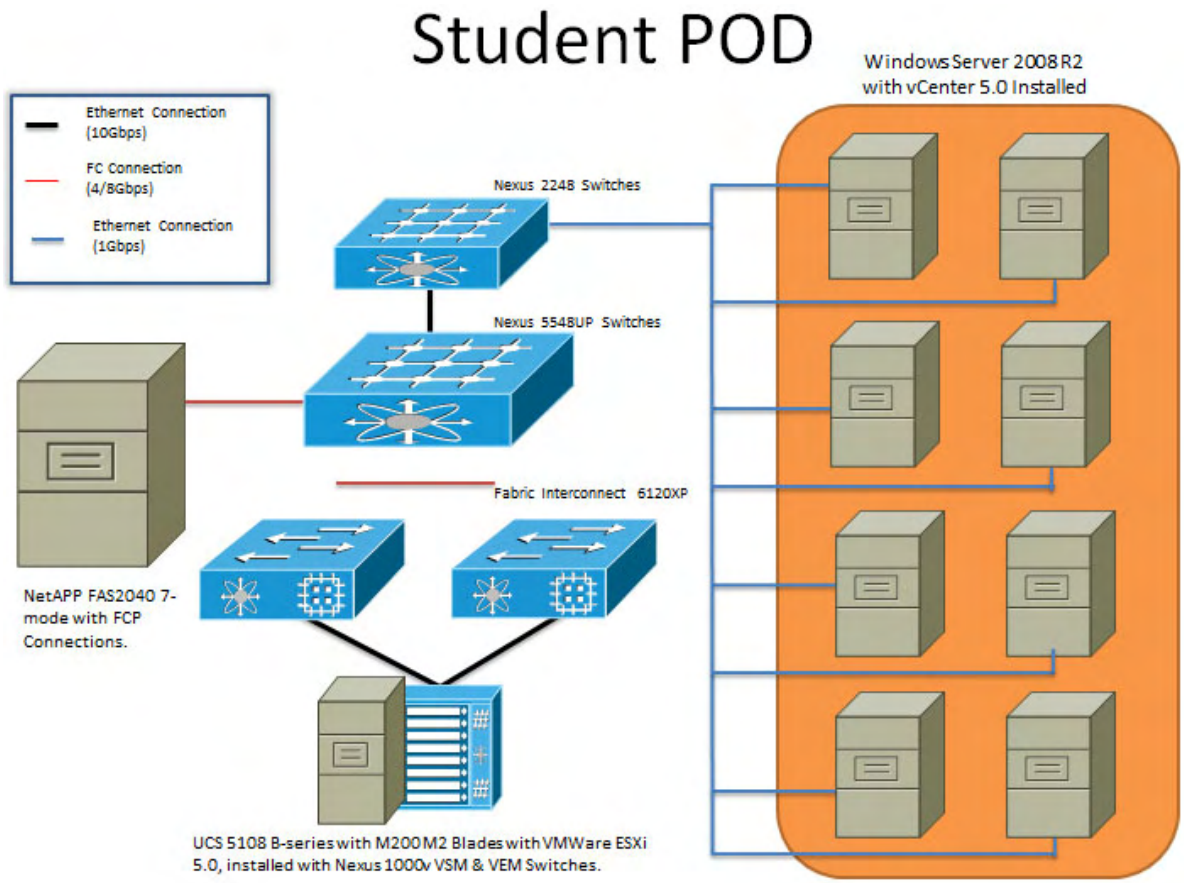
Activity Objective

In this activity, you will use the Data Center Unified Computing Design lab topology and Cisco UCS to examine, identify, and verify Cisco UCS hardware components. After completing this activity, you will be able to meet these objectives:

- Examine Cisco UCS cluster configuration
- Identify Cisco UCS Fabric Interconnect switches configuration
- Identify Cisco UCS chassis configuration
- Identify Cisco UCS IOM configuration
- Identify Cisco UCS Server Blade configuration
- Connect to Cisco UCS Server Blade using KVM console
- Decommission and re-acknowledge the assigned Cisco UCS Server Blade

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

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

- Two Cisco UCS 6120XP Fabric Interconnect switches
- Two Cisco UCS 5108 Chassis
- Two Cisco UCS 2104XP IO Modules
- Eight Cisco UCS B200-M2 Server Blades

Task 0: Connecting to the UCS Lab

In this task, you will connect to the Cisco UCS equipment.

Note You will conduct this task on Cisco UCS equipment shared between the pods. For that reason, you will only examine the setup and will not change any parameters if not required by the task.

Activity Procedure

Complete these steps:

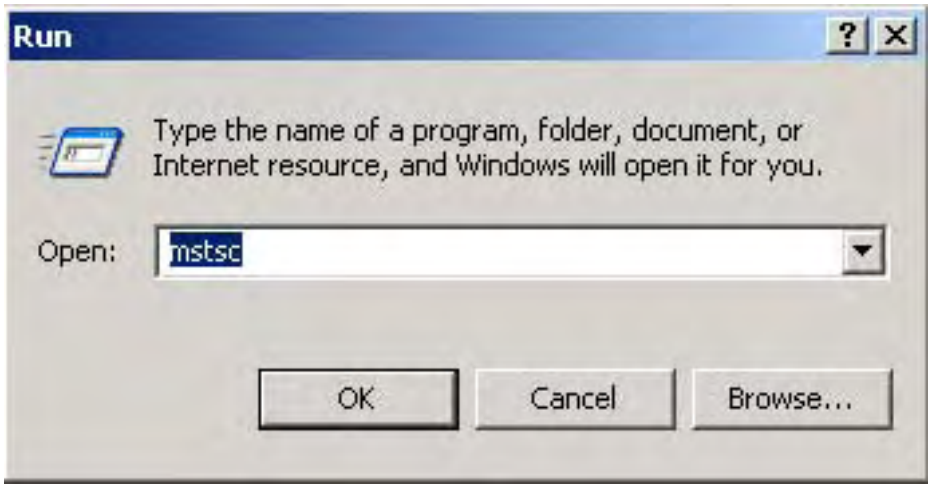
Step 1 Your instructor will assign you a pod and a password.

Step 2 Open a remote desktop to the IP address given by your instructor.

Step 3 Ensure that the port number is included to the end. .e.q. 115.42.173.79:102X0

Step 4 Login in as ‘administrator’ with the password ‘P@ssw0rd’.

Step 5 You should be presented with the student desktop.



Task 1: Examining Cisco UCS Cluster Configuration

In this task, you will examine the Cisco UCS equipment general information and verify the basic management configuration.

Note You will conduct this task on Cisco UCS equipment shared between the pods. For that reason, you will only examine the setup and will not change any parameters if not required by the task.

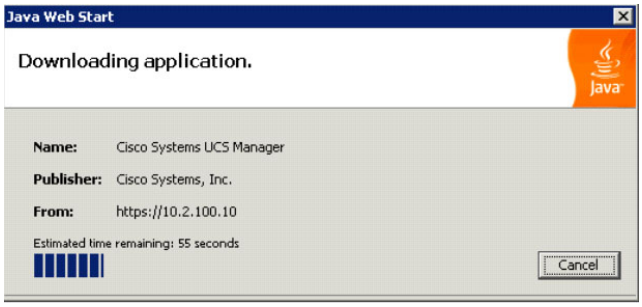
Activity Procedure

Complete these steps:

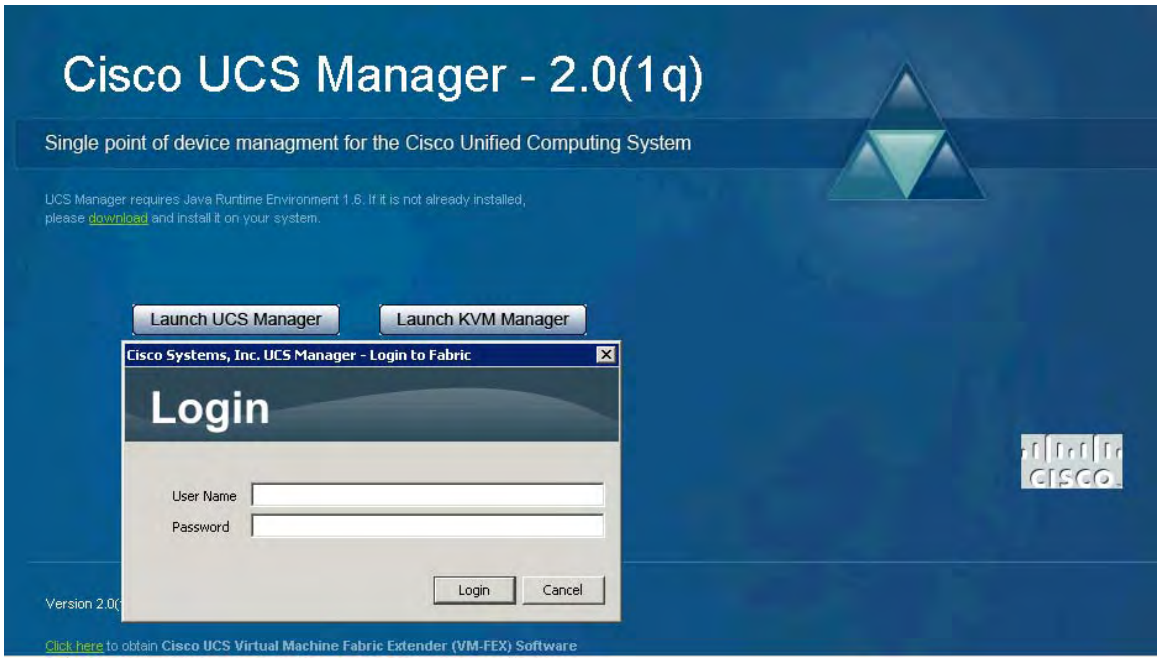
Step 7 Connect to the student desktop as demonstrated by your instructor.

Step 8 Once connected to the student desktop, launch a web browser and connect to the UCS Manager Cluster IP address 10.2.100.10 or double click the Cisco UCS Manager Icon on the desktop.

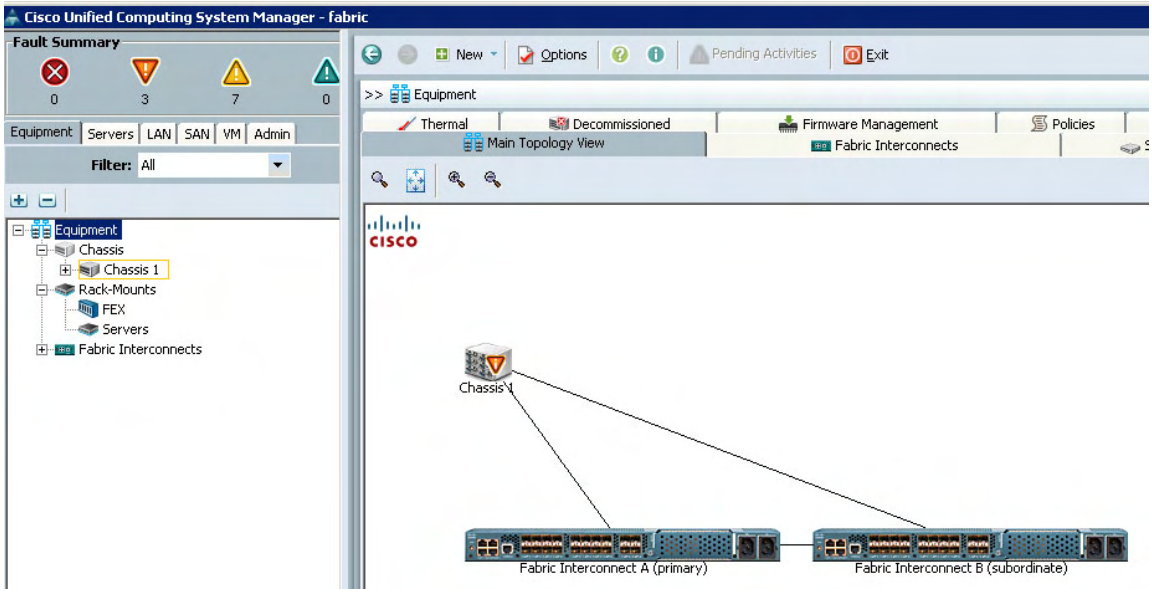
Step 9 If this is the first launch of the Cisco UCS Manager from the assigned student desktop, the launch sequence begins by downloading the Cisco UCS Manager Java application.



Step 10 When the download is finished, you will be prompted to enter the login credentials. User name: ‘admin’ and password ‘cisco123’.

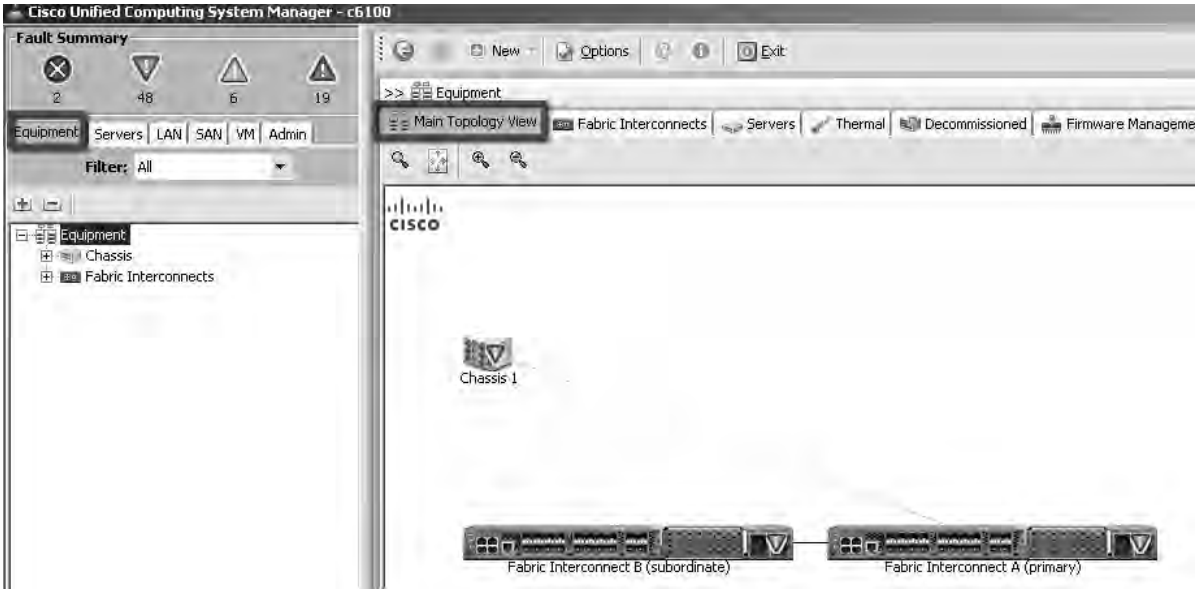


Step 11 When successfully authenticated, the Cisco UCS Manager application launches and the Cisco UCS Manager window appears.

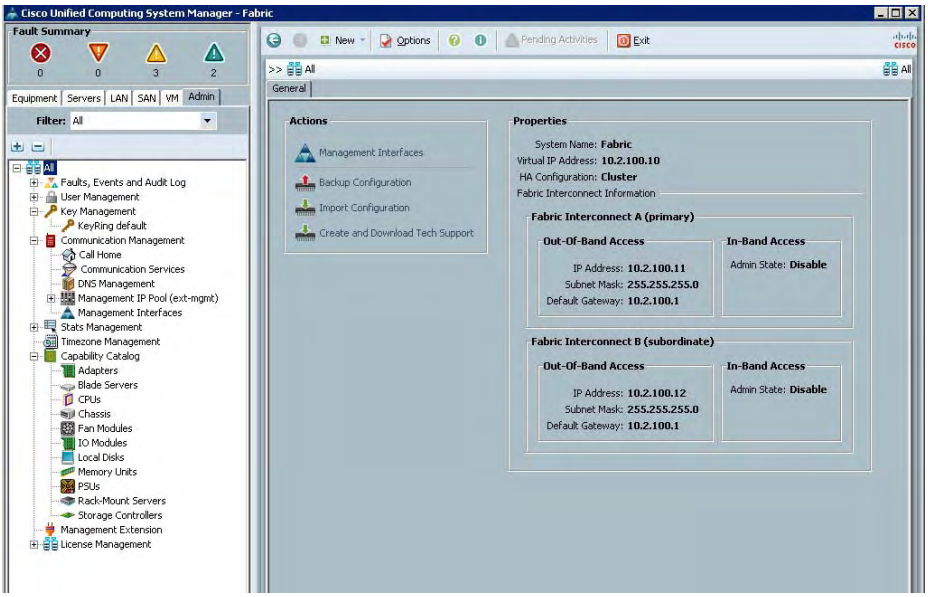


Step 12 Examine the Cisco UCS topology by selecting the **Equipment** tab in the left pane and then clicking the **Main Topology View** tab in the right pane (if not already selected). You will see the Cisco UCS topology similar to the one below: Cisco UCS 5108 Chassis and two Cisco UCS6120XP Fabric Interconnect switches.

**



Step 13 Select the **Admin** tab in the left pane of the window to examine and verify the basic management information presented in the **General** tab on the right pane. Select the **All** option in the left pane tree structure to see the Cisco UCS cluster and individual Fabric Interconnect switch management information.



1. What are the Cisco UCS Fabric Interconnect A and B management IP addresses, subnet mask, and default gateway?

_____

2. What is the high-availability configuration setting?

_____

3. What is the cluster name?

_____

Task 2: Examining Cisco UCS Fabric Interconnects

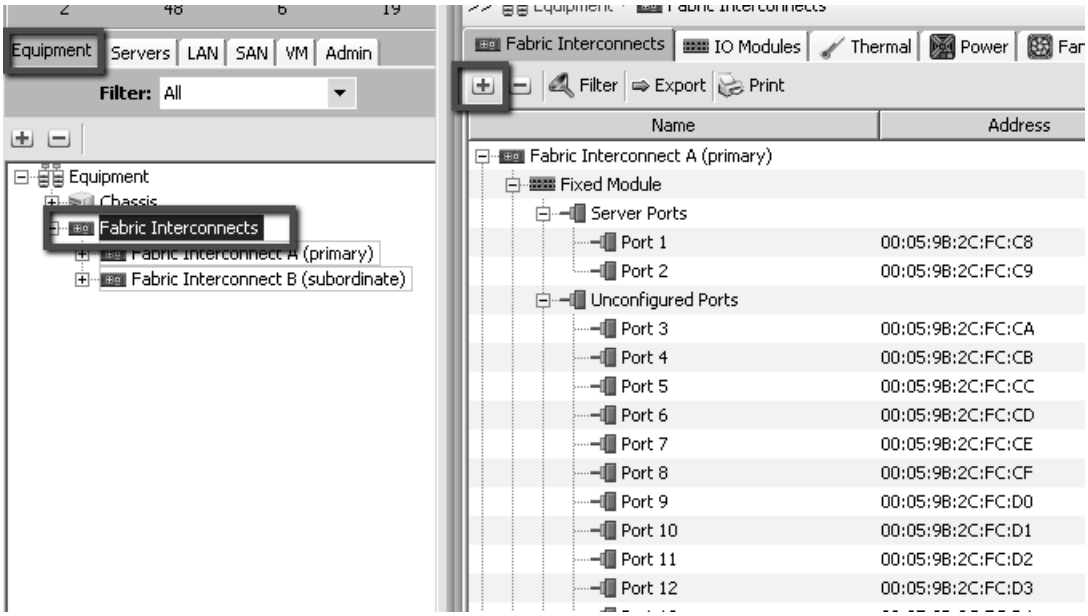
In this task, you will examine the Cisco UCS Fabric Interconnects information and applied configuration.

Note You will conduct this task on Cisco UCS equipment shared between the pods. For that reason, you will only examine the setup and will not change any parameters if not required by the task.

Activity Procedure

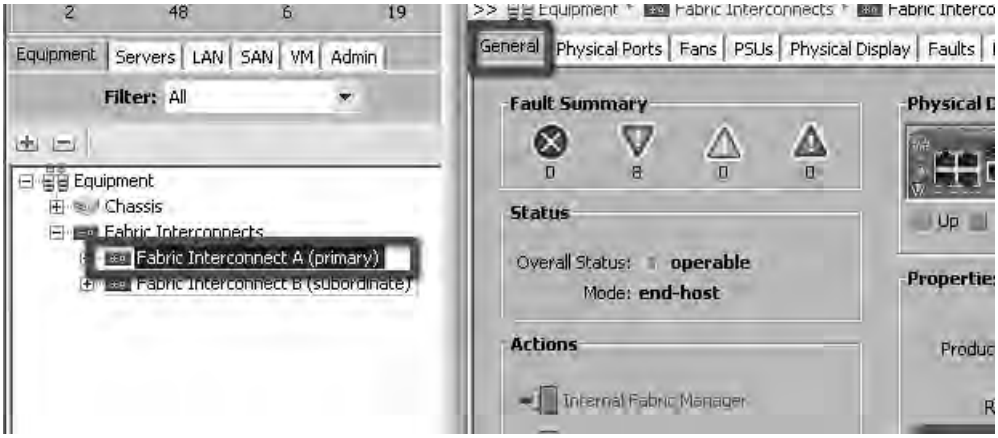
Complete these steps:

Step 1 Click the **Equipment** tab in the left pane to switch back to the Cisco UCS components view. Next, expand and select the **Fabric Interconnects** option in the tree structure to see the details about the Cisco UCS Fabric Interconnect A and B interfaces.



1. What is the total number of interfaces in a single Cisco UCS Fabric Interconnect switch?

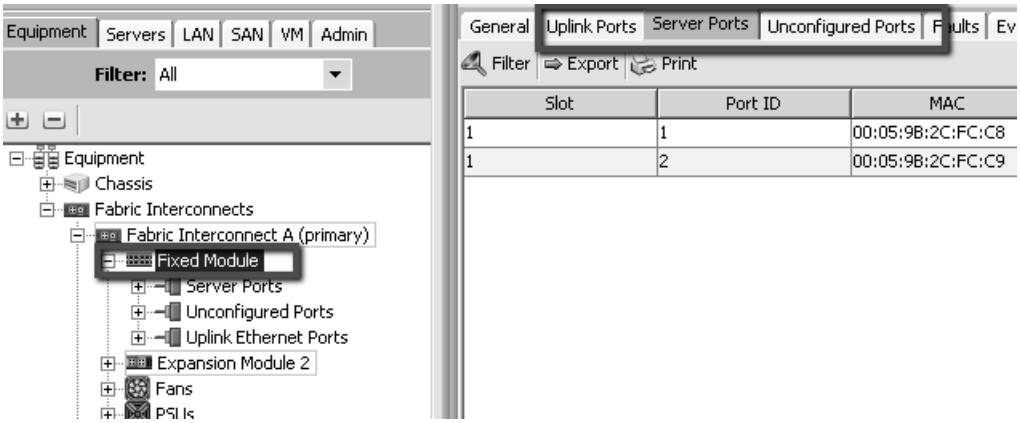
Step 2 Examine the Fabric Interconnect A information by selecting the **Fabric Interconnect A** option in the tree structure in the left pane. Examine the information available in the **General** tab on the right pane.



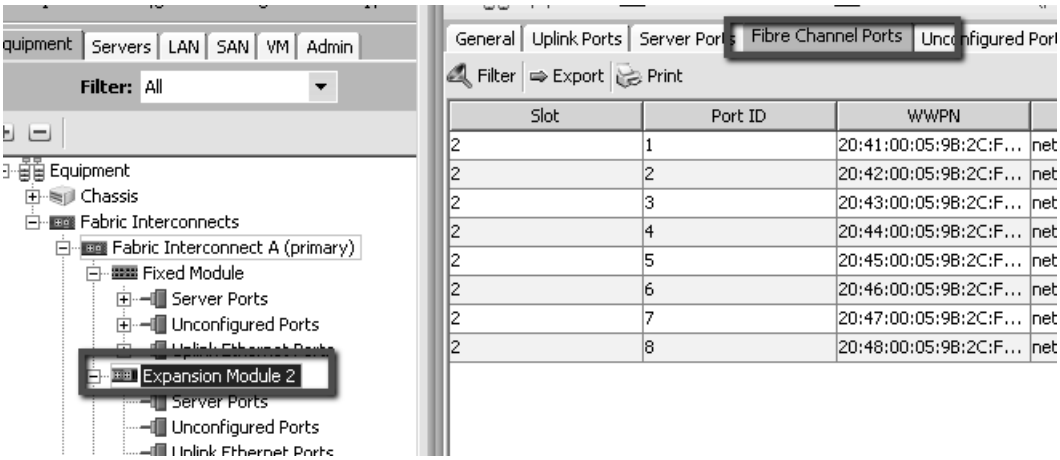
2. What is the total size of the Cisco UCS Fabric Interconnect A memory?

3. What is the high-availability state, cluster link state, and Cisco UCS Fabric Interconnect A role?

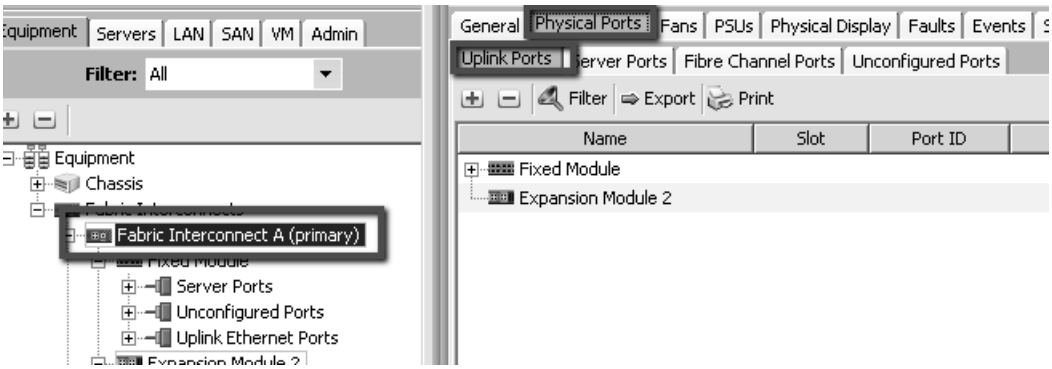
Step 3 Examine the Fabric Interconnect A fixed module interfaces configuration and status. Expand the **Fabric Interconnect A** option in the tree structure on the left pane. Next, expand the **Fixed Module** option. To examine the interfaces information, browse between **Server Ports**, **Unconfigured Ports,** and **Uplink Ethernet Ports** tabs in the right pane.



Step 4 Examine the Fabric Interconnect A expansion module interfaces configuration and status. Select the **Expansion Module 2** option under the **Fabric Interconnect A** option in the tree structure on the left pane. Navigate to the **Fibre Channel Ports** tab in right pane.



Step 5 The interfaces information can be examined by choosing the various tabs in the right pane when **Fabric Interconnect A** option is selected in the tree structure on the left pane. Browse between the **Uplink Ports**, **Server Ports**, **Fibre Channel Ports**, and **Unconfigured Ports** in the right pane.



4. What is the type of expansion module installed in the individual Fabric Interconnect?

_____

5. How many and which interfaces are configured for connectivity from Fabric Interconnect A to the upstream LAN network?

_____

6. How many and which interfaces are configured for the server connectivity on the Fabric Interconnect A?

_____

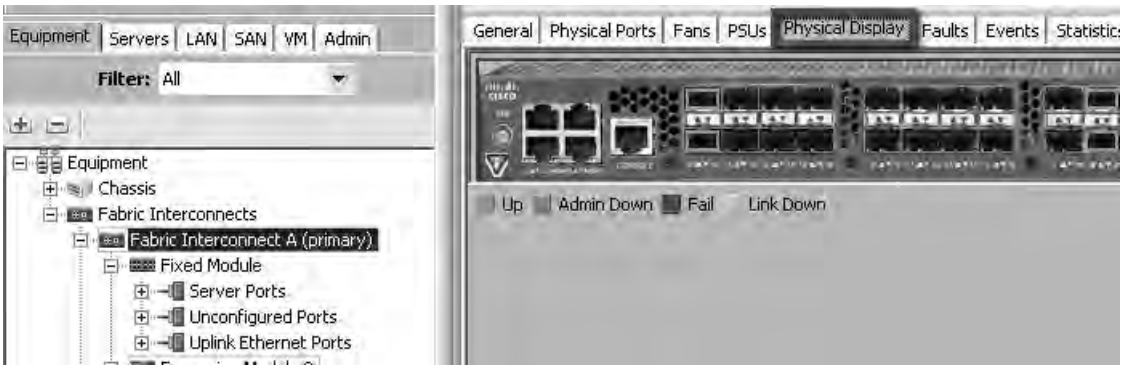
7. How many and which interfaces are available for the SAN connectivity on the Fabric Interconnect A?

_____

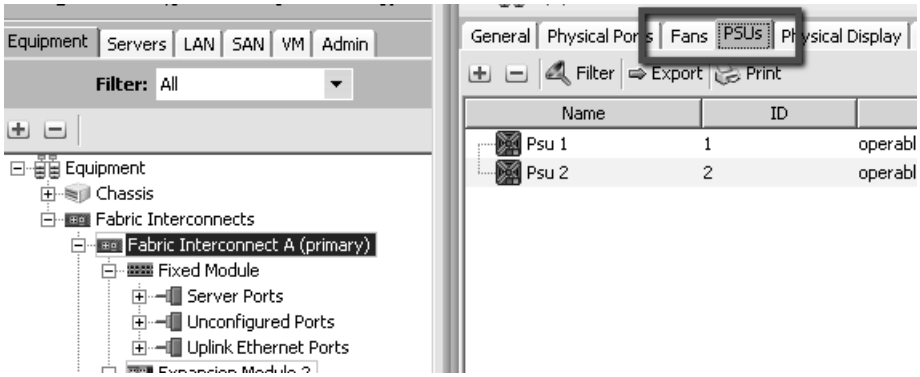
8. How many and which interfaces are available for future system expansion (for example, if additional chassis would be added) on the Fabric Interconnect A?

_____

Step 6 Check the physical outlook of the Fabric Interconnect by selecting **Fabric Interconnect A** in the left pane and then the **Physical Display** tab in the right pane. Move your mouse over an individual port and wait for the balloon-tip to appear—it shows brief information about the interface: its port number and type.



Step 7 Finally, check the fan and power supply status by browsing between **Fans** and **PSUs** tabs in the right pane. Both fans and power supplies should be operational.



Task 3: Examining Cisco UCS Chassis

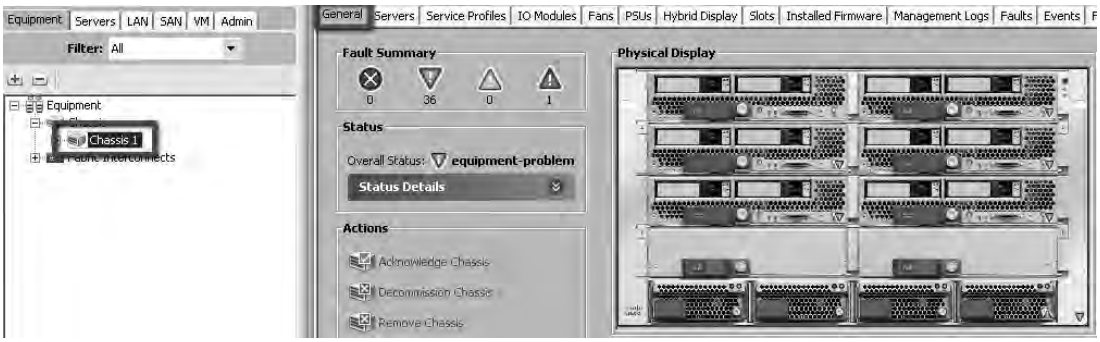
In this task, you will examine the Cisco UCS Chassis information and configuration.

Note You will conduct this task on Cisco UCS equipment shared between the pods. For that reason, you will only examine the setup and will not change any parameters if not required by the task.

Activity Procedure

Complete these steps:

Step 1 Select the **Equipment** tab in the left pane to switch to the Cisco UCS components view. Next, expand the **Chassis** option in the tree structure and select **Chassis 1**. Examine the general chassis information in the **General** tab on the right pane. Expand the **Part Details**, **Status Details**, **Power State Details**, and **Connection Details** to examine the detailed information.

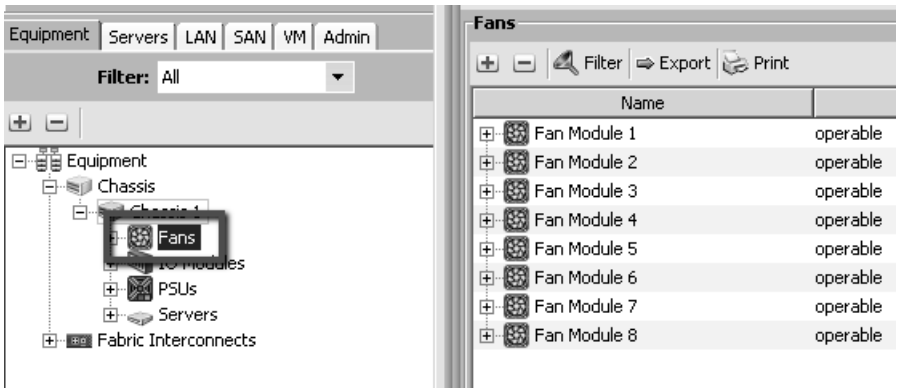


1. What is the ID of the chassis?

2. What is the maximum number of blades that the chassis can host?

3. How many power supplies can be installed in the chassis and what type of power scheme is used?

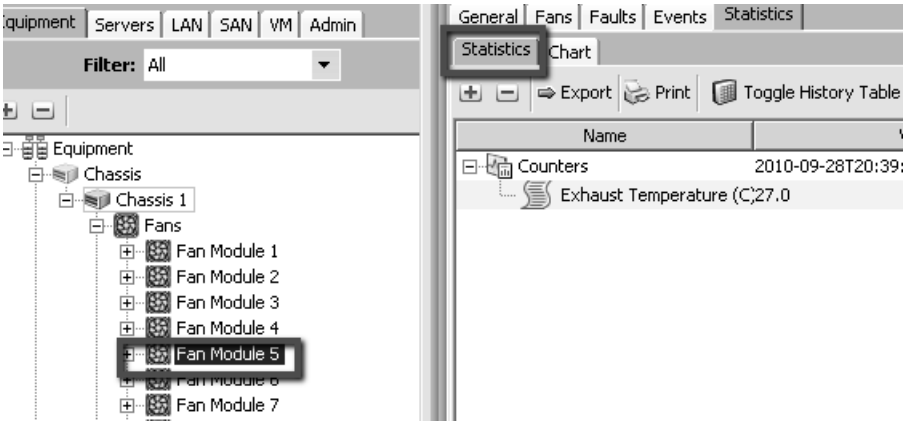
Step 2 Expand the **Chassis 1** option in the left pane and select the **Fans** option.



4. How many fan modules are installed and are operational in the chassis?

Step 3 Navigate to the **Fans** tab in the right pane to examine and verify the fan operation.

Step 4 Select an individual fan module in the left pane and click the S**tatistics** tab in the right pane to examine the exhaust temperature.



Task 4: Examining Cisco UCS I/O Modules

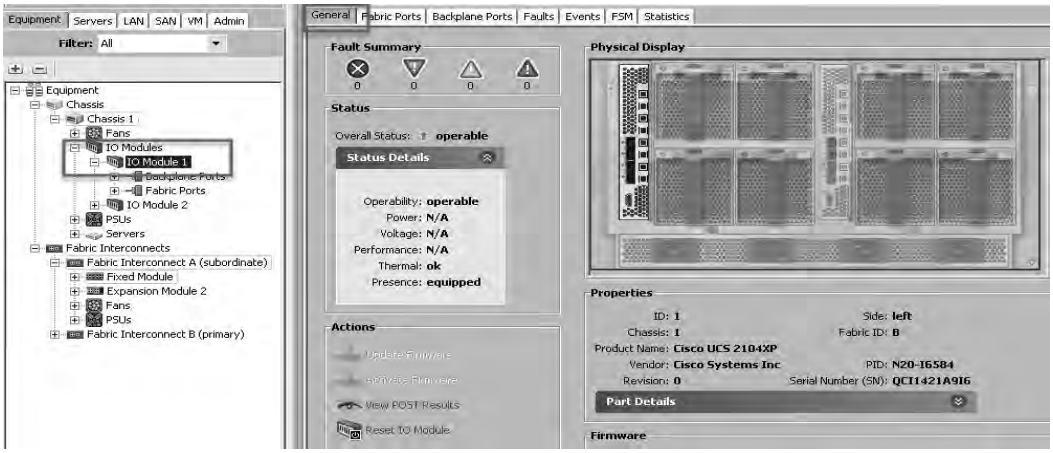
In this task, you will examine the Cisco UCS I/O modules information and configuration.

Note You will conduct this task on Cisco UCS equipment shared between the pods. For that reason, you will only examine the setup and will not change any parameters if not required by the task.

Activity Procedure

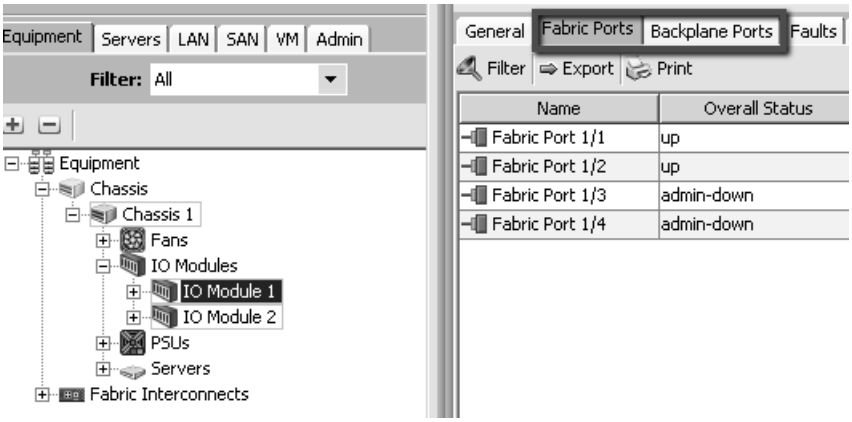
Complete these steps:

Step 1 Expand the **IO Modules** option under **Chassis 1** in the tree on the left pane and select **IO Module 1**. Navigate to the **General** tab in the right pane and explore the I/O Module information.



1. What is the I/O Module part name?

Step 2 Now browse between the **Fabric** and **Backplane Ports** tabs to examine the information about the uplink and server ports.



2. How many interfaces are available and how many interfaces are used on the I/O module to connect to the Fabric Interconnect switch?

3. How many interfaces are available for blade server connectivity?

Task 5: Examining Cisco UCS Server Blades

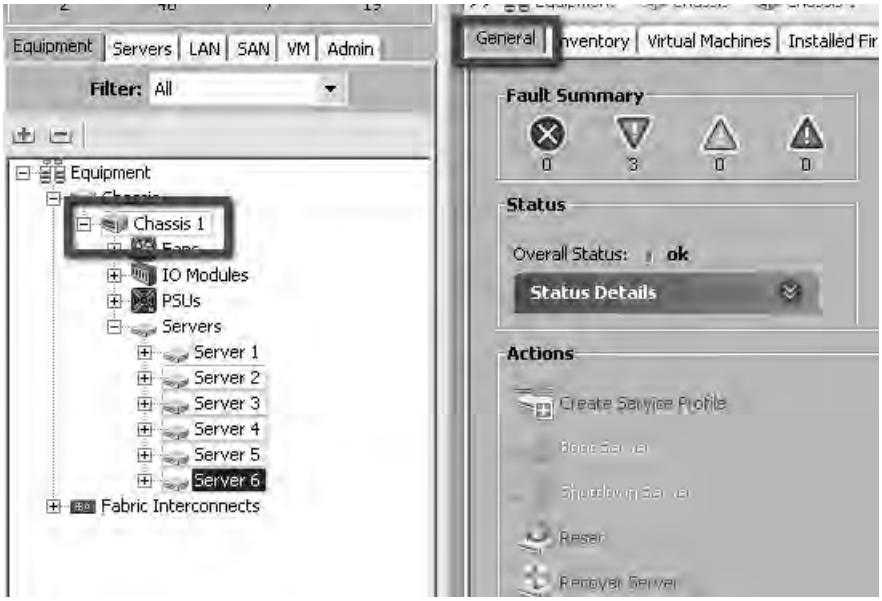
In this task, you will examine the Cisco UCS Server Blades information and configuration.

Note You will conduct this task on Cisco UCS equipment shared between the pods. For that reason, you will only examine the setup and will not change any parameters if not required by the task.

Activity Procedure

Complete these steps:

Step 1 On your team's assigned server as listed in the table Team Blade Assignments in your Lab Reference Guide. Next, select the **General** tab in the right pane and explore the basic server blade properties.



1. What is the type of the assigned server blade?

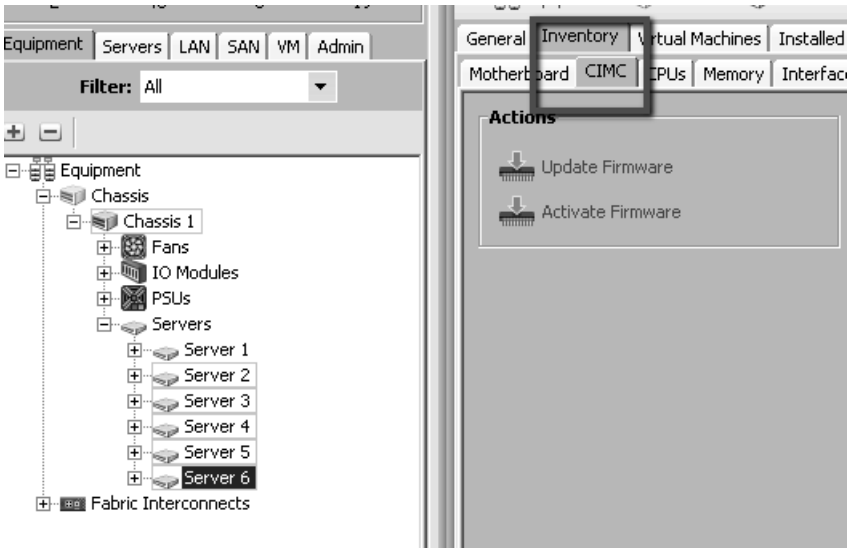
2. How many processors does the server blade have?

3. What is the number of cores and threads per processor?

4. How much memory does the server blade have?

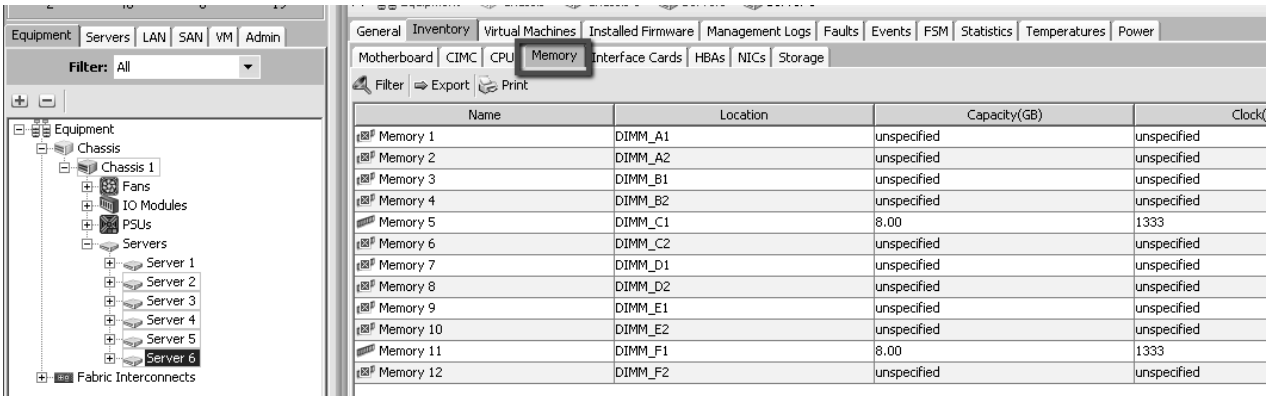
5. How many adapters does the server blade have?

Step 2 Select the **Inventory** tab in the right pane and examine the detailed inventory information by examining the individual server blade components. First, select the **CIMC** (Formerly **BMC)** tab in the right pane to examine the management information of the server blade.



6. What is the IP address of the server blade management interface?

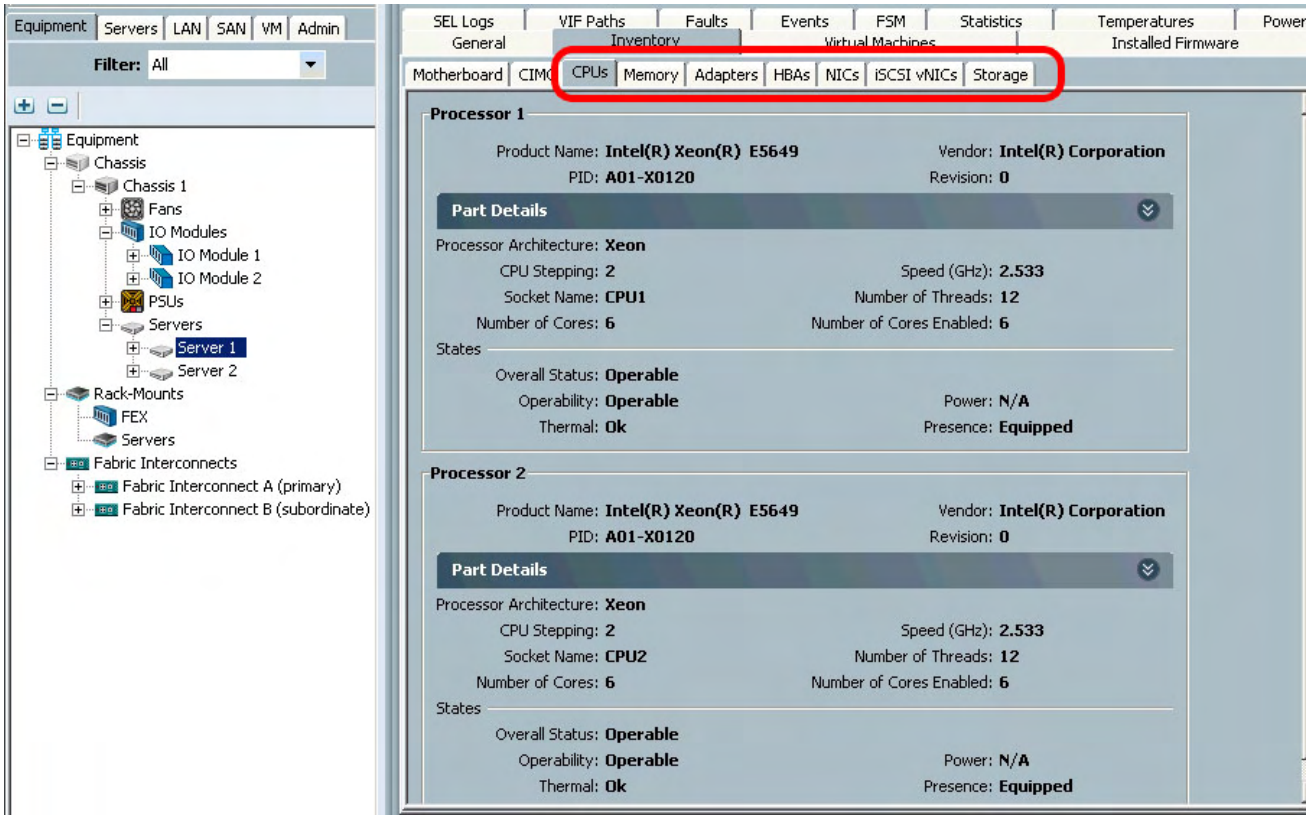
Step 3 Examine the memory configuration to verify which memory DIMMs are populated.



7. Which memory DIMM slots are populated?

8. What is the size of the individual DIMM module?

Step 4 Examine other server blade components by browsing between the **CPUs**, **Adapters, HBAs**, **NICs**, and **Storage** tabs.



9. What is the type of the processors on the server blade?

_____

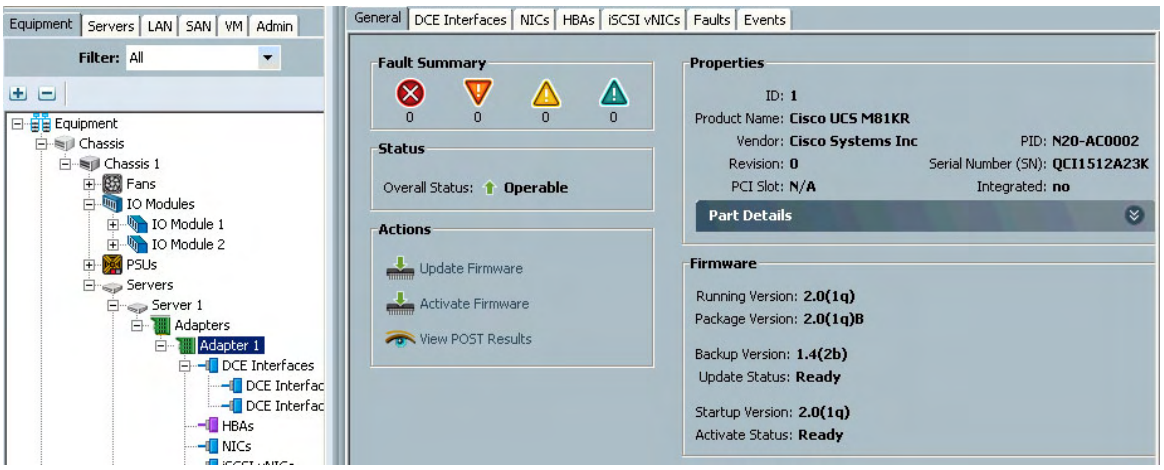
10. What is the processor speed and architecture?

_____

11. What is the type and size of the local storage?

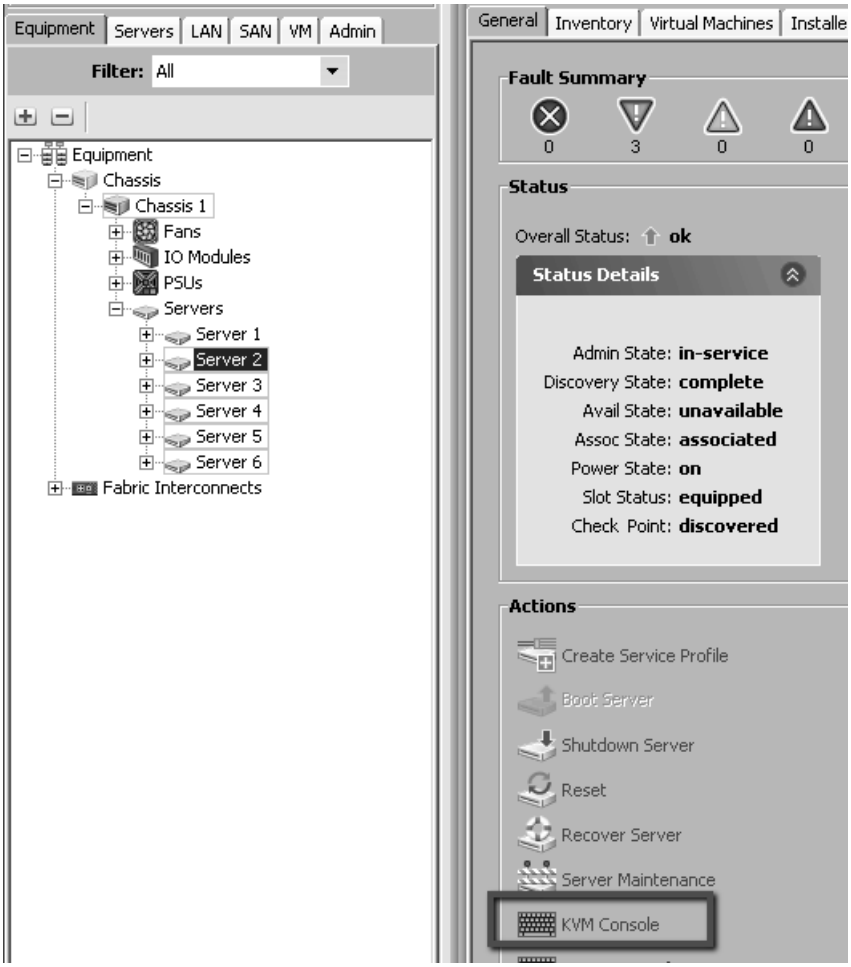
_____

Step 5 Expand the assigned server blade and the **Interface Cards** option in the tree structure in the left pane. Next, select the **Interface Card 1**, navigate to the **General** tab on the right pane, and expand the **Part Details** section.

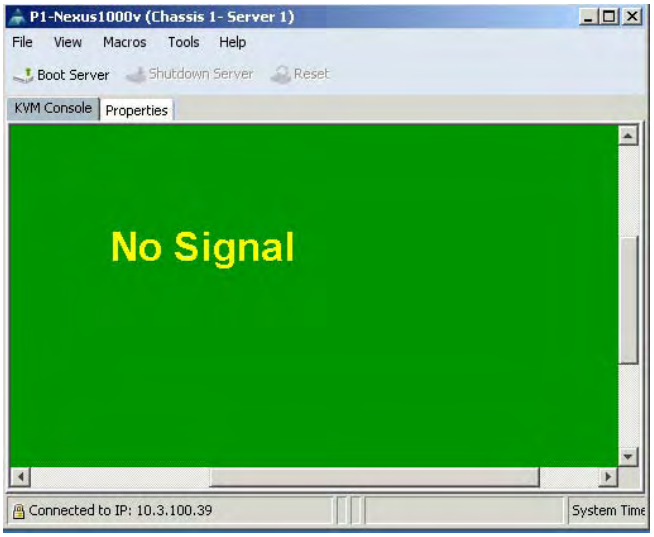


12. What is the type of the interface adapter and what kind of connectivity does it support?

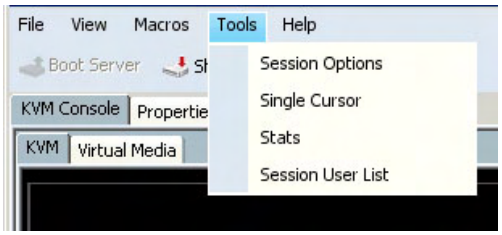
Step 6 Select the assigned server blade in the left pane and navigate to the **General** tab on the right pane. Click the **KVM Console** option under the **Actions** section to examine the server console output.

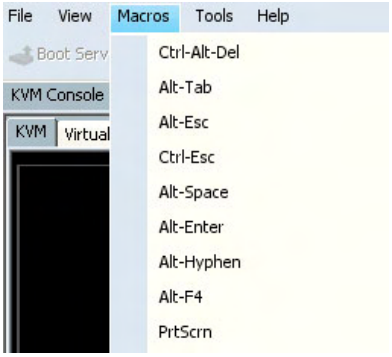


Step 7 The KVM startup screen shows and the KVM window appears. (You may get a security warning, click RUN)

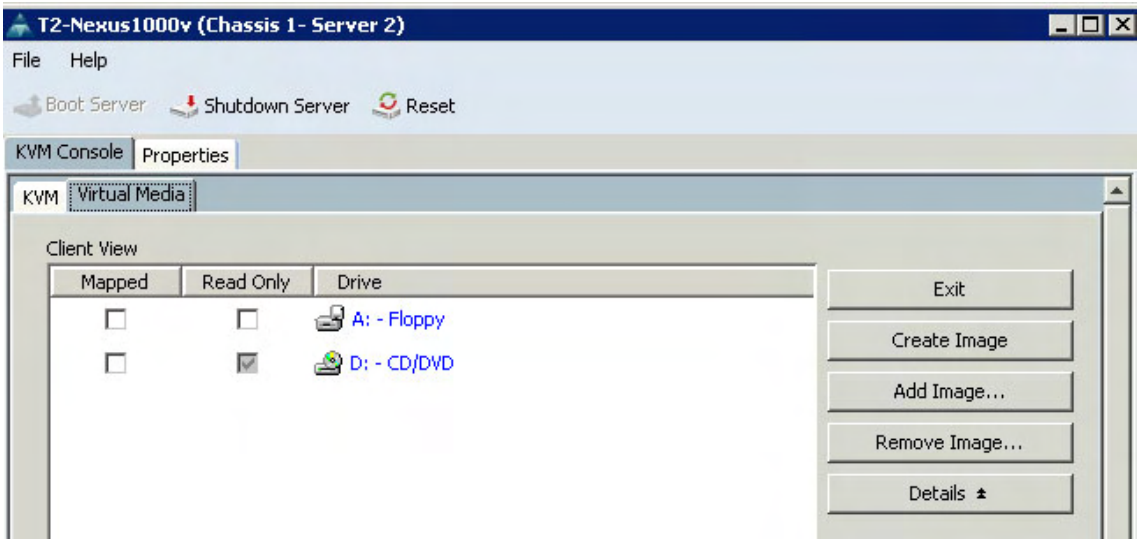


Step 8 Explore the options available in the KVM Console. You can send various keystroke combinations accessing the Macros menu or change the behavior under Tools > Session Options.

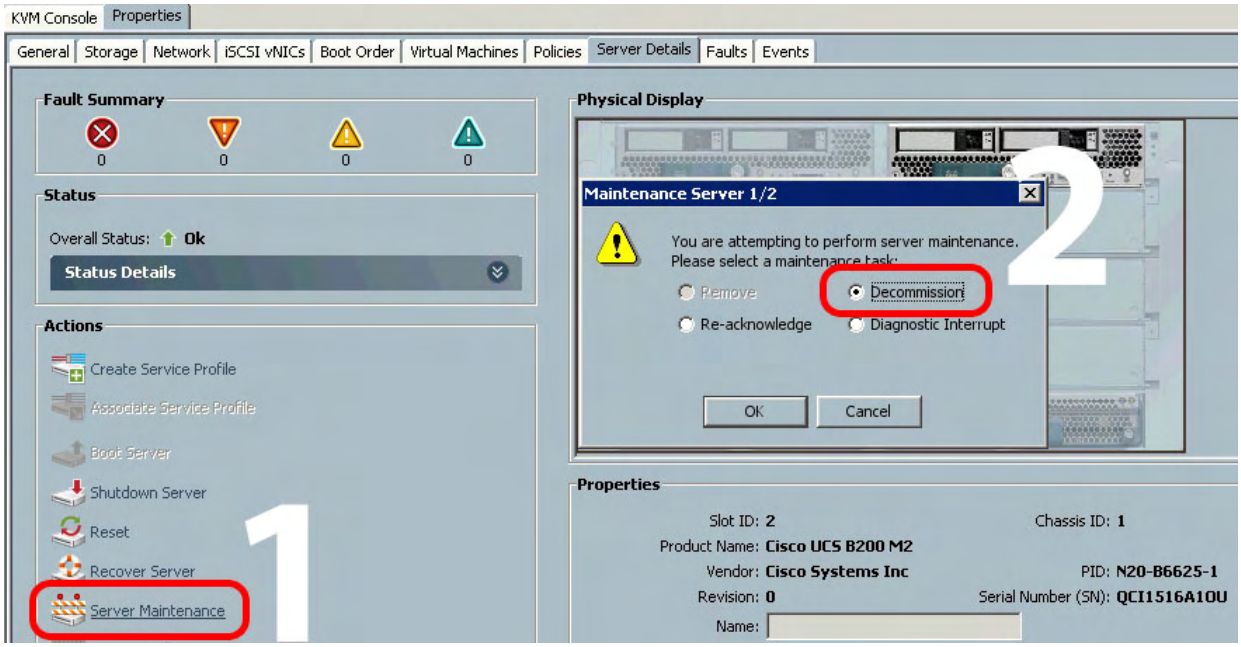


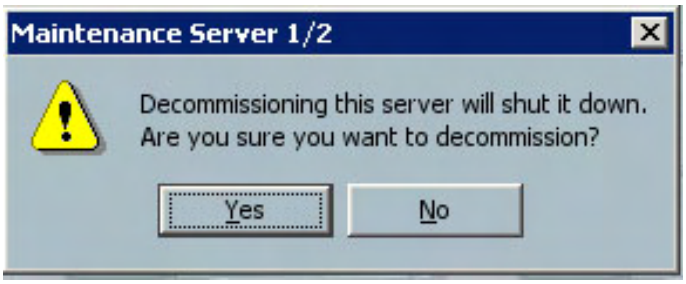


Step 9 Open the virtual media dialog by selecting the **Virtual Media** option under the Virtual Media Tab. Here you can map a locally attached media or ISO image to the blade. The ISO image must be accessible by the computer from where the KVM was launched. The option is useable when installing an operating system or other application on the server blade.

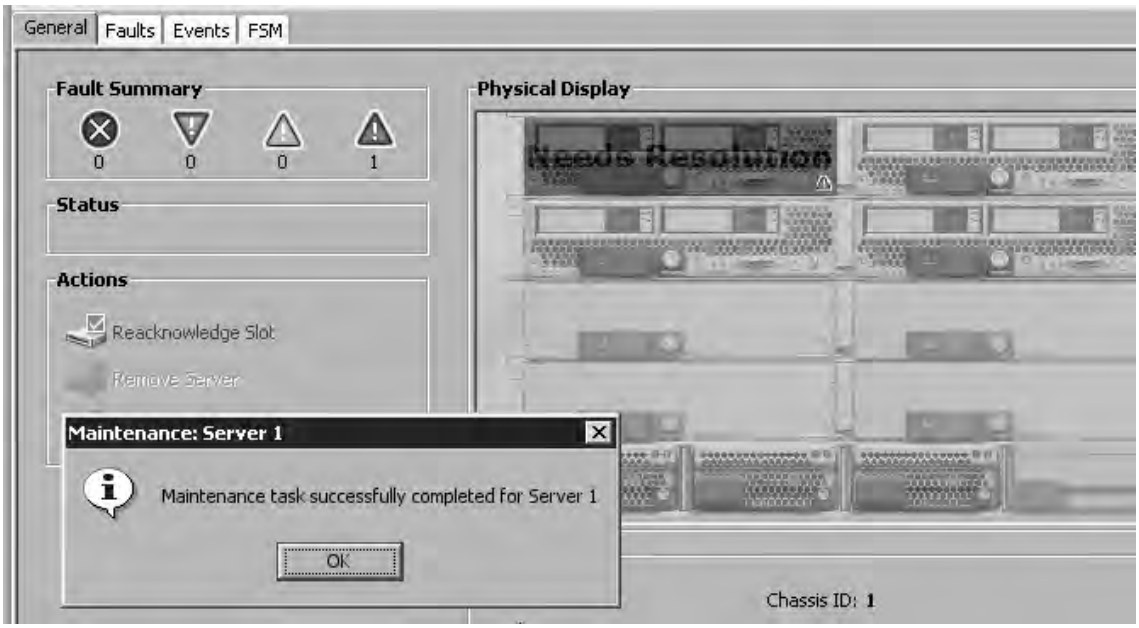


Step 10 Disable the server blade by decommissioning it. Select **Server Maintenance** under Properties -> Server Details -> Actions**,** and select the **Decommission** option.

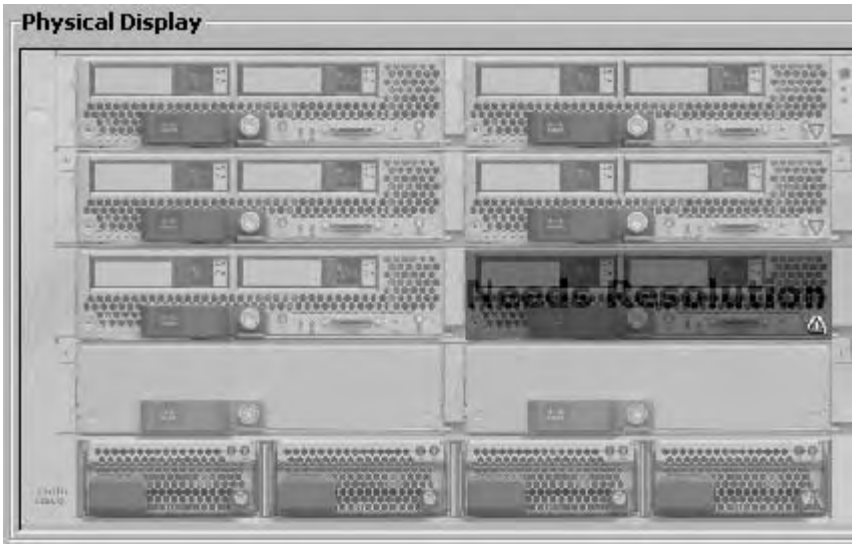




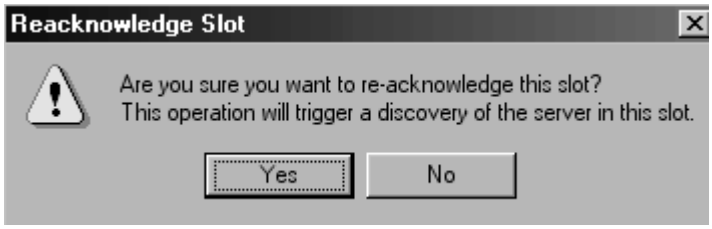
Step 11 The blade will be disabled and marked with “Needs Resolution”, in red, over it. Successful decommissioning is indicated by the message window stating that the maintenance task completed successfully. The KVM Console closes.



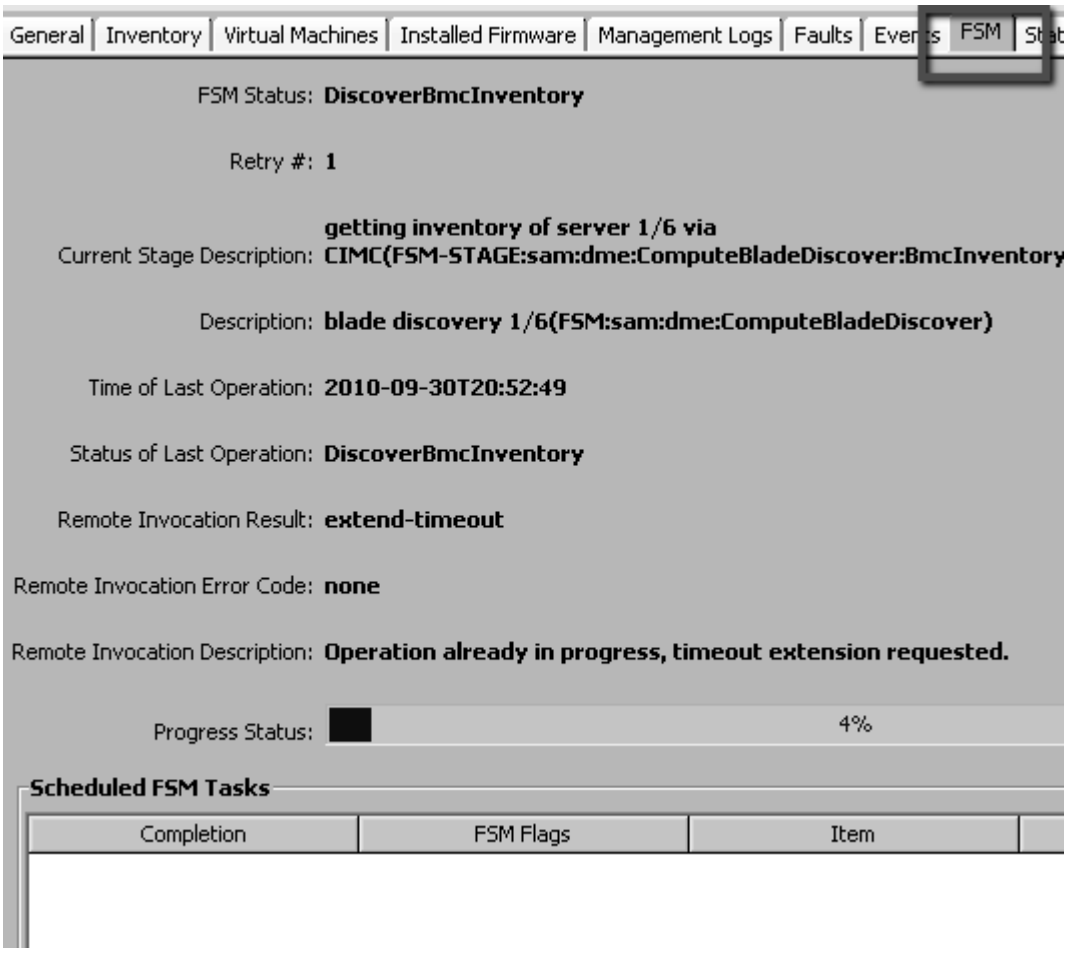
Step 12 Re-acknowledge the blade by selecting the **Reacknowledge Slot** action. This will enable the blade and activate the blade discovery.



Step 13 Confirm the re-acknowledge action by selecting **Yes**.



Step 14 Select the **FSM** tab to observe the blade discovery process, by means of which the Cisco UCS acquires inventory information about the blade.



Step 15 If closed, re-open the KVM Console for the blade; if not started, select the **Re-acknowledge** option under Server Maintenance to start the discovery process again. Observe the KVM Console output. You should see the discovery process booting the Cisco UCS operating system on the blade used to gather the inventory information.

Lab 3-1: Upgrading Cisco UCS Components

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

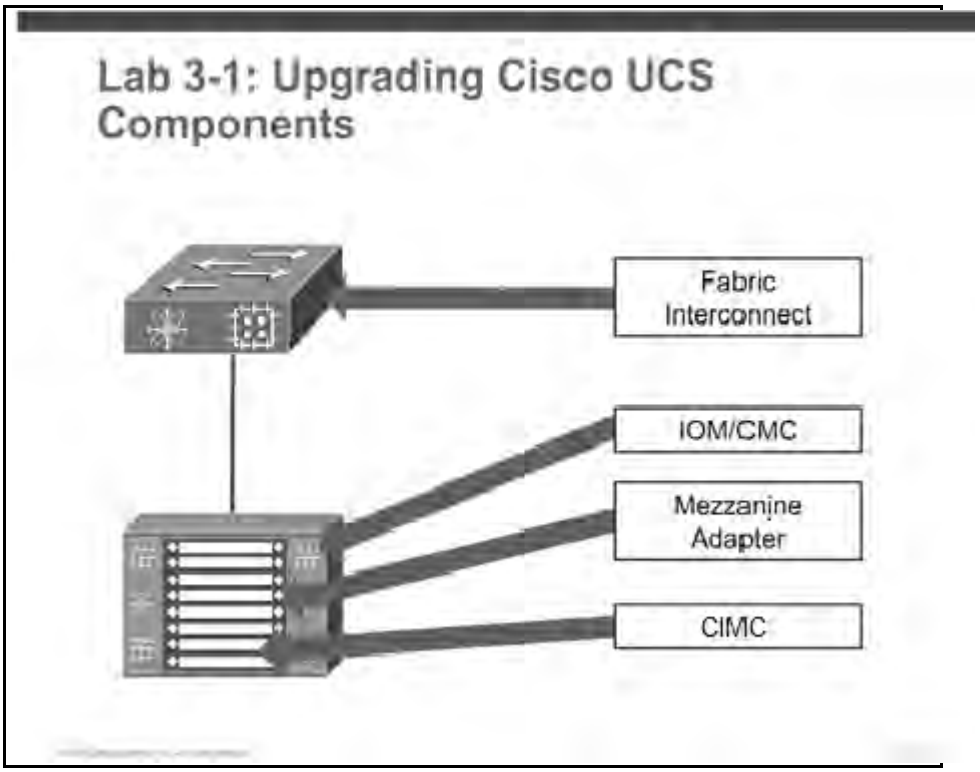
Activity Objective

In this activity, you will perform the steps necessary to upgrade code levels on several Cisco UCS components. After performing this lab, you should be able to:

- Explore firmware management options in Cisco UCS Manager
- Update the firmware on a CIMC
- Update the firmware on an interface card
- Explain how to update the firmware on an I/O module and a Fabric Interconnect

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:

- A configured Cisco UCS environment
- IP access to Cisco UCS Manager
- Preloaded firmware bundles loaded into Cisco UCS Manager

Task 1: Explore Firmware Management Options

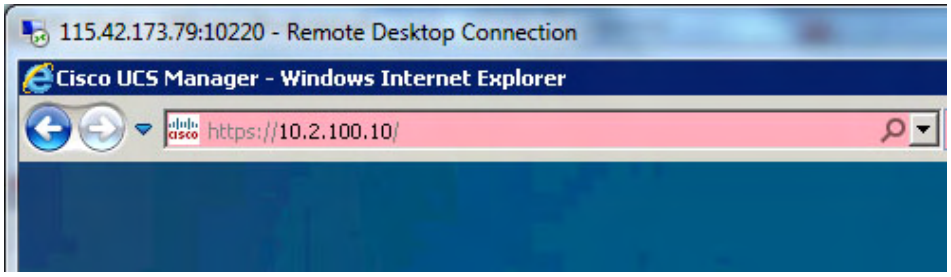
In this task, you will explore firmware management options in Cisco UCS Manager.

Activity Procedure

Complete these steps:

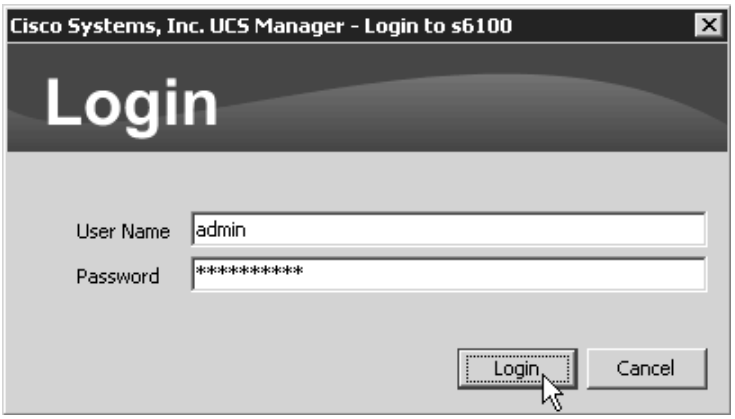
Step 1 Log into your student desktop according to the instructions provided by your instructor.

Step 2 Open Internet Explorer and log into the Cisco UCS Manager by entering the Cluster IP address as given by your instructor.

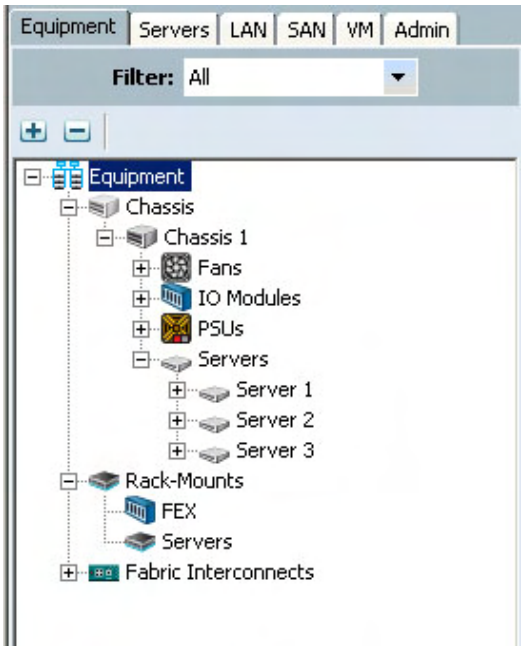


Step 3 Click **Launch UCS Manager** to start Cisco UCS Manager.

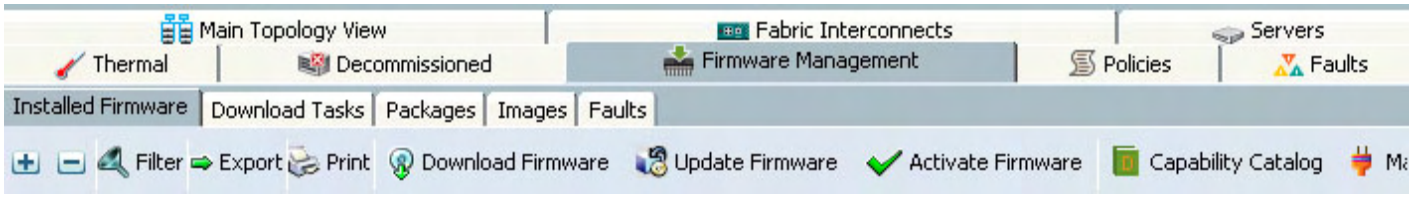
Step 4 Log into Cisco UCS Manager using the username and password: “admin” & “cisco123”.



Step 5 Choose the **Equipment** tab in the navigation pane.

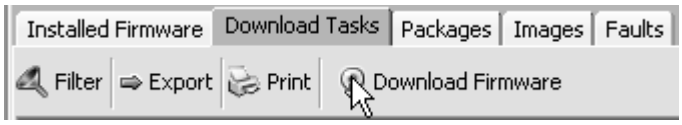


Step 6 Choose the **Equipment** icon as shown in the previous step, and then choose the **Firmware Management** tab in the content pane.

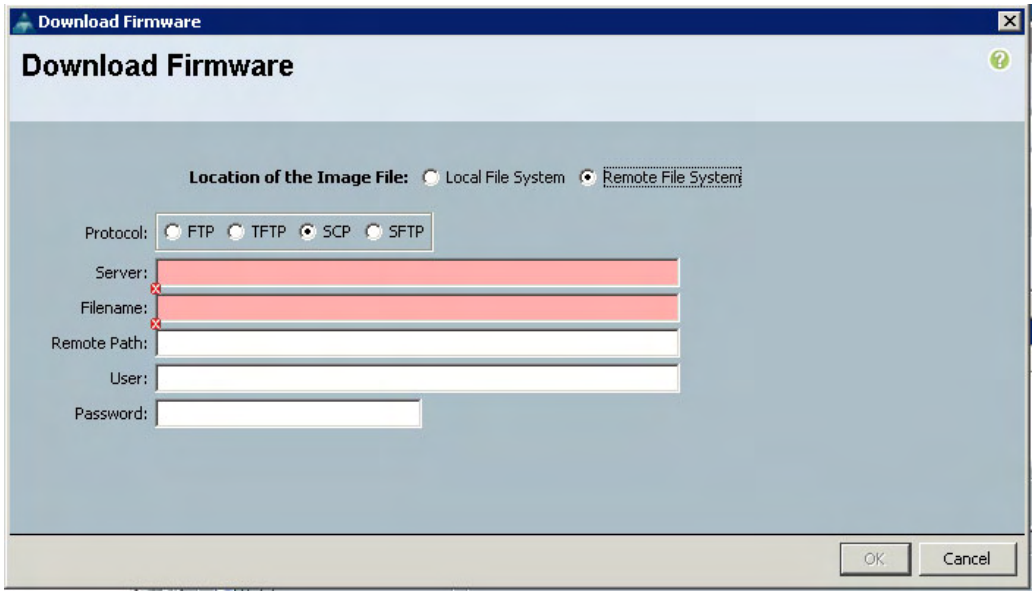


Step 7 Take a few minutes to explore the tabs available under Firmware Management. Pay particular attention to Packages and Download Tasks tabs.

Step 8 Choose the **Download Tasks** tab, and click the **Download Firmware** link.

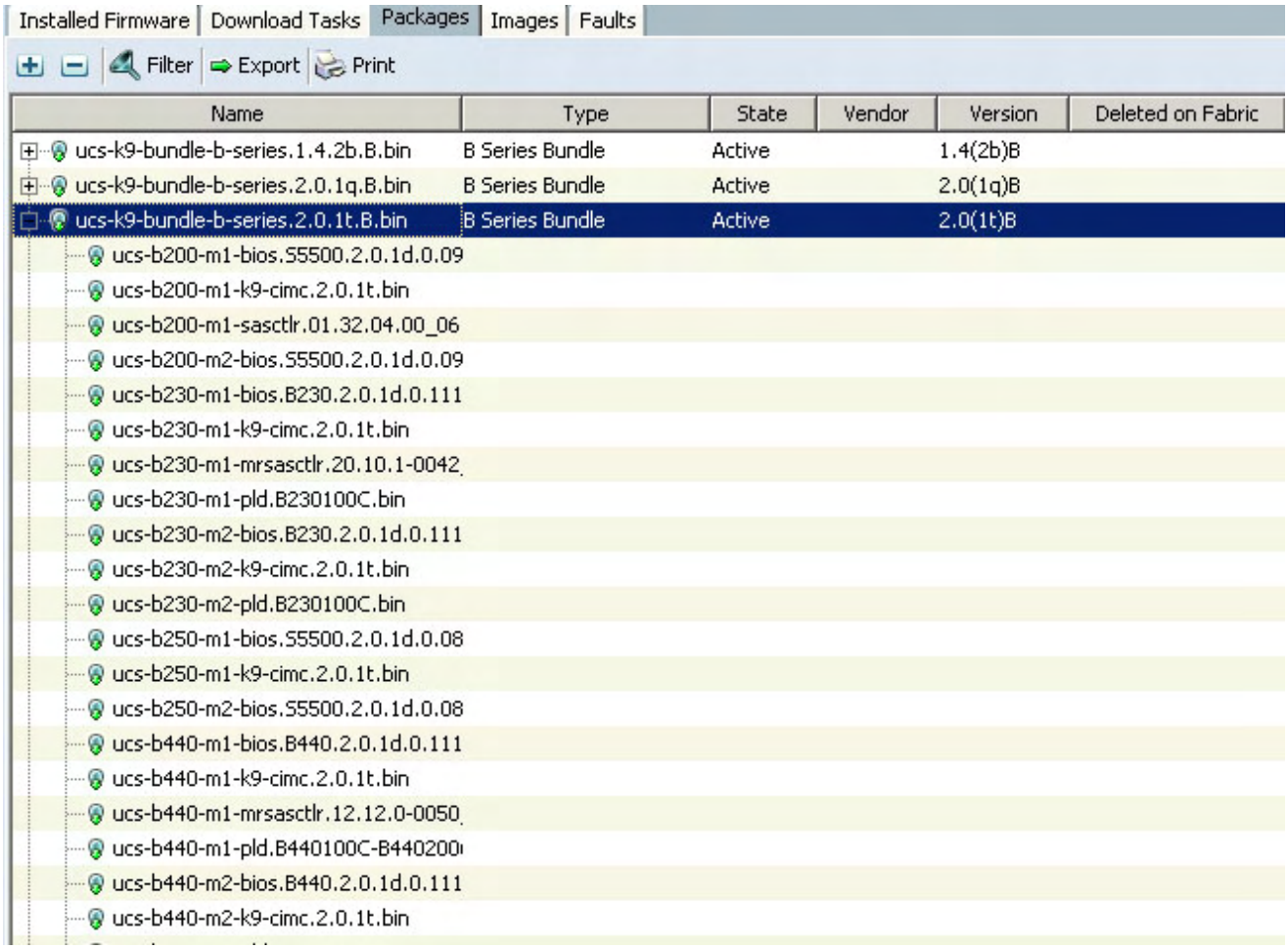


Step 9 Review the information that is needed to download a new firmware package to the Cisco UCS Manager. Click **Cancel** when you have reviewed the configuration fields.



In this exercise, the necessary firmware packages already have been transferred to the Fabric Interconnect.

Step 10 Click the **Packages** tab and expand one or more of the installed packages. Review the various images that make up the package.



Depending on the lab environment in which you are performing these labs, the number and versions of labs that are installed may differ from these examples. This is normal.

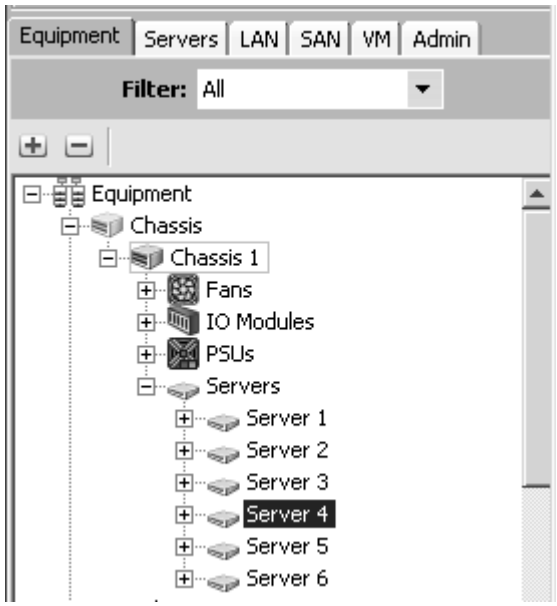
Task 2: Upgrade a CIMC (Formerly BMC)

In this task, you will update the firmware on a CIMC.

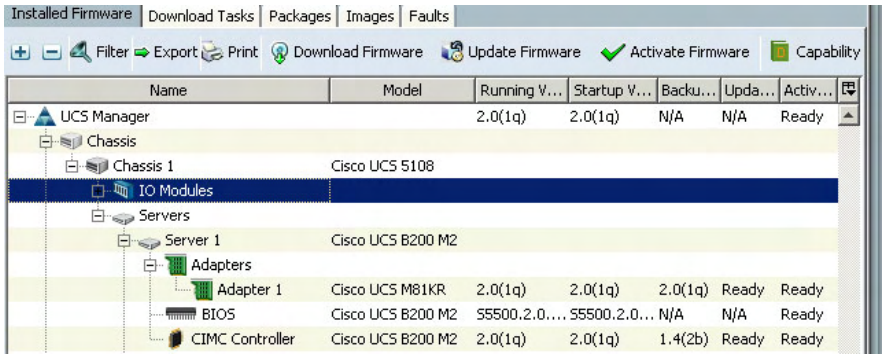
Activity Procedure

Complete these steps:

Step 1 Choose the server that is assigned to your team. This task will use Server 4 as an example.



Step 2 Click the **Installed Firmware** tab in the content pane, and review the Running Version and Startup Version values for your server's CIMC.



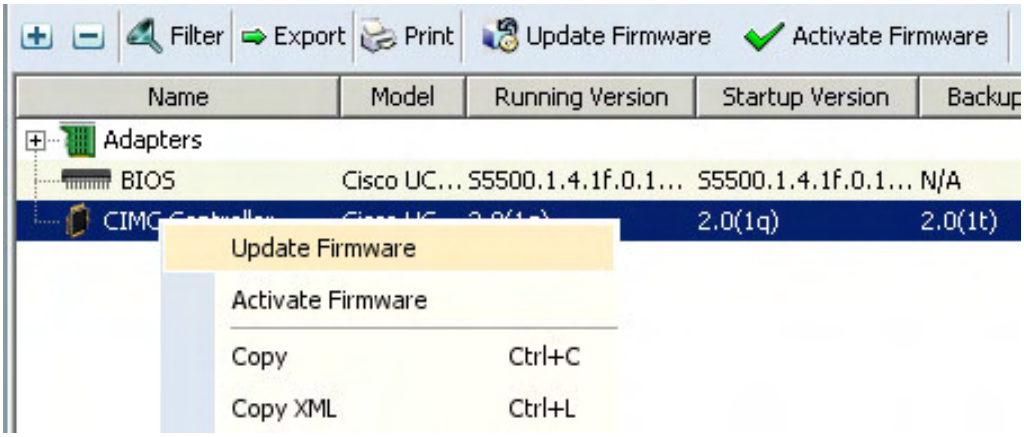
Step 3 Review:

Update Firmware -> Sets the Backup Version

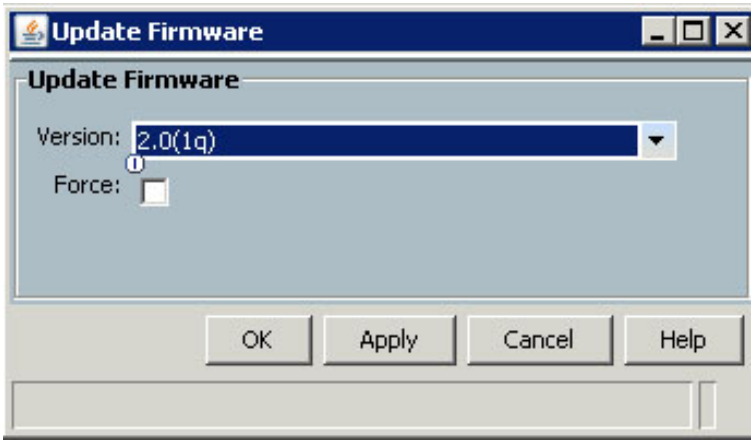
Activate Firmware -> Sets the Startup Version

Rebooting (occurs during activation) -> Sets Running Version to match Startup Version

Step 4 Right-click the **CIMC Controller** line and choose **Update Firmware**.

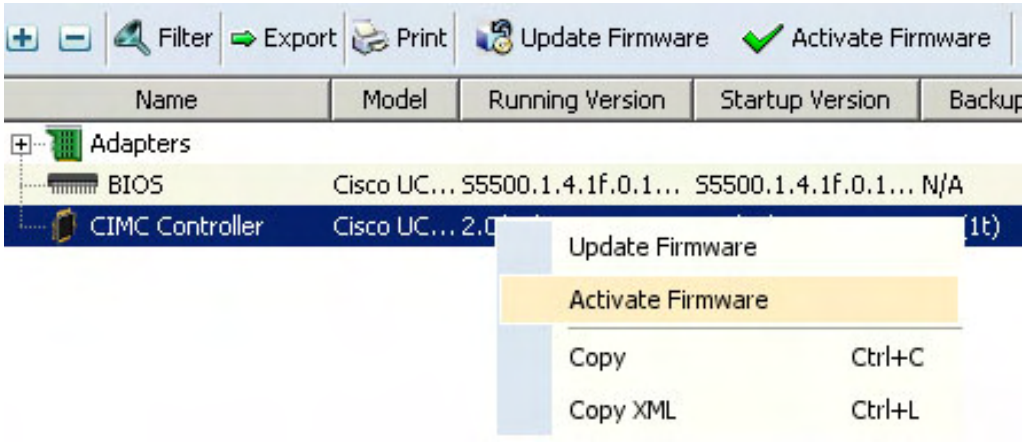


Step 5 There are two versions available, for the lab, we will be switching from the Running Version to the 2.0(1q). Do not select any firmware less than 2.0(1q). In the Update Firmware dialog **select the 2.0(1q), then click OK**.

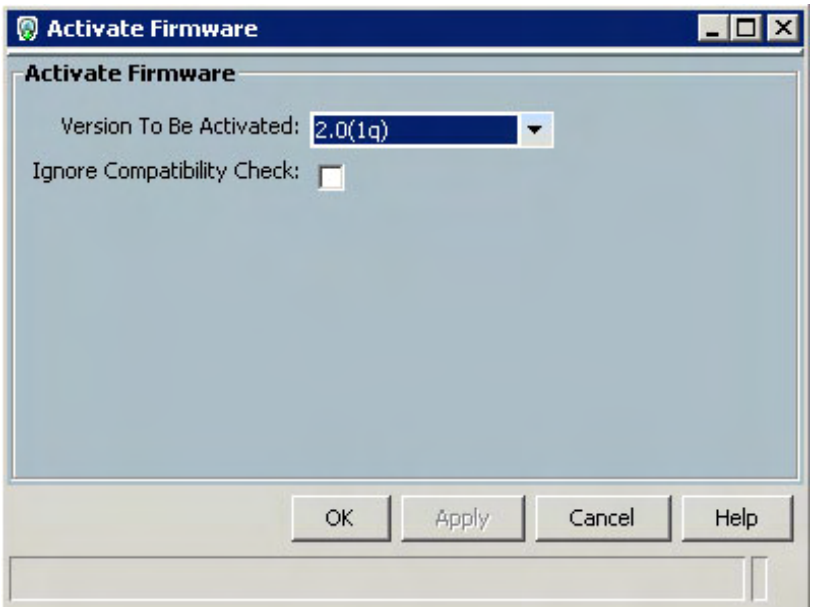


Step 6 Depending on the versions of code already running or installed as the backup version on your CIMC, the update status may move to Updating. This is necessary only if the version that you selected was not already loaded on the CIMC. If your CIMC moves to an Updating status, wait until the Update Status has changed to Ready. Note that your selected version is now listed as the Backup Version.

Step 7 After verifying that the version that you selected is listed as the Backup Version and the Update Status is Ready, right-click the **CIMC Controller** line again and choose **Activate Firmware**.

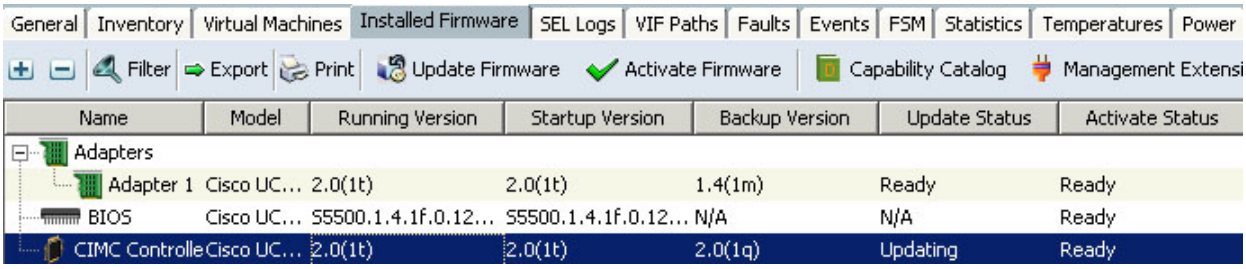


Step 8 Choose the same version as in the previous step and click **OK**.



Step 9 Observe the Activate Status values as they change. They should move from Activating to Rebooting to Ready. Also note that the Startup Version has been updated to your selected version, while the Running Version retains the previous version.

Step 10 After the Activate Status has resolved to Ready, observe the Running Version, Startup Version, and Backup Version values as they change.



Step 11 Try repeating the process, to ensure you understand the difference between updating and activating. When you are done, it does not matter which version is the Running, Startup or Backup version.

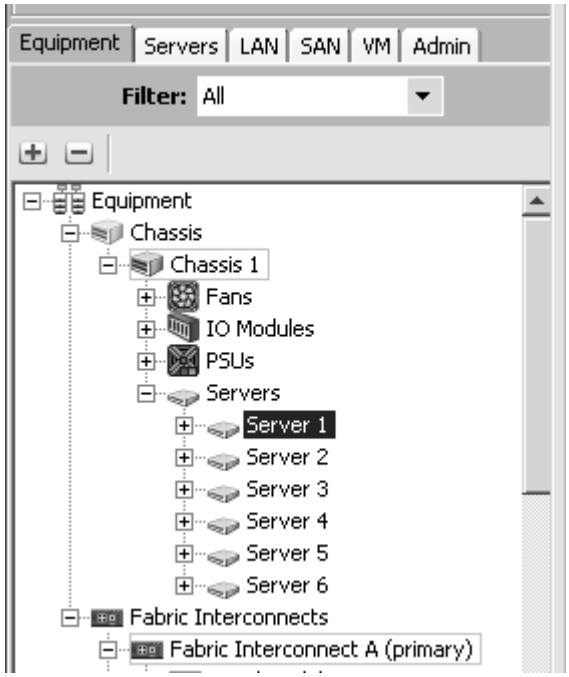
Task 3: Upgrade an Interface Card

In this task, you will verifying the firmware on an interface card.

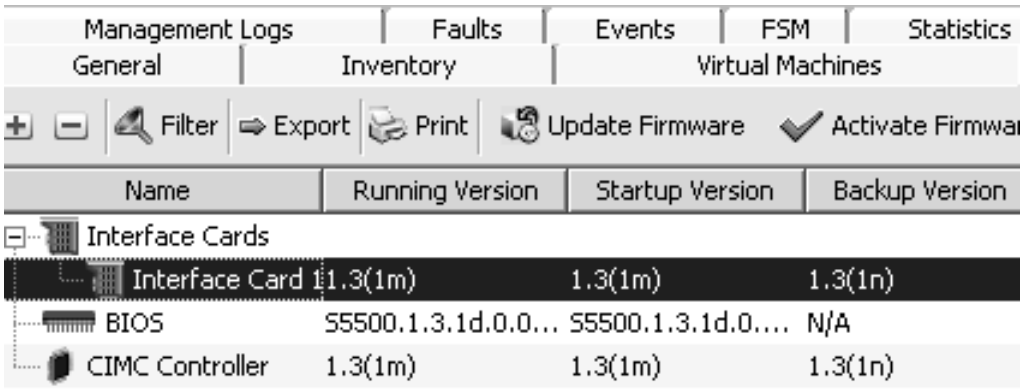
Activity Procedure

Complete these steps:

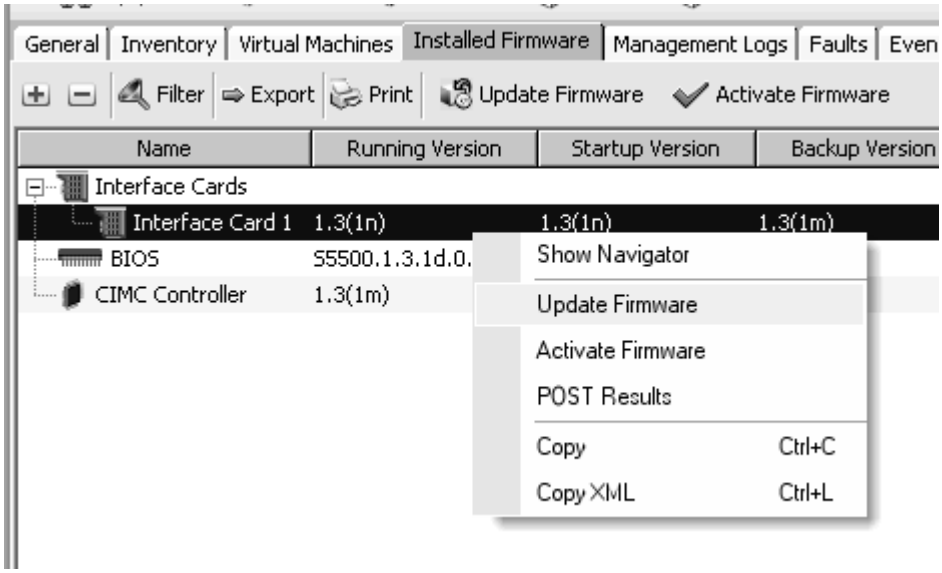
Step 12 Choose the server that is assigned to your team. This task will use Server 4 as an example.



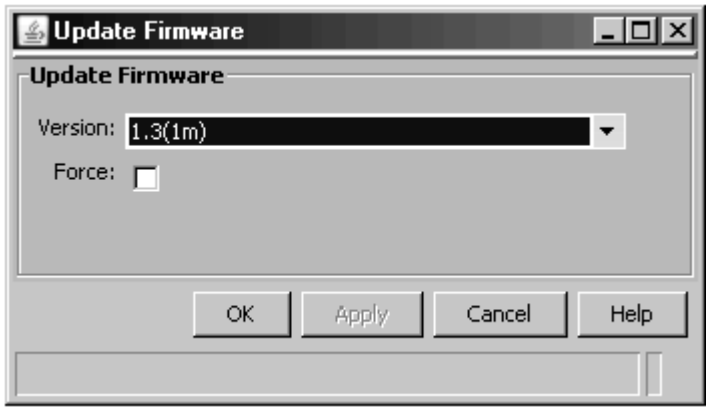
Step 13 Click the **Installed Firmware** tab in the content pane and review the Running Version and Startup Version values for your server's Interface Card.



Step 14 Right-click the **Interface Card 1** line and choose **Update Firmware**.

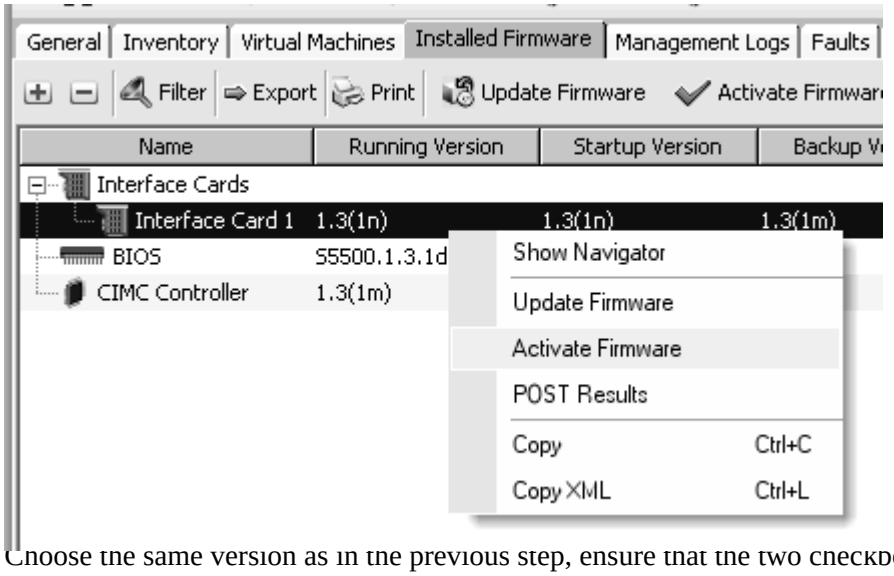


Step 15 There are two versions available. For the lab, we will be switching from the Running Version to the Backup Version. In the Update Firmware dialog select the Backup Version and click OK.

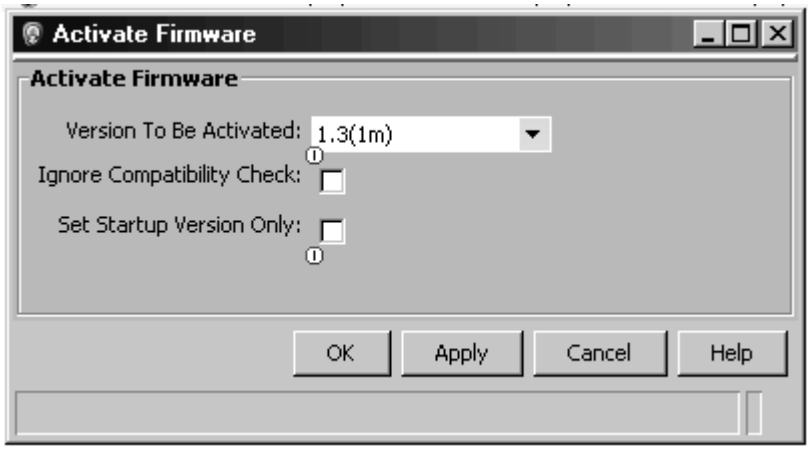


Step 16 If the task had been done, the update status may move to Updating. This is necessary only if the version that you selected was not already loaded on the Interface Card. If your Interface Card moves to an Updating status, wait until the Update Status has changed to Ready. Note that your selected version is now listed as the Backup Version.

Step 17 After verifying that the version that you selected is listed as the Backup Version and that the Updating Status is Ready, right-click the **Interface Card** line again and choose **Activate Firmware**.

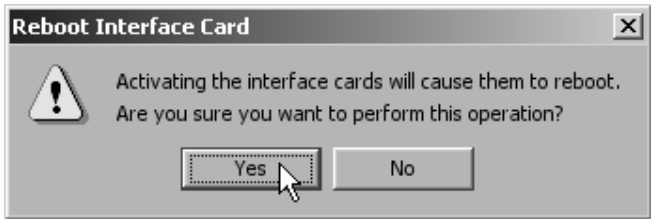


Step 18 Choose the same version as in the previous step, ensure that the two checkboxes are cleared, and click **OK**.



Note that clearing the “Set Startup Version Only” checkbox will cause a reboot of the blade server. If left checked, the selected version would take effect only on the next reboot of the blade.

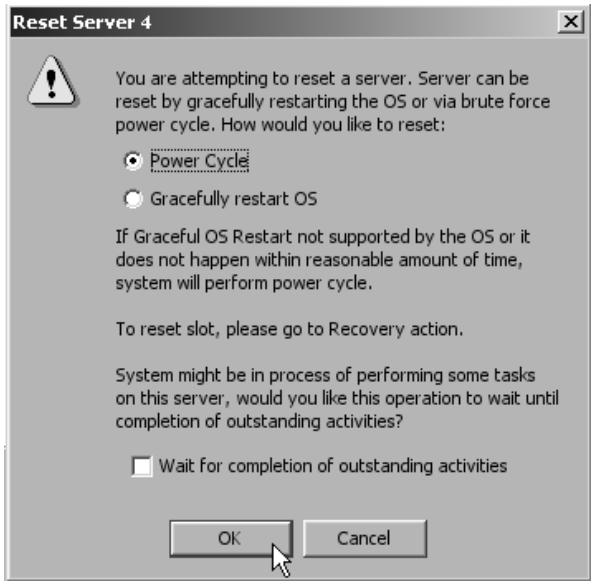
Step 19 Click **N**o to confirm that you would like the Interface Card to be rebooted.



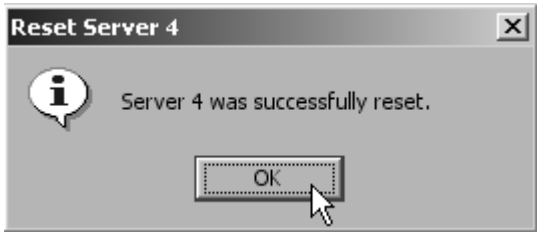
Step 20 Observe the Activate Status values as they change. They should move from Activating to Pending-Next-Boot. (This can take awhile).

Step 21 Because your blade should have been powered down prior to this action, the status will not change until the blade is powered on. In a production environment, the firmware update can be left in this state and will be applied after it is booted. To force the update to take effect, manually power cycle the blade to cause it to boot. Click the **General** tab, and then choose **Reset**.

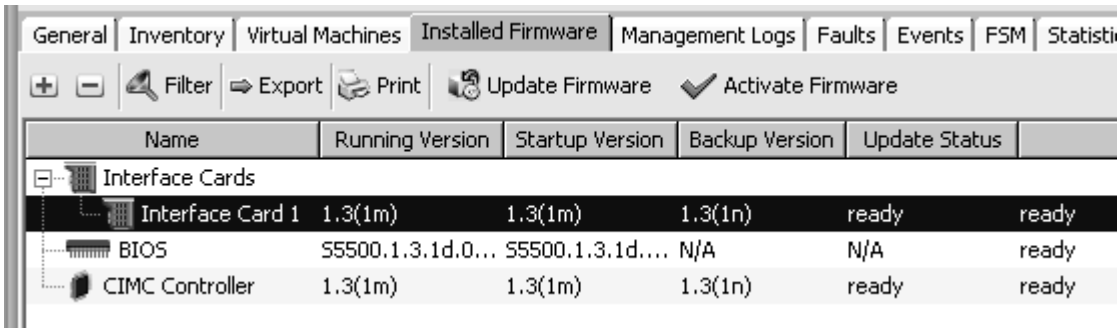
Step 22 Ensure that **Power Cycle** is selected, and click **OK**.



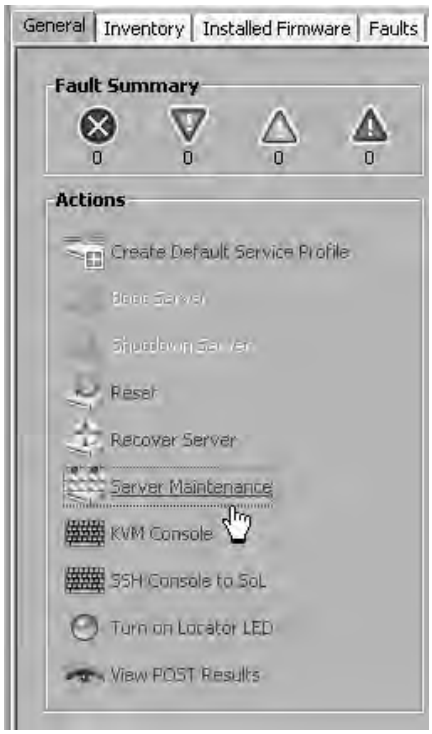
Step 23 Click **OK** to clear the confirmation message.



Step 24 Return to the **Installed Firmware** tab, and observe the Running Version update to your selected version.



Step 25 To ensure that the blade is properly powered down, return to the **General** tab and click **Server Maintenance**.



Step 26 Choose **Re-acknowledge** and click **OK**.

Task 4: Explore Other Upgrade Options

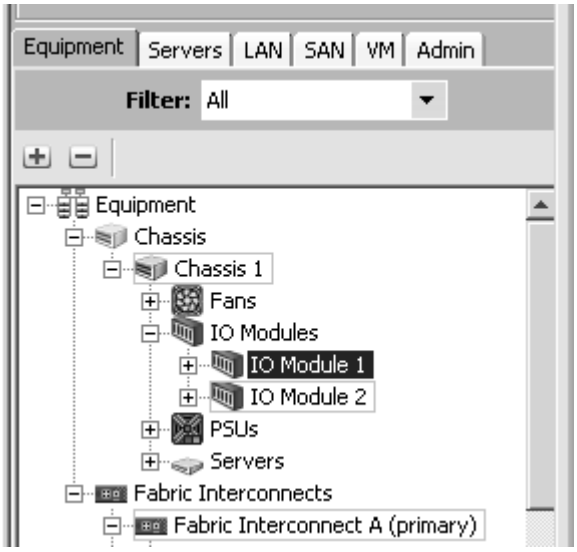
In this task, you will learn how to update the firmware on an IO module and a Fabric Interconnect.

Activity Procedure

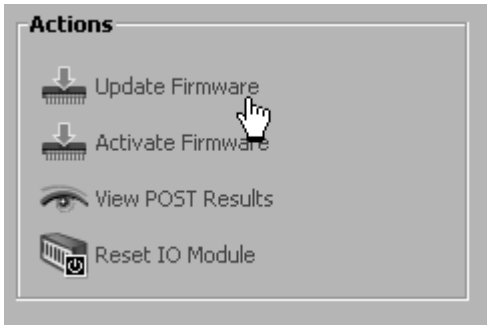
This is a shared environment. *Do not* update any code levels on shared components such as IO modules or Fabric Interconnects unless specifically directed to by your instructor.

Complete these steps:

Step 1 Choose an **IO Module** within the **Equipment** tab.

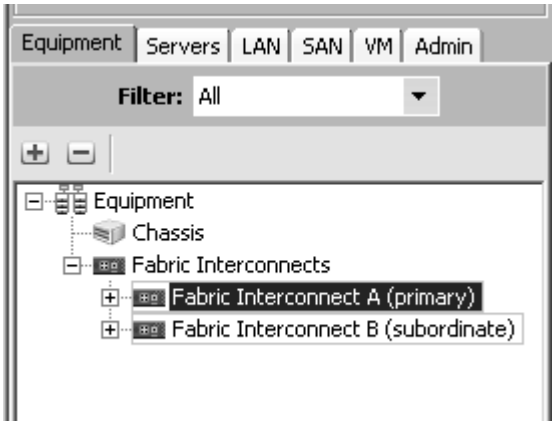


Step 2 In the **Actions** window, click **Update Firmware**.

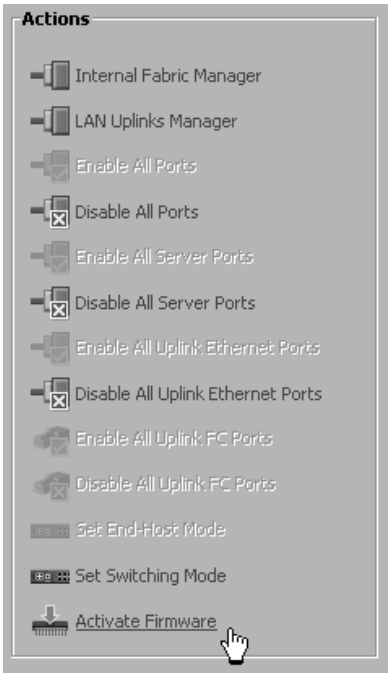


Step 3 Review the options available. Click **Cancel.** *Do not update firmware on the IO Module.*

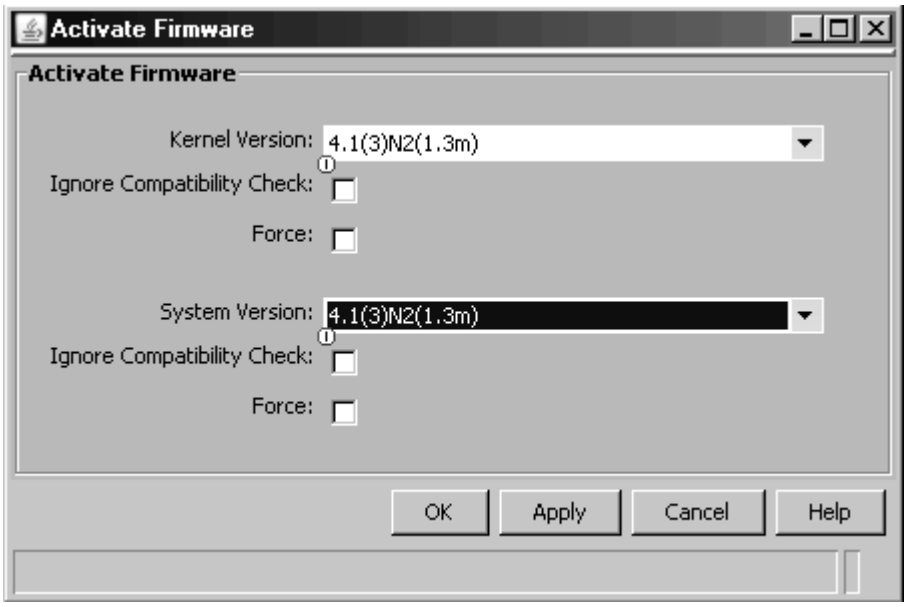
Step 4 Choose a Fabric Interconnect from the Equipment tab.



Step 5 In the **Actions** window, choose **Activate Firmware**.



Step 6 Review the available options, and then click Cancel. Do not update firmware on the Fabric Interconnect.



Lab 6-1: Creating Simple Service Profiles

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

Activity Objective

In this activity, you will perform the steps necessary to create a service profile and install an operating system on a blade server. After performing this lab, you should be able to:

Create an IP pool range for KVM access

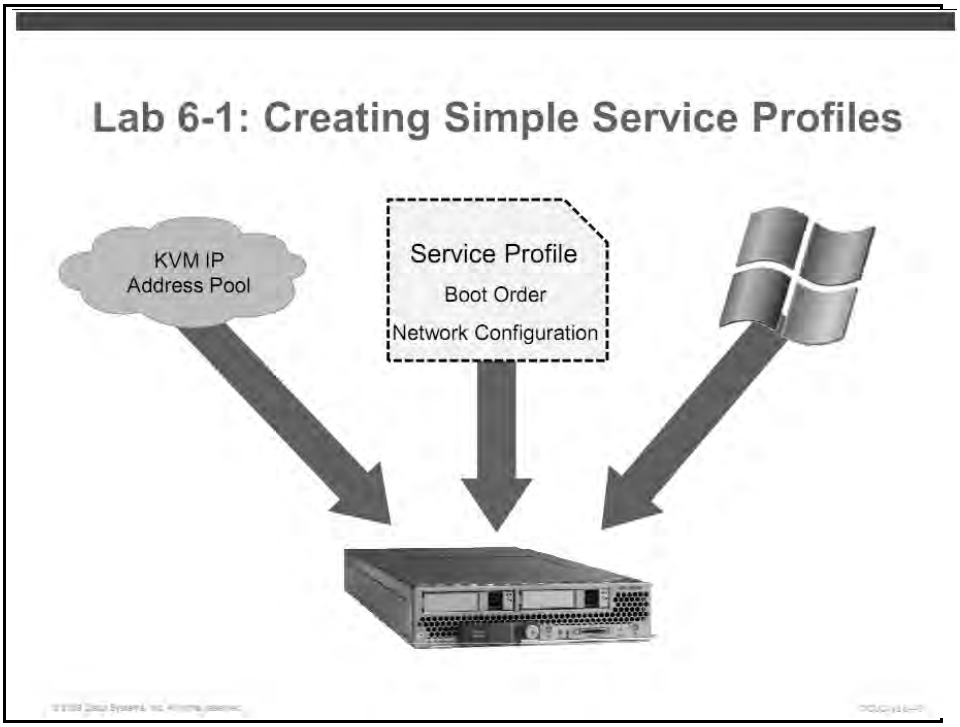
Create a service profile

Associate a service profile with a physical blade

Boot a blade server and install an operating system

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:

- (2) Cisco UCS 6100 Fabric Interconnects
- One blade server
- ISO image of an operating system (optional)

Task 1: Create an IP Range for KVM Access

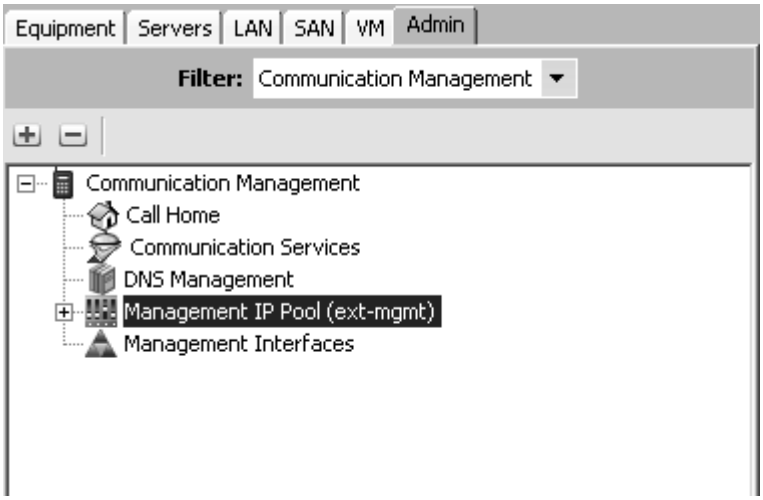
In this task, you will create a pool of IP addresses to be used for KVM access to the blade servers.

Activity Procedure

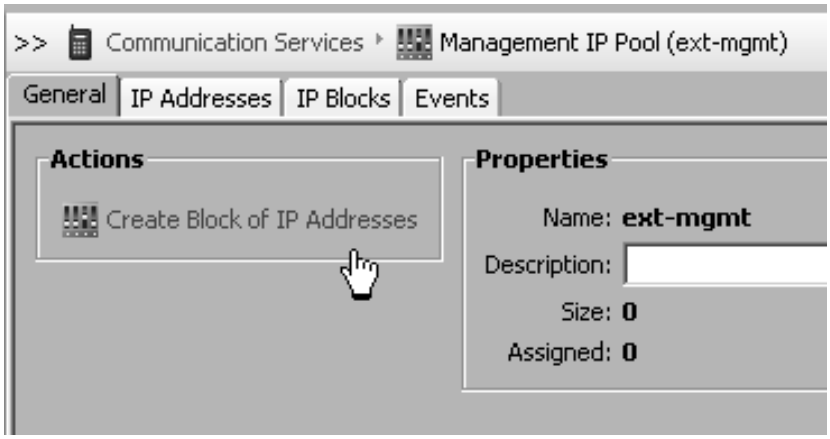
Complete these steps:

Step 1 Log into the Cisco UCS Manager.

Step 2 Choose the **Admin** tab in navigation pane. It may be helpful to adjust the **Filter** field to **Communications Services** for the next tasks.

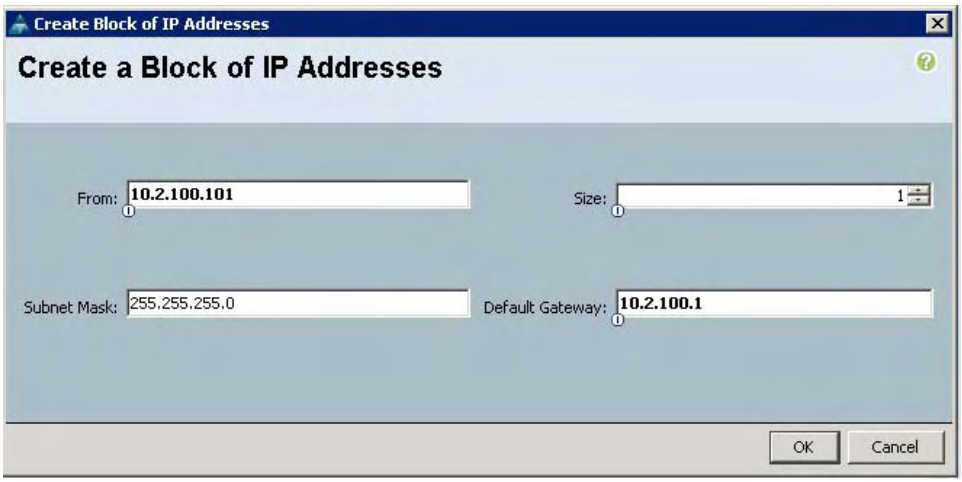


Step 3 Choose **Management IP Pool (ext-mgmt)** within the Communications Services subsection as shown in the previous example. In the **Actions** window, click the **Create Block of IP Addresses** link.



Step 4 For the initial classroom setup, a pool of 16 addresses was created [10.2.100.100 - 10.2.100.116]. If this pool still exists, please delete it.

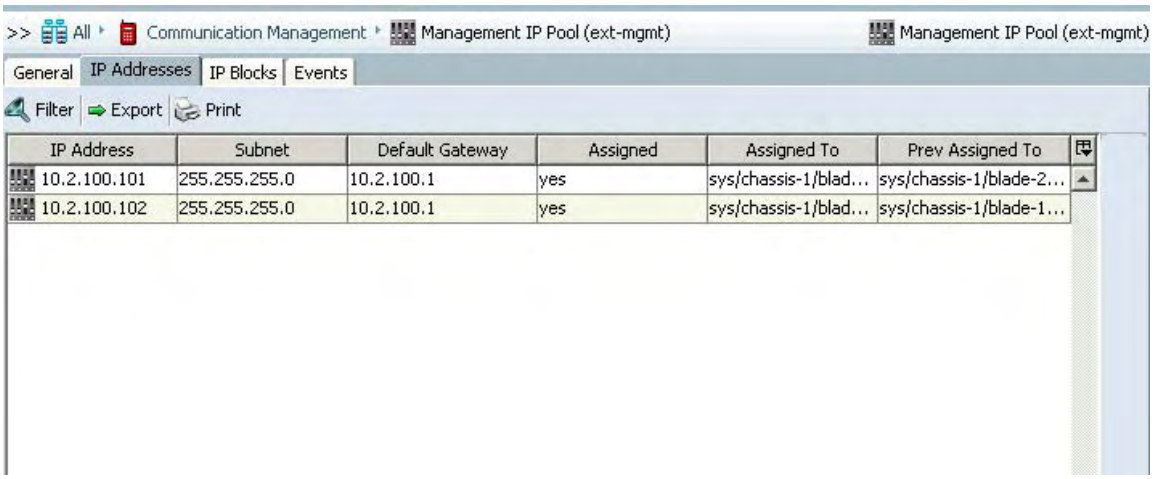
Step 5 Create a single address pool, note that this address will become associated with a physical server and each team can use many different addresses throughout the labs. Create a block of **one** IP address starting at 10.2.100.ZZ where ZZ=100 + Pod Number and click **OK**. (Subnet Mask and Default Gateway as below.)



Note In a production environment, you would not create individual IP addresses in this manner. It is done in this lab only to allow all teams the opportunity to practice creating the IP ranges.

Step 6 Click **OK** to clear the confirmation window.

Step 7 Choose the **IP Addresses** tab and validate that your newly created IP address has become associated with a blade server. (You have no control over which IP address becomes assigned to which blade).



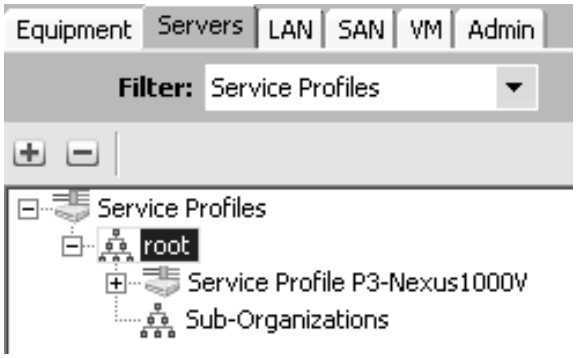
Task 2: Create a Service Profile

In this task, you will create a service profile to be deployed on a blade server.

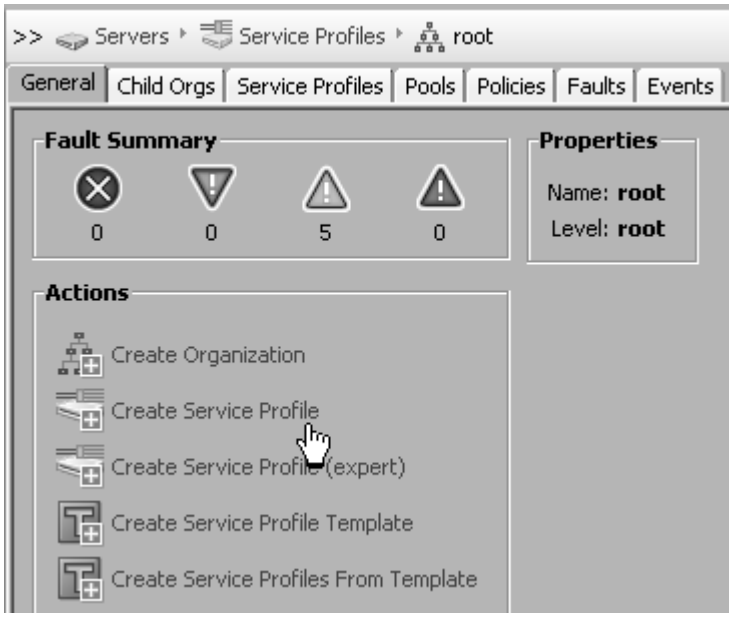
Activity Procedure

Complete these steps:

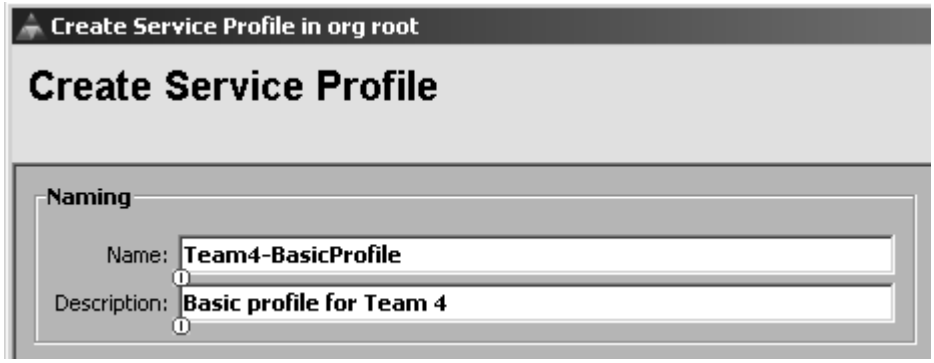
Step 1 Click the **Servers** tab in the navigation pane, and navigate to the **root** organization under Service Profiles.



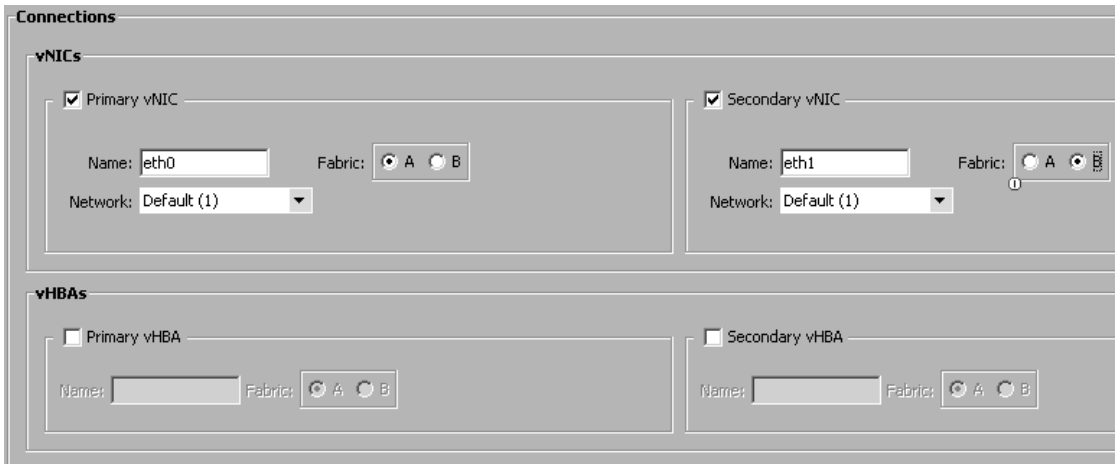
Step 2 Click Create Service Profile in the Actions frame.



Step 3 Name your profile **TeamX-BasicProfile**, replacing X with your team number. Provide a description of your choosing.

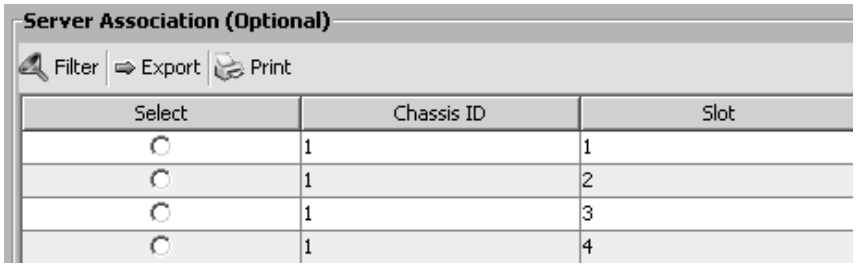


Step 4 Choose two vNICs and no vHBAs. Make sure that one vNIC connects to Switch A and one to Switch B. Make sure the vHBA boxes are unchecked.



Step 5 Choose **virtual CD-ROM** as the primary boot device, and local-disk as the secondary boot device.

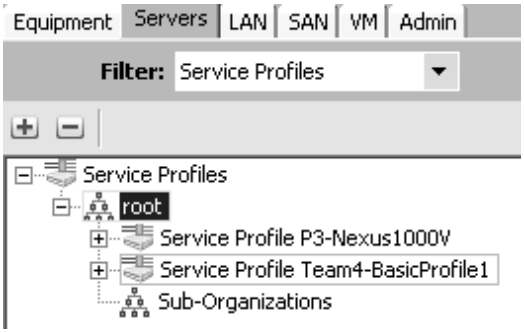
Step 6 Finally, make sure that no blade server is selected. You will manually choose a server in a later task.



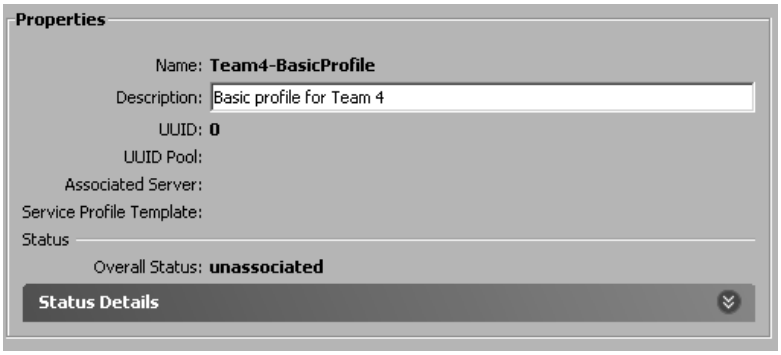
Step 7 Click **OK** to create the service profile.

Step 8 Click **OK** to confirm creation of the service profile.

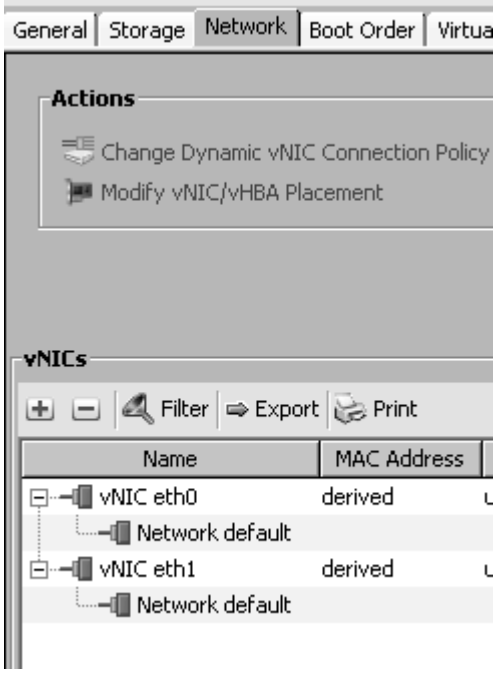
Step 9 Expand the **root** organization and explore your service profile.



Step 10 In your profile Properties, note that its status is unassociated.

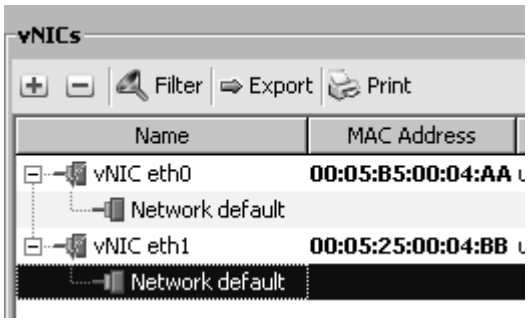


Notice that the MAC Address is derived; this will work for most CNA cards but not the M81KR VIC, as there are no BIA addresses for NICs or HBAs



Double Click on the word 'derived' and set the address as below, replacing XX with your team number. (Pod 1= 01, Pod 2 = 02, …)

vNIC eth0 **00:25:B5:00:XX:AA**
vNIC eth1 **00:25:B5:00:XX:BB**



Click 'Save Changes'

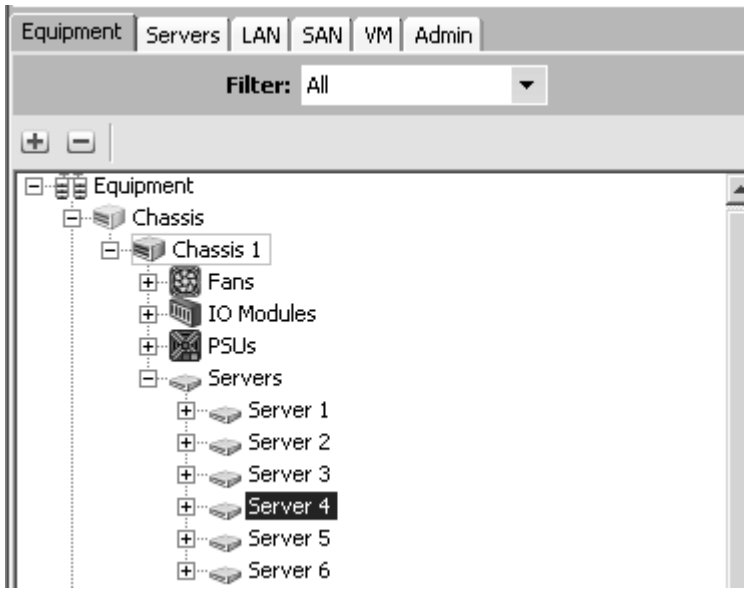
Task 3: Associate Service Profile

In this task, you will associate your service profile with a blade server.

Activity Procedure

Complete these steps:

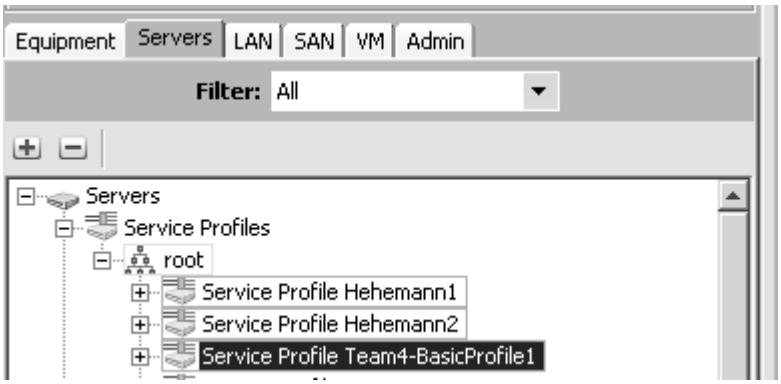
Step 1 Choose the **Equipment** tab in the navigation pane, and navigate to your team's blade server. Ask your instructor which blade server is assigned to your team.



Step 2 Click the **KVM Console** link in the **Actions** window of the **General** tab, and wait for the KVM console to load.

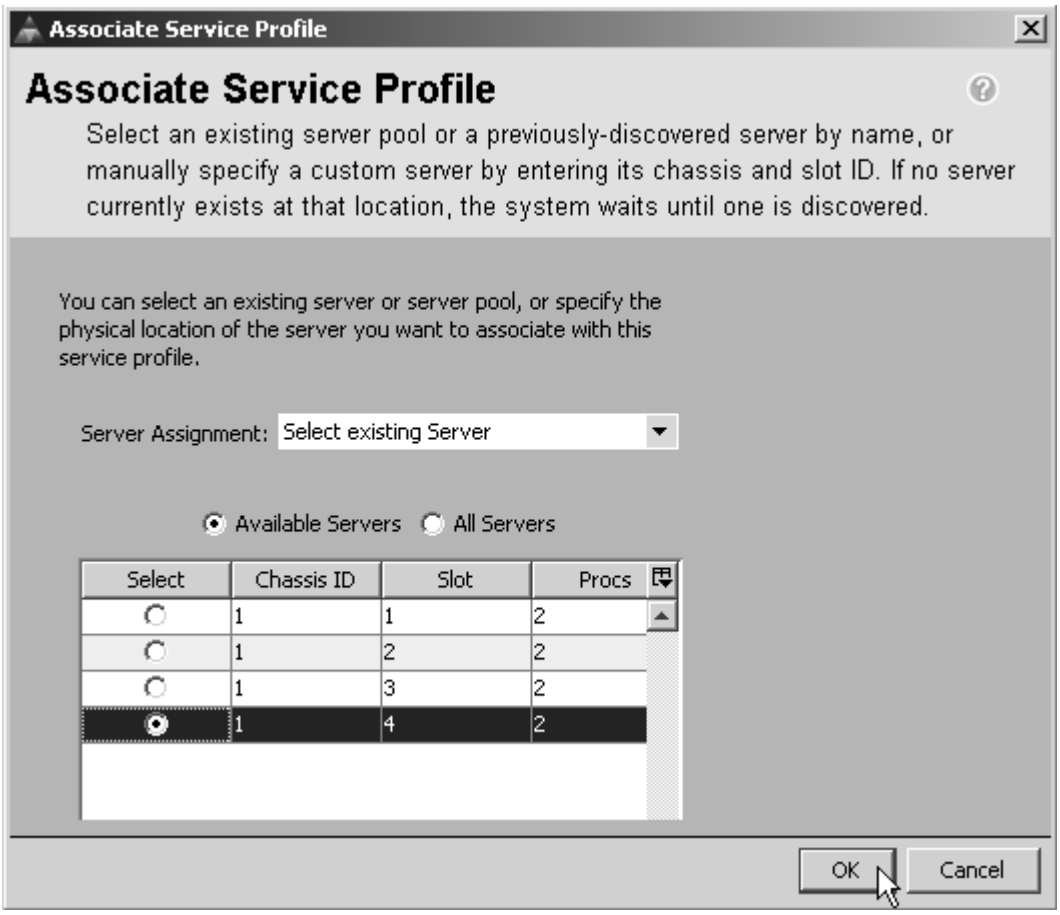
Step 3 The KVM console has successfully loaded when the screen appears similar to this figure. A green display with the text “No Signal” is normal for a blade that is powered down.

Step 4 Leaving the KVM console open, return to the Cisco UCS Manager and choose your service profile in the **Servers** tab.

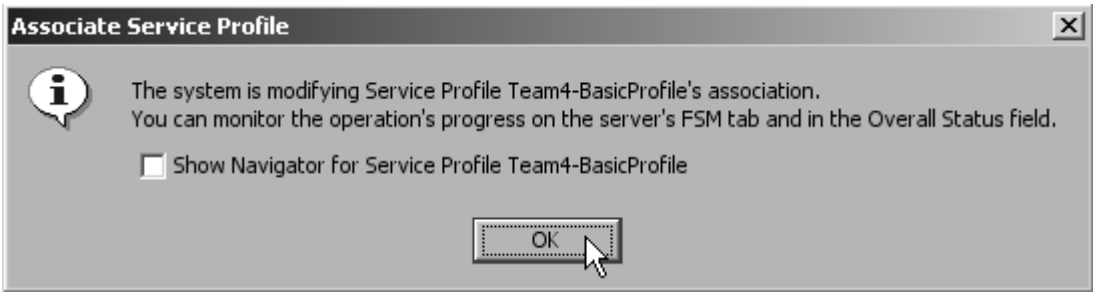


Step 5 In the Actions pane, click the Change Service Profile Association link.

Step 6 Choose **Select Existing Server** in the **Server Assignment** field, and then click the radio button for your team blade server. Click OK to associate your service profile to your blade.

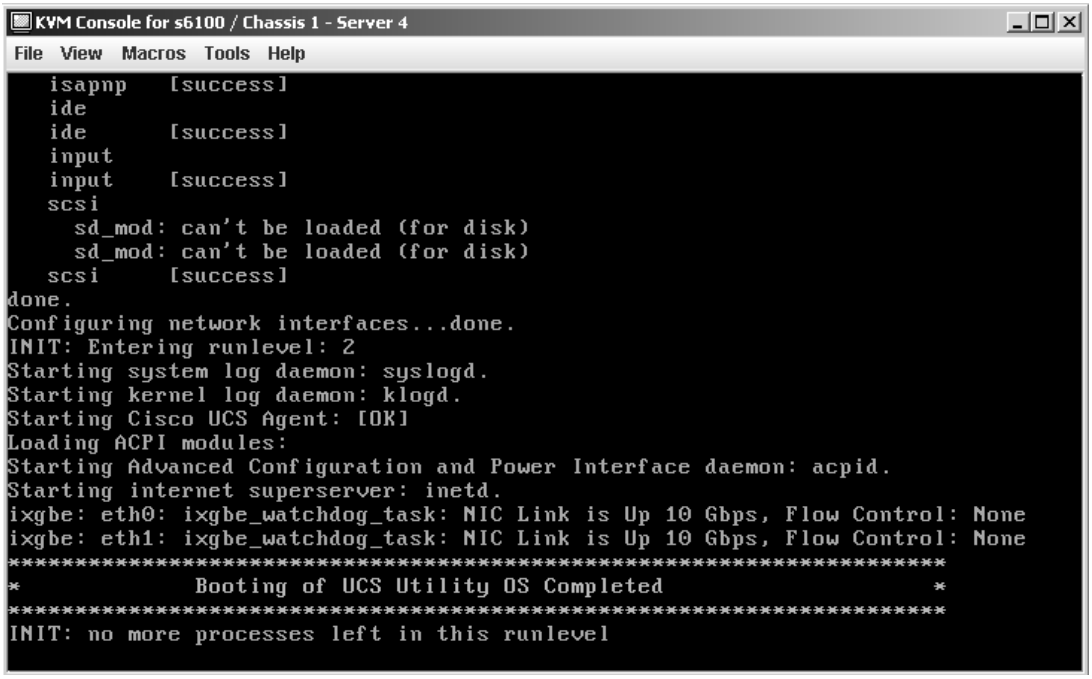


Step 7 Click **OK** to confirm association of the service profile to your blade server.

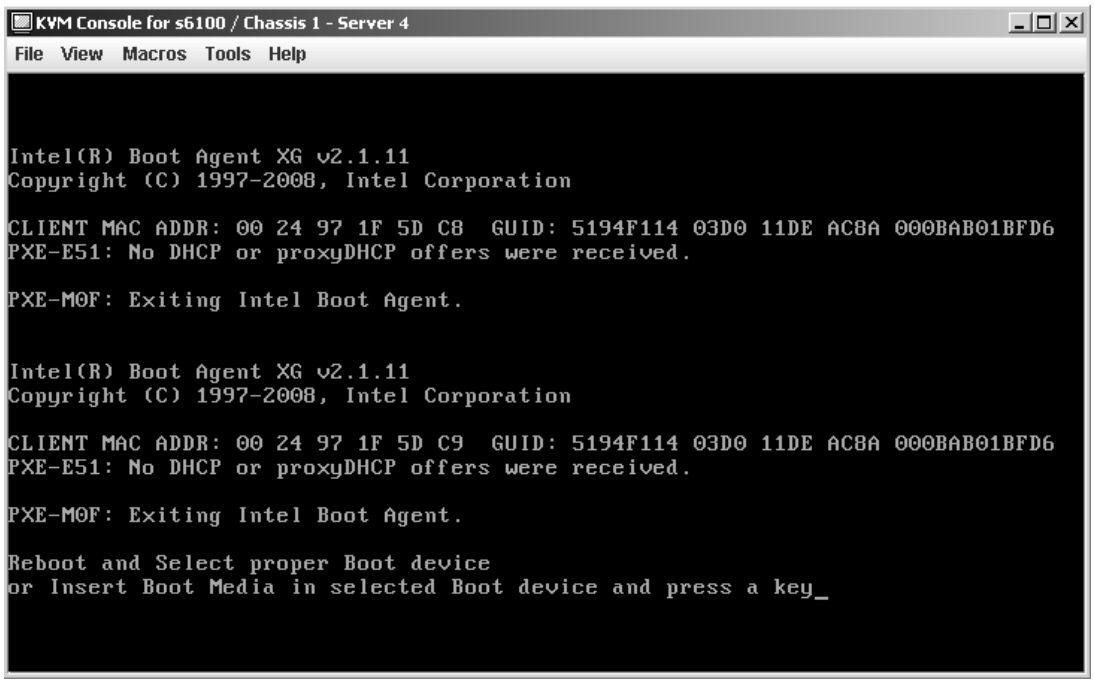


Step 8 Watch the KVM window to see the blade server begin to boot.

Step 9 Observe as the blade server performs a PXE boot from the Cisco UCS Manager and runs the Cisco UCS Utility Operating System (UUOS) setup routines. No administrator intervention is necessary at this phase.



Step 10 After UUOS has completed configuring the blade according to the service profile, the blade will be rebooted again. The blade is finished booting when it is unable to find a valid boot device. Note that a previous student may have left an operating system on the local disks. If your blade boots into an operating system, you may skip the next optional task or ask your instructor for further assistance.



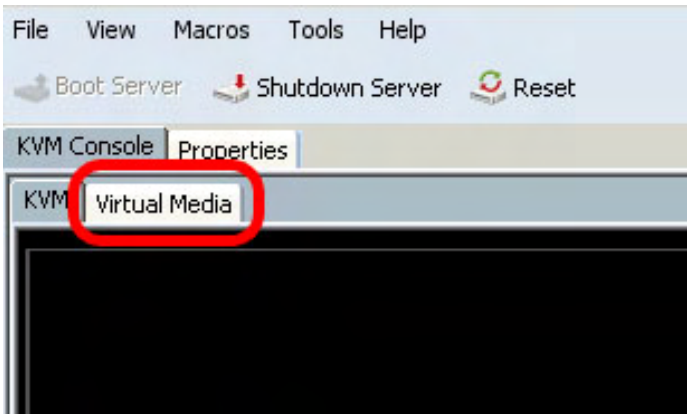
Task 4: Begin Installing an Operating System

In this task, you will begin installing an operating system on the local disk of your blade server by using virtual media.

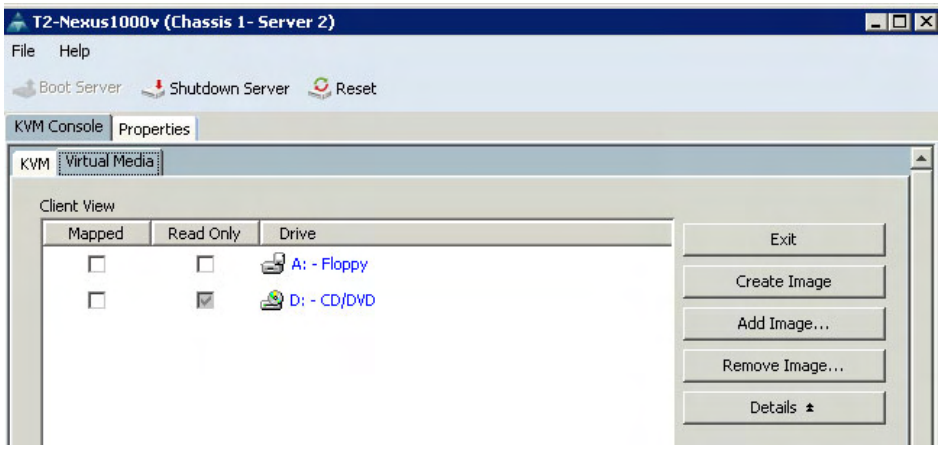
Activity Procedure

Complete these steps:

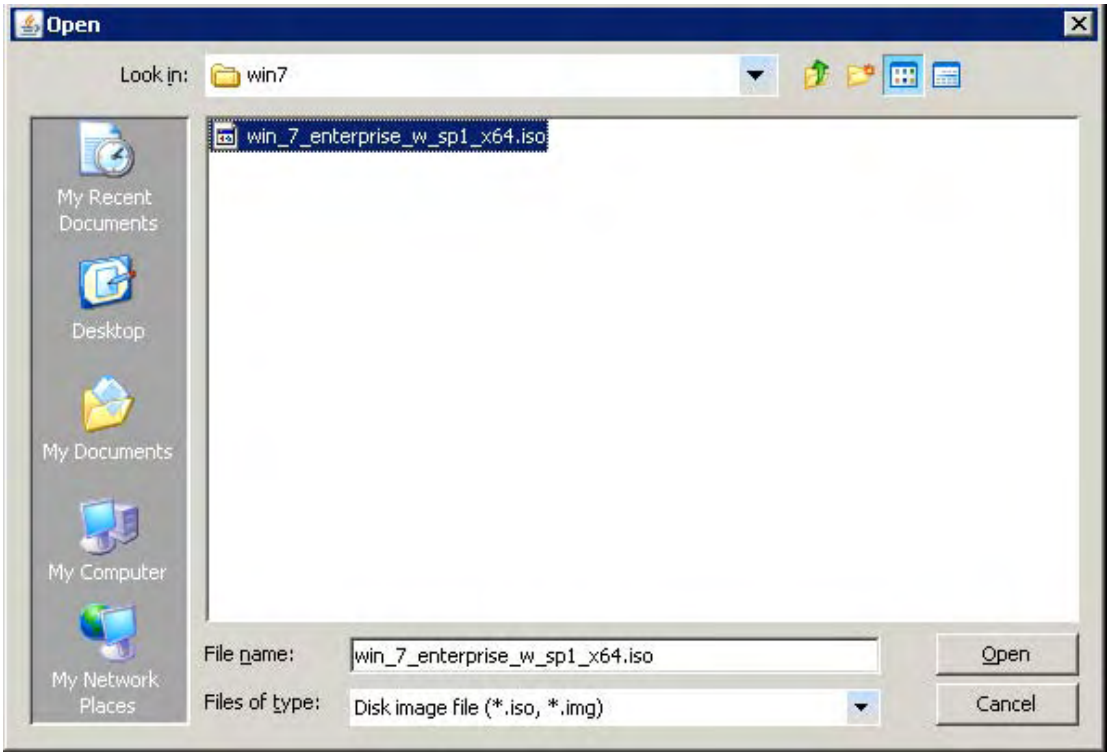
Step 1 From your blade's KVM window, choose **Virtual Media Tab**.



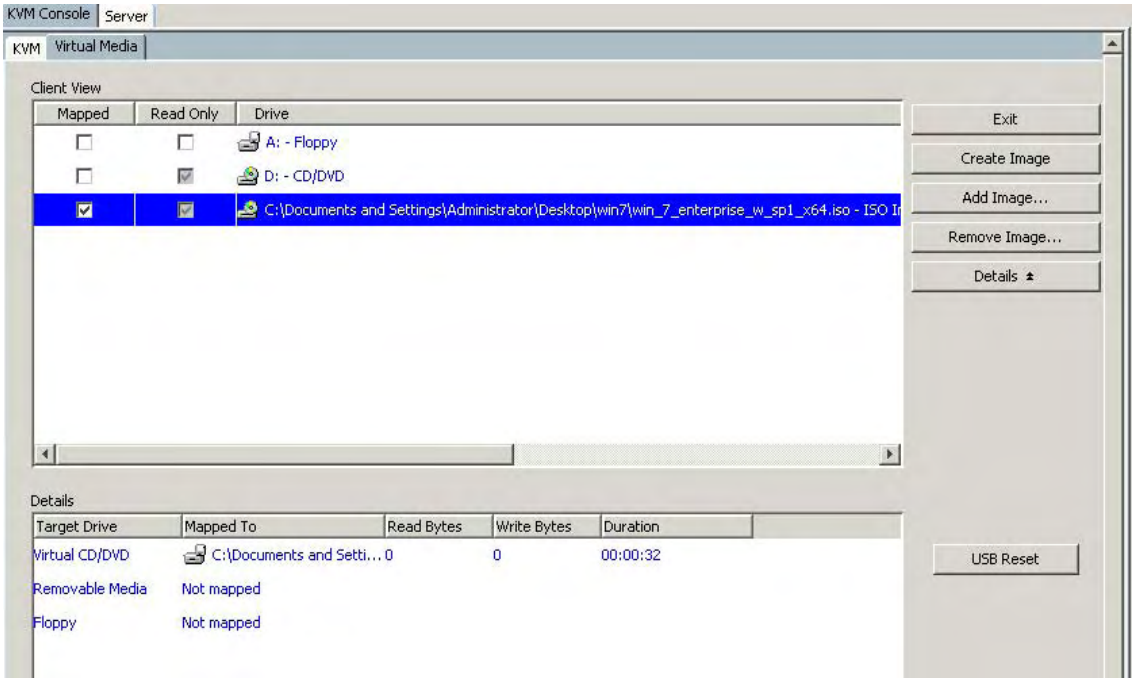
Step 2 When the Virtual Media tab launches, click **Add Image.**



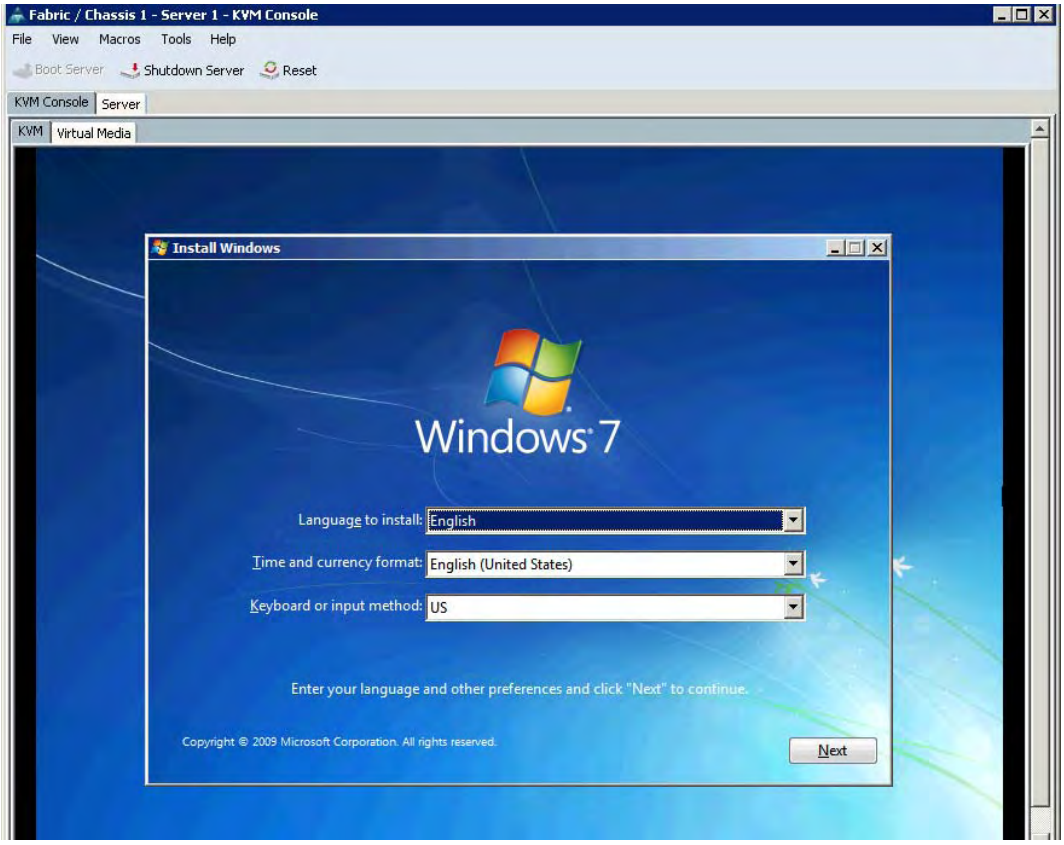
Step 3 Your instructor will provide you with the proper filename to select. Choose the image and click **Open**. Desktop\Win7\win_7_enterprise_w_sp1_x64.iso



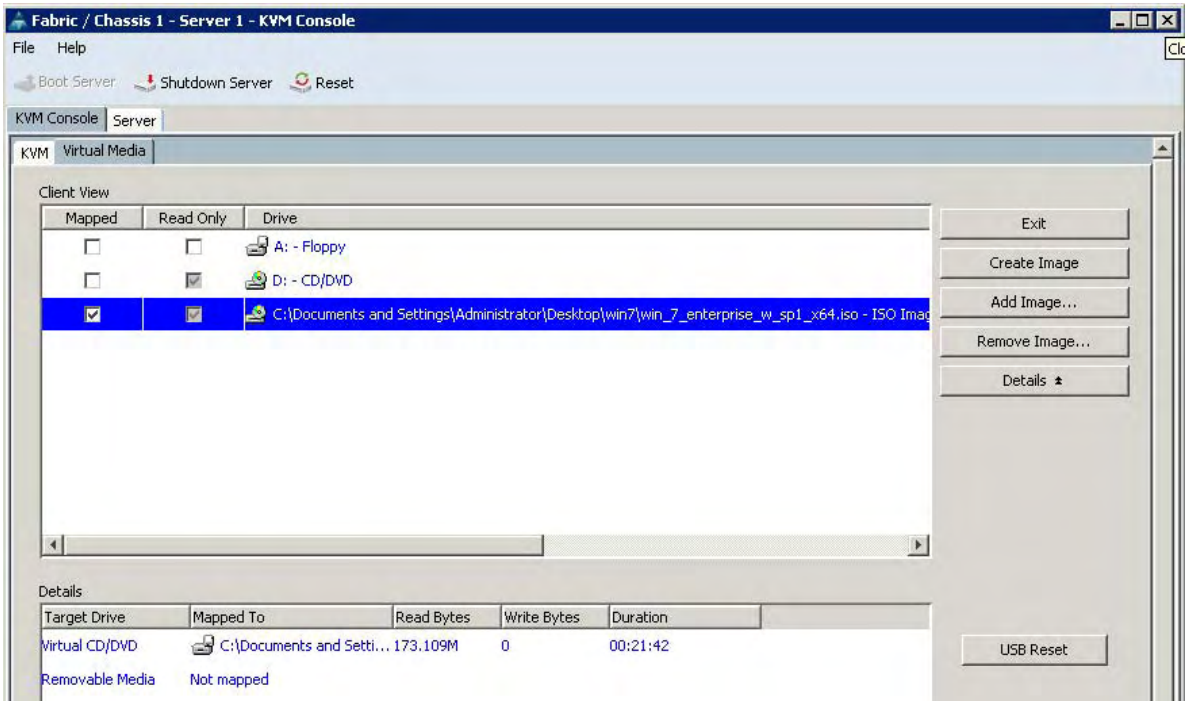
Step 4 When the filename appears as a device, click the **Mapped** checkbox. This presents the image to the server as a CD-ROM. At this time, also click the **Details** button. This will present more information about the mappings and show when data is being transferred from the virtual CD-ROM device.



Step 5 Return focus to the KVM window and press any key. The blade server will rescan for boot devices and begin booting from the ISO image that you specified.

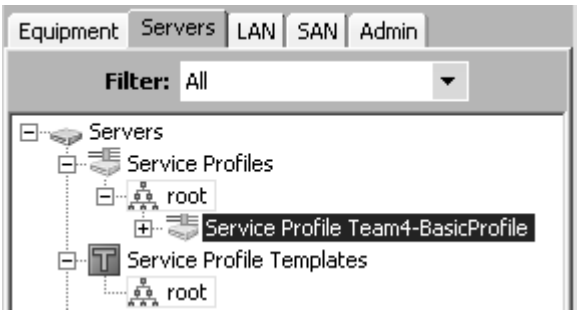


Step 6 Return to the Virtual Media Session and observe the data transfer counters.



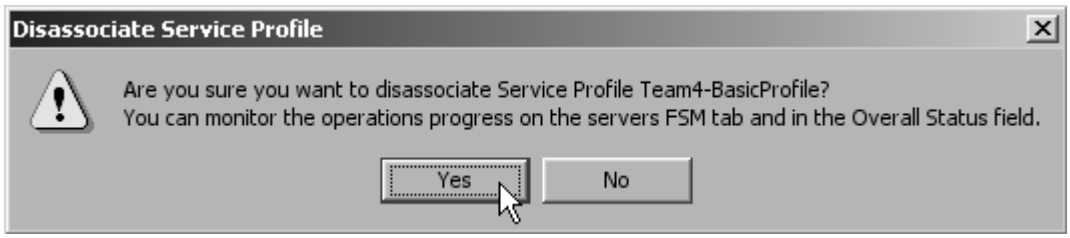
Step 7 There is no need to continue with the operating system installation. Close the Virtual Media Session.

Step 8 Return to the **Servers** tab and navigate to your service profile.



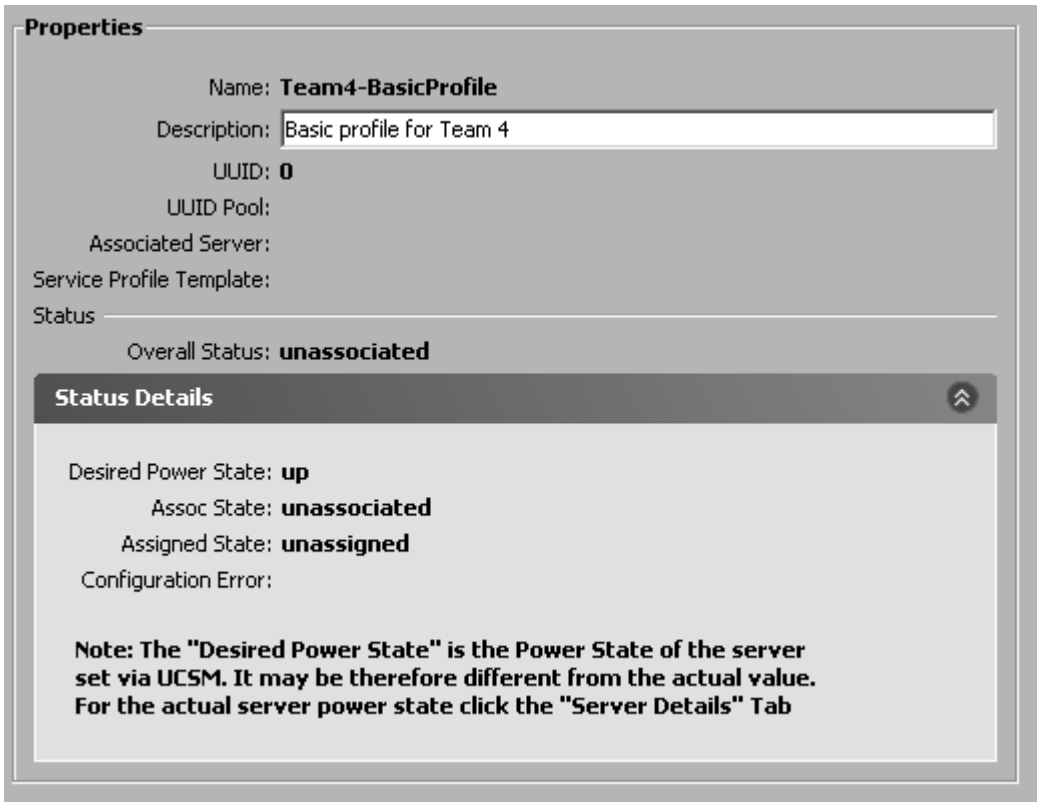
Step 9 In the Actions window, click Disassociate Service Profile.

Step 10 Click **Yes** to confirm the disassociation.



Step 11 Watch the KVM window to observe the disassociation process. It may take several minutes before the disassociation process begins. Cisco UCS Manager will attempt to give the operating system running an opportunity to gracefully shut down .In this case, there was no running operating system, so, eventually Cisco UCS Manager forcibly restarts the blade.

Step 12 The blade will again boot the UUOS to perform any necessary disassociation actions. When it is complete, the blade will be powered off. Return to the Cisco UCS Manager and verify that your service profile is now "unassociated."



Lab 6-2: Configuring Resource Pools

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

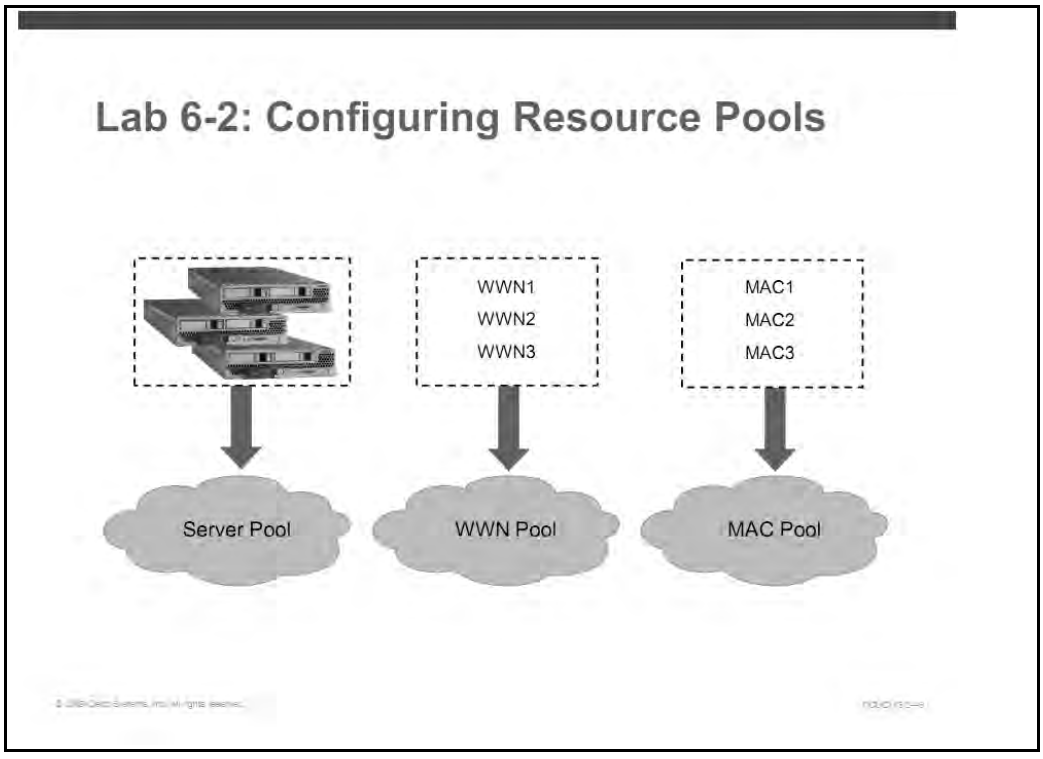
Activity Objective

In this activity, you will create many different types of resource pools within Cisco UCS Manager. After performing this lab, you should be able to:

- Create a MAC pool
- Create a WWNN pool
- Create a WWPN pool
- Create a UUID Suffix pool
- Create a manually populated server pool
- Create an automatically populated server pool

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:

- (2) Cisco UCS 6100 Fabric Interconnects
- One blade server

Task 1: Create a MAC Pool

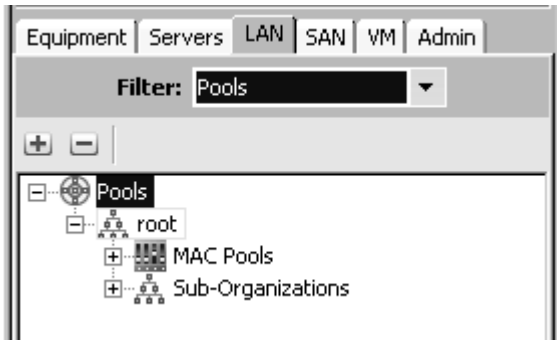
In this task, you will create a MAC pool for your mobile service profiles to use.

Activity Procedure

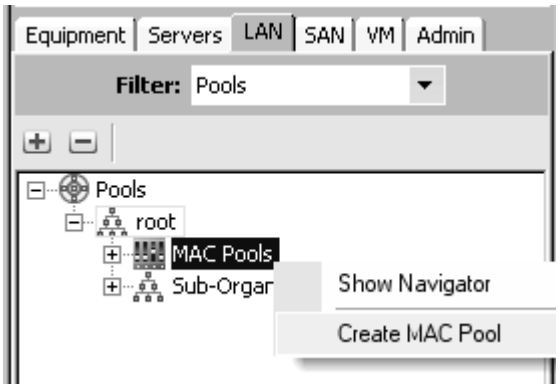
Complete these steps:

Step 1 Log into the Cisco UCS Manager if necessary.

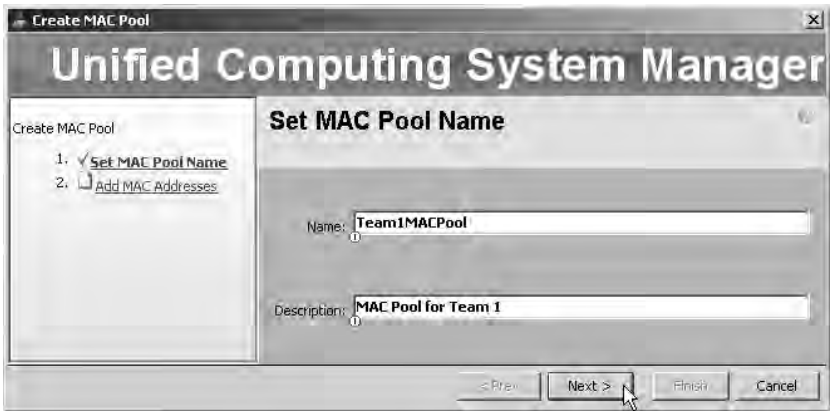
Step 2 Choose the **LAN** tab in the navigation pane. It may be useful to adjust the **Filter** setting to **Pools** for the following tasks.



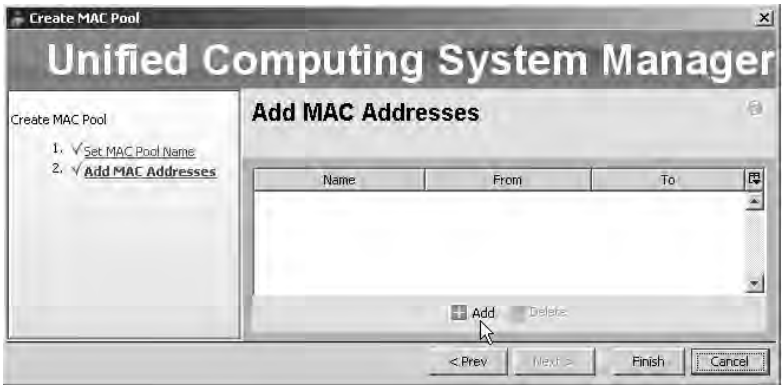
Step 3 Right-click **MAC Pools** and choose **Create MAC Pool**.



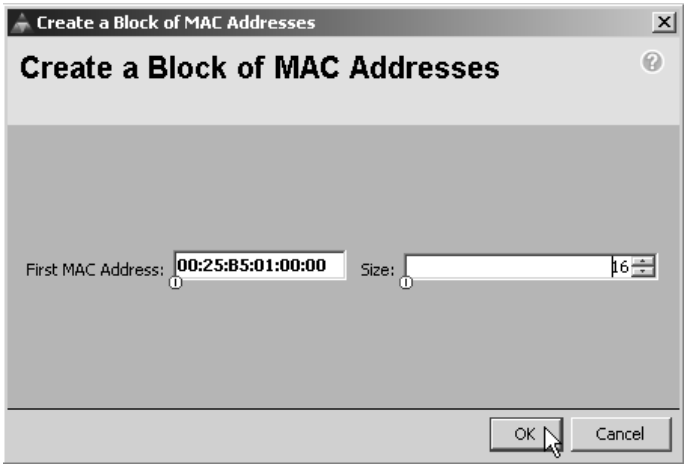
Step 4 Name your MAC Pool **TeamXMACPool**. Replace X with your team number. Optionally, provide a description for your pool and click **Next**.



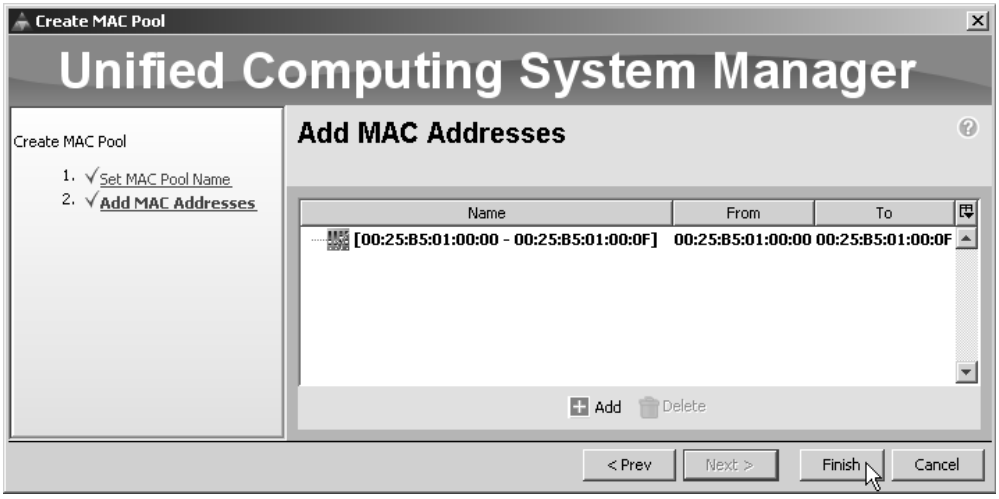
Step 5 Click **Add** to add MAC addresses to your pool.



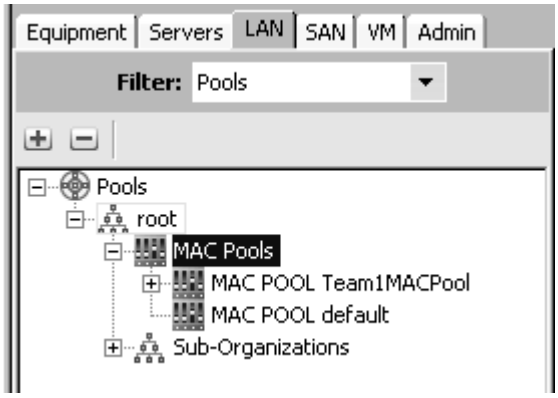
Step 6 Note that the first three octets of the MAC address have been prepopulated with a Cisco OUI and cannot be modified. Change the fourth octet to your team number (00:25:B5:XX:00:00). In this example, it has been changed to 01 for Team 1. Specify 16 addresses to be created and click **OK**.



Step 7 Verify that the proper range has been added to the block and click **Finish**. The range should be from 00:25:B5:XX:00:00 to 00:25:B5:XX:00:0F.



Step 8 Expand the **MAC Pools** icon in the navigation pane and verify that your pool has been created.



Task 2: Create a World Wide Node Name Pool

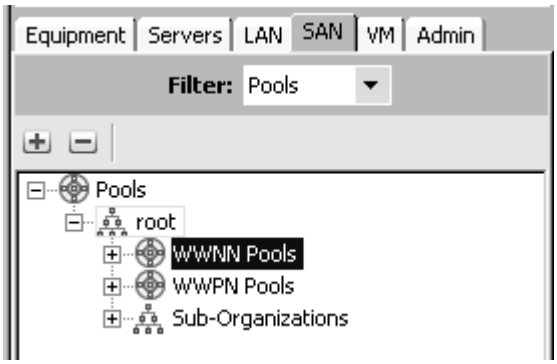
In this task, you will create a WWNN pool for your mobile service profiles to use.

Activity Procedure

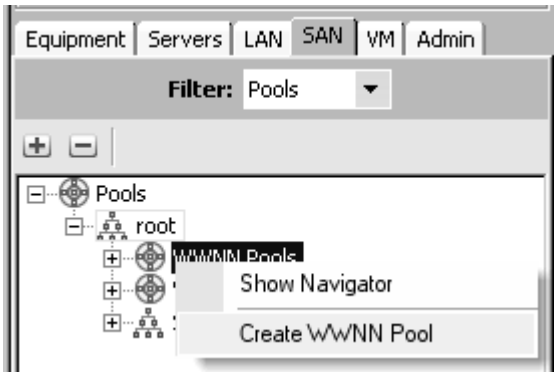
Complete these steps:

Step 1 Log into the Cisco UCS Manager.

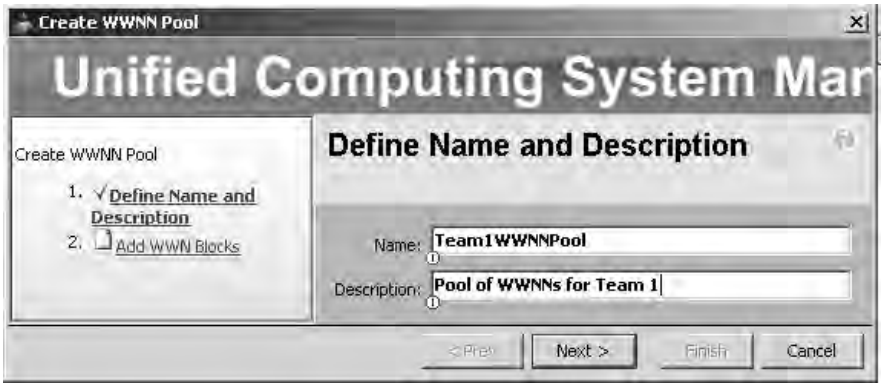
Step 2 Choose the **SAN** tab in the navigation pane. It may be useful to adjust the **Filter** setting to **Pools** for the following tasks.



Step 3 Right-click WWNN Pools and choose Create WWNN Pool.

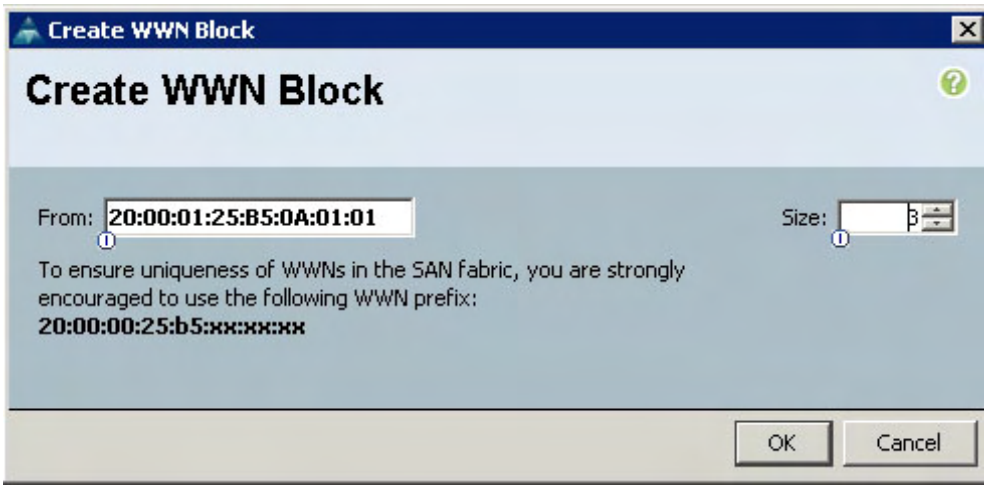


Step 4 Name your WWNN Pool **TeamXWWNNPool**. Replace X with your team number. Optionally, provide a description for your pool and click **Next**.

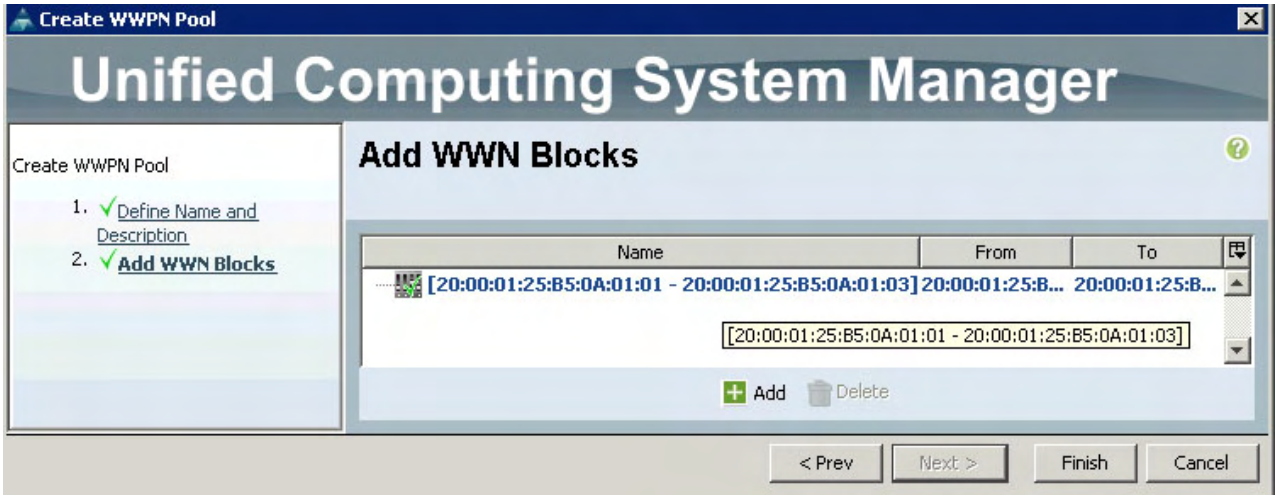


Step 5 Click **Add** to add WWNNs to your pool.

Step 6 Cisco UCS Manager does not prepopulate any of the WWN fields. However, it will only accept values that begin with 2 or 5, in accordance with WWN standards. Create your pool beginning with 20:00:01:25:B5:0**Y**:0**X**:01, replacing X with your team number; i.e Team 1 = 01, Team 2 = 02, and Y with "A" for odd and "B" for even team numbers. Create a pool of three (3) WWNs, and click **OK**.

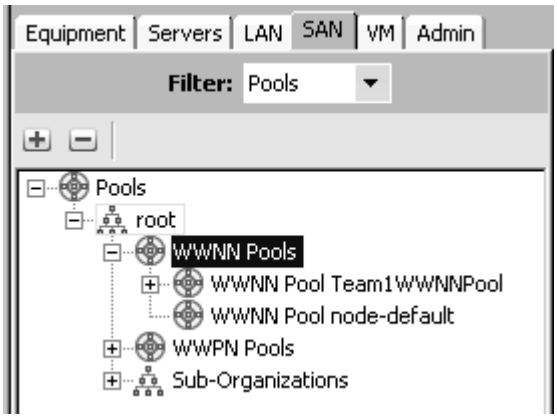


Step 7 Verify that the proper range has been added to the block and click **Finish**.



Step 8 Click **OK** to confirm creation of the WWNN Pool.

Step 9 Expand the **WWNN Pools** icon in the navigation pane and verify that your pool has been created.



Task 3: Create a World Wide Port Name Pool

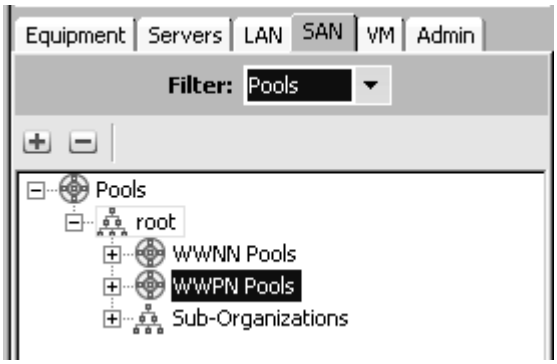
In this task, you will create a WWPN pool for your mobile service profiles to use.

Activity Procedure

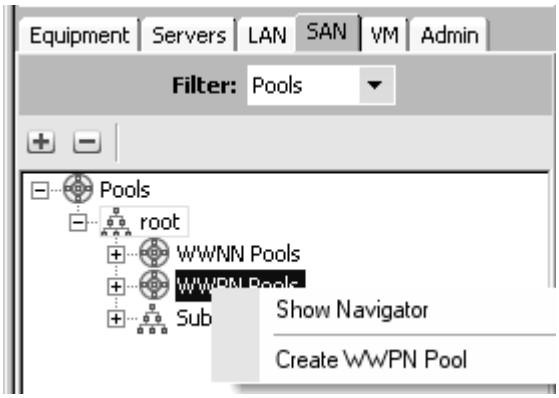
Complete these steps:

Step 1 Log into the Cisco UCS Manager.

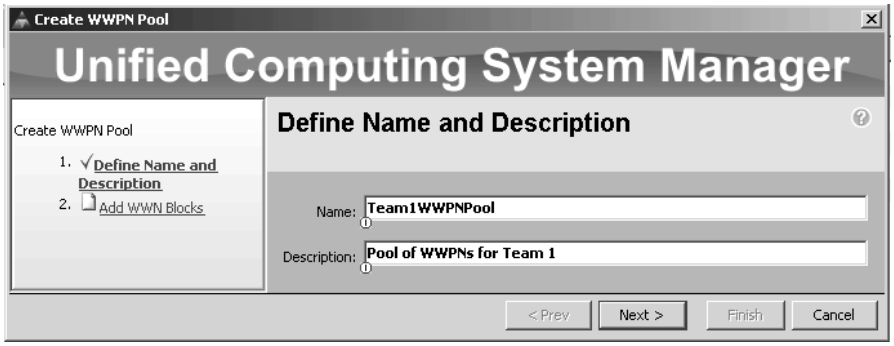
Step 2 Choose the **SAN** tab in navigation pane. It may be useful to adjust the **Filter** setting to **Pools** for the following tasks.



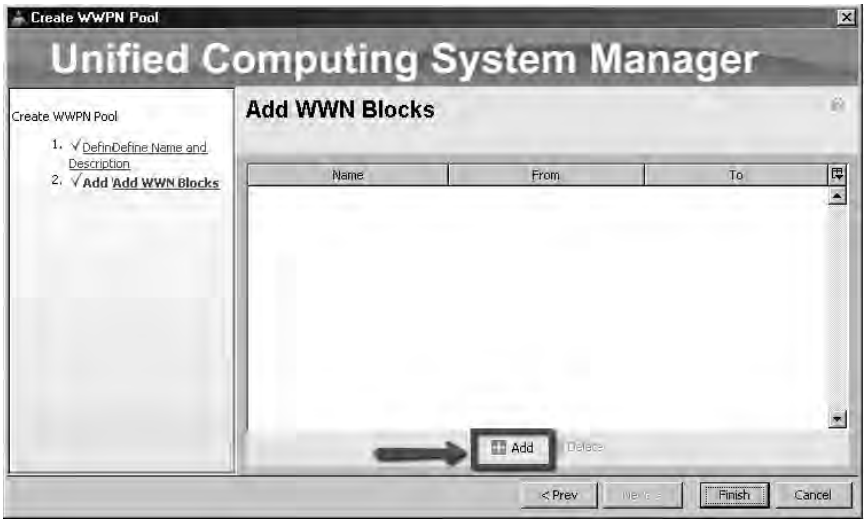
Step 3 Right-click WWPN Pools and choose Create WWPN Pool.



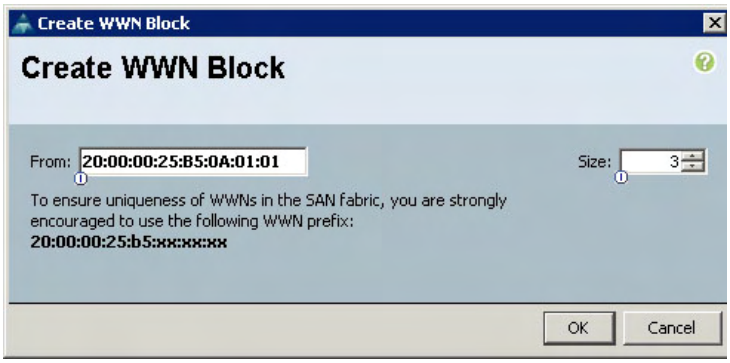
Step 4 Name your WWPN Pool **TeamXWWPNPool**. Replace X with your team number. Optionally, provide a description for your pool and click **Next**.



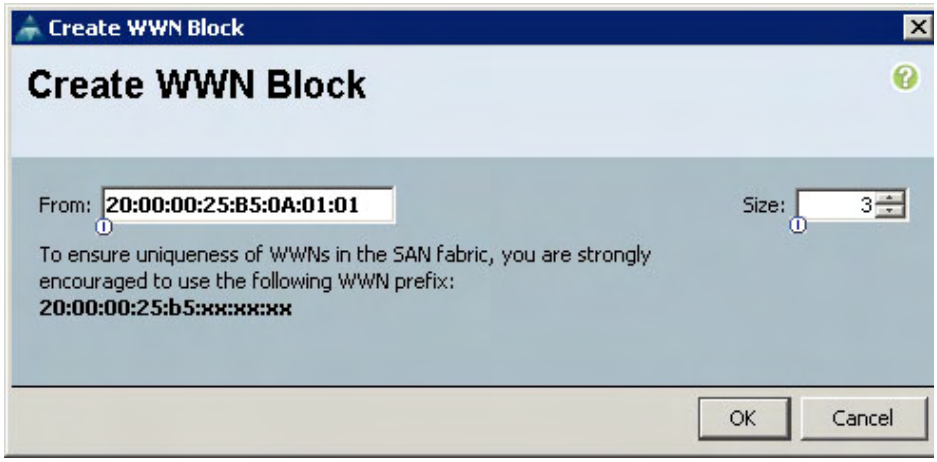
Step 5 Click **Add** to add WWPNs to your pool.



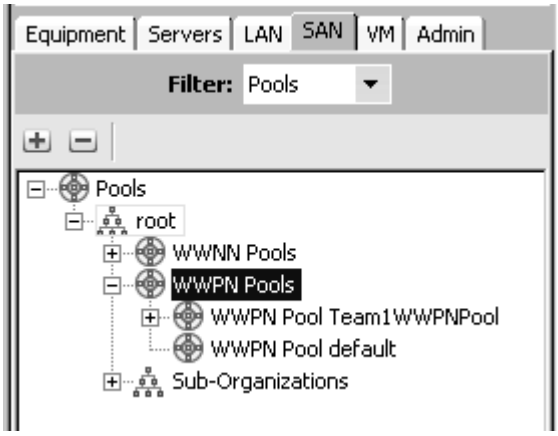
Step 6 Cisco UCS Manager does not prepopulate any of the WWN fields. However, it will only accept values that begin with 2 or 5, in accordance with WWN standards. Create your pool beginning with 20:00:00:25:B5:0**Y**:0**X**:01, replacing Y with "A" for even and "B" for odd team numbers and X with your team number. Create a pool of three (3) WWPNs starting from 01, and click **OK**.



Step 7 Verify that the proper range has been added to the block and click **Finish**.



Step 8 Expand the **WWPN Pools** icon in the navigation pane and verify that your pool has been created.



Task 4: Create a UUID Suffix Pool

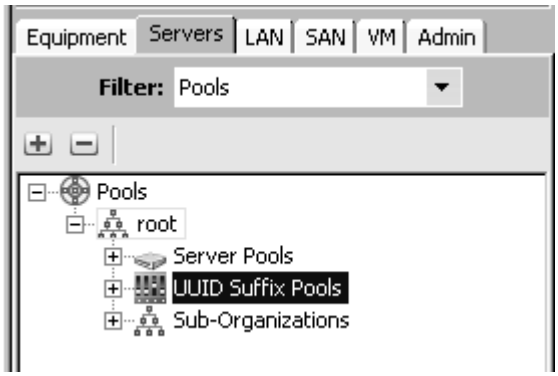
In this task, you will create a UUID Suffix pool for your mobile service profiles to use.

Activity Procedure

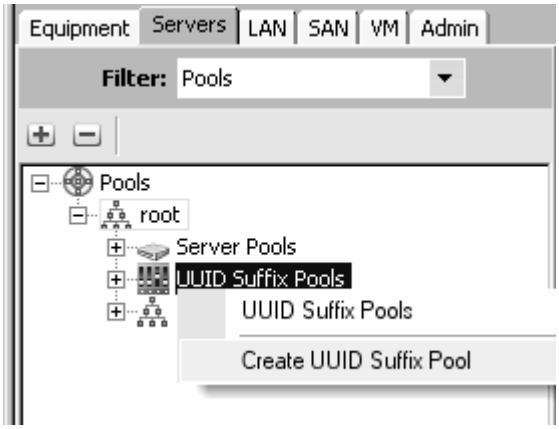
Complete these steps:

Step 1 Log into the Cisco UCS Manager if necessary.

Step 2 Choose the **Servers** tab in navigation pane. It may be useful to adjust the **Filter** setting to **Pools** for the following tasks.

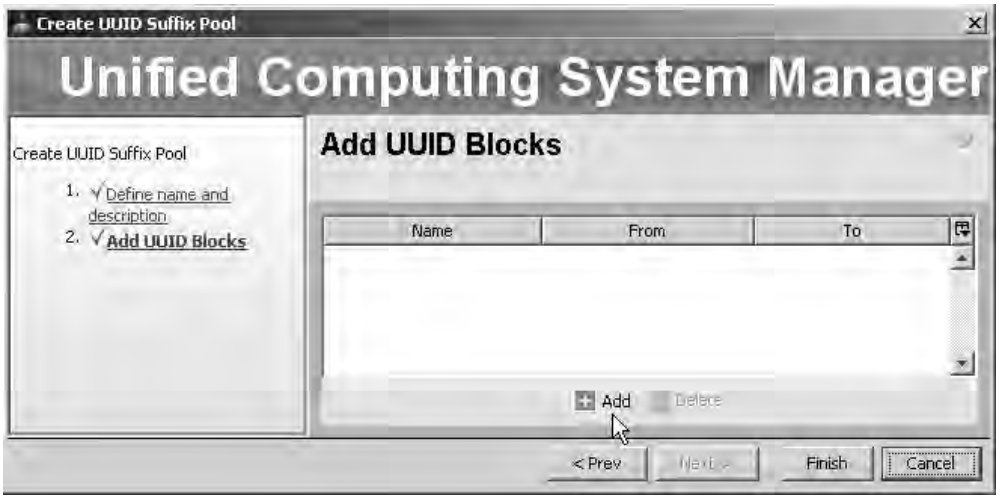


Step 3 Right-click UUID Suffix Pools and choose Create UUID Suffix Pool.

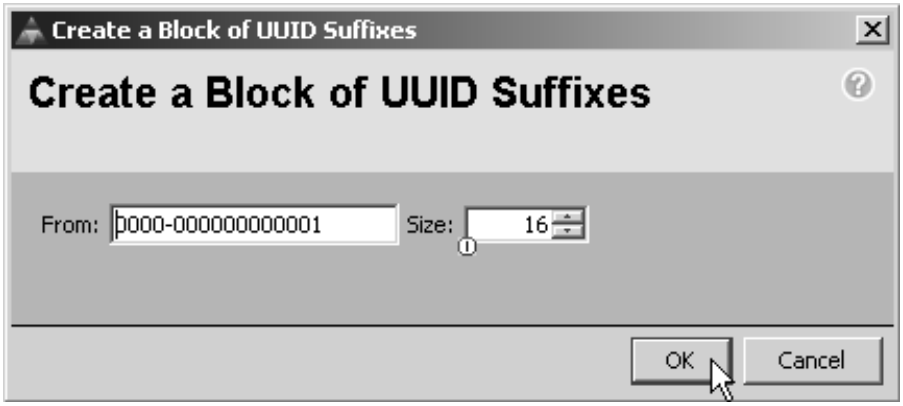


Step 4 Name your UUID Pool **TeamXUUIDPool**. Replace X with your team number. Optionally, provide a description for your pool. Select Prefix type: other and set the last digit of the prefix to your team number and click **Next**.

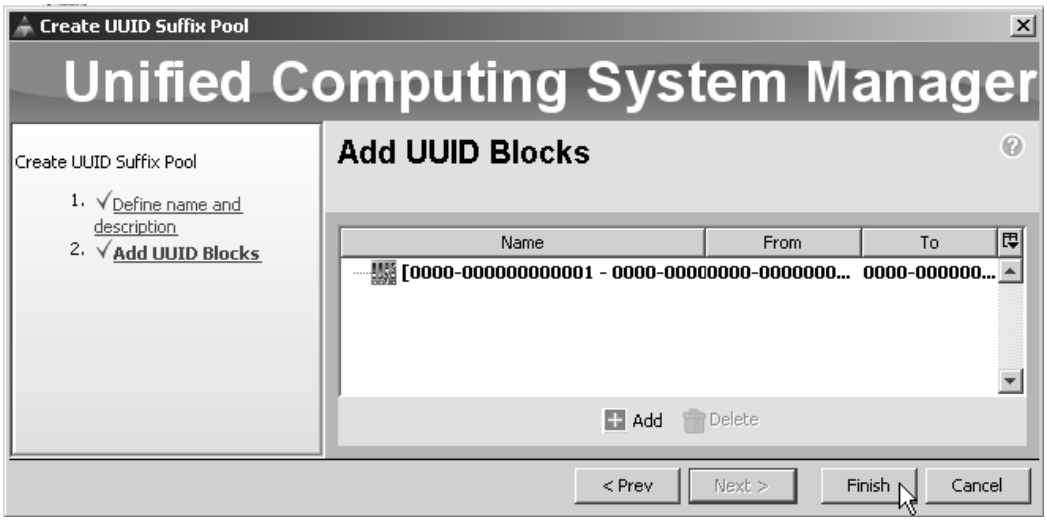
Step 5 Click **Add** to add UUIDs to your pool.



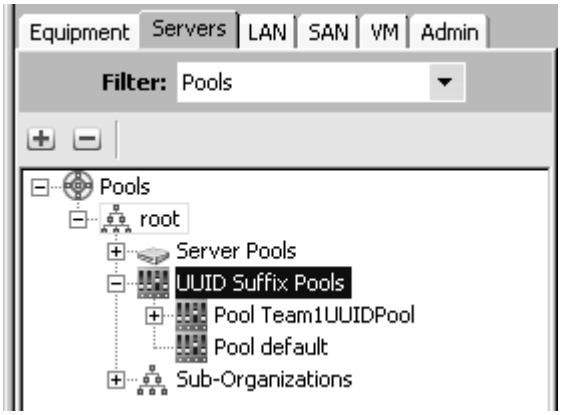
Step 6 Create a pool of 16 UUIDs and click **OK**.



Step 7 Verify that the proper range has been added to the block and click **Finish**.



Step 8 Expand the **UUID Suffix Pools** icon in the navigation pane and verify that your pool has been created.



Task 5: Create a Manually Populated Server Pool

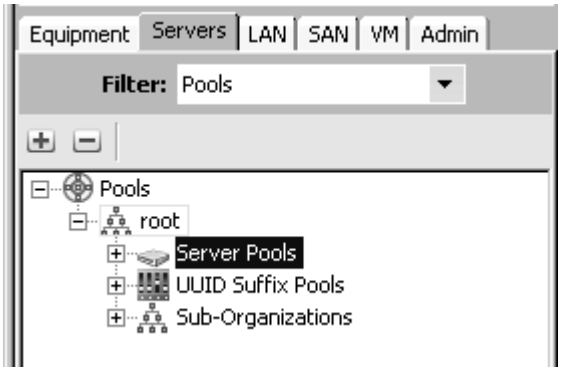
In this task, you will create a manually populated server pool that contains your assigned server.

Activity Procedure

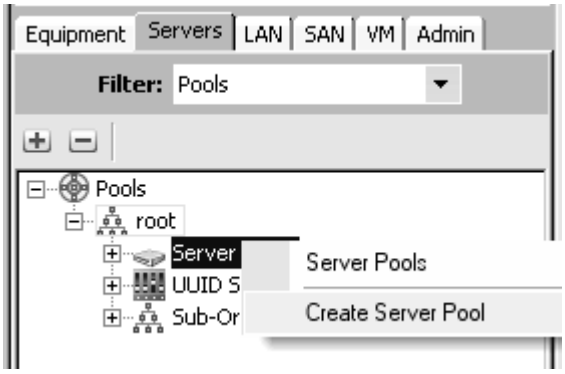
Complete these steps:

Step 1 Log into the Cisco UCS Manager.

Step 2 Choose the **Servers** tab in the navigation pane. It may be useful to adjust the **Filter** setting to **Pools** for the following tasks.

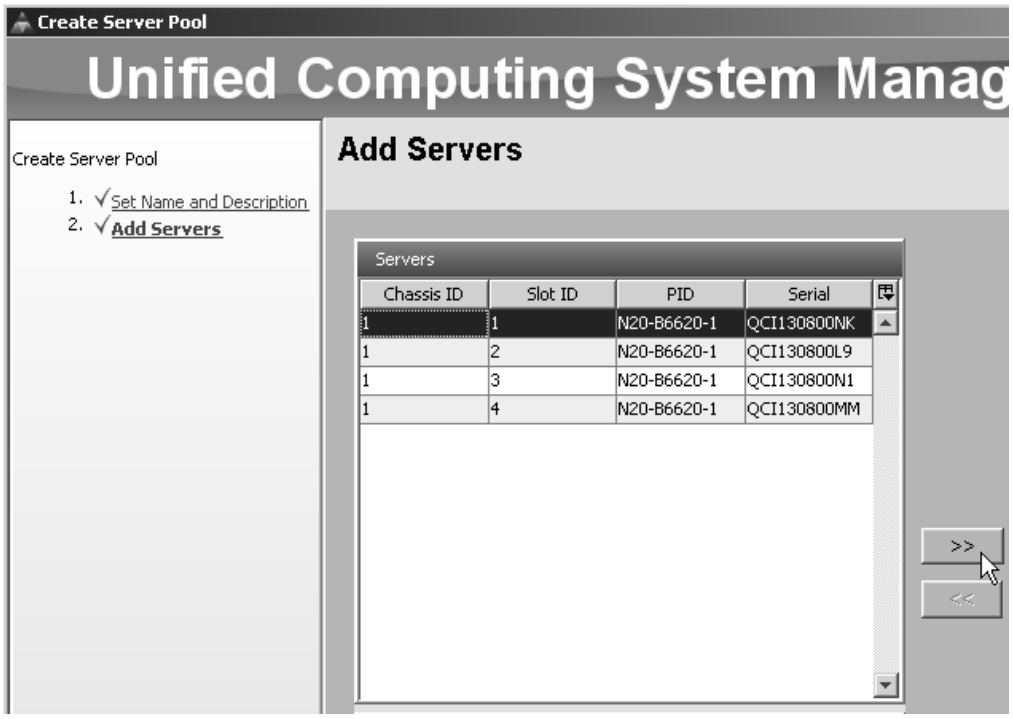


Step 3 Right-click Server Pools and choose Create Server Pool.

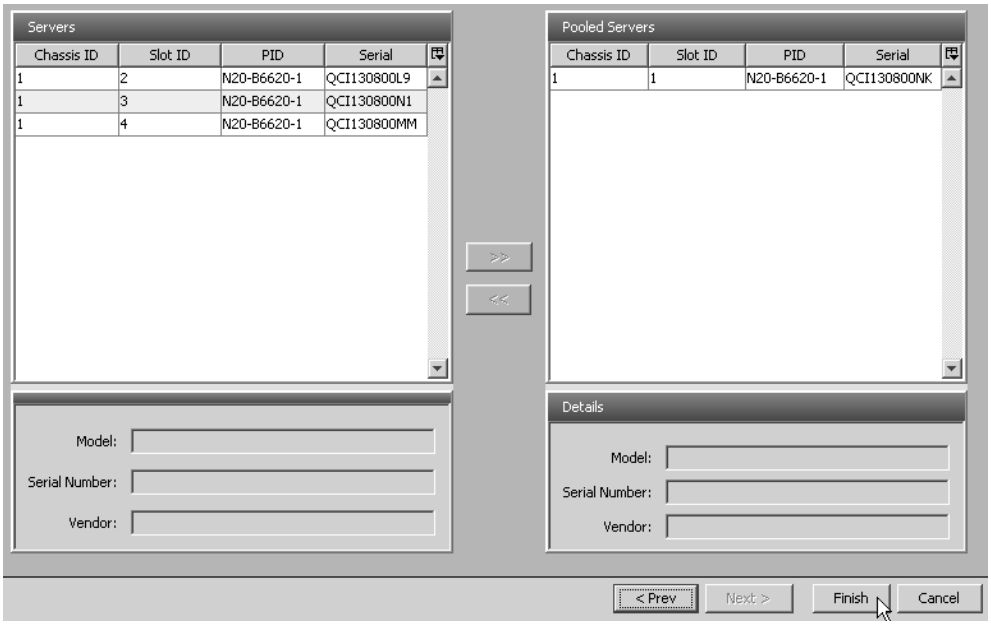


Step 4 Name your server pool **TeamXServerPool**. Replace X with your team number. Optionally, provide a description for your pool and click **Next**.

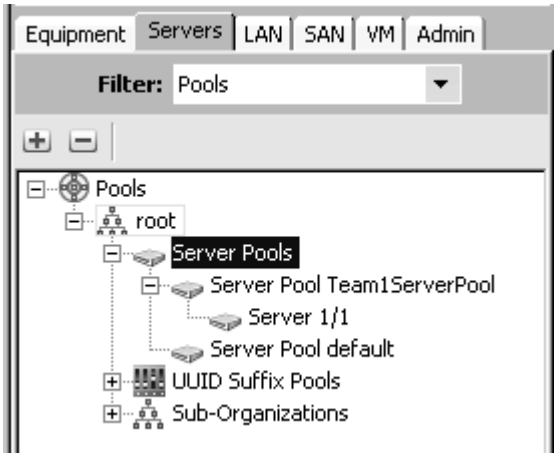
Step 5 Choose your team server and click the right arrow. Refer to your Lab Reference Guide for your assigned server.



Step 6 Make sure that your team server now appears in the right column and click **Finish**.



Step 7 Expand the **Server Pools** icon and verify that your pool has been created. Expand your pool and verify that it contains your team server.



Task 6: Create an Automatically Populated Server Pool

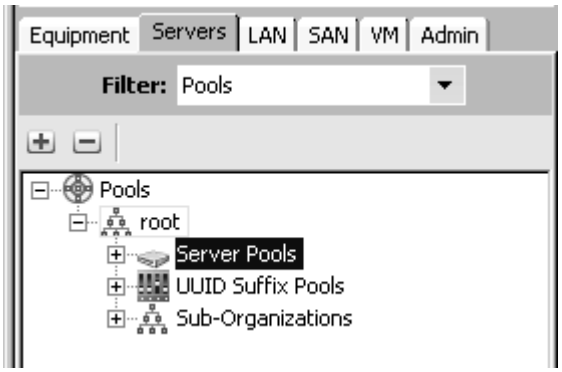
In this task, you will create an automatically populated server pool that contains your assigned server.

Activity Procedure

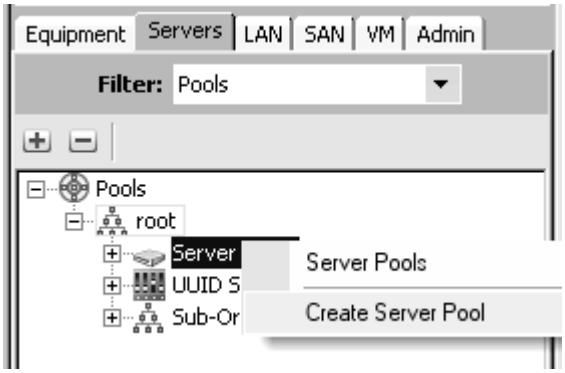
Complete these steps:

Step 1 Log into the Cisco UCS Manager.

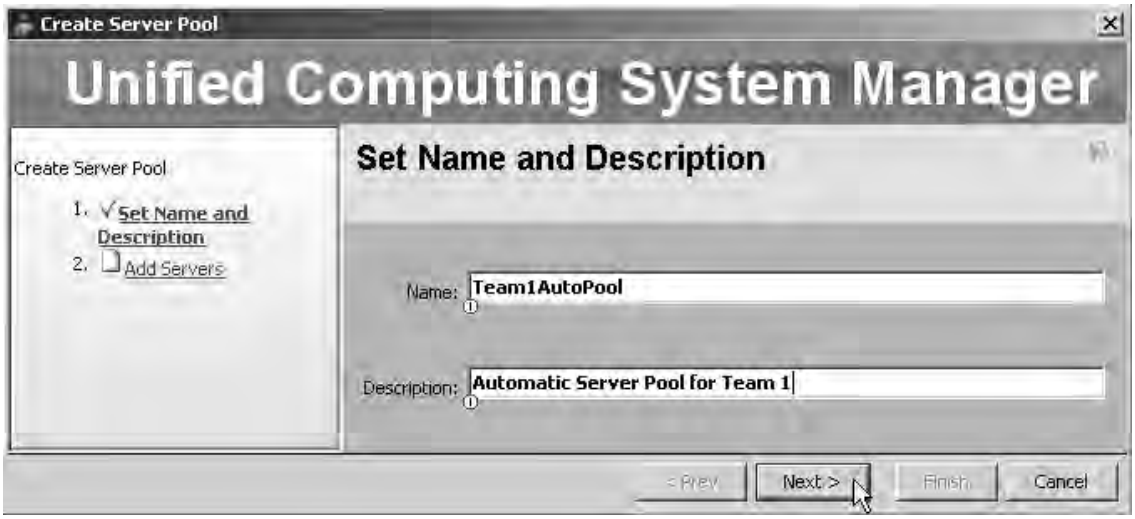
Step 2 Choose the **Servers** tab in navigation pane. It may be useful to adjust the **Filter** setting to **Pools** for the following tasks.



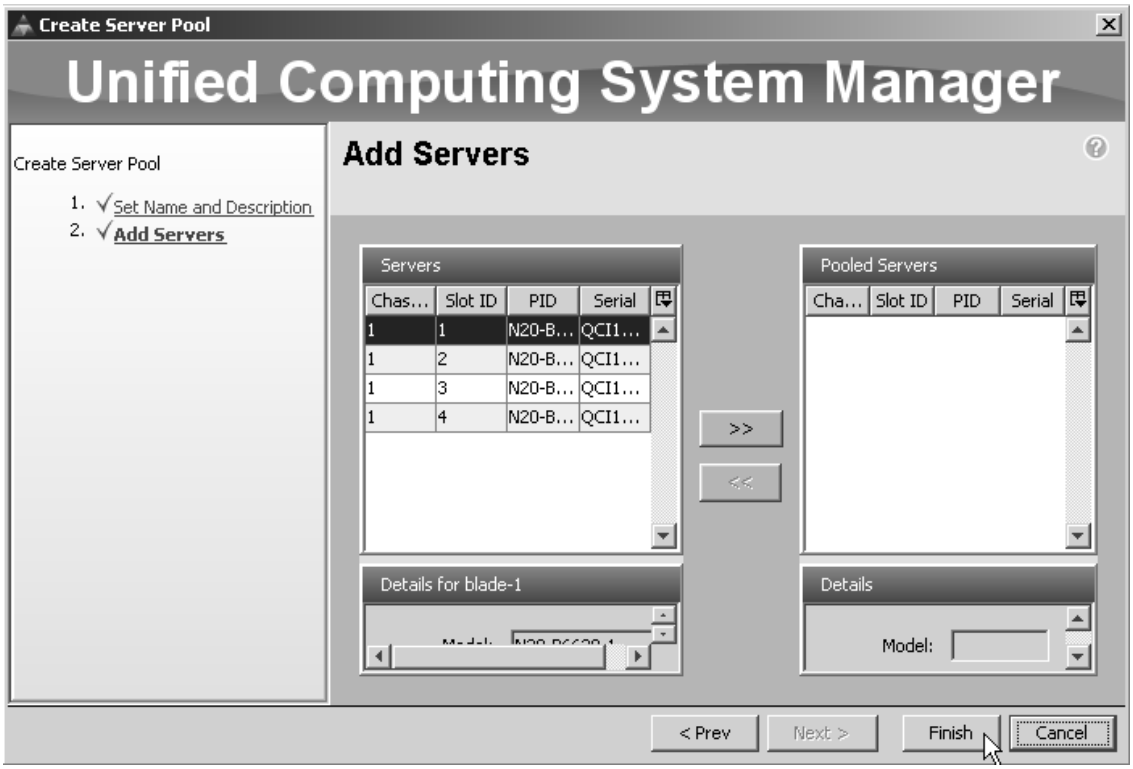
Step 3 Right-click Server Pools and choose Create Server Pool.



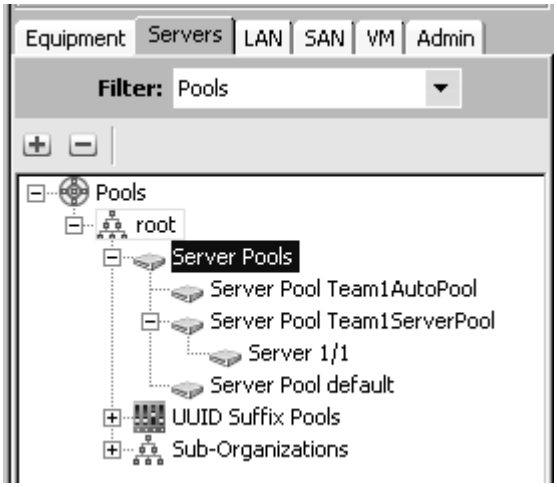
Step 4 Name your server pool **TeamXAutoPool**. Replace X with your team number. Optionally provide a description for your pool and click **Next**.



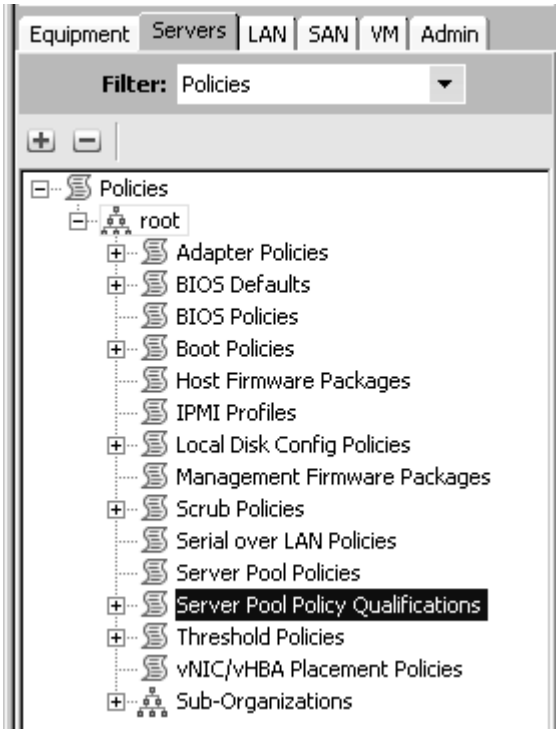
Step 5 Do not choose any servers and click **Finish**.



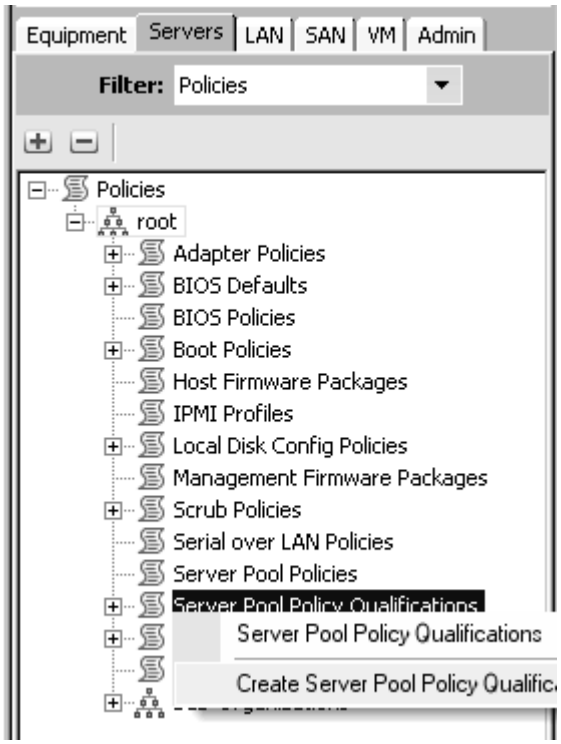
Step 6 Expand the **Server Pools** icon and verify that your pool has been created. Expand your pool and verify that it does not contain any servers.



Step 7 Change the **Filter** setting in the navigation pane to **Policies**.

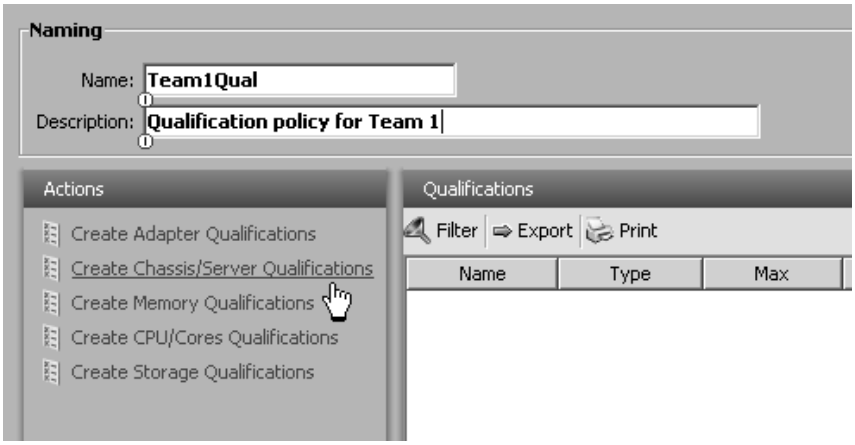


Step 8 Right-click Server Pool Policy Qualifications and click Create Server Pool Policy Qualification.

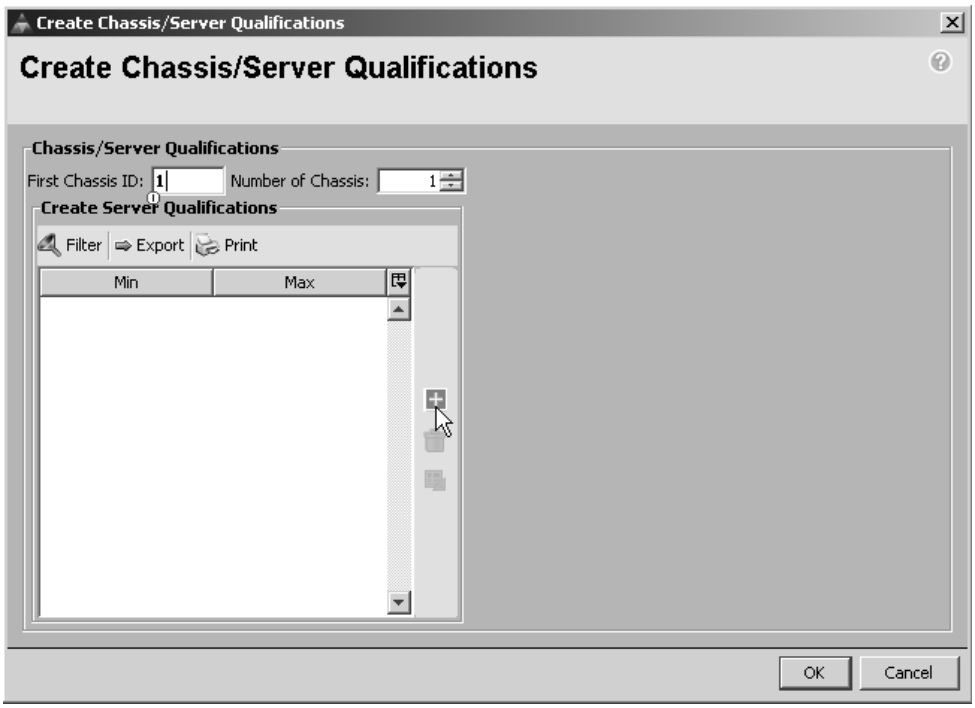


Step 9 Name your qualification **TeamXQual**. Replace X with your team number. Provide an optional description.

Step 10 Click Create Chassis/Server Qualifications.

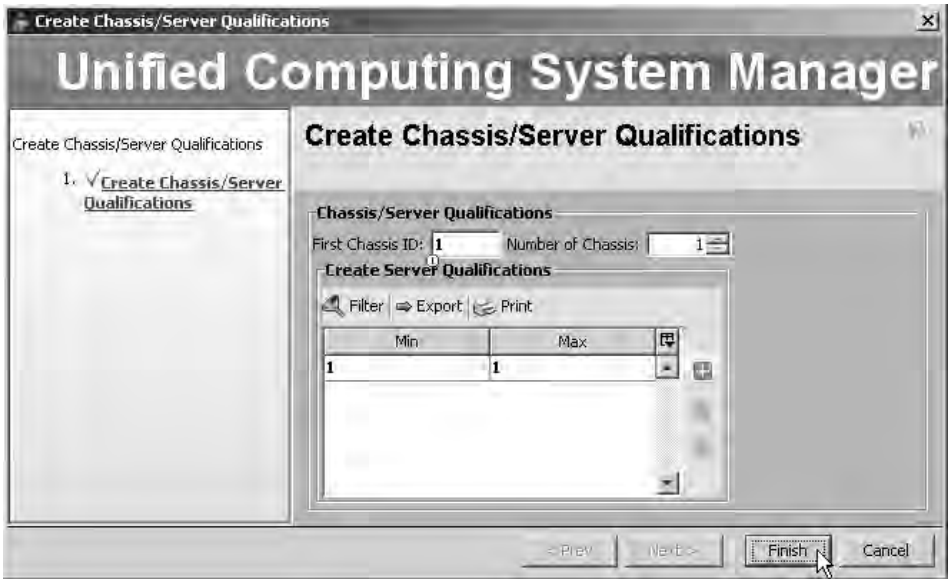


Step 11 If your assigned server is in a chassis other than 1, change **the First Chassis ID** to the chassis containing your assigned server. Click **Add** to add the server qualification.

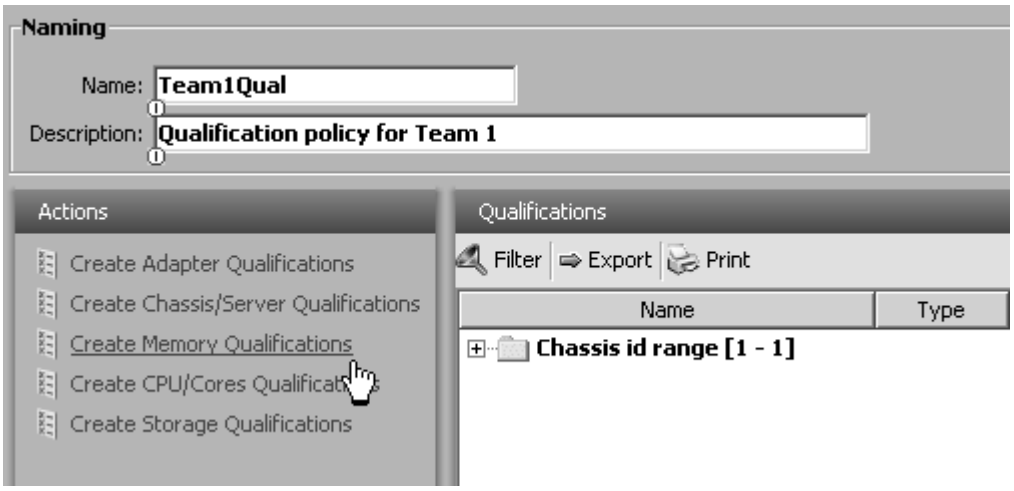


Step 12 Set the **First Slot ID** to your assigned server and click **Finish Stage**.

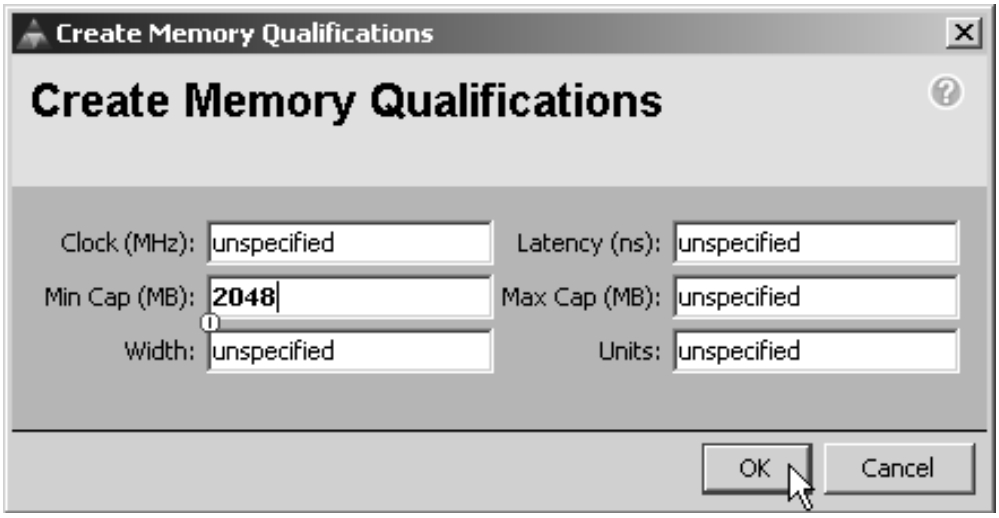
Step 13 Verify that your qualification has been added and click **Finish**.



Step 14 Click Create Memory Qualifications.

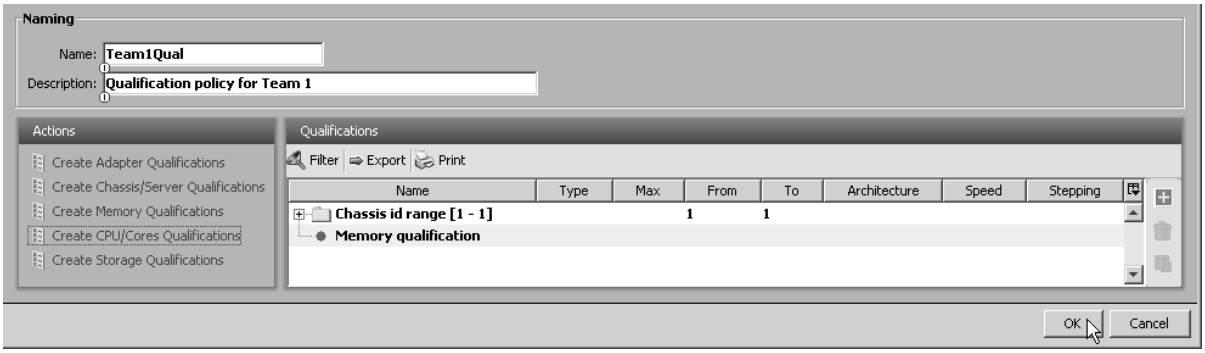


Step 15 Set **Min Cap** to **2048** and click **OK**.

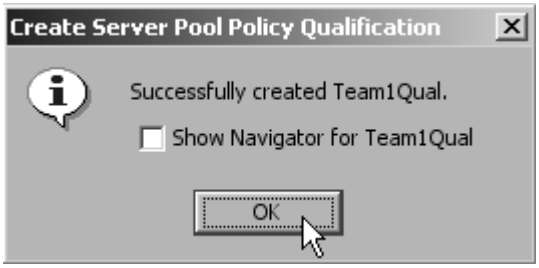


Step 16 Spend a few minutes exploring the other qualifications that could be added to your policy. If you would like to experiment with other qualifications, verify with your instructor which policies will match your assigned server.

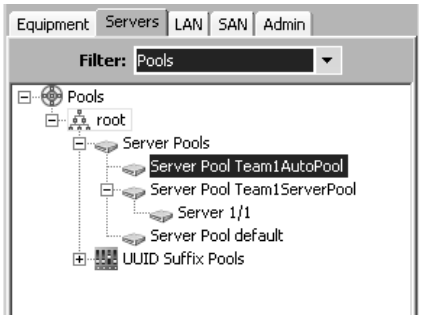
Step 17 When you are satisfied with your qualifications, click **OK**.



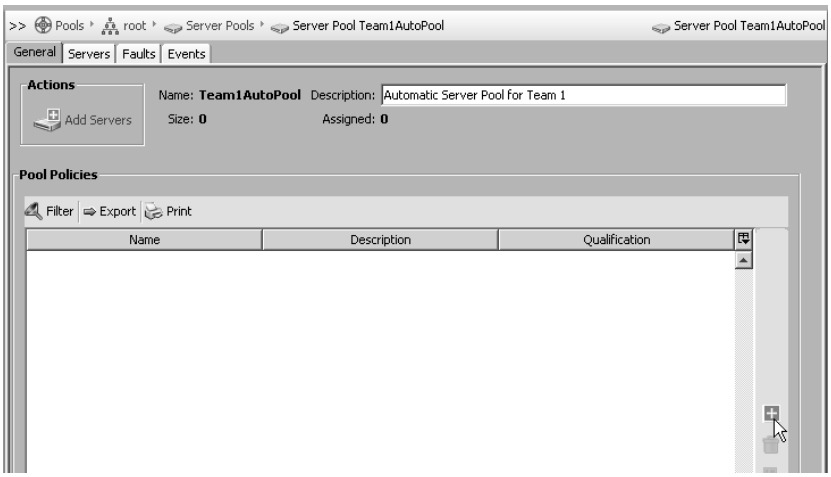
Step 18 Click **OK** to dismiss the confirmation message.



Step 19 Change the **Filters** field back to **Pools** and navigate to your **TeamXAutoPool**.

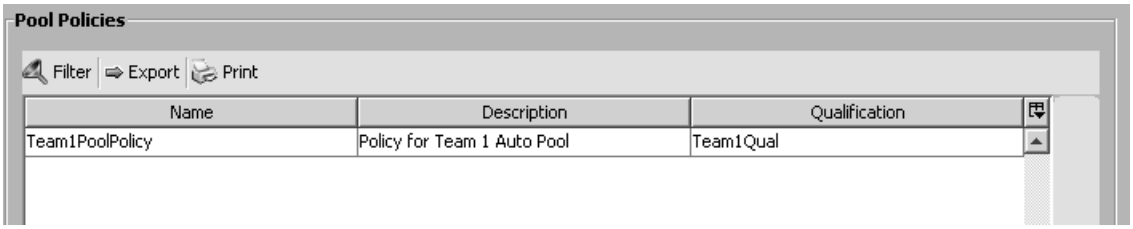


Step 20 In your server pool content pane, click **Add** to add a Pool Policy.

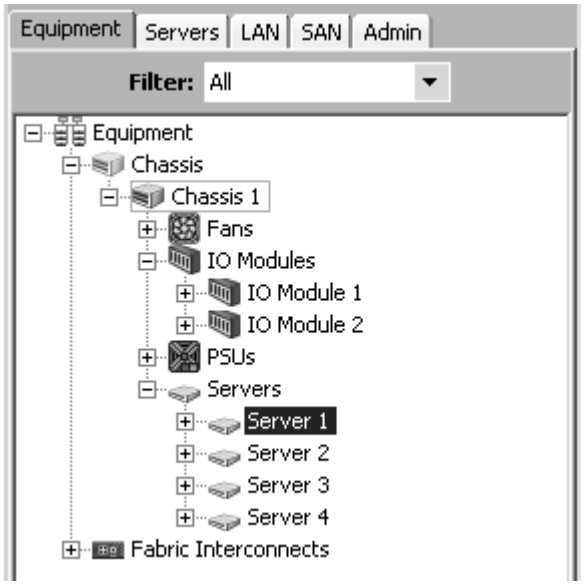


Step 21 Name your Server Pool Policy **TeamXPoolPolicy**. Replace X with your team number. Add an optional description, and choose the TeamXQual qualification that you created. Click **OK**.

Step 22 Verify that your policy has been created and associated with your team's qualification policy.



Step 23 Servers are only added to automatically populated pools at discovery time. As such, your assigned server will not yet appear in your pool. To rediscover your server, you can perform a re-acknowledge operation. Choose the **Equipment** tab in the navigation pane and navigate to your assigned server.

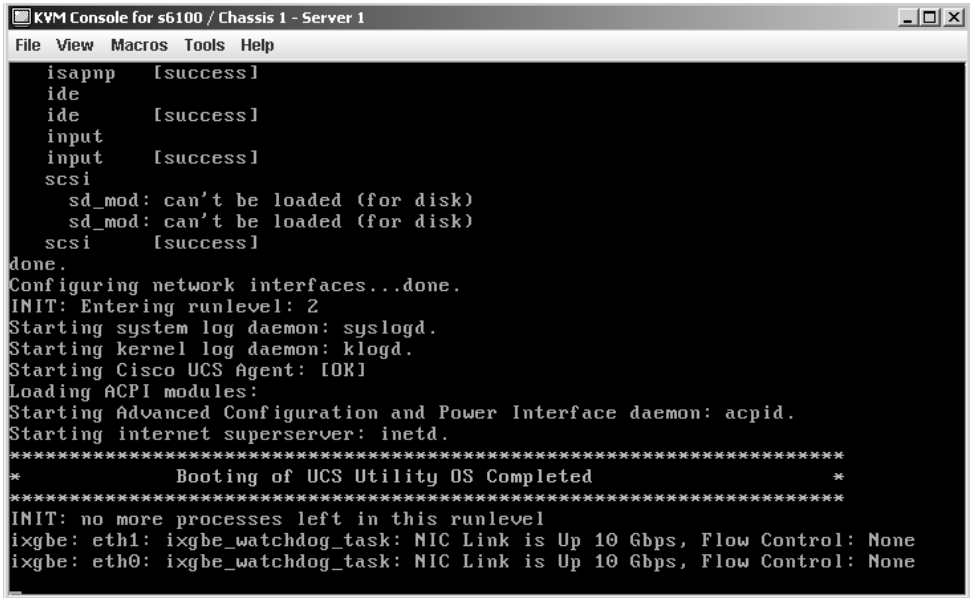


Step 24 In the **Actions** window of the content pane, click **Server Maintenance**.

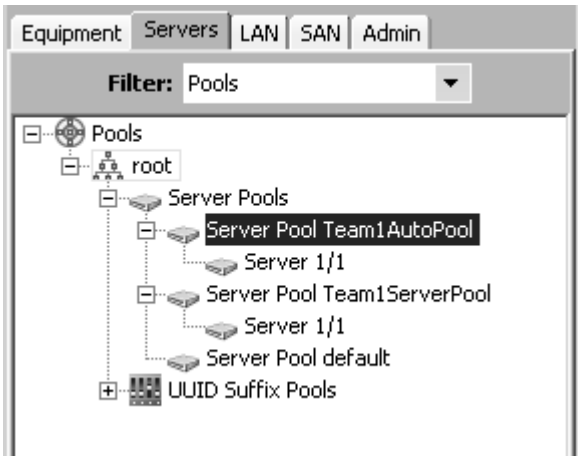
Step 25 Choose **Re-acknowledge** and click **OK**.

Step 26 Launch the KVM for your server.

Step 27 Observe the re-acknowledge process. When complete, the server will power down.



Step 28 After the server powers down, close the KVM console. Return to the **Servers** tab and navigate to your **TeamXAutoPool**. Verify that your assigned server has been added to your pool.



Lab 6-3: Creating Mobile Service Profiles

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

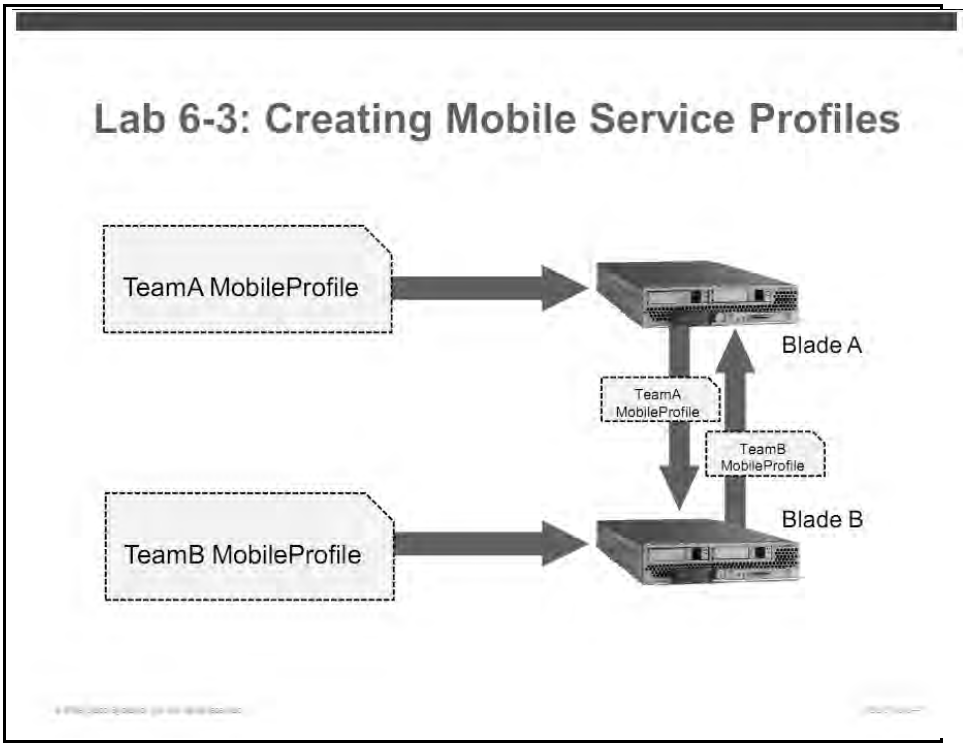
Activity Objective

In this activity, you will create SAN-booted service profiles that can be moved between blade servers. After completing this exercise, you should be able to:

- Configure Fibre Channel uplinks to provide SAN connectivity to the Fabric Interconnects
- Configure VLANs in Cisco UCS Manager
- Create a mobile service profile with virtualized identifiers
- Move service profiles between physical blades
- Observe how blade servers communicate with devices outside of the Cisco UCS platform

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:

- (2) Cisco UCS 6100 Fabric Interconnects
- WWNN, WWPN, and MAC pools that are created from the previous exercise.

Task 1: Establish SAN Connectivity

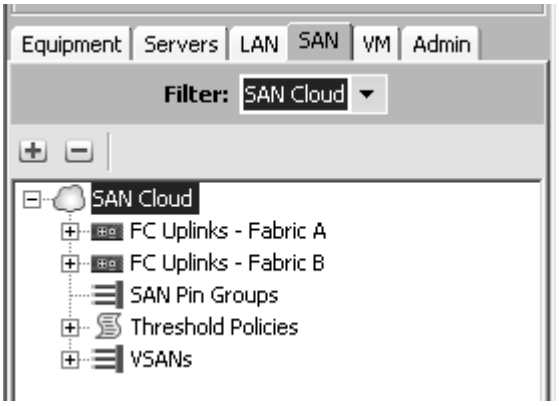
In this task, you will configure Fibre Channel uplinks to provide SAN connectivity to the Fabric Interconnects.

Activity Procedure

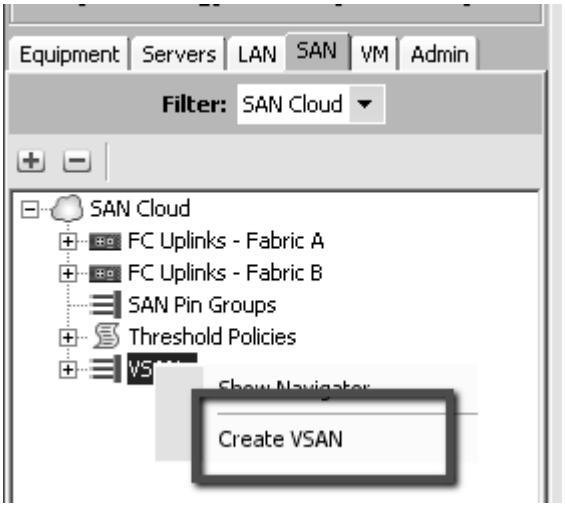
Complete these steps:

Step 1 Log into Cisco UCS Manager if necessary.

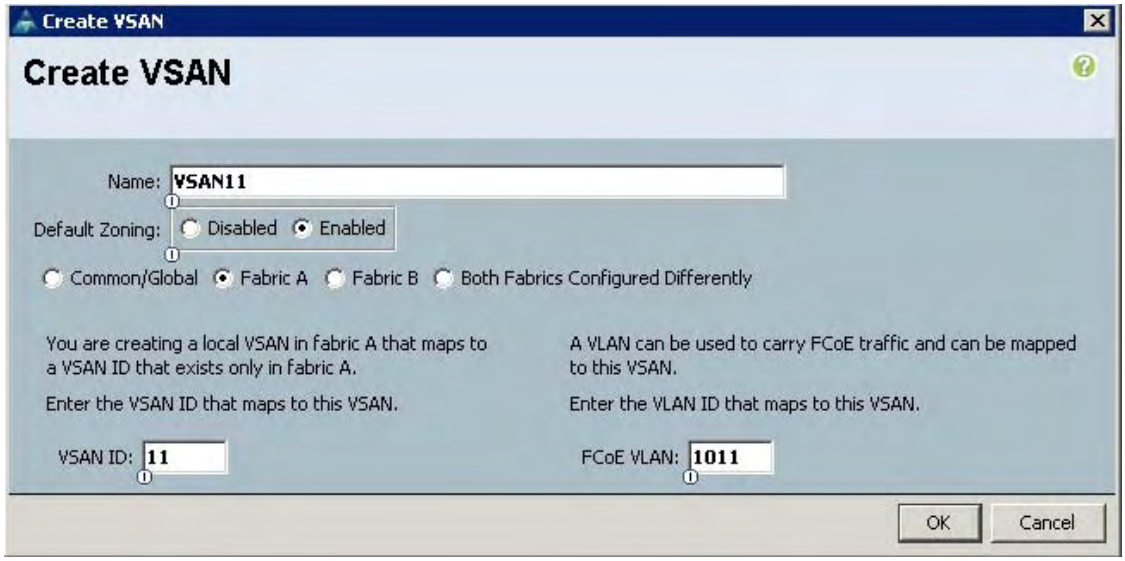
Step 2 In the navigation pane, choose the **SAN** tab. It may be helpful to set the **Filter** field to **SAN Cloud** for the following steps.



Step 3 Right-click the **VSANs** icon and choose **Create VSAN**.

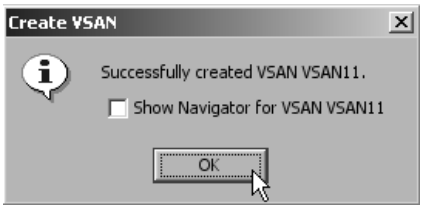


Step 4 Create a VSAN according to the values in your Lab Reference Guide; see "VSAN, Fabric, and FCoE VLAN Assignments."

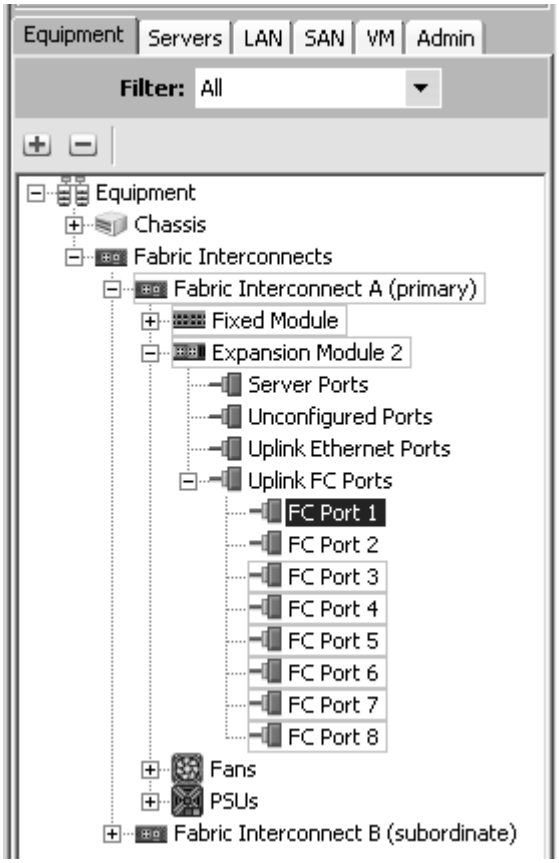


Note: In this lab topology, only two VSANs will be used and shared by all teams. Each team is given the opportunity to create a VSAN to practice this task, but be careful to use the designed VSAN in the later steps.

Step 5 Click **OK** to confirm creation of your VSAN.

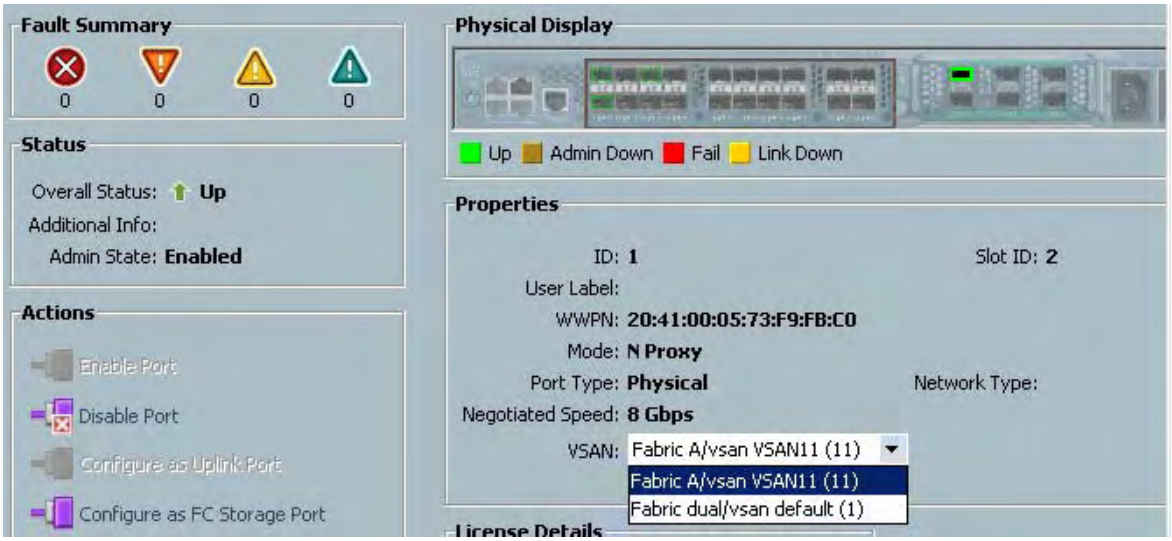


Step 6 In the navigation pane, choose the Equipment tab and ensure that the Filter value is set to All. Expand Fabric Interconnect A, Expansion Module, and Uplink FC Ports objects. Choose the FC Port 1 icon under Fabric Interconnect A.

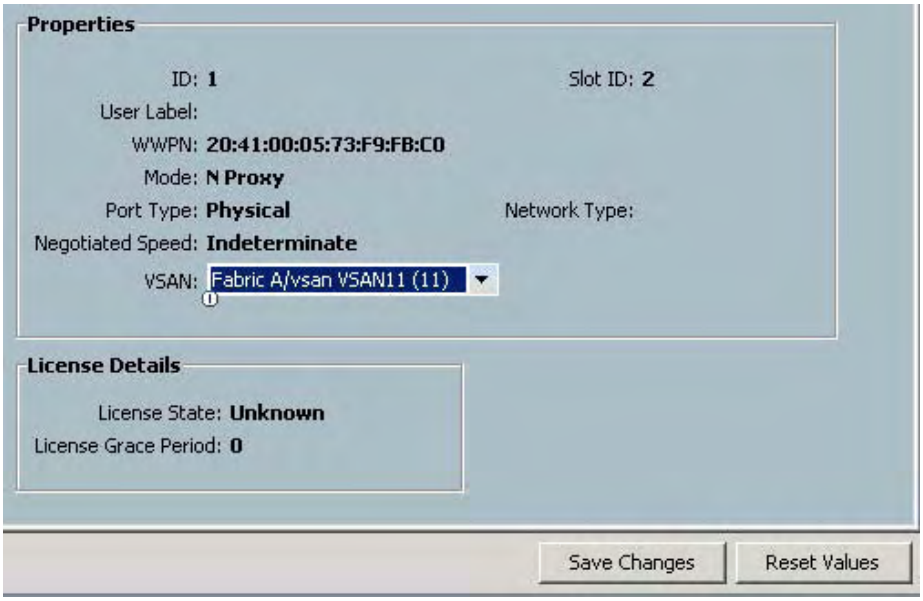


Step 7 In the content pane, change the VSAN field to **Fabric A/vsan VSAN11**.

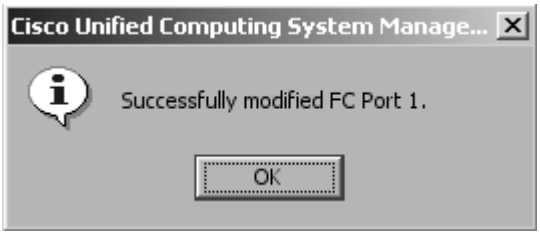
Note: All teams will use VSAN 11 in this step, regardless of team number.



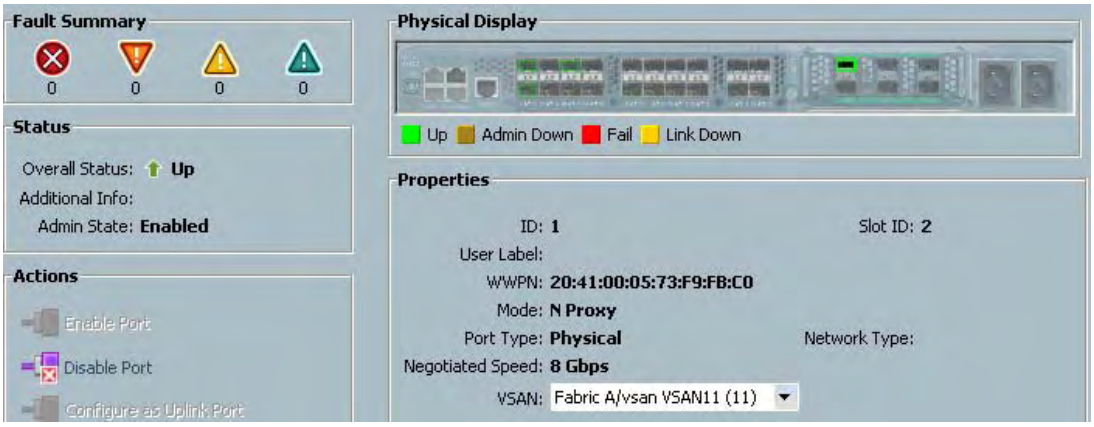
Step 8 Click **Save Changes** to apply the VSAN configuration to this port.



Step 9 Click **OK** to confirm the configuration change.



Step 10 Check to ensure that the Admin state of the port is enabled and that the Overall Status is now up.



Note: If your port does not move to an "Up" state, check to ensure that you have selected Fabric A/vsan VSAN11, which may not be the VSAN that you created in the earlier steps. Also check to ensure that you are modifying the port on Fabric Interconnect A. If you verify both of these items and the port still does not initialize, contact your instructor for assistance.

Step 11 Repeat the same process for port FC Port 1 on Fabric Interconnect B, and assigning the port to **Fabric B/vsan VSAN12**.

Task 2: Establish LAN Connectivity

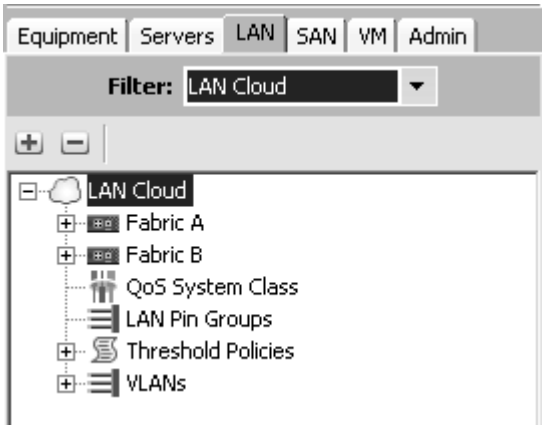
In this task, you will configure a VLAN for your blade server.

Activity Procedure

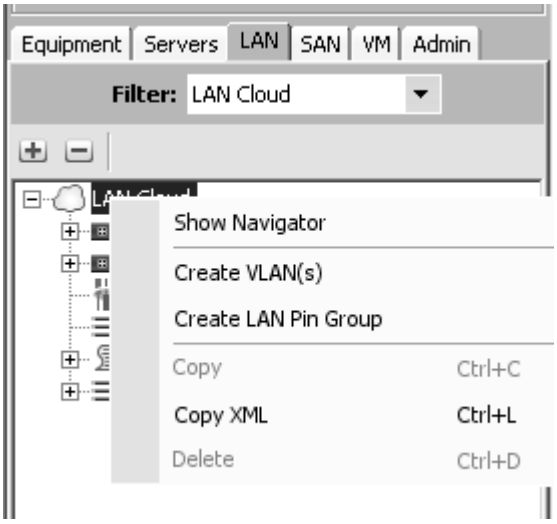
Complete these steps:

Step 1 Log into Cisco UCS Manager if necessary.

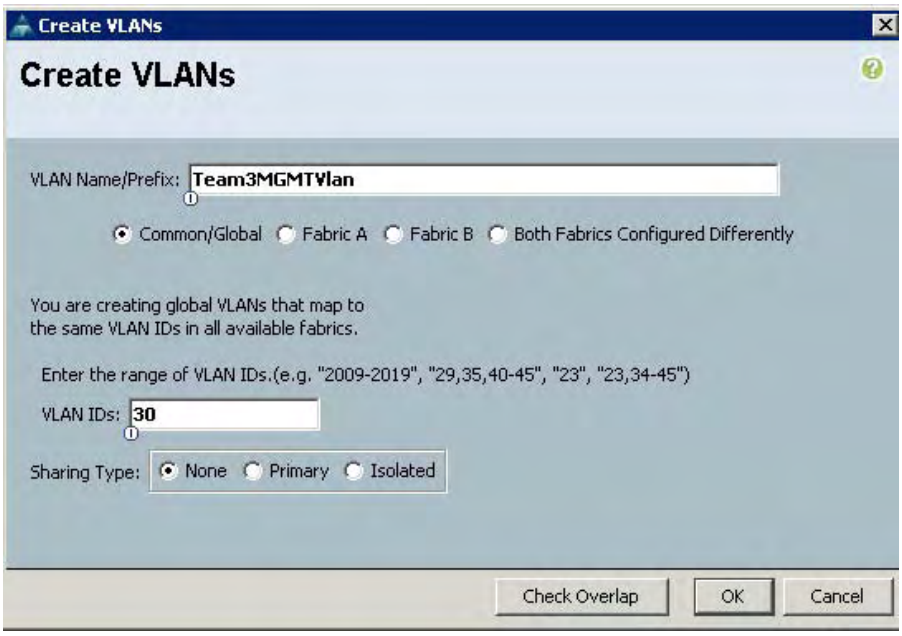
Step 2 In the navigation pane, choose the **LAN** tab. It may be helpful to set the **Filter** field to **LAN Cloud** for the following steps.



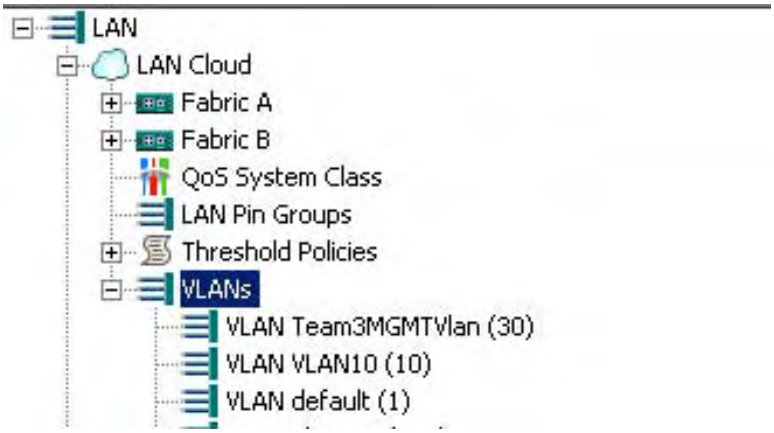
Step 3 Right-click the **LAN Cloud** icon and choose **Create VLAN**.



Step 4 Name your VLAN **TeamXMGMTVLAN**, replacing X with your team number. Set the VLAN ID to **X0**, replacing X with your team number. For example, Team 1 will use 10, Team 2 will use 20, and so on.



Step 5 Expand the VLANs icon and ensure that your team's VLAN now appears.



Task 3: Create a Mobile Service Profile

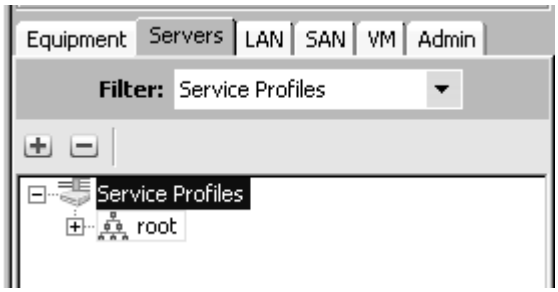
In this task, you will create a mobile service profile.

Activity Procedure

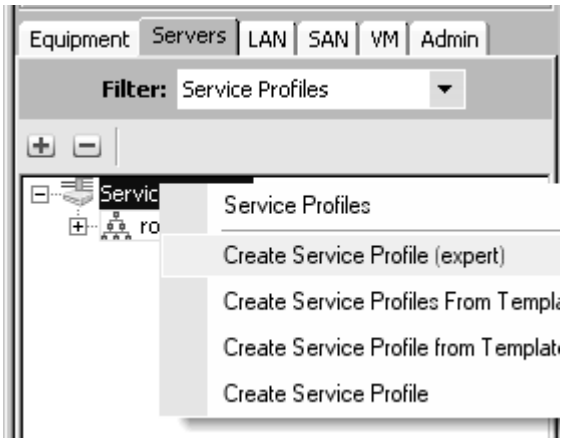
Complete these steps:

Step 1 Log into Cisco UCS Manager if necessary.

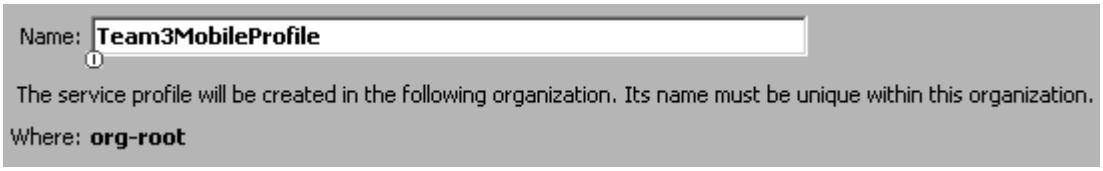
Step 2 In the navigation pane, choose the **Servers** tab. It may be helpful to set the **Filter** field to **Service Profiles** for the following steps.



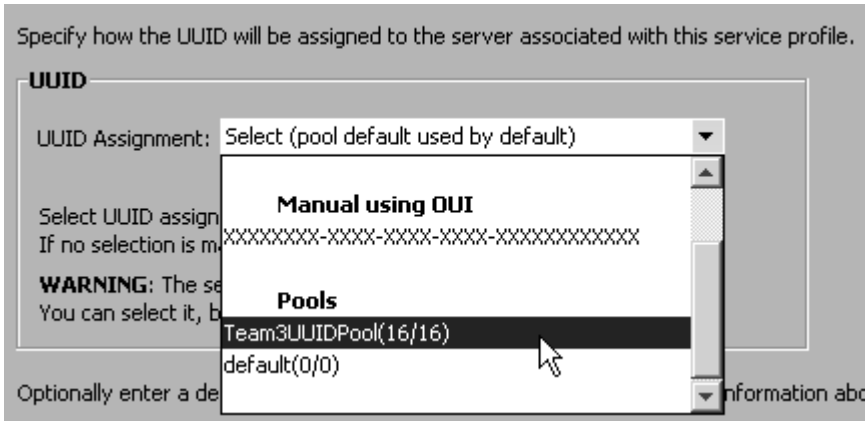
Step 3 Right-click the Service Profiles icon and choose Create Service Profile (expert).



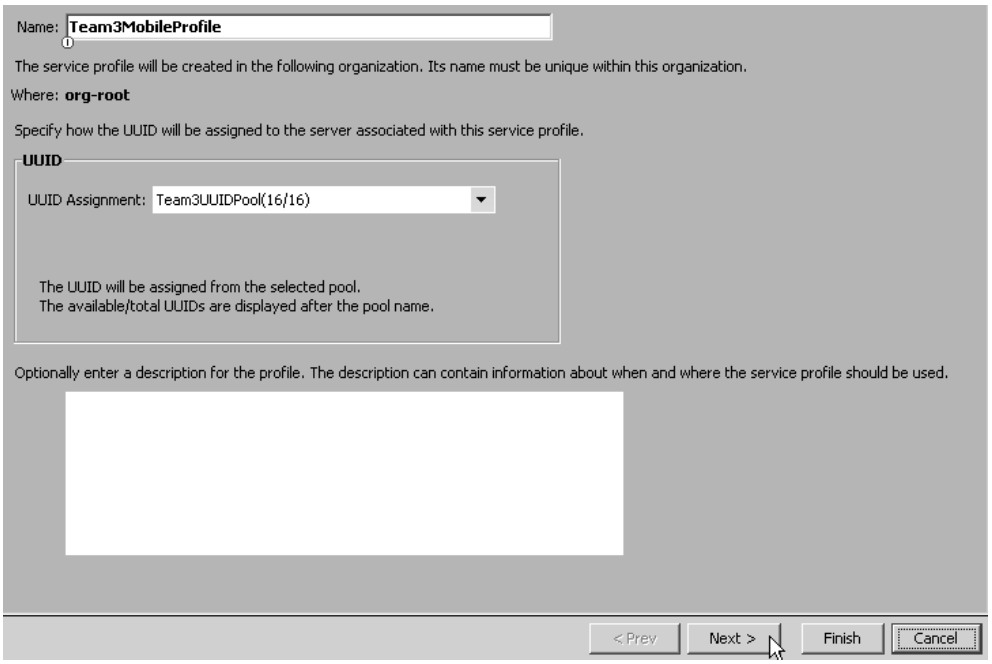
Step 4 Name your profile **TeamXMobileProfile**, replacing X with your team number.



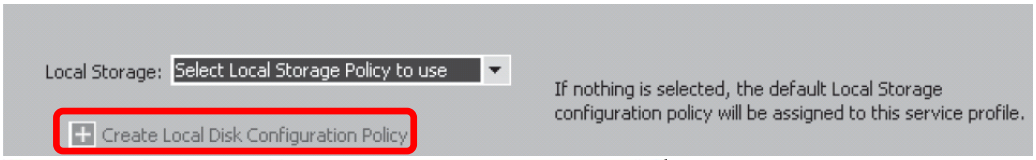
Step 5 In the UUID selection field, choose your team's UUID pool.

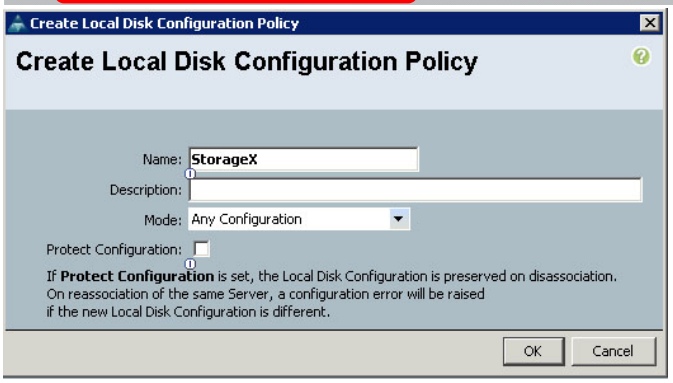


Step 6 Click **Next**.

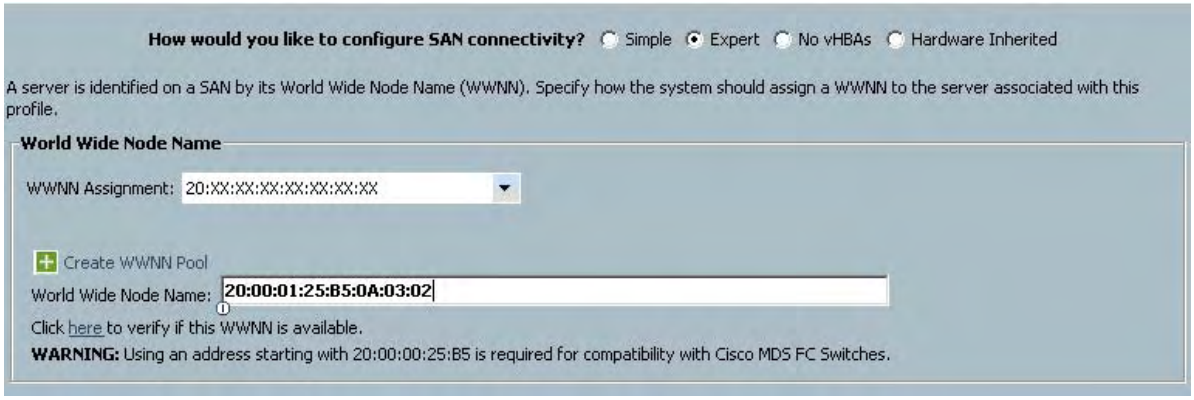


Step 7 Create a Local Storage Policy "**StorageX**" (X=team number) by clicking on **Create Local Disk Configuration Policy**. Choose Any Configuration for the Mode option & uncheck "**Protect Configuration**"





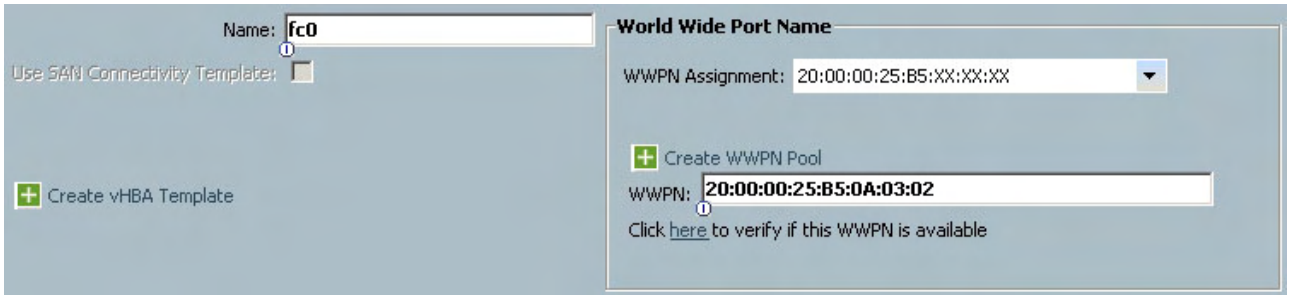
Step 8 Specify **Expert** SAN configuration, and set WWNN Assignment to **Manual Using OUI** -> 20:XX:XX:XX:XX:XX:XX. Manually specify the WWNN 20:00:01:25:B5:0Y:0X:02, replacing X with your team number and Y with "A" for odd and "B" for even team numbers.



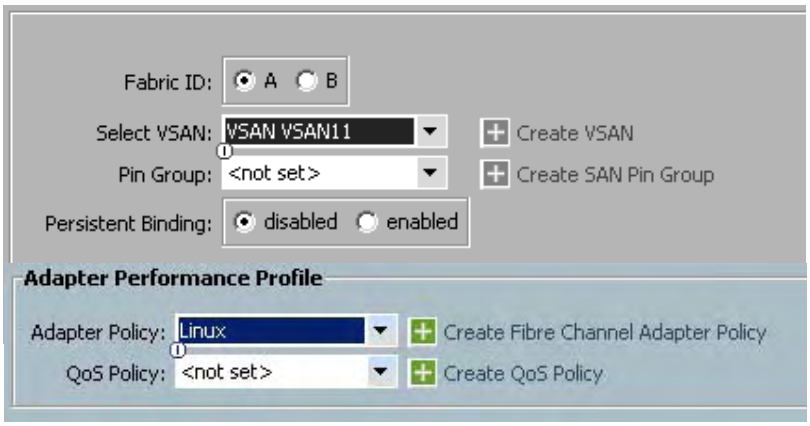
Note: Normally, you would choose from your team's pool. In this lab environment, however, we want to be certain that a specific value is selected. Note that it is permissible to specify manually a value that also exists in a pool. Doing so will mark it as assigned in the pool and will not be assigned automatically to other service profiles.

Step 9 Click **Add** to create a vHBA.

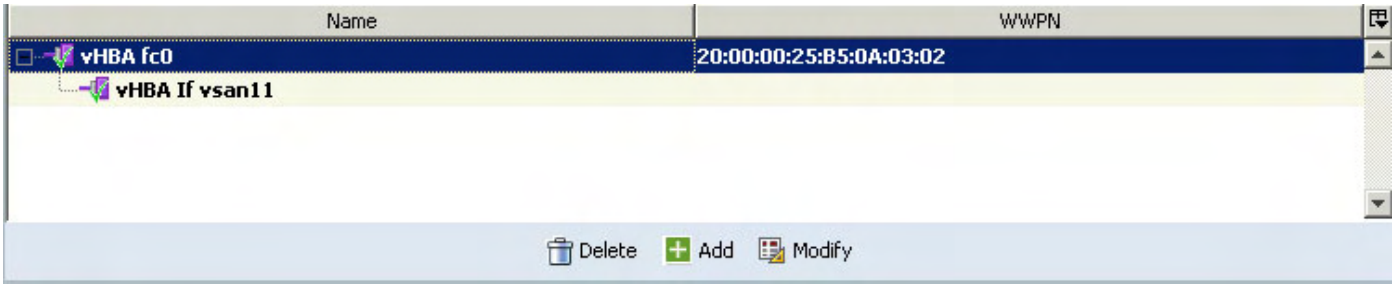
Step 10 Name the vHBA **fc0** and choose **Manual using OUI** ->and specify the WWPN 20:00:00:25:B5:0Y:0X:02, replacing X with your team number and Y with "A" for odd and "B" for even team number.



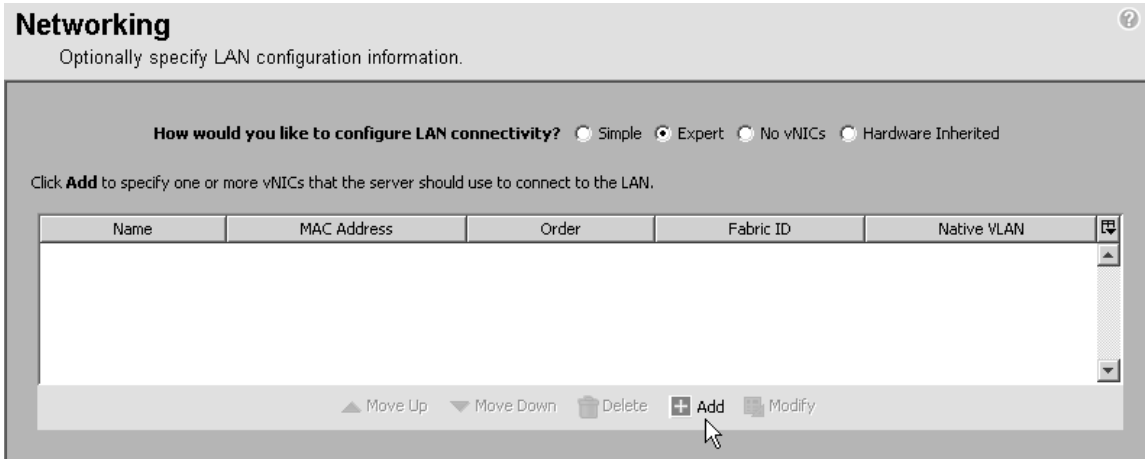
Step 11 Choose Fabric ID "A" & VSAN "11" for odd and "B" VSAN "12" for even team numbers.



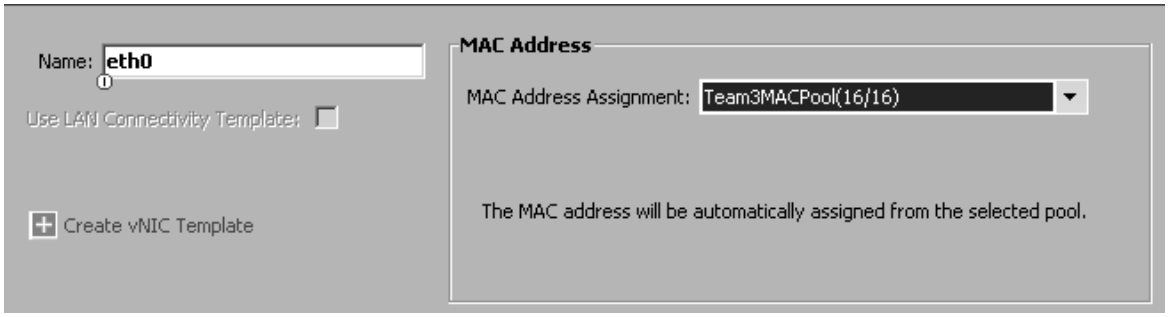
Step 12 Verify that your vHBA has been added to the profile with the proper WWPN. Click **Next**.



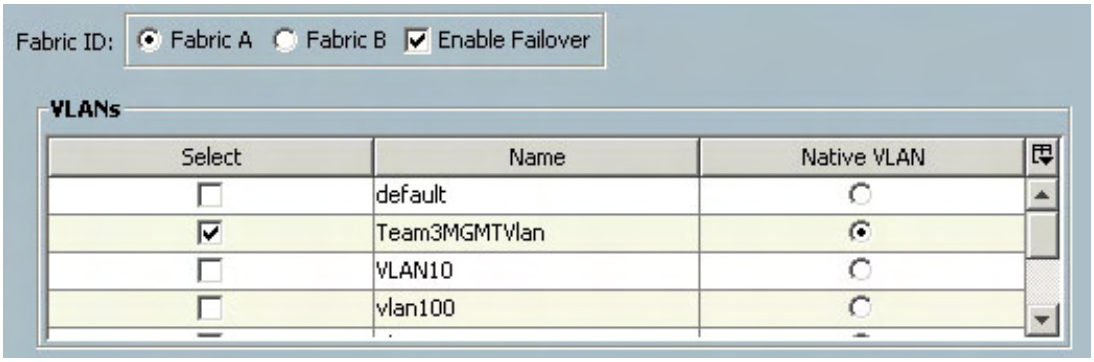
Step 13 Choose **Expert** LAN configuration and click **Add** to create a vNIC.



Step 14 Name the vNIC **eth0** and choose your team's MAC pool.

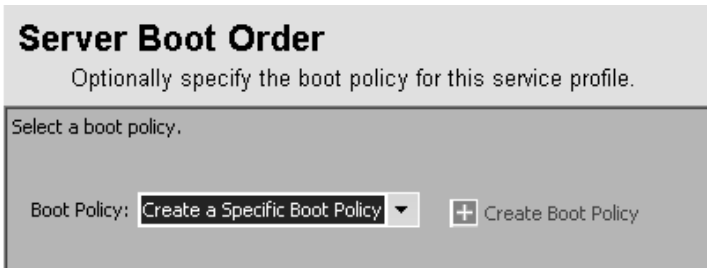


Step 15 Choose **Fabric A** and ensure that the **Enable Failover** box is checked. Choose your team's VLAN and ensure that the **Native VLAN** box is checked. Click **OK**.



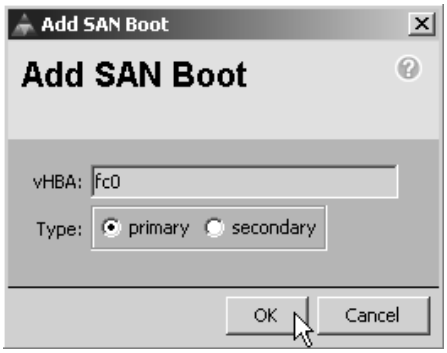
Step 16 Verify that your vNIC is now listed and click **Next**.

Step 17 Click Create a Specific Boot Policy and name it TXBootPol; where X is your team number.



Step 18 Expand the vHBAs section and double click **vHBA fc0**.

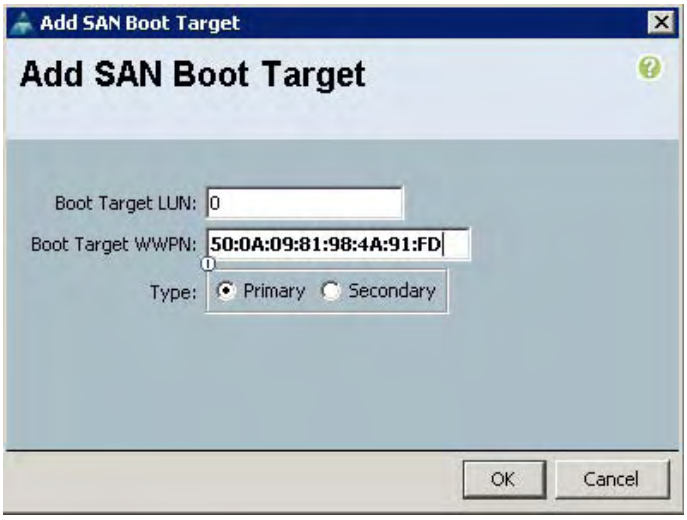
Step 19 Click **OK**.



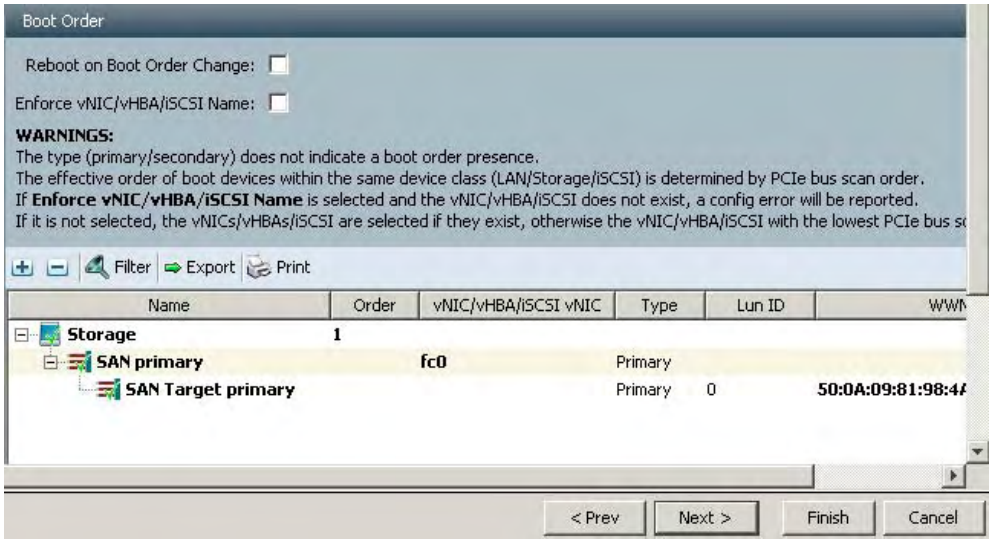
Step 1 Click Add SAN Boot Target.

Step 20 Set the Boot Target WWNN to the value that is specified below; see "Boot Target." Be careful to type this value correctly; otherwise, the profile will be unable to boot. Click **OK**.

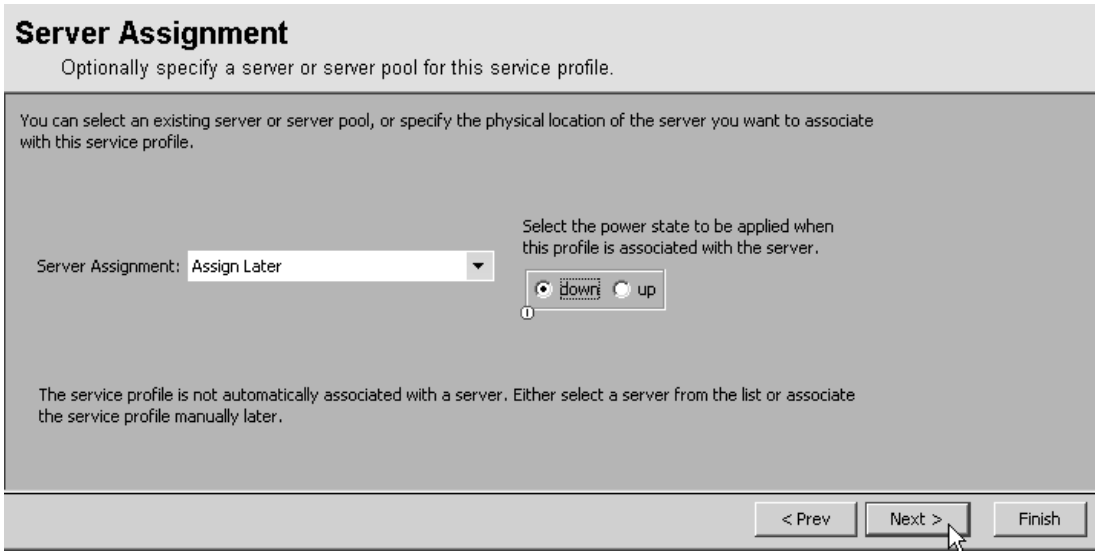
Team Number	VSAN ID	VSAN Name	UCS Fabric	FCoE VLAN	SAN Boot Target WWN
Odd -1,3,5,7	11	VSAN11	A	1011	50:0A:09:81:98:4A:91:FD
Even - 2,4,6,8	12	VSAN12	B	1012	50:0A:09:82:98:4A:91:FD



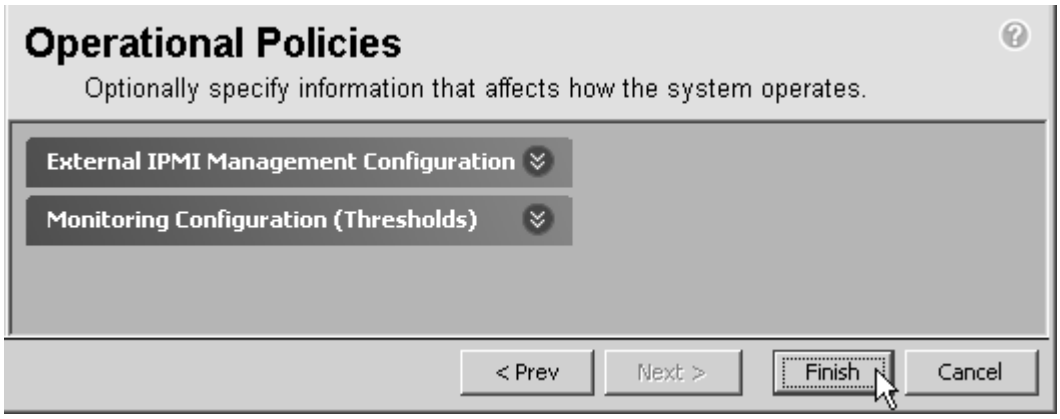
Step 21 Verify that the SAN Target has been added and click **Next**.



Step 22 Leave Server Assignment set to **Assign Later** and change the power state setting to **Down**. Click **Next**.

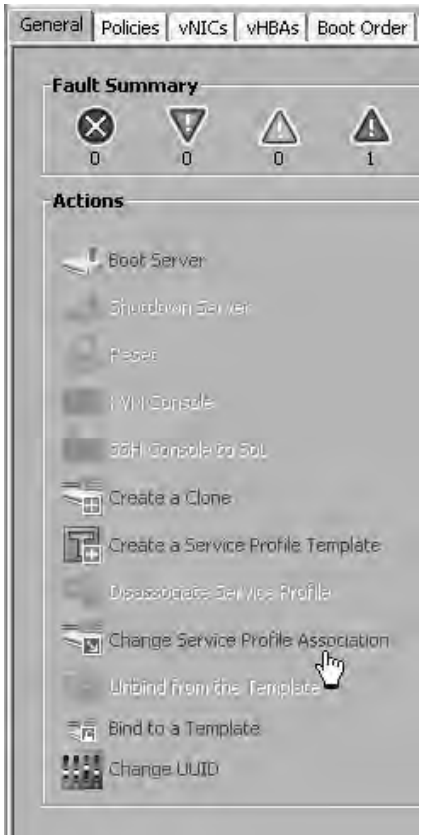


Step 23 Spend a few moments reviewing the optional Operational Policies (do not select any or change defaults) and click **Finish**.

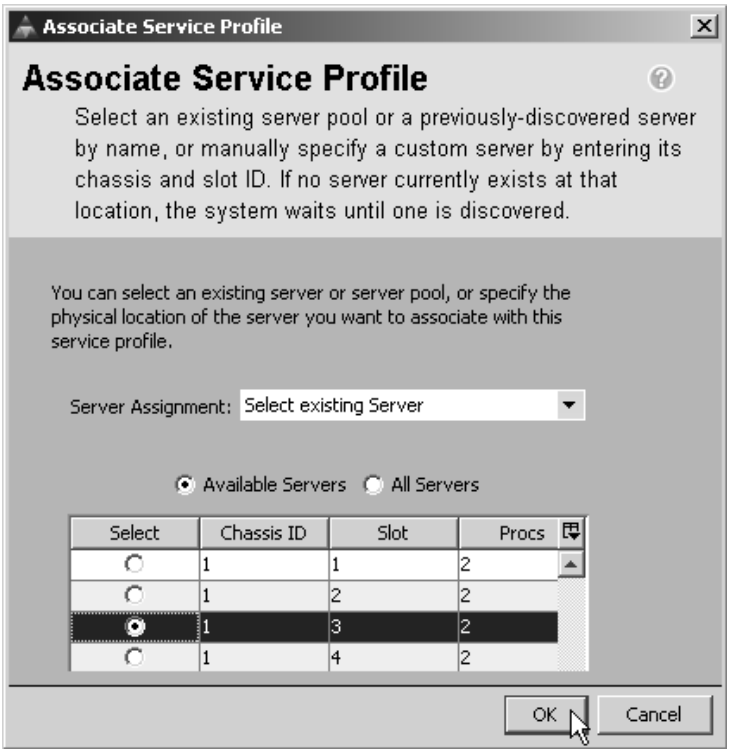


Step 24 Click **OK** to confirm creation of the Service Profile.

Step 25 In the content pane, choose the **General** tab, and choose **Change Service Profile Association**.



Step 26 Choose your team server and click **OK**.



Step 27 Click **KVM Console** and observe the configuration process.

- After the Cisco UCS Utility operating system has configured the blade, the blade will power down.

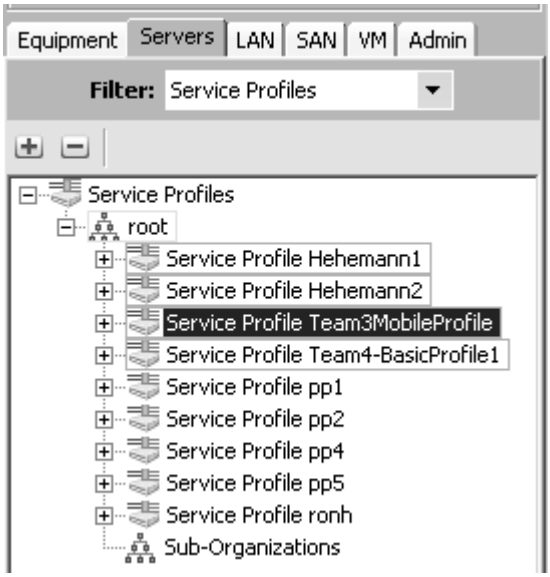
Task 4: Boot and Migrate a Mobile Service Profile

In this task, you will boot the mobile service profile and then move it to another physical blade.

Activity Procedure

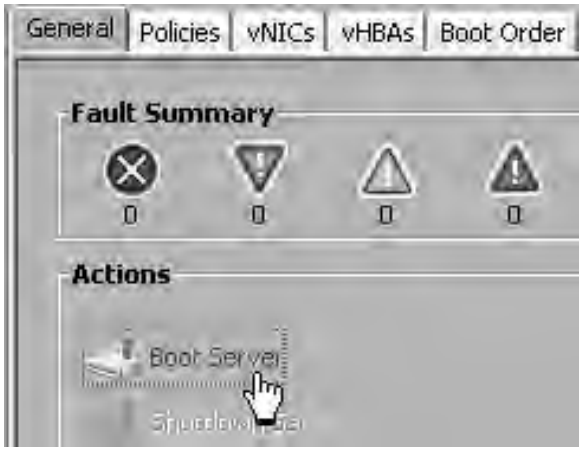
Complete these steps:

Step 1 In the navigation pane, choose the **Servers** tab. It may be helpful to set the **Filter** field to **Service Profiles** for the following steps. Choose your team's service profile.

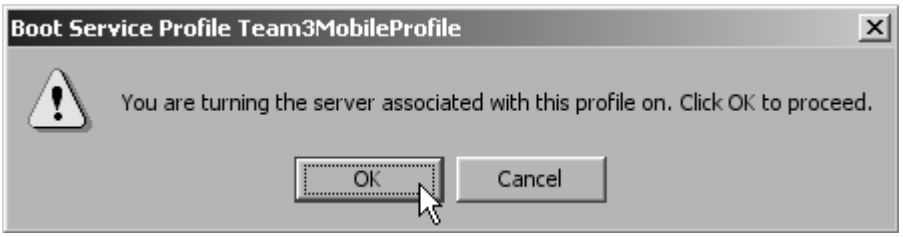


Step 2 In the content pane, choose the **General** tab. Launch a KVM session for your blade if not already started from the previous task.

Step 3 Click **Boot Server**.



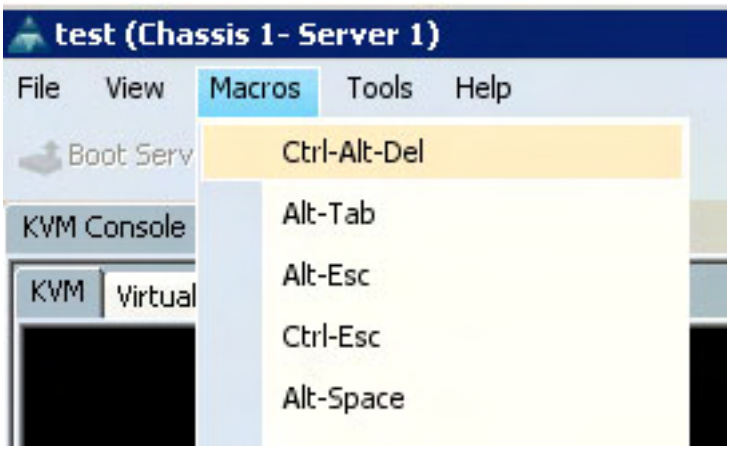
Step 4 Click **OK**.



Step 5 Click **OK**.

Step 6 Return to the KVM window and watch your server boot.

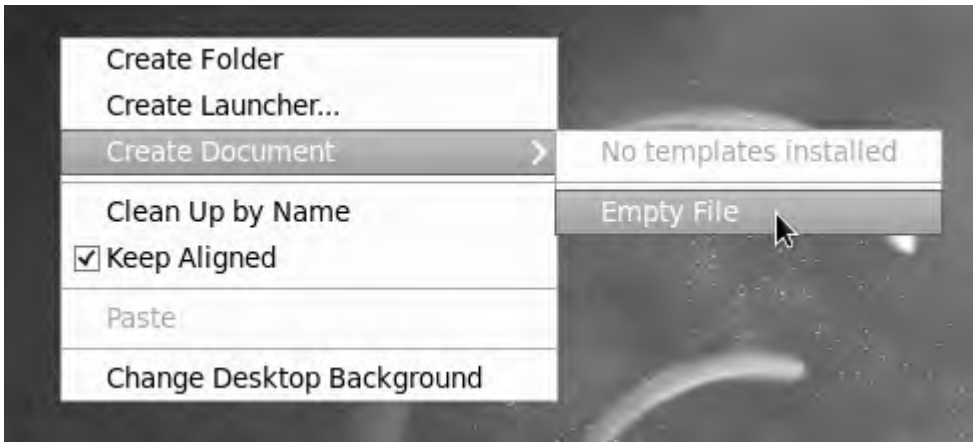
Step 7 To send a Ctrl+Alt+Delete signal to Linux to log in, click **Macros**, then **Ctrl-Alt-Delete**.



Step 8 Log into Linux using username **admin**, password **cisco123**.

Step 9 Spend a few minutes exploring the system. See if you can determine which physical blade your service profile is running on from evidence in the operating system.

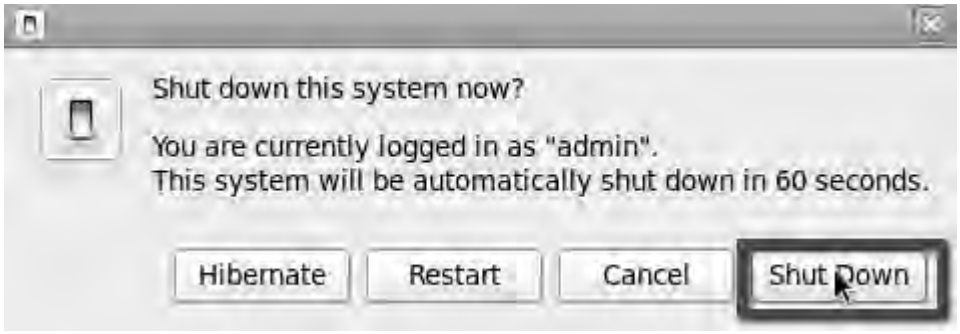
Step 10 Right-click in any open space on the desktop and click **Create Document >Empty File**.



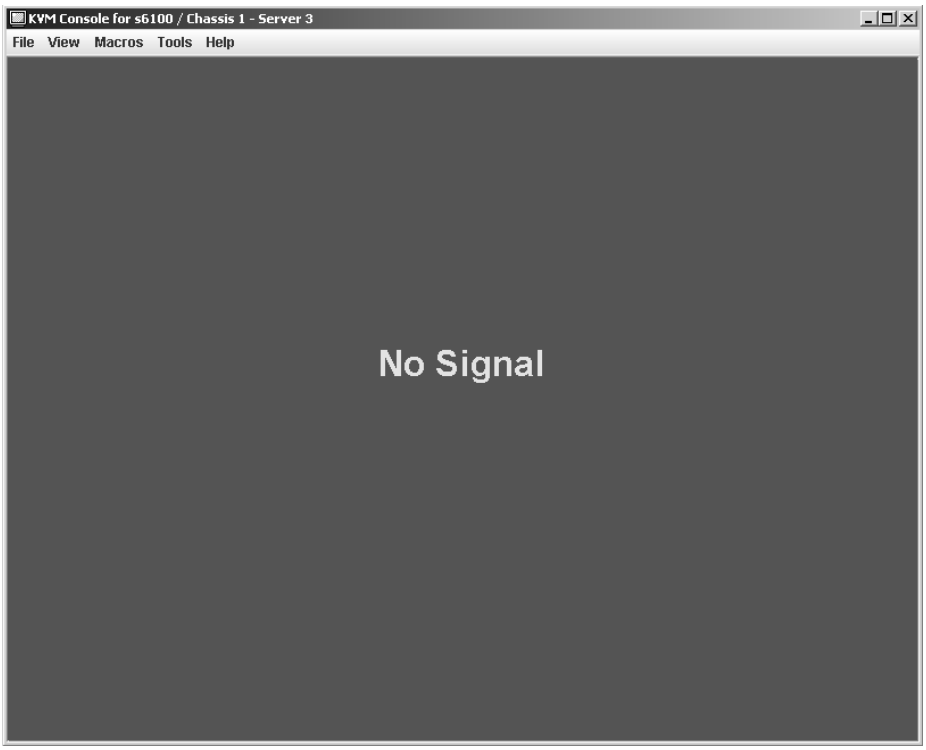
Step 11 Name the file anything that you would like, distinguishing this host as your team's service profile. For example, use your team number and first names.

Step 12 Click **System**, then **Shut Down**.

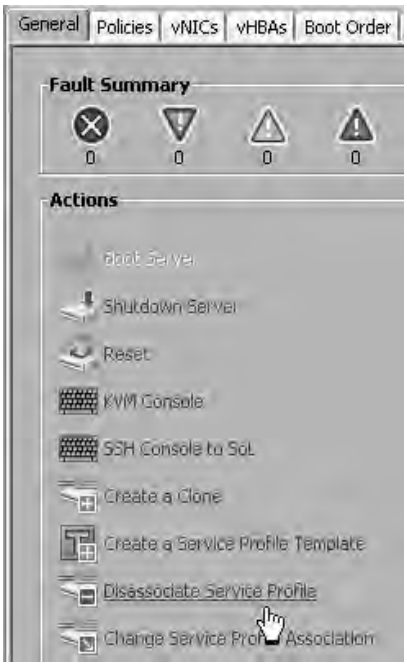
Step 13 Then select Shut Down on the Dialog box.



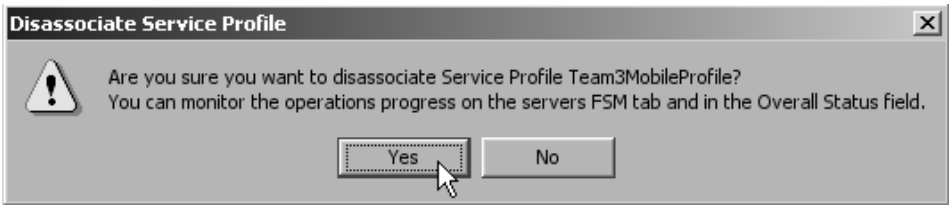
Step 14 Wait until the KVM console shows that the system is shut down before continuing to the next task.



Step 15 Return to the Cisco UCS Manager Window and click **Disassociate Service Profile**.



Step 16 Click **Yes**.



Step 17 Watch the KVM window to see the Cisco UCS Utility operating system boot and remove the personalization from the blade.

Step 18 Find another team that has reached this same step. If you need assistance finding a team, ask your instructor. Ensure that both teams have completed the disassociation of the service profile from their blade.

Step 19 Associate your service profile with the other team's blade server.

Step 20 Launch a KVM window and monitor the association process.

Step 21 After the association is complete, boot your service profile, which is now associated with the other team's server.

Step 22 When Linux boots, log in by using the same process as in the previous steps.

Step 23 Verify that your team's text file appears on the desktop.

Task 5: Examine Blade Appearance from External Devices

In this task, you will explore the manner in which the blade server communicates with devices outside of Cisco UCS.

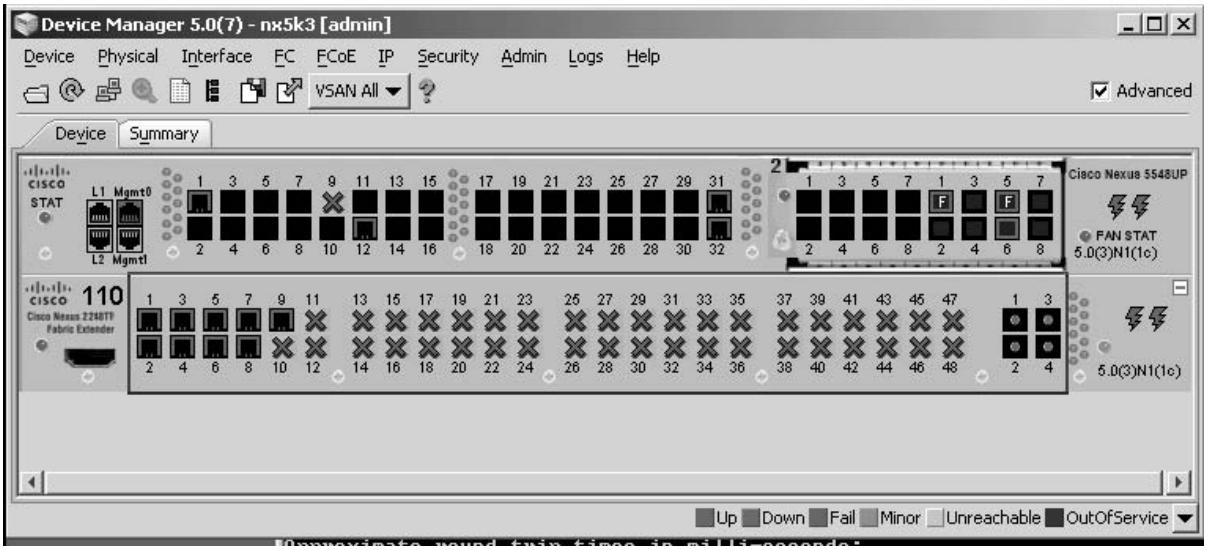
Activity Procedure

Complete these steps:

Step 1 Minimize the Cisco UCS Manager windows, if any. Find the Cisco Device Manager icon on your student desktop and double-click it.

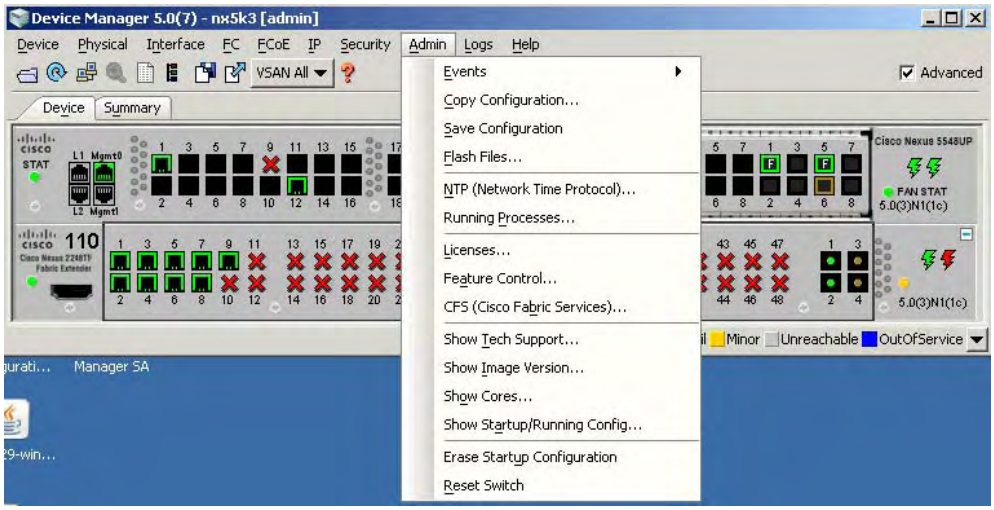
Step 2 Enter Device Name of 10.2.0.2. You may need to click the options button to ensure that SNMPv3 is checked. Enter user name of 'admin' followed by password ‘cisco123’. Click **Open**.

Step 3 Ignore any warning that appear. Click the **Summary** tab. Note connected interfaces. Specifically, note that the switch is reporting which Fabric Interconnect is visible. When you are finished on this tab, return to the **Device** tab.

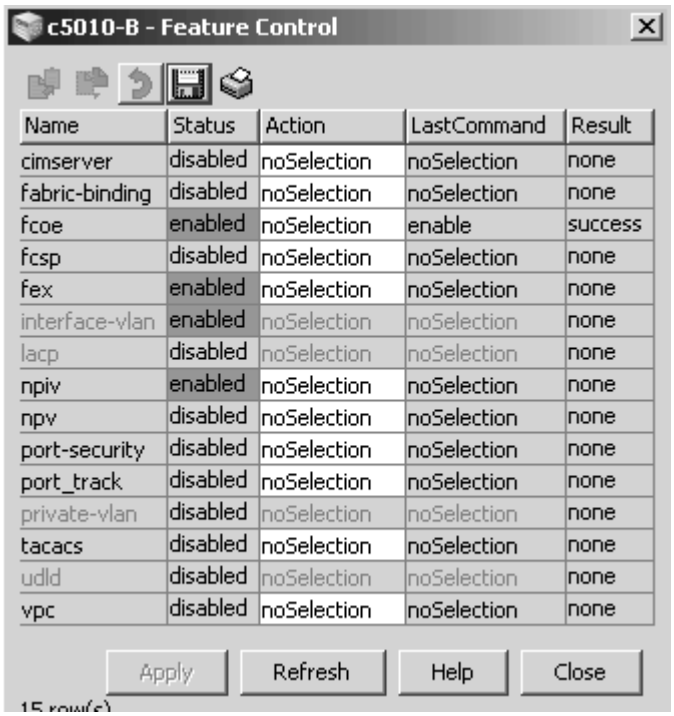


Step 4 The text in the “Connected To” field for the Fabric Interconnects is being returned by the Fabric Interconnect during the login process. This is useful information for mapping connections or troubleshooting connection problems.

Step 5 Click **Admin** and **Feature Control**.

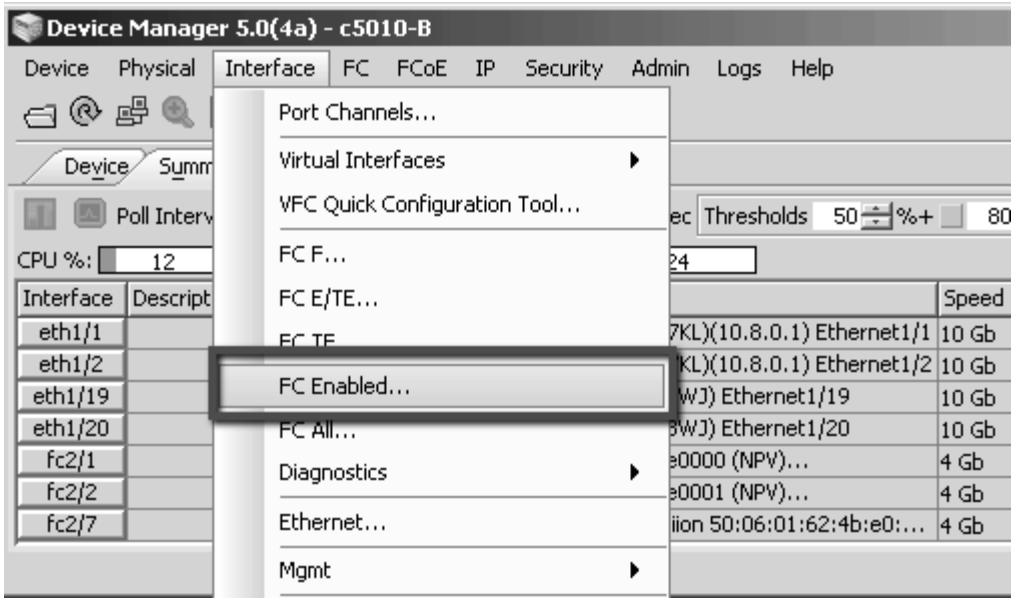


Step 6 Find the line **npiv**. NPIV is the feature on the switch that supports multiple Fibre Channel devices logging in through the same physical port. Note that the feature is enabled.

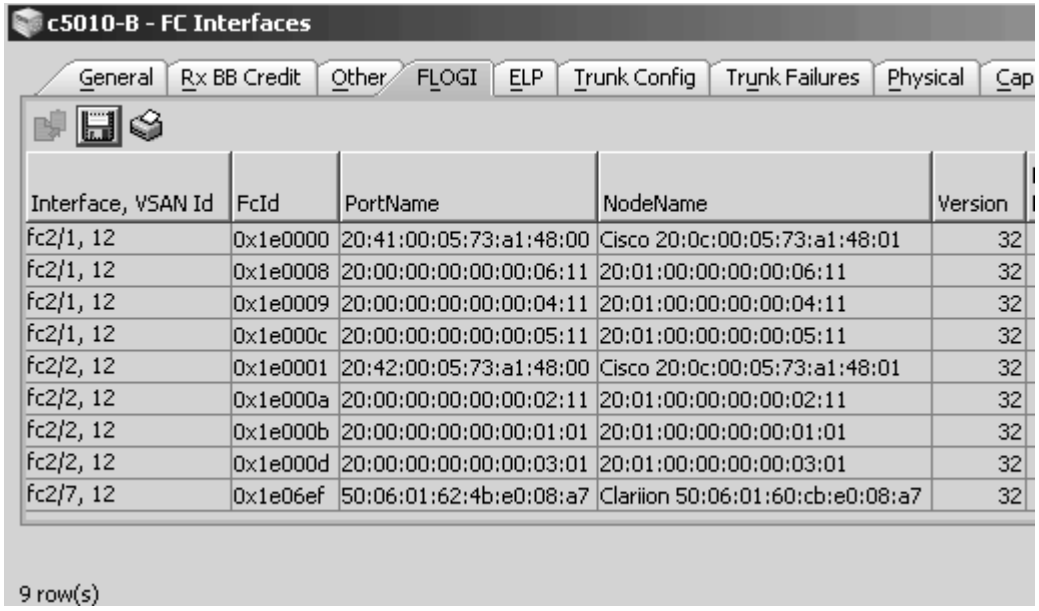


Step 7 Close the **Feature Control** window.

Step 8 Click **Interface** and **FC Enabled**.

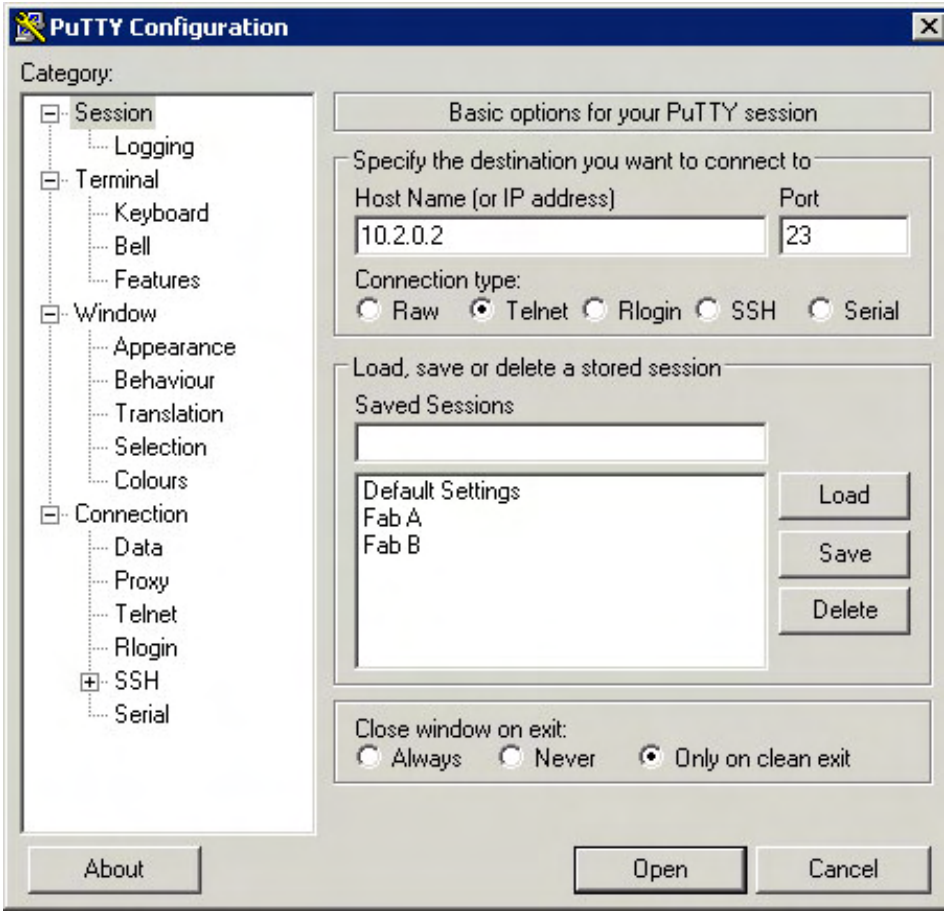


Step 9 Choose the **FLOGI** tab. Find your server's virtualized WWPN and WWNN and note the physical interface that it is logged into. There may be several other teams that are WWNNs logged into the same physical interface. Click **Close**.

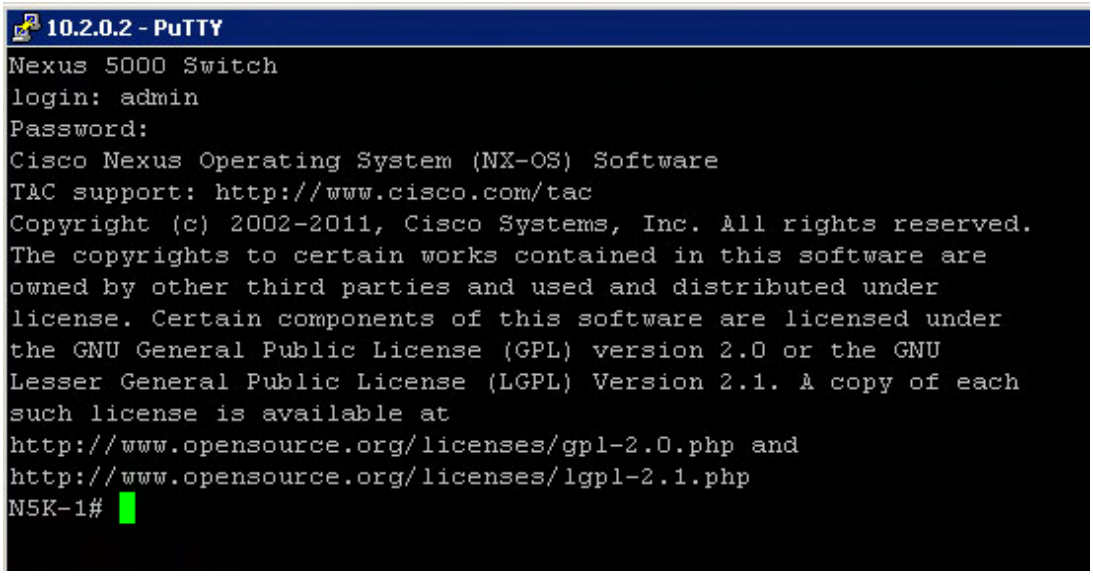


Step 10 Find and double-click the **putty.exe** icon on your student desktop.

Step 11 Use Putty to Telnet 10.2.0.2. Enter the IP address, Select Telnet and click **Open**.



Step 12 Log into the switch by using the username and password: admin / cisco123.



Step 13 Ping the IP address of your Linux server 10.2.X0.20

```
N5K-1# ping 10.2.30.20
PING 10.2.30.20 (10.2.30.20): 56 data bytes
64 bytes from 10.2.30.20: icmp_seq=0 ttl=63 time=0.902 ms
64 bytes from 10.2.30.20: icmp_seq=1 ttl=63 time=7.347 ms
64 bytes from 10.2.30.20: icmp_seq=2 ttl=63 time=9.972 ms
64 bytes from 10.2.30.20: icmp_seq=3 ttl=63 time=10.048 ms
64 bytes from 10.2.30.20: icmp_seq=4 ttl=63 time=9.901 ms

--- 10.2.30.20 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.902/7.634/10.048 ms
N5K-1#
```

Step 14 Enter **sh mac address-table dynamic**.

```
N5K-1# sh mac address-table dynamic
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link
   VLAN     MAC Address      Type      age     Secure NTFY    Ports
---------+-----------------+--------+---------+------+----+------------------
* 999      0015.c64a.97da    dynamic   0          F    F  Eth100/1/48
* 100      0005.73f9.fbc0    dynamic   0          F    F  Eth100/1/9
* 40       0050.5690.7c79    dynamic   0          F    F  Eth1/2
* 30       0025.b501.016f    dynamic   110        F    F  Eth1/1
```

Step 15 Look at the output from the previous command. You should see an entry with the Cisco UCS OUI (0025.b5, in this format) and a value from the MAC address pool that you created in the previous exercise

Step 16 Spend a few minutes running **show** commands against other VLANs, the physical port with which your MAC address is associated, and so on. Some examples would be:

Step 17 **show running-conf interface** *ethx/y*

Step 18 Type **exit** to log out of the switch and close the PuTTY window.

Step 19 Return to Cisco UCS Manager and disassociate your service profile from the physical blade.

Lab 7-1: Testing High Availability

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

Activity Objective

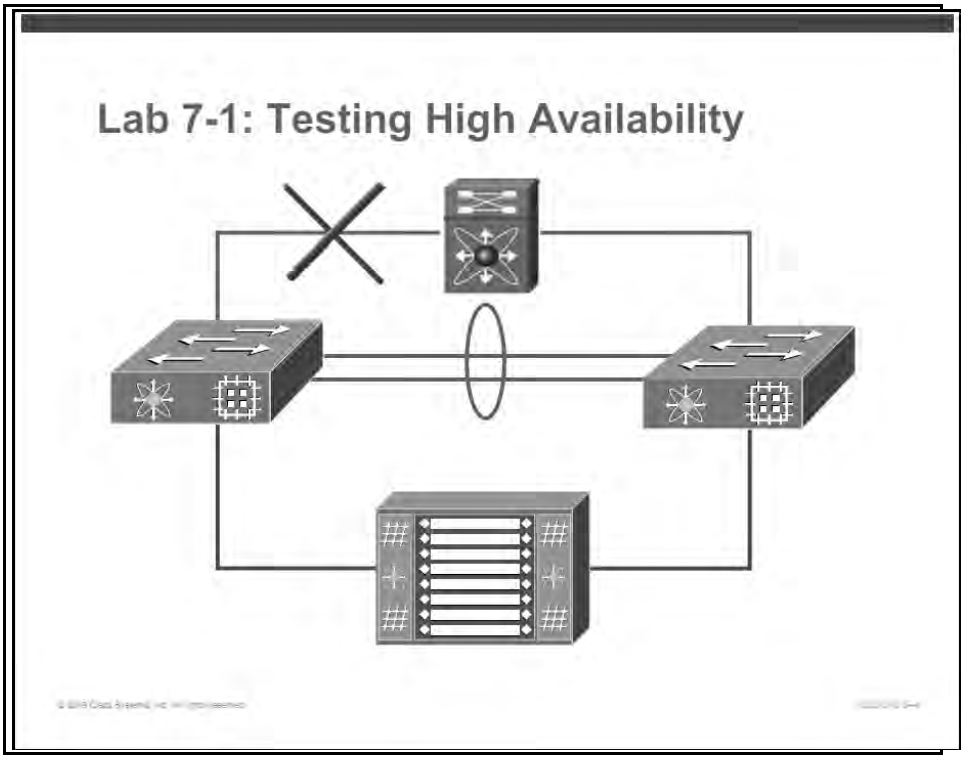
In this activity, you will demonstrate the high availability capabilities of converged network adapters and the Cisco UCS 6100 Fabric Interconnects. You will observe the failover capabilities of converged network adapters, and see a demonstration of Fabric Interconnect failover. When you complete this exercise, you should be able to:

Demonstrate the failover capabilities of Cisco UCS CNAs

Check the cluster status of a Cisco UCS Manager cluster and manually fail over a Cisco UCS Manager cluster

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:

- (2) Cisco UCS 6100 Fabric Interconnects
- Redundant upstream Ethernet switching
- Mobile service profile from previous exercise

Task 1: Demonstrate Ethernet Failover

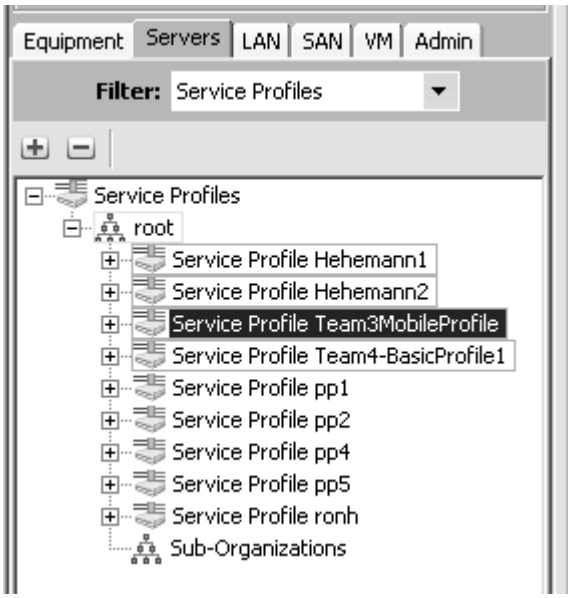
In this task, you will demonstrate the failover capabilities of Cisco UCS CNAs.

Activity Procedure

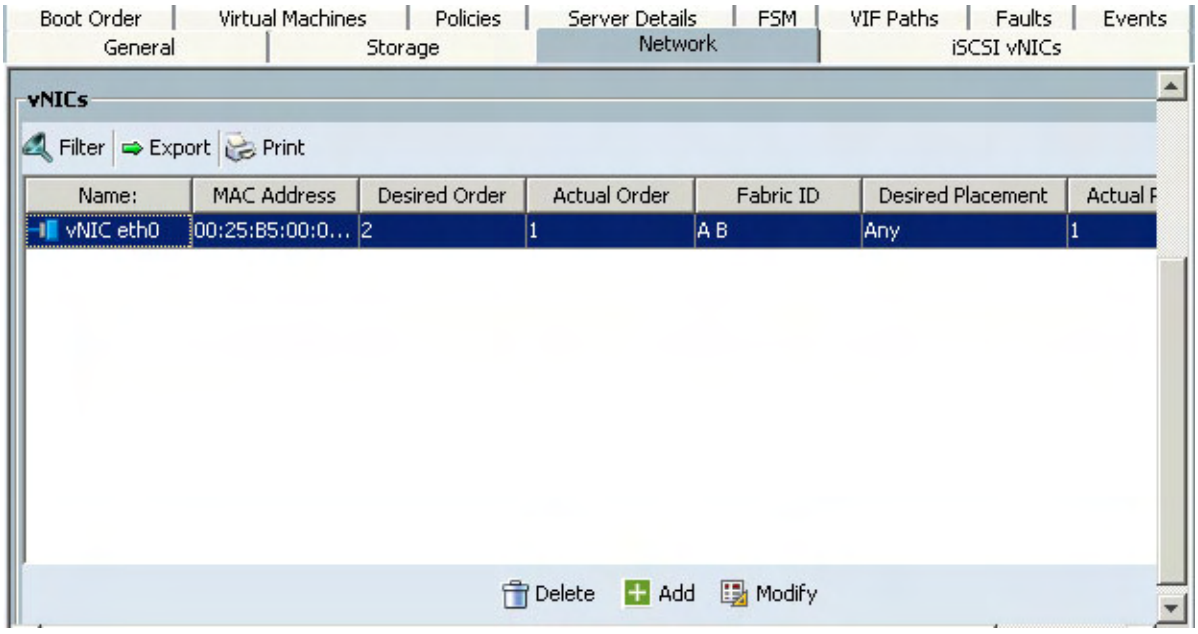
Complete these steps:

Step 1 Log into Cisco UCS Manager if necessary.

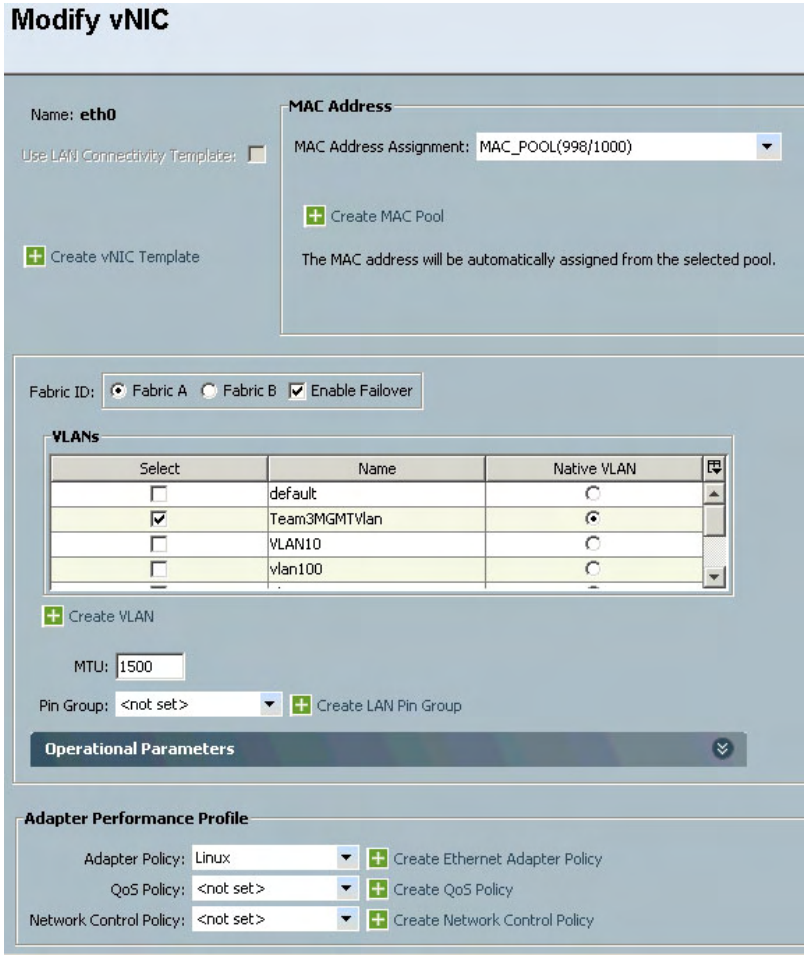
Step 2 In the navigation pane, choose the **Servers** tab. It may be helpful to set the **Filters** field to **Service Profiles** for the following steps. Choose your team's mobile service profile.



Step 3 In the content pane, choose the **vNICs** tab and click Modify at the options below.

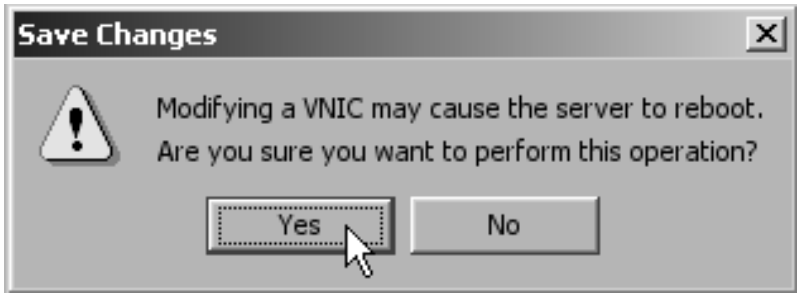


Step 4 In the Properties section, ensure that Fabric ID is set to **Fabric A** and that **Enable Failover** is checked. If not, adjust the settings as necessary and click **Save Changes**.



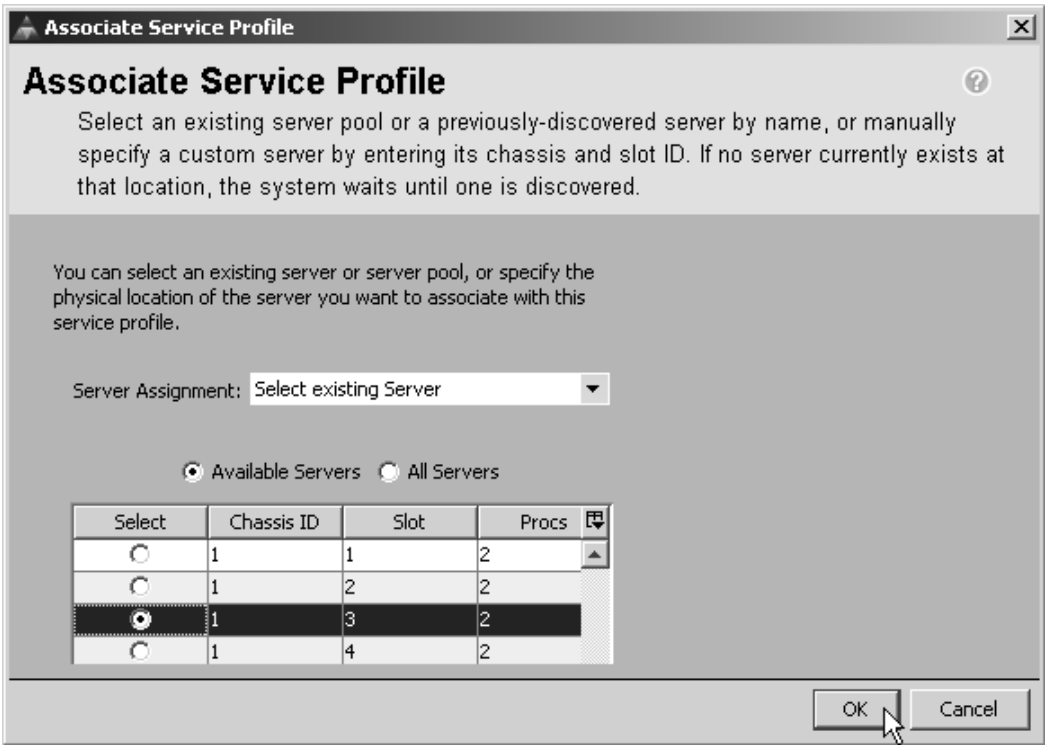
Note: If you do need to adjust any settings and your profile is currently associated with a blade, you will receive a warning that your server may be rebooted.

Step 5 If you adjusted any settings and your profile was associated with a blade, you will receive a warning that you blade may be rebooted. Click **Yes**. If you did not adjust any settings, or if your blade was not associated with a blade, move to the next step.

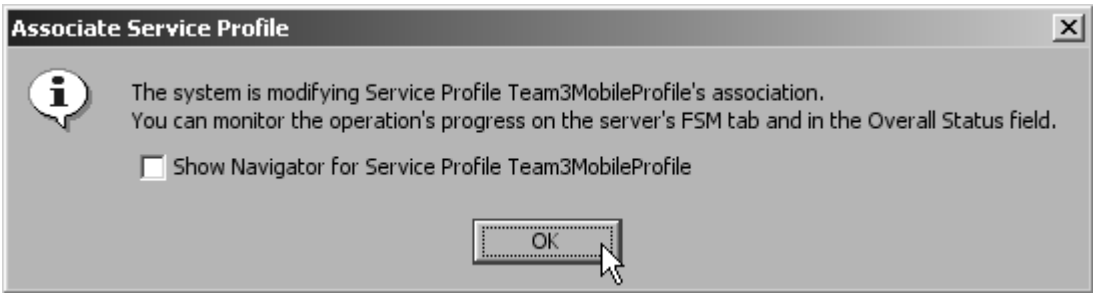


Step 6 If your service profile was already associated with a blade, skip this step. Otherwise, associate your service profile with your team server. In the navigation pane, choose your service profile icon. In the content pane, choose the General tab and click Change Service Profile Association.

Step 7 Choose your team server and click **OK**.

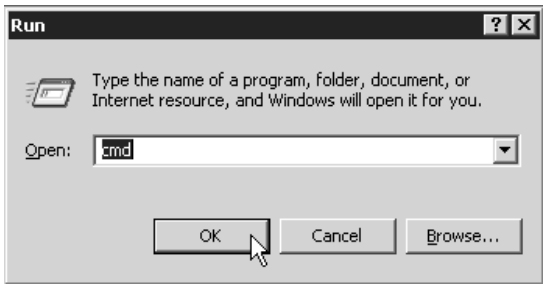


Step 8 Click **OK**.

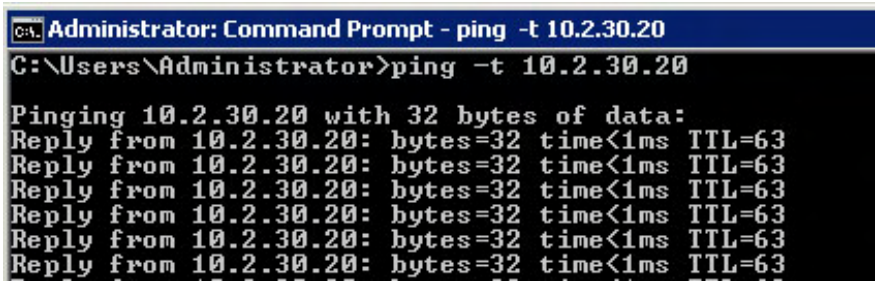


Step 9 Allow the association to complete, watching the process on the KVM console if desired. Ensure that your blade server operating system is booted.

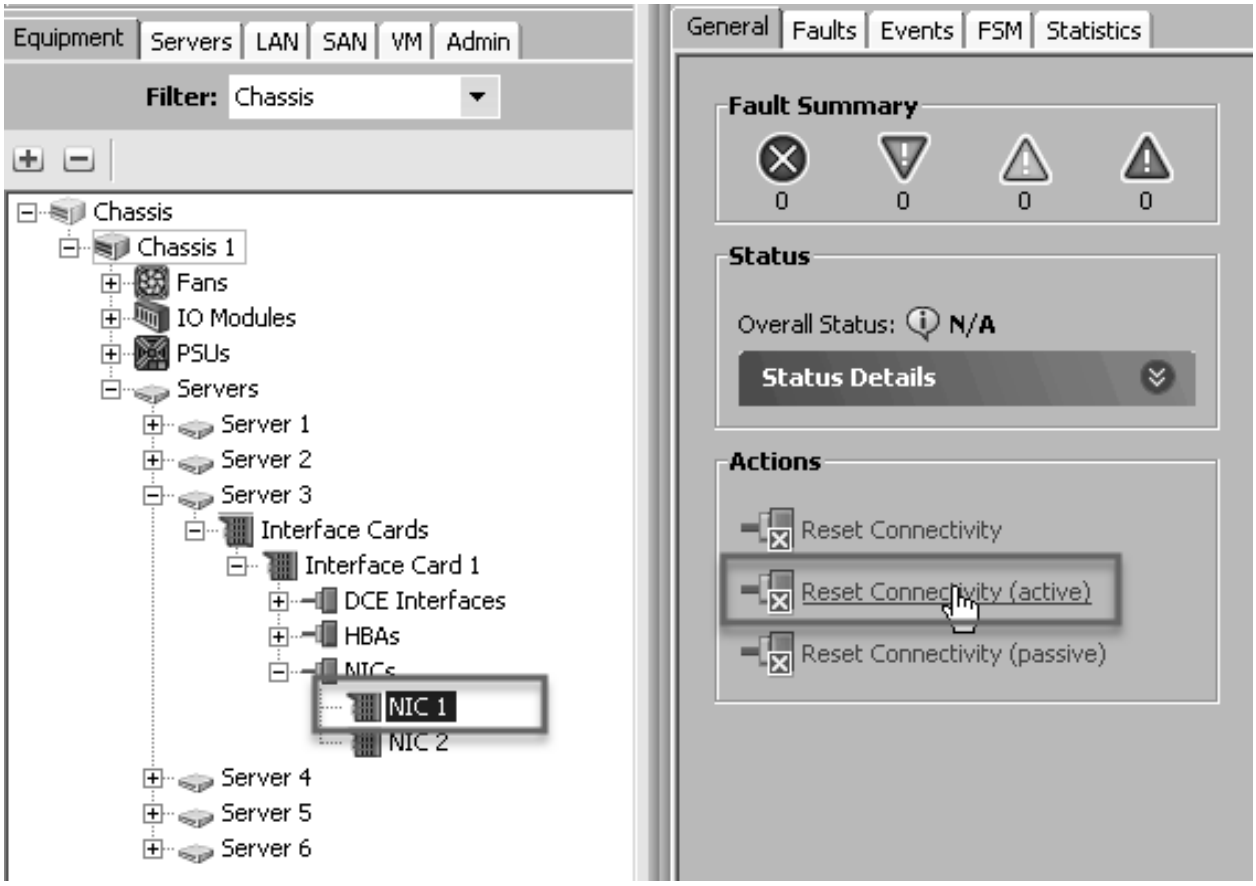
Step 10 From your student desktop (not your blade server operating system), open a command prompt by clicking **Start,** then **Run**, and entering **cmd**.



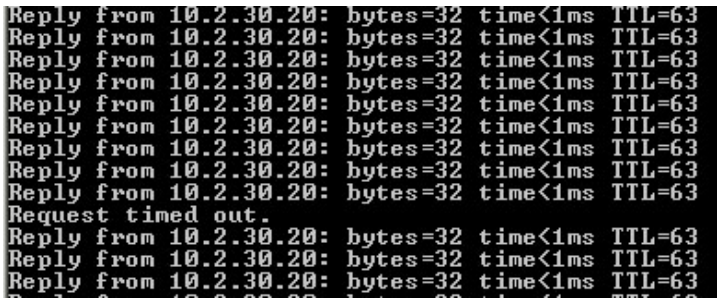
Step 11 At the command prompt, enter **ping –t 10.2.30.20**, replacing X with your team number. This is the address on the interface of your blade server vNIC.

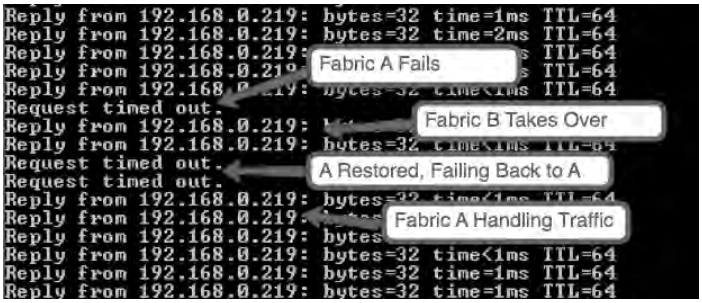


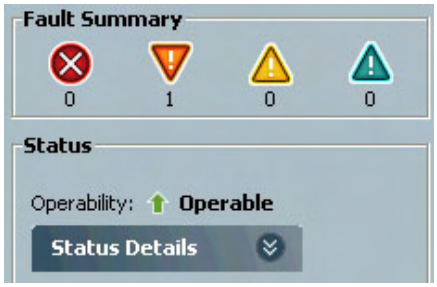
Step 12 In the equipment pane, expand your Server blade until you see NIC 1. Click on NIC 1 and then on the general table click **Reset Connectivity (Active),** this will briefly fail Fabric A. Fabric B will take over until Fabric A recovers. This may need to be done twice to see any effect.



Step 13 Observe the ping output. The left image shows short distruption in connectivity for the failover to happen. The image on the right gives a sample of the output in the past using 1.3 firmware.Notice the fault message appearing as soon as the reset function is pressed.







Step 14 Cancel ping process by pressing **Ctrl-C** and close the command prompt windows.

Task 2: Explore Fabric Interconnect High Availability

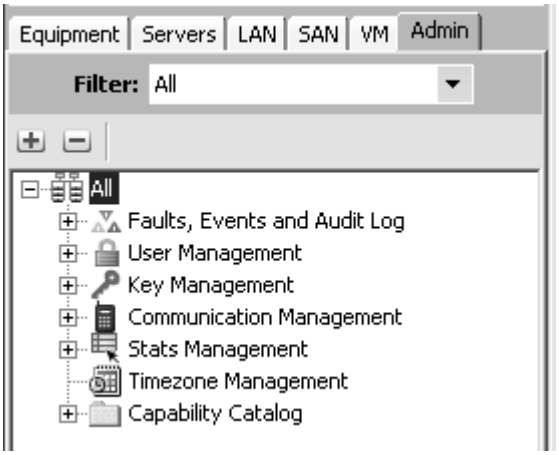
In this task, you will check the cluster status of a Cisco UCS Manager cluster and manually fail over a Cisco UCS Manager cluster.

Activity Procedure

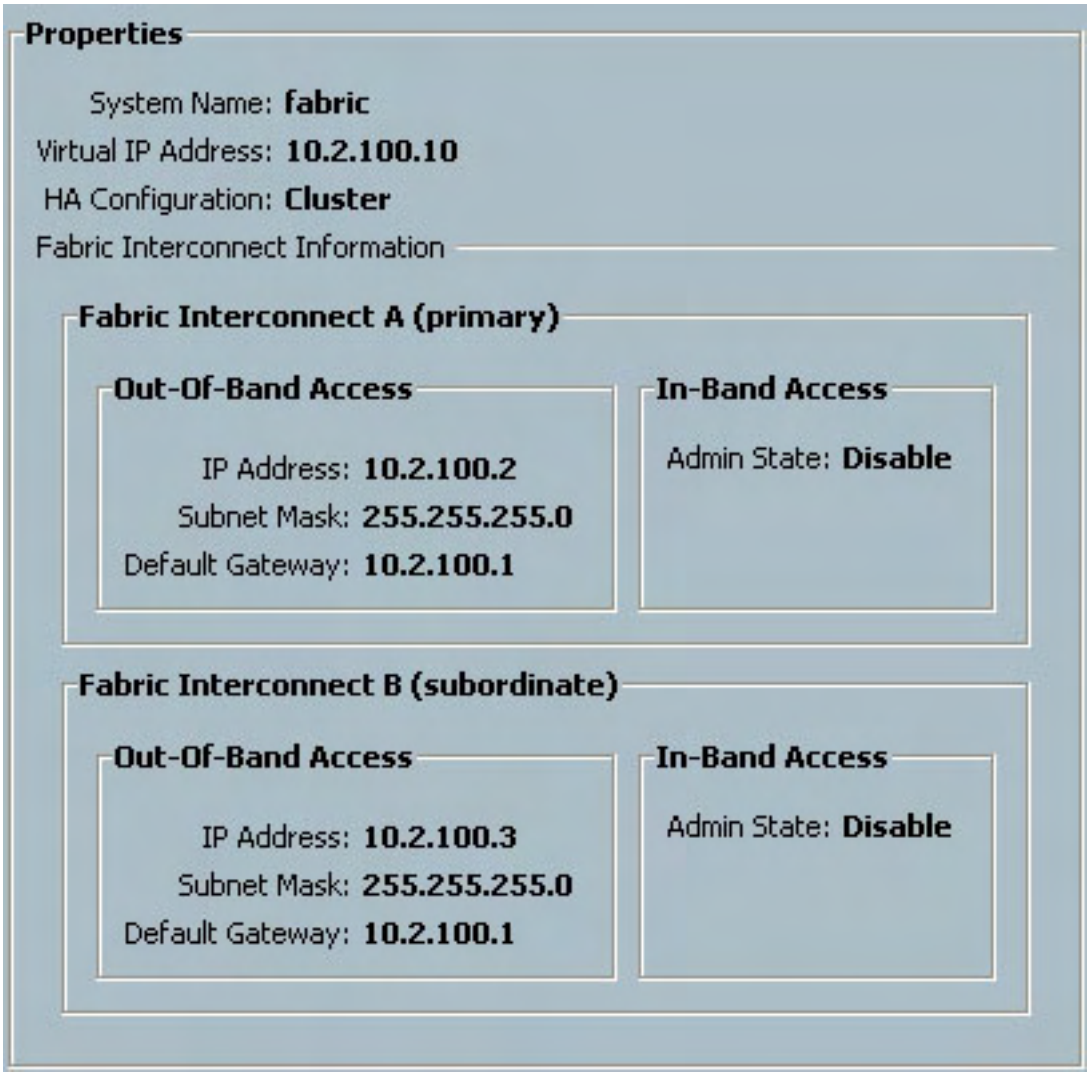
Complete these steps:

Step 1 Log into Cisco UCS Manager if necessary.

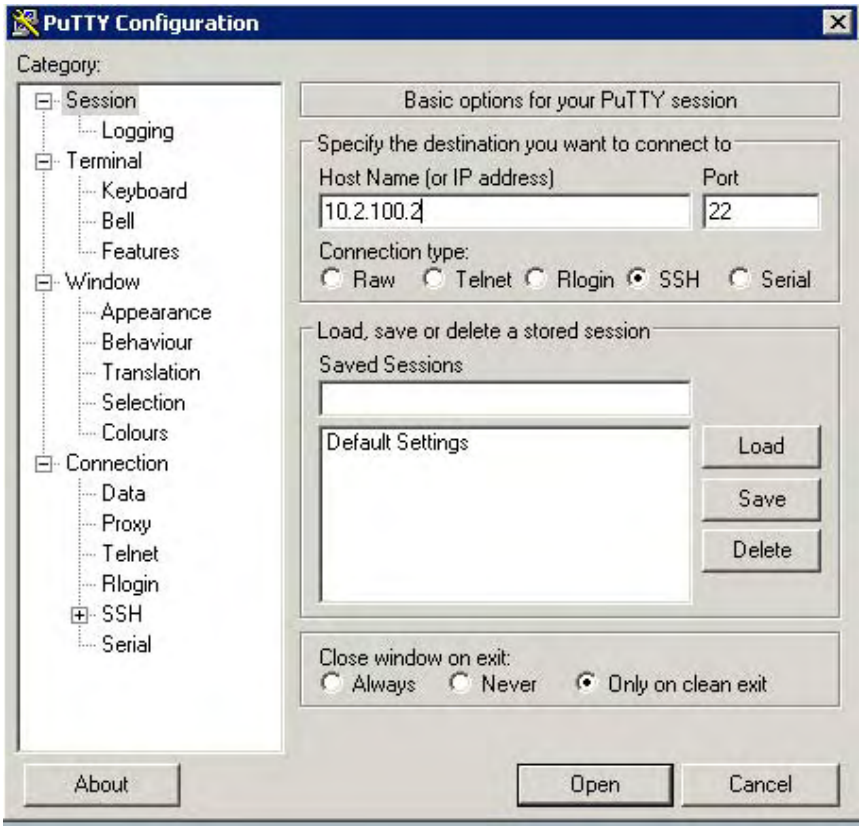
Step 2 In the navigation pane, choose the **Admin** tab and ensure that the **All** icon is selected.



Step 3 In the content pane, review the system properties, including the HA Configuration. Note the System IP Address field.



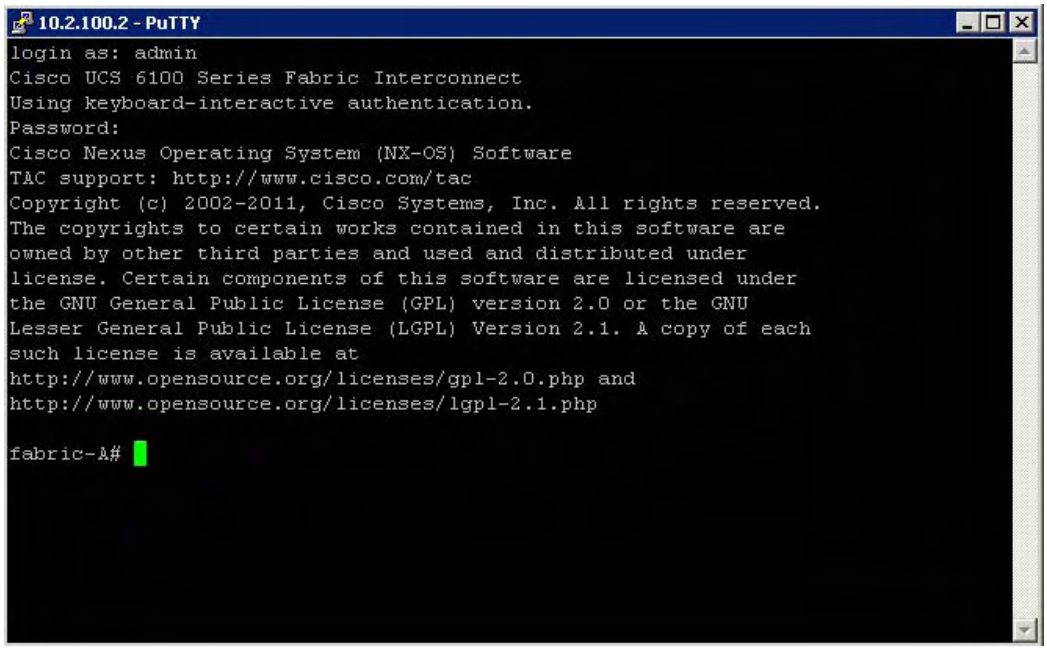
Step 4 Open a PuTTY session to the IP address that was noted in the previous step.



Note: By using the system, or cluster, address, you ensure that you are connecting to the primary node.

Step 5 If you receive a warning message such as this, click **Yes**.

Step 6 Log in using the username 'admin' and password 'cisco123' that you have been using to log into the Cisco UCS Manager GUI.



Step 7 Note the suffix on the hostname in the command prompt. This example, s6100-A, shows that you are connected to Fabric Interconnect A. Run the command **show cluster state**.

Step 8 Run the command show cluster extended –state.

```
fabric-A# show cluster extended-state
Cluster Id: 0x9f21b44c15a511e1-0x99a5000573f9fbc4

Start time: Wed Nov 23 08:15:25 2011
Last election time: Wed Nov 23 08:17:39 2011

A: UP, PRIMARY
B: UP, SUBORDINATE

A: memb state UP, lead state PRIMARY, mgmt services state: UP
B: memb state UP, lead state SUBORDINATE, mgmt services state: UP
   heartbeat state PRIMARY_OK

INTERNAL NETWORK INTERFACES:
eth1, UP
eth2, UP

HA READY
Detailed state of the device selected for HA storage:
Chassis 1, serial: FOX1507GQTD, state: active
fabric-A#
```

Step 9 While it is possible to query the cluster state from the default Cisco UCS CLI, any cluster management actions must be run from the local-mgmt CLI. Connect to the local-mgmt CLI by running the command **connect local-mgmt**.

```
fabric-A# connect local-mgmt
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

fabric-A(local-mgmt)#
```

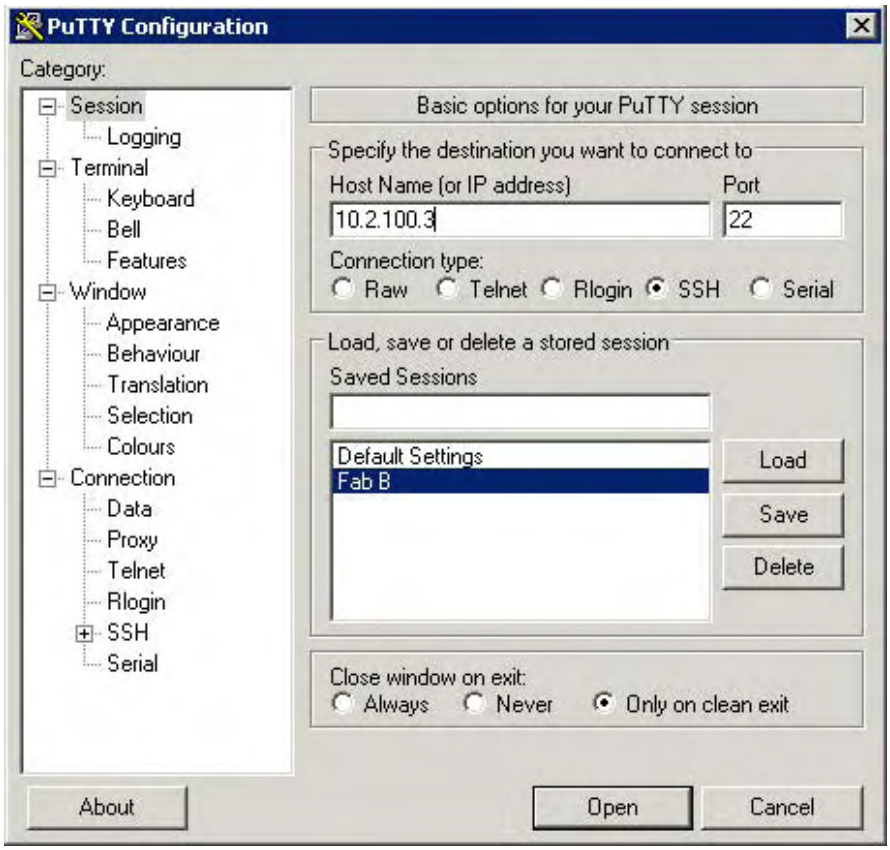
Step 10 Try to force this node to become primary by running **cluster force primary**. Are you successful? Why not? What is this command used for?

```
fabric-A(local-mgmt)# cluster force primary
Cluster Id: 0x9f21b44c15a511e1-0x99a5000573f9fbc4
request failed: cannot accept  force command when election has successfully comp
leted
fabric-A(local-mgmt)#
```


Note: The command **cluster force primary** functions only when the normal election process for a cluster has failed. Because this cluster is healthy, the command is not accepted.

Step 11 Enter **exit** to return to the default Cisco UCS CLI. Then enter **exit** again to log out of the CLI.

Step 12 Open a PuTTY session to Fabric Interconnect B as noted earlier in this task.



Step 13 If you receive a warning such as this, click **Yes**.

Step 14 Log in by using the username and password you have used previously to log into the Cisco UCS Manager GUI.

```
login as: admin
Cisco UCS 6100 Series Fabric Interconnect
Using keyboard-interactive authentication.
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

fabric-B#
```

sh

Step 15 Run **show cluster state** to confirm that Fabric Interconnect is still the subordinate node.

```
fabric-B# sh cluster state
Cluster Id: 0x9f21b44c15a511e1-0x99a5000573f9fbc4

B: UP, SUBORDINATE
A: UP, PRIMARY

HA READY
fabric-B#
```


Step 16 Connect to the local-mgmt CLI.

```
fabric-B# connect local-mgmt
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

fabric-B(local-mgmt)#
```

Step 17 Try to take over the cluster by running the **cluster force primary** command. Are you successful? Why not?

```
c6100-B(local-mgmt)# cluster force primary
Cluster Id: 0x8c6df3b2dc6011df-0x9577000573a14804
request failed: cannot accept  force command when election has successfully comp
leted
c6100-B(local-mgmt)#
```

Note: As you saw on the primary node, the cluster **force** command can be used only when the normal election process has failed.

Step 18 All teams must be at this step before continuing. Let your instructor know that you have reached this step and wait for further instructions before continuing.

Step 19 When all teams have reached this step, the instructor will perform a failover from the primary node by using the command **cluster lead b**. Do not perform this command yourself!

Step 20 Do you see any disruption to your CLI session?

Step 21 If you had any open Cisco UCS Manager session, you might receive an error such as this. If so, click **Re-Login**.

Notes: While the data-switching functions are active/active between the two Fabric Interconnects, only the primary node offers the GUI via HTTP. When the cluster fails over, the HTTP service on the relinquishing node is stopped and started on the new primary. It might take up to 30 seconds for the HTTP service to be started on the new primary node, so if the HTTP request is unsuccessful, wait a few minutes and reload.

If your system has never connected to the HTTP service on the new primary node, the Cisco UCS Manager application might need to be downloaded again. This is normal.

Step 22 Run the **show cluster state** command. Which node is now the primary node?

```
c6100-B(local-mgmt)# sh cluster state
Cluster Id: 0x8c6df3b2dc6011df-0x9577000573a14804

B: UP, PRIMARY
A: UP, SUBORDINATE

HA READY
c6100-B(local-mgmt)#
```


Lab 7-2: Backing Up and Importing Configuration Data

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

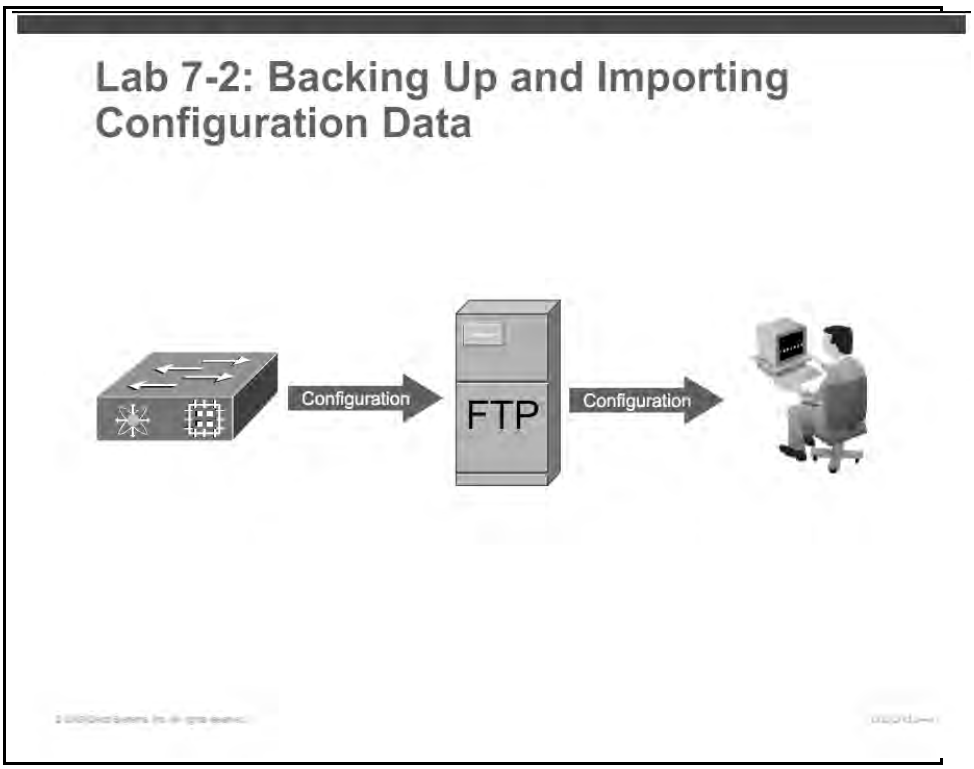
Activity Objective

In this activity, you will perform several activities related to backup and import operations for restoring Cisco UCS configuration.

- Create a full-state backup
- Create a configuration backup
- Create an import job to restore a configuration backup file

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:

- Configured Cisco UCS environment
- Network-accessible FTP server

Task 0: Configure FileZilla FTP Server

Task 0 should already have been completed, verify the steps have been completed. In this task, you will configure your desktop machine as a FileZilla FTP Server.

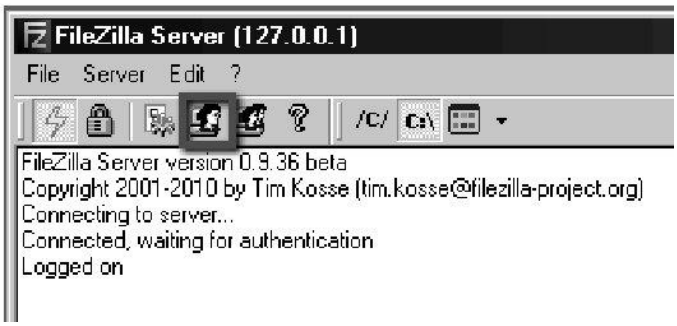
Activity Procedure

Complete these steps:

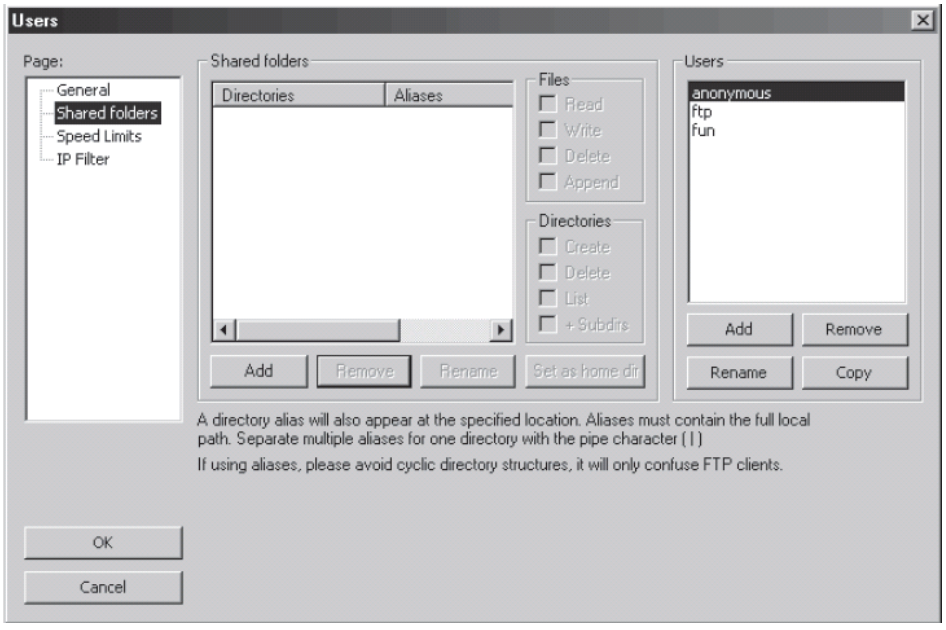
Step 1: On your desktop machine, create the directory, C:\FTP; if it does not exist.

Step 2: Open the FileZilla Server Interface by double-clicking the desktop icon.

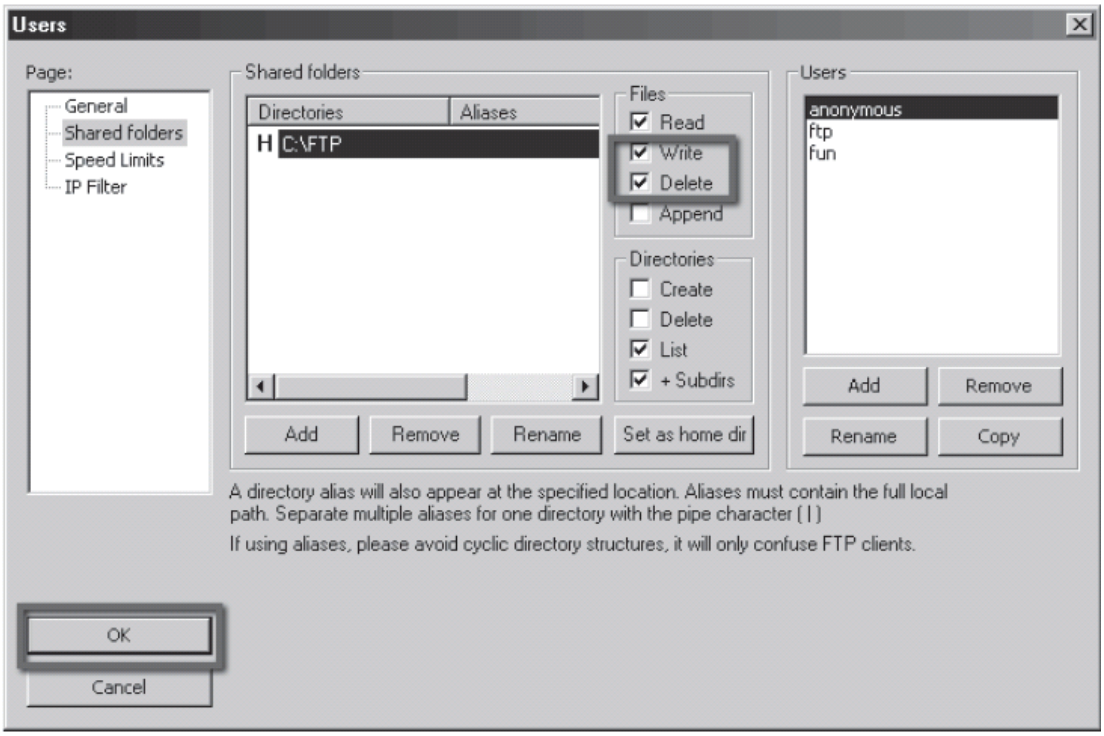
Step 3: Open the **Users** window by clicking on the icon or selecting **Edit > Users** from the menu.



Step 4: **Shared Folders** in the **Page**: section, to grant the anonymous



Step 5: Verify that 'anonymous' has **Read**, **Write** and **Delete** access to the Files in the **C:\FTP_files** directory then click **OK**.



Task 1: Create a Full State Backup

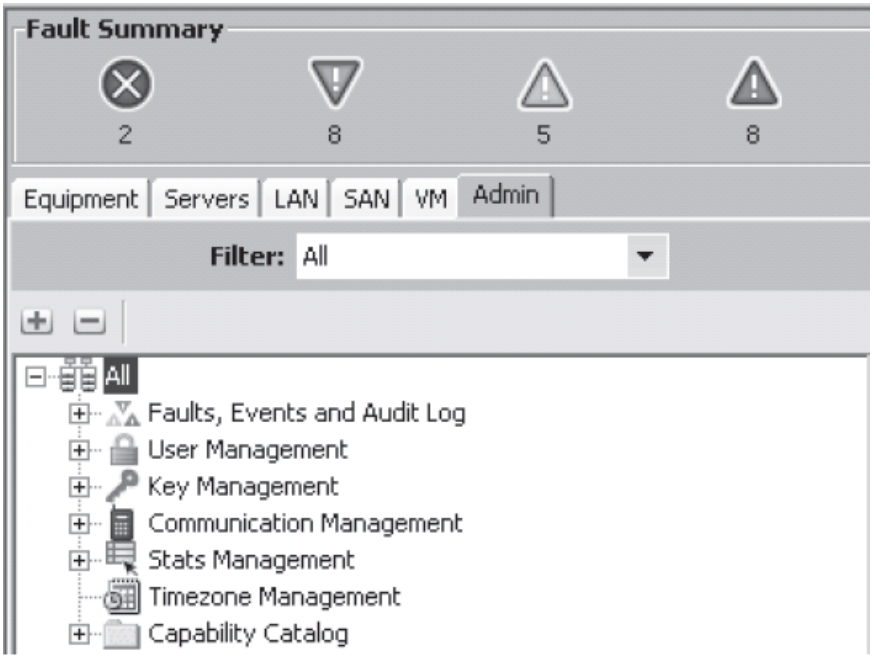
In this task, you will create a full-state backup of the Cisco UCS configuration.

Activity Procedure

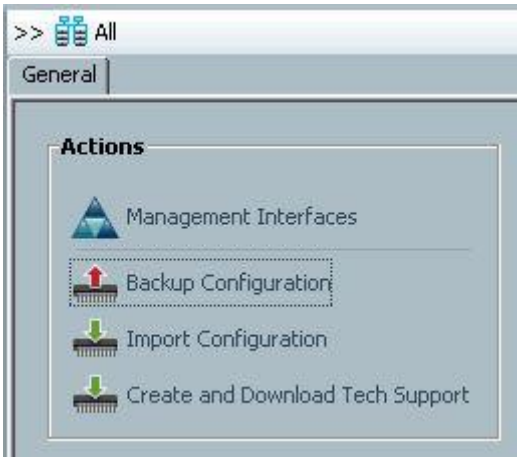
Complete these steps:

Step 6: Log into the Cisco UCS Manager.

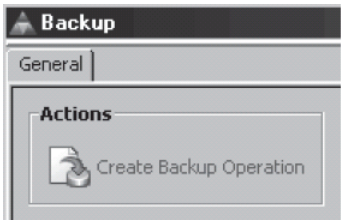
Step 7: Choose the **Admin** tab in the navigation pane. Ensure that the **Filter** value is set to **All**, and choose the **All** icon.



Step 8: Click the **Backup** link.



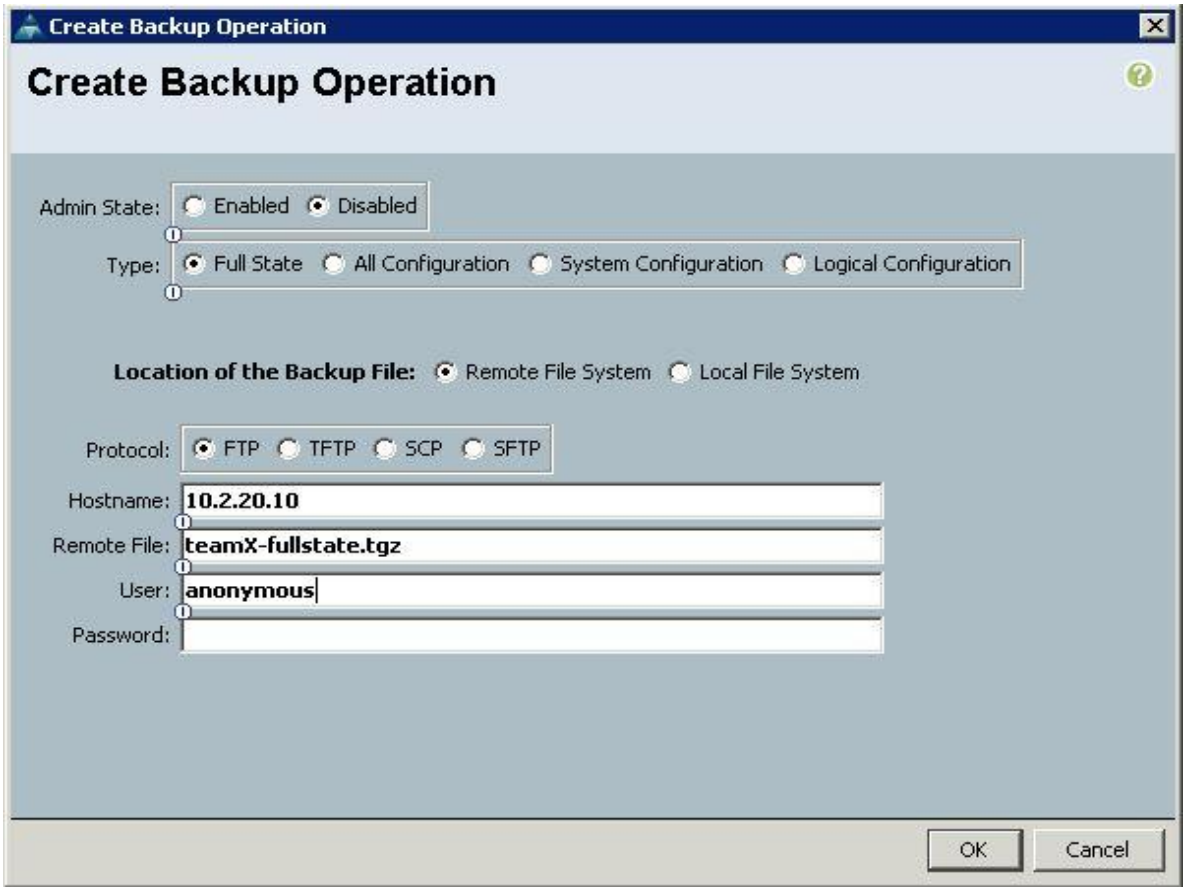
Step 9: In the resulting Backup Configuration window, click **Create Backup Operation**.



Step 10: Leave the Admin State **disabled**. Choose a **Full state** backup and the **FTP** protocol. Use the IP address of your desktop machine for the FTP Server. Name the remote file **teamX-fullstate.tgz**, replacing X with your team number. Finally, provide the username 'anonymous'.It is not necessary to provide a password at this time. Click **OK**.

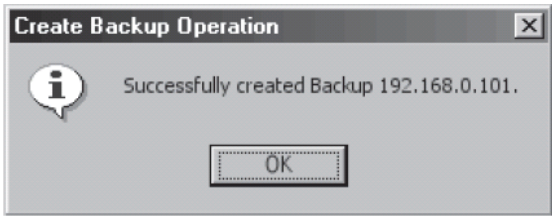
***** Use Your Student Desktop IP Address *****

Note: The filename does not require an extension. For this task, "tgz" specifies a standard UNIX convention for a "gzipped tar file," sometimes also written as ".tar.gz." Full state backups are stored as gzipped tar files.

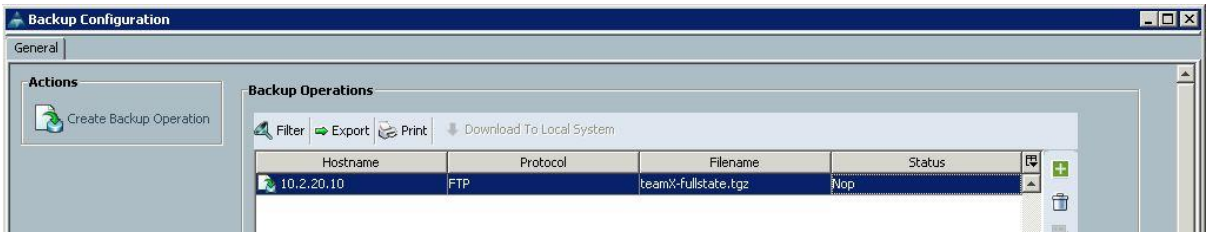


Note: In the current version of Cisco UCS Manager, only one backup operation can be created per hostname or IP address. In our lab environment, you can configure multiple DNS names that resolve to the same IP address on the FTP server to allow each team the ability to create a backup operation. A future release of Cisco UCS Manager should allow additional backup operations.

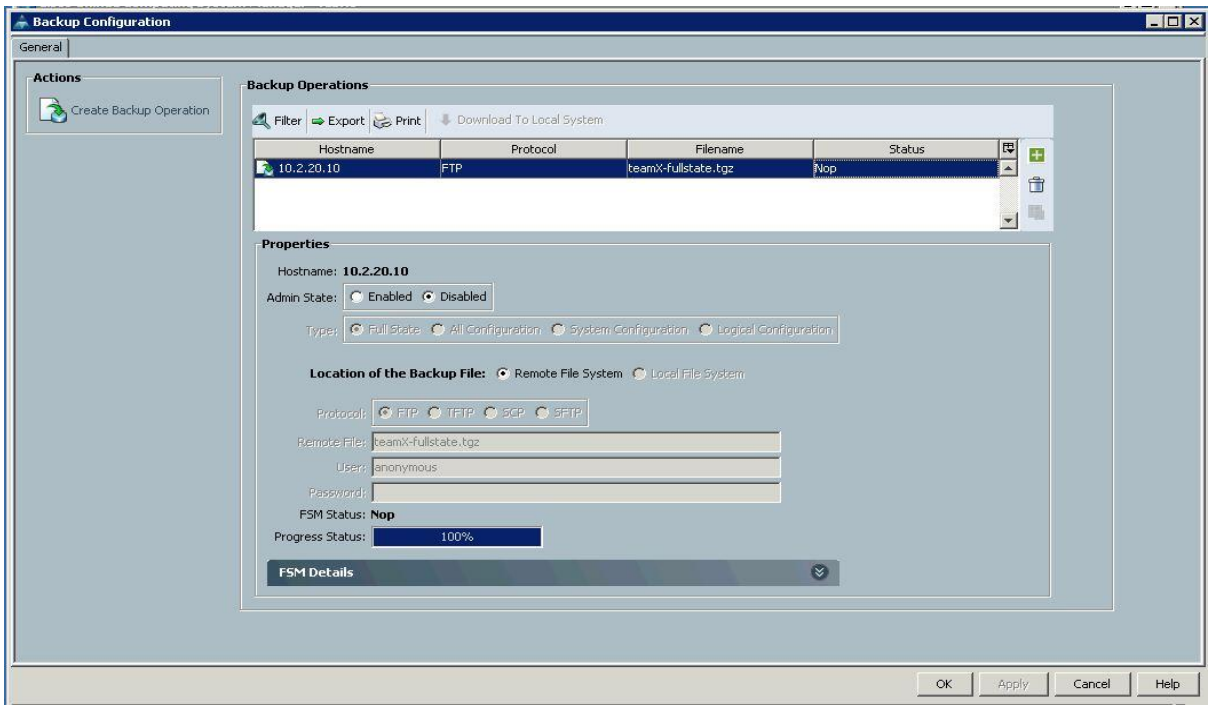
Step 11: Observe the Create Backup Operation status message, and click **OK**.



Step 12: Choose your team's backup operation in the table and verify the settings. Note the FSM Status of "nop" (No Operation), which indicates that the Finite State Machine for this icon has no further work to do and is not in an error state.



Step 13: Set the Admin State to **enabled**, enter the password specified in your Lab Reference guide under FTP Server, and click **Apply**.



Step 14: Expand the **FSM** Status and watch the backup process complete.

Step 15: When the backup is complete, the progress status should be 100%, the FSM Status should be nop, and the FSM Details should show a status of backupSuccess.

Step 16: Minimize any open Cisco UCS Manager windows and return to your student desktop.

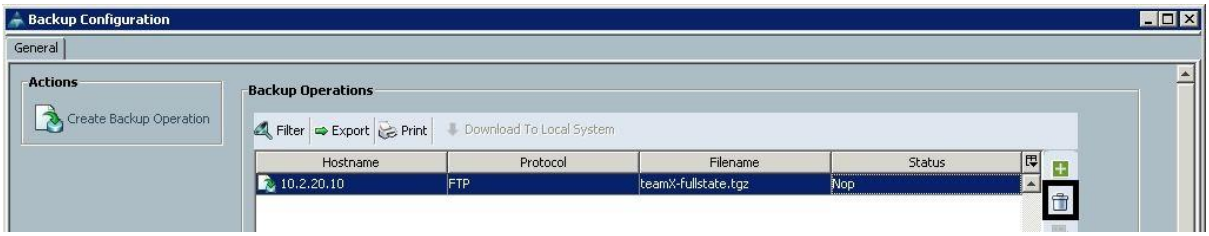
Step 17: Click **Start**, **Run**, and then enter c:\FTP_files. Click **OK**.

Step 18: Verify that you can see your team's full state backup.

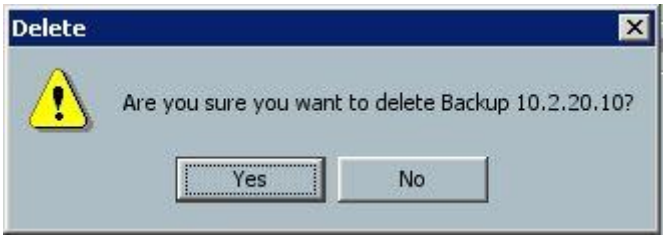
Step 19: Because we will not be using the full system backups in our lab, delete the file from the FTP server to clean up for the next student. Right-click your team's full state backup and choose **Delete**.

Step 20: Close the window and return to the Cisco UCS Manager Backup window.

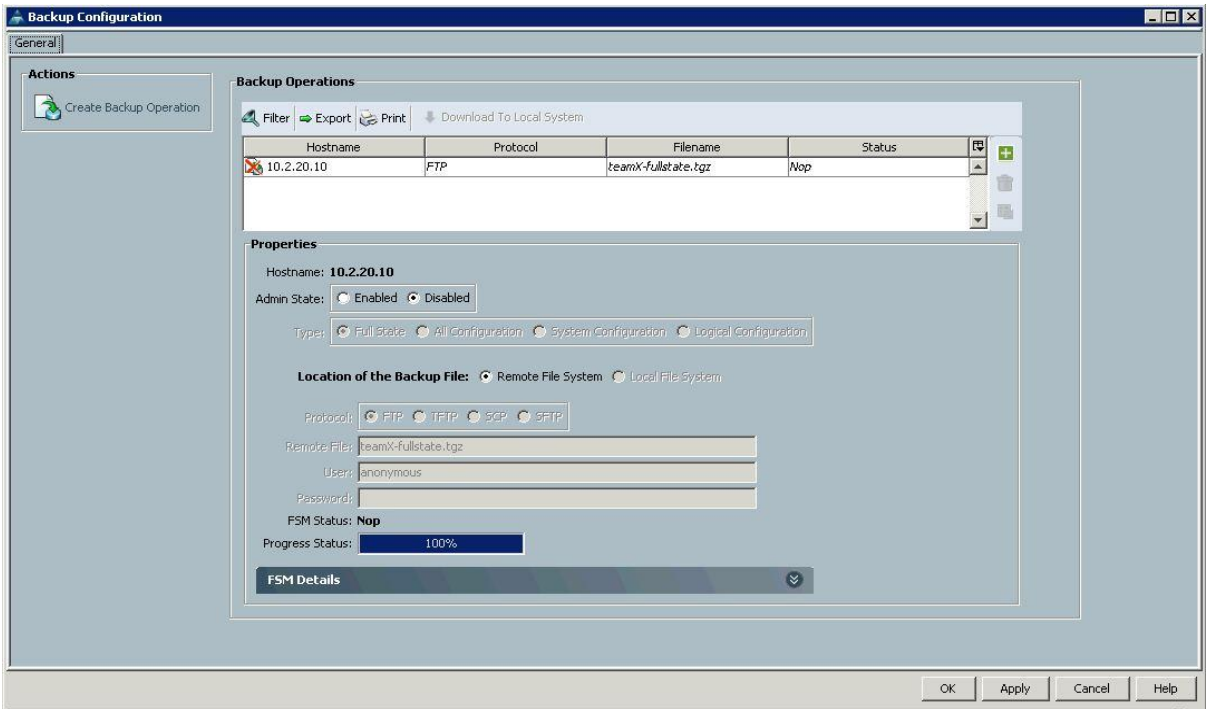
Step 21: Choose your team's full state backup icon and click the trashcan icon to delete the icon.



Step 22: Click **Yes** to confirm the deletion.



Step 23: Click **OK** to apply the changes and close the **Backup** window.



Task 2: Create a Configuration Backup

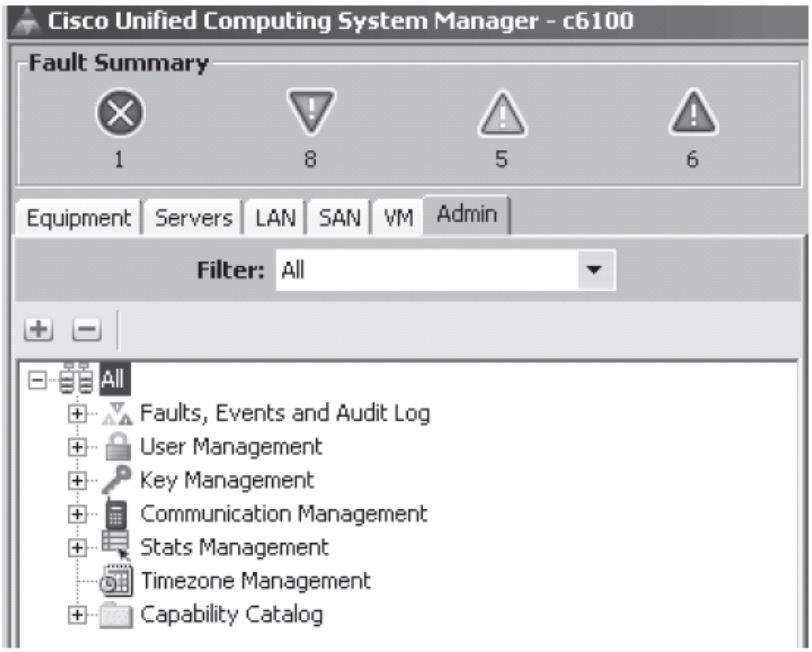
In this task, you will create an XML configuration-level backup of the Cisco UCS configuration.

Activity Procedure

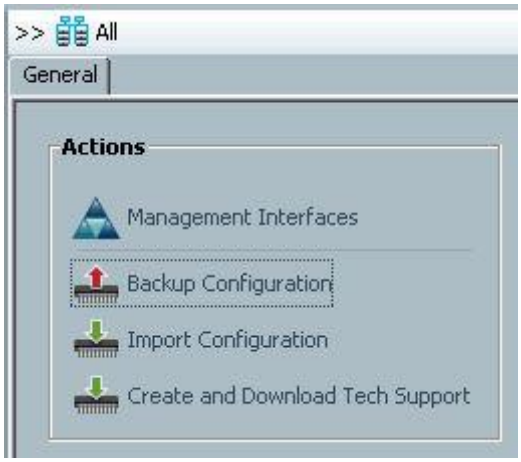
Complete these steps:

Step 1: Log into the Cisco UCS Manager if necessary.

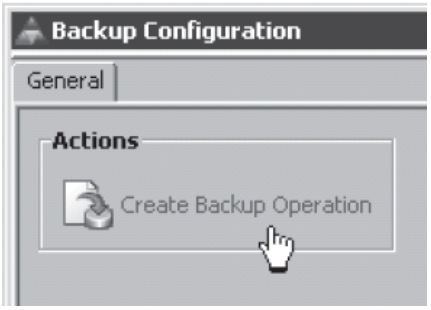
Step 2: Choose the **Admin** tab in the navigation pane. Ensure that the Filter value is set to **All**, and choose the **All** icon.



Step 3: Click the **Backup** link.



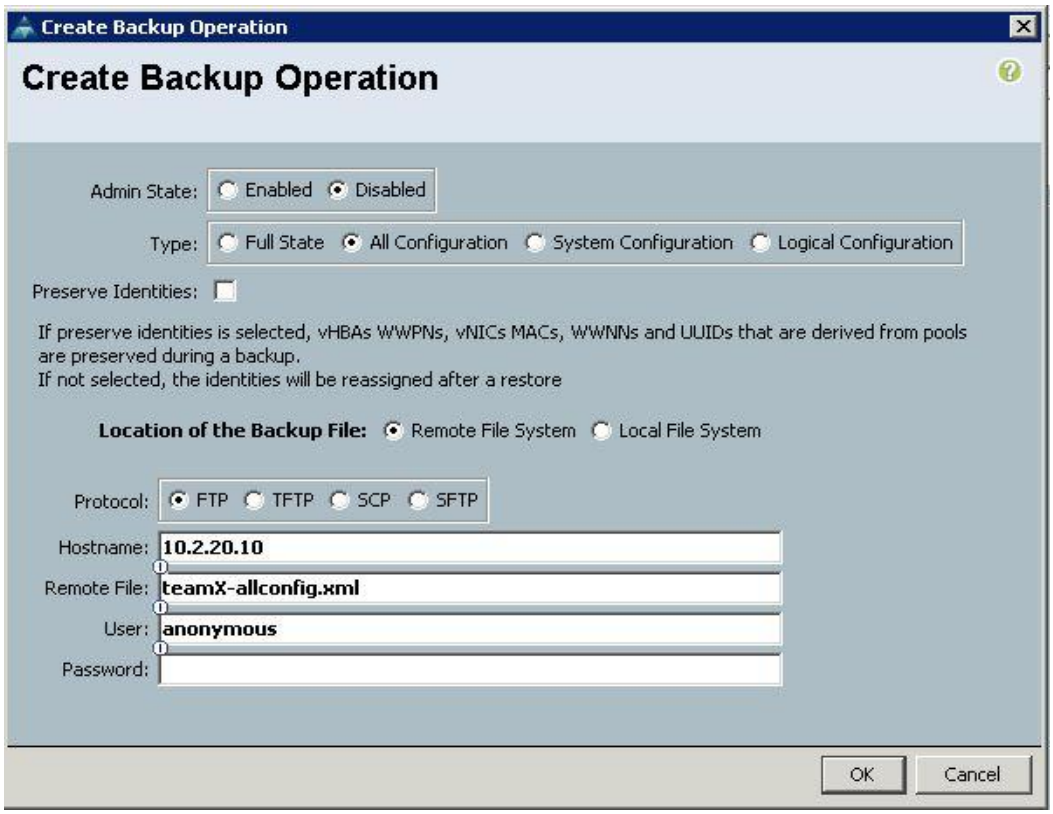
Step 4: In the resulting Backup Configuration window, click **Create Backup Operation**.



Step 5: Leave the Admin State disabled. Choose All configuration backup and the FTP protocol. For the hostname use your desktop IP Address. Name the remote file **teamX-allconfig.xml**, replacing X with your team number. Finally, provide the username from the Lab Reference Guide. It is not necessary to provide a password at this time. Click **OK**

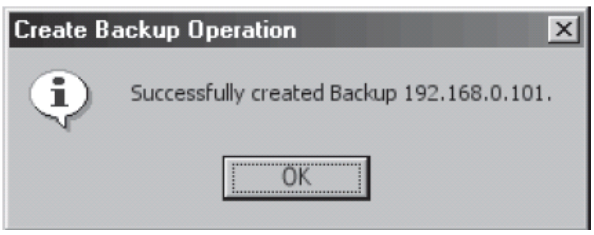
***** Use Your Student Desktop IP Address *****

Note: The filename does not require an extension. For this task, "xml" specifies a standard XML text file. Configuration backups are stored as XML text files.



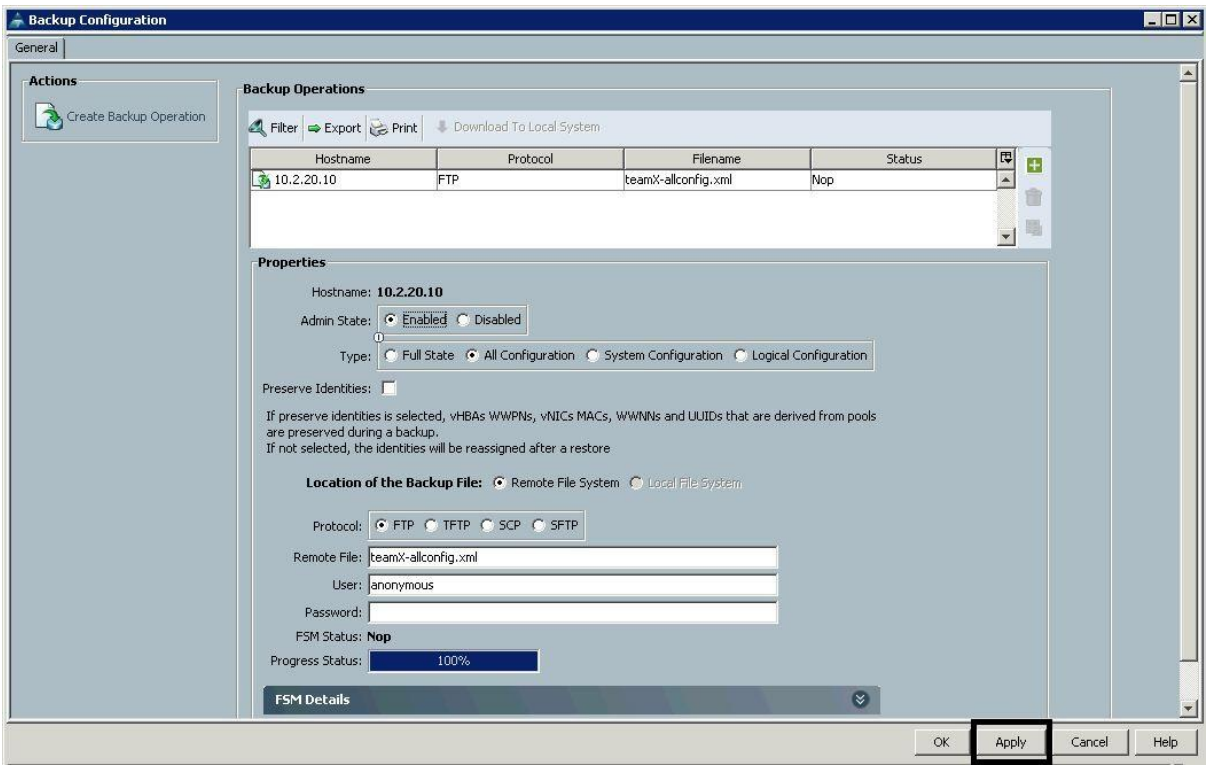
Note: In the current version of Cisco UCS Manager, only one backup operation can be created per hostname or IP address. In our lab environment, we have configured multiple DNS names that resolve to the same IP address on the FTP server to allow each team the ability to create a backup operation. A future release of Cisco UCS Manager should allow additional backup operations.

Step 6: Click **OK**.



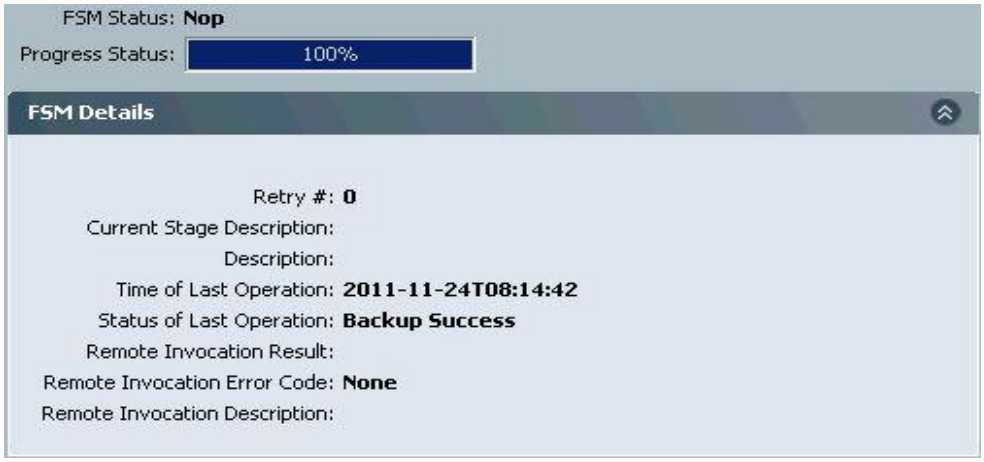
Step 7: Choose your team's backup operation in the table and verify the settings as you did for the full state backup.

Step 8: Set the Admin State to **enabled**, enter the password that was specified in your Lab Reference guide under FTP Server, and click **Apply**.



Step 9: Depending on the speed of the FTP server, you might not see any activity in the FSM Details before the backup completes. Configuration backups and the related transfer to the FTP server happen very quickly.

Step 10: When the backup is complete, the progress status should be 100%, the FSM Status should be nop, and the FSM Details should show a status of backupSuccess.



V

Step 11: Minimize any open Cisco UCS Manager windows and return to your student desktop.

Step 12: Click **Start, Run**, and then enter C:\FTP_Files

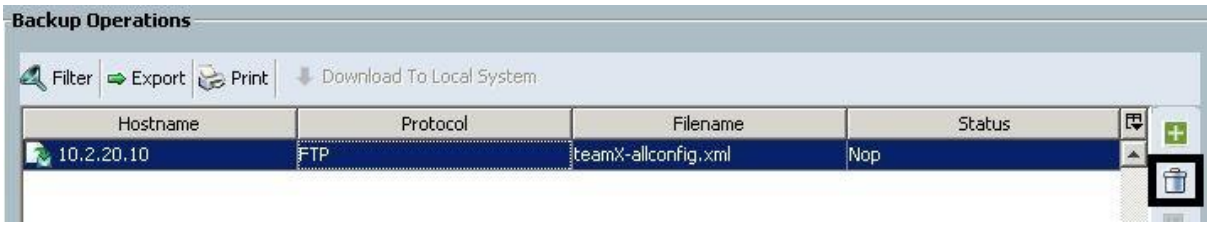
Step 13: Verify that you can see your team's configuration backup on the FTP server.

Step 14: Double-click the XML file on the FTP server folder. This will launch an Internet Explorer or a FireFox window to display the XML-formatted backup.

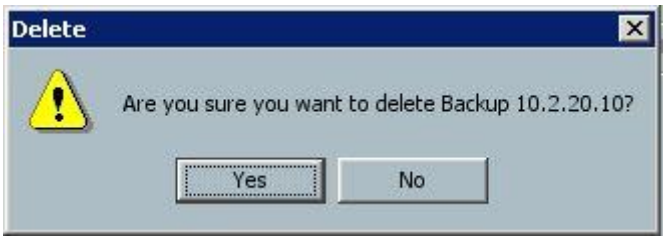
Step 15: Spend a few minutes reviewing the contents of the backup. When you are finished, close the Internet Explorer windows that are displaying the XML and return to the c:\FTP_files window. Right-click your team's XML file and click **Delete**.

Step 16: Close the window and return to the Cisco UCS Manager Backup Configuration window.

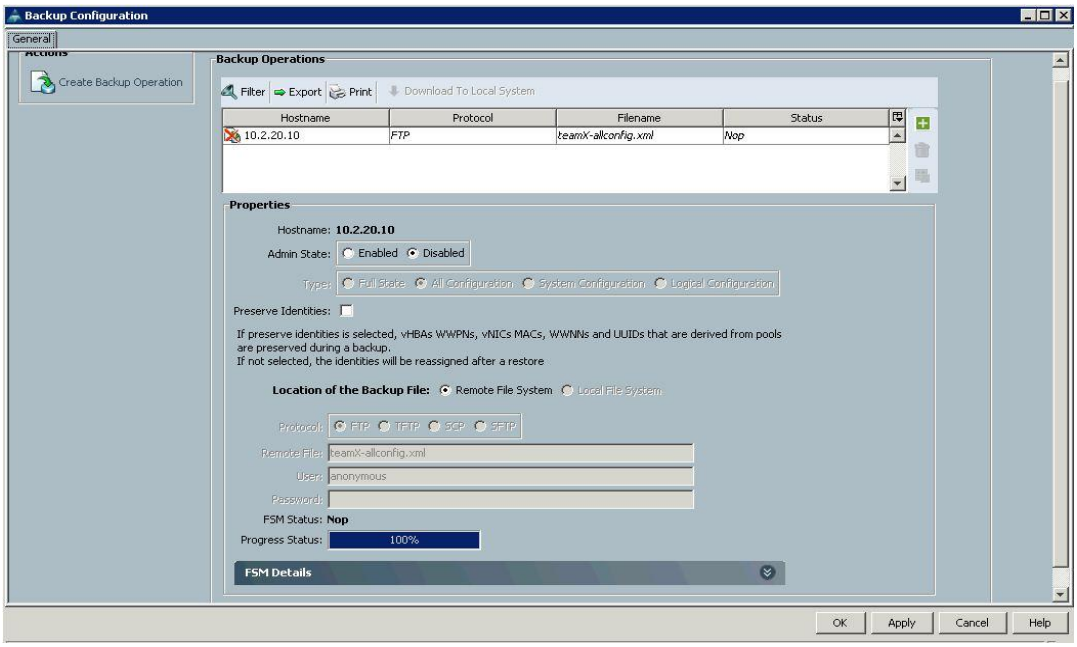
Step 17: Choose your team's **All** configuration backup icon and click the trashcan icon to delete the icon.



Step 18: Click **Yes** to confirm the deletion.



Step 19: Click **OK** to apply the changes and close the Backup Configuration window.



Task 3: Create an Import Job

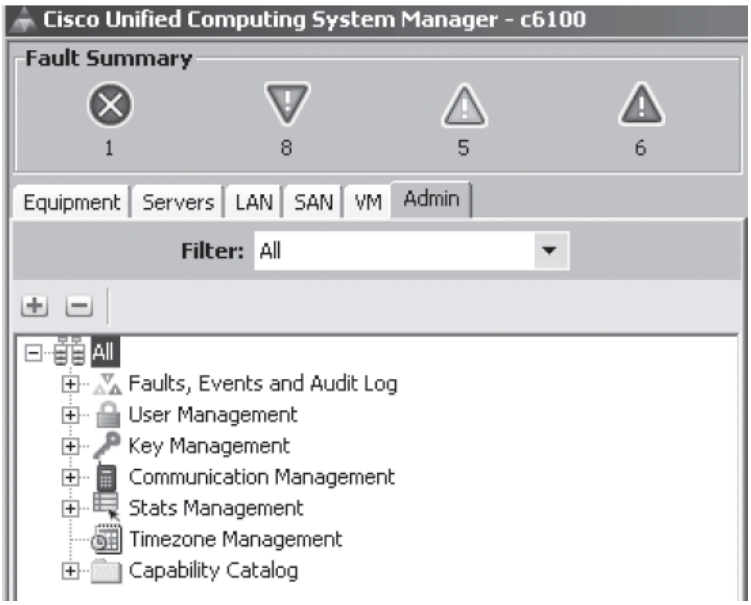
In this task, you will create an import job to restore a configuration backup from an FTP server.

Activity Procedure

Complete these steps:

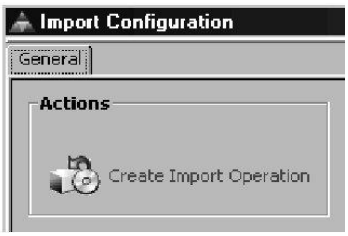
Step 1: Log into the Cisco UCS Manager if necessary.

Step 2: Choose the **Admin** tab in the navigation pane. Ensure that the **Filter** value is set to **All**, and choose the **All** icon.



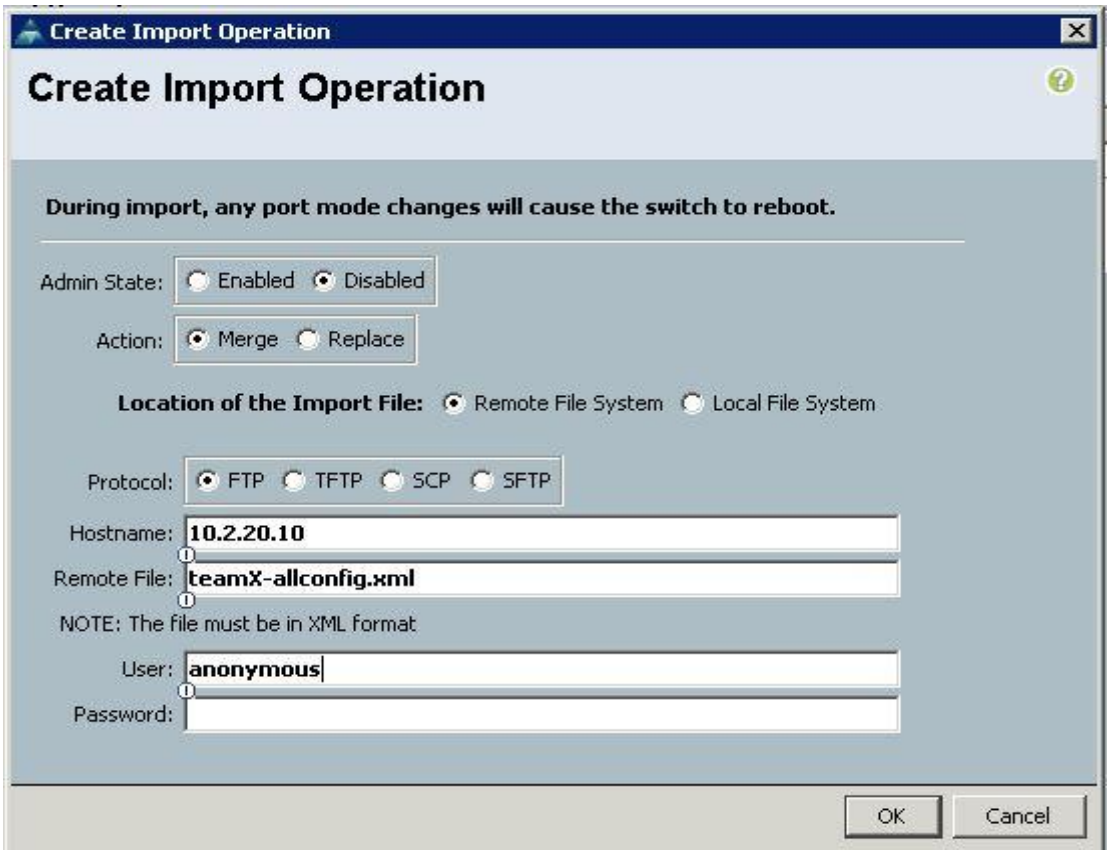
Step 3: Click the Import Configuration link.

Step 4: In the resulting Import Configuration window, click **Create Import Operation**.



Step 5: Leave the Admin State disabled and the Action as merge. Set the hostname, "FTP Server." As the lab is a shared environment, we will not actually be restoring backups to avoid conflicts or disruptions. Put

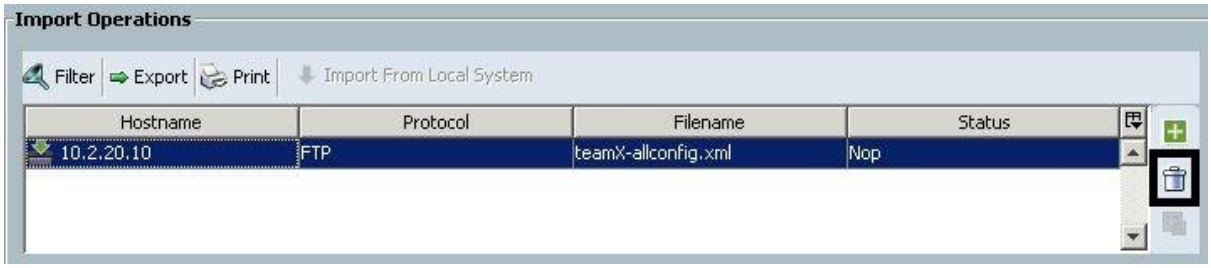
any legal values in remote file and user fields. No password is necessary. Click OK to save your import operation icon.



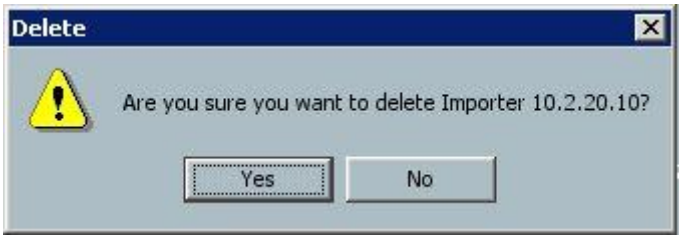
Step 6: Click **OK** to confirm the Create Import Operation status.

Step 7: Take a few moments to review your import operation.

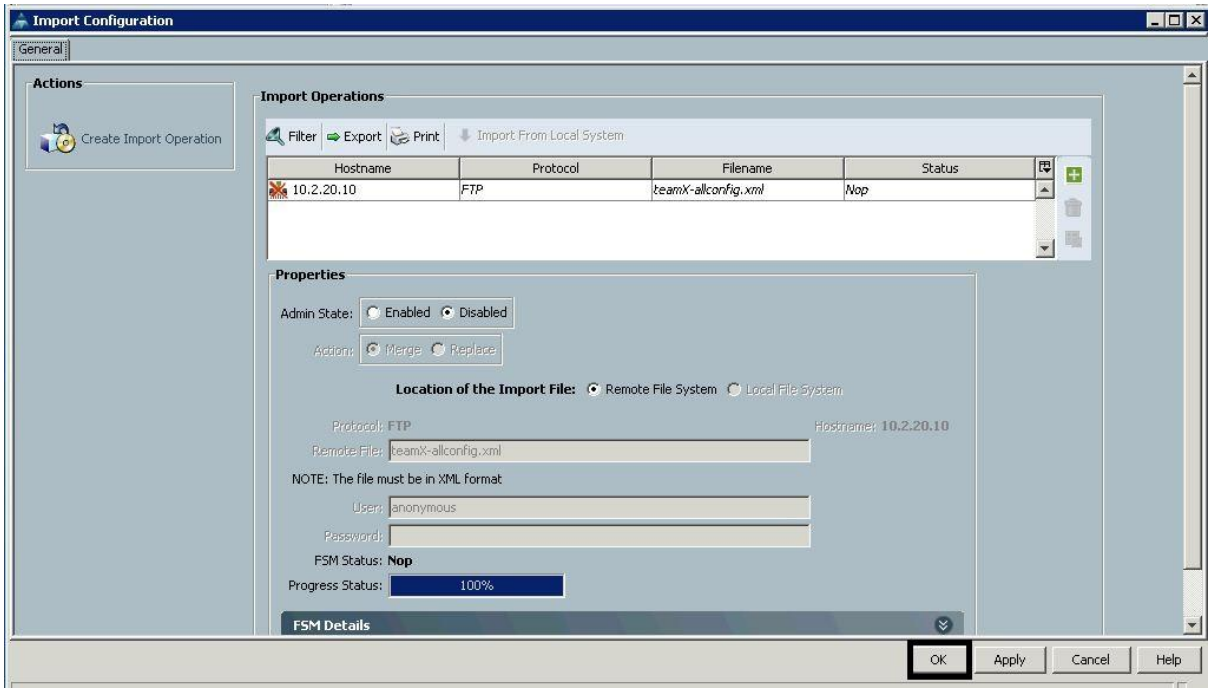
Step 8: If we were actually going to run this import, you would enable it in the same way that you enabled the backup operations completed previously. Because we are not running the import, delete your import operation icon by selecting it in the table and clicking the trashcan icon.



Step 9: Click **Yes** to confirm deletion of your import operation icon.



Step 10: Click **OK** to apply your changes and close the Import Configuration window.



Lab 7-3: Reporting

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

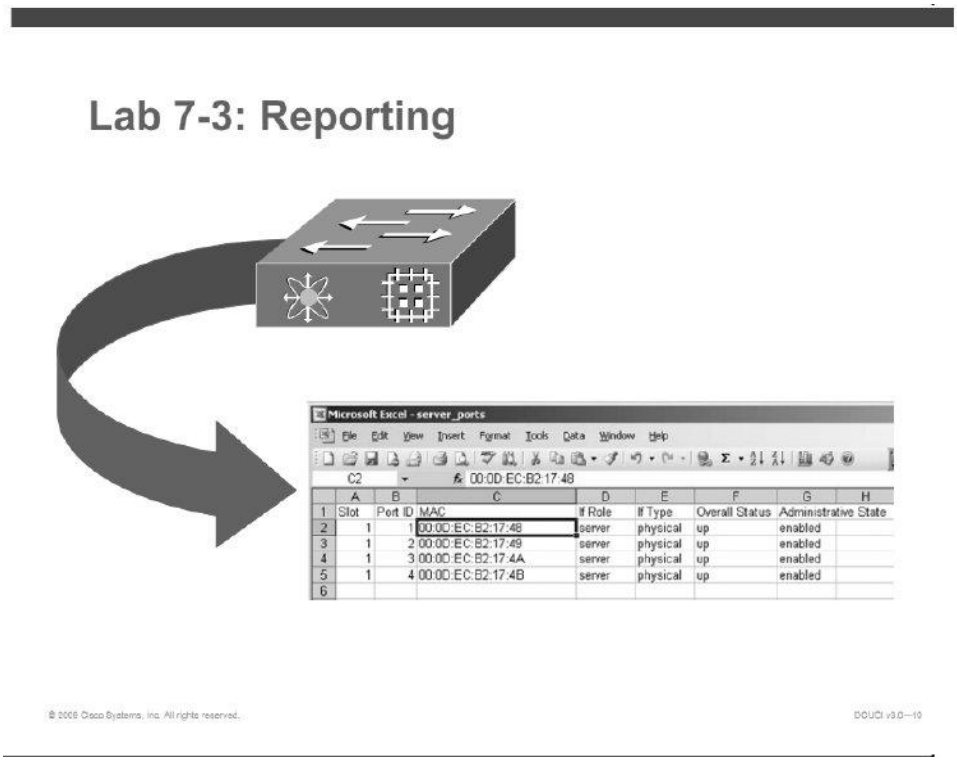
Activity Objective

In this activity, you will explore and configure the reporting capabilities of the Cisco UCS platform. After completing this lab, you should be able to:

- Configure threshold policies
- Configure Call-Home
- Configure external logging servers
- Export event and fault information

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:

- (2) Cisco UCS 6100 Fabric Interconnects

Task 1: Create Threshold Policies

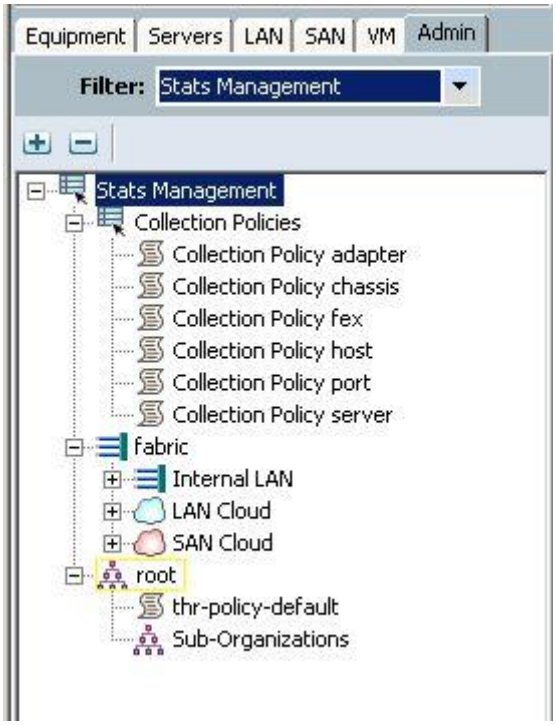
In this task, you will configure threshold policies.

Activity Procedure

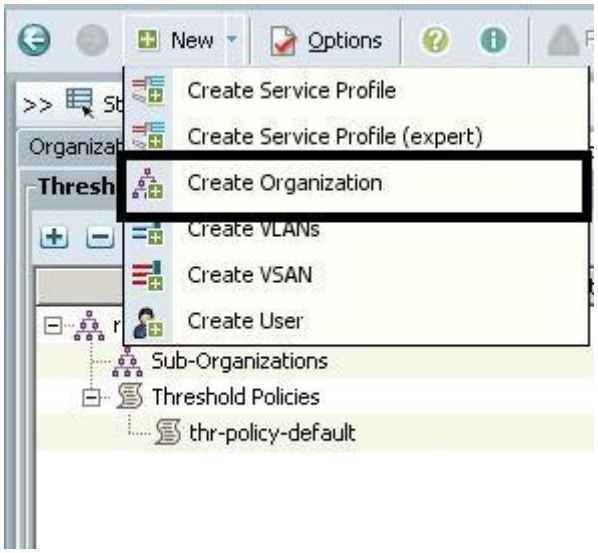
Complete these steps:

Step 1: Log into Cisco UCS Manager if necessary.

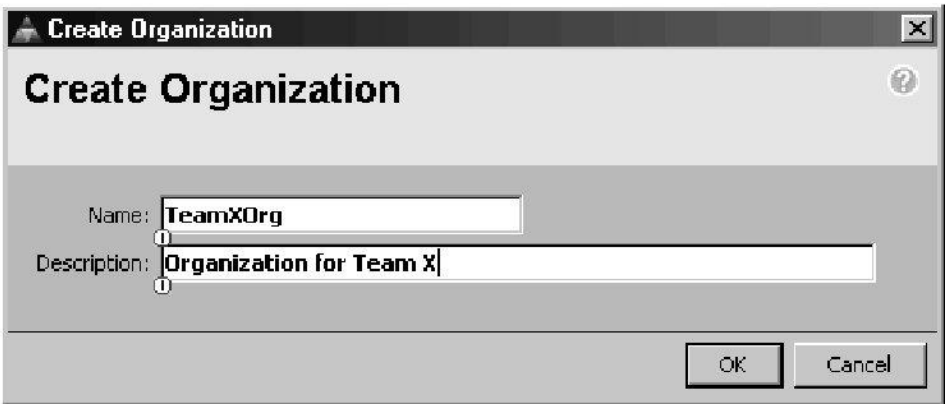
Step 2: Choose the **Admin** tab in the navigation pane. It may be helpful to set the **Filter** value to **Stats Management** for the following tasks.



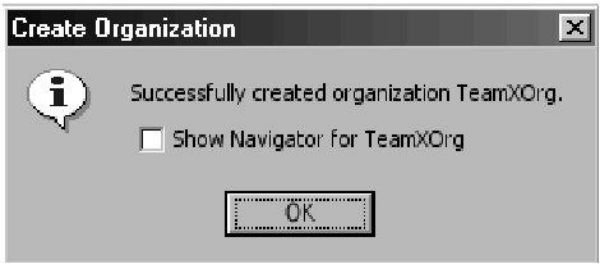
Step 3: Create an organization for your team. In the content pane, click **New** and choose **Create Organization.**



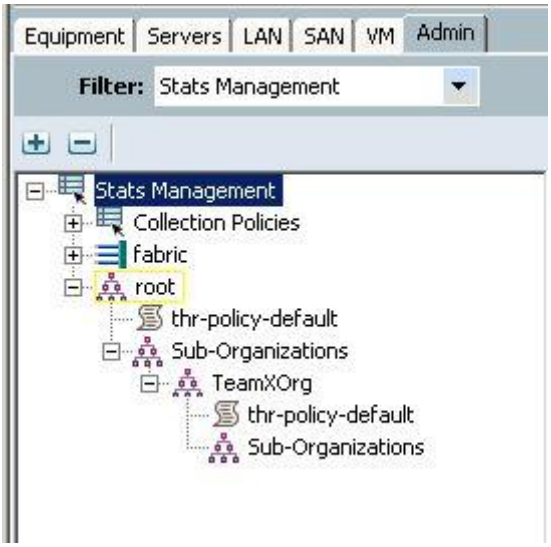
Step 4: Name your organization **TeamXOrg,** replacing X with your team number. Click **OK.**



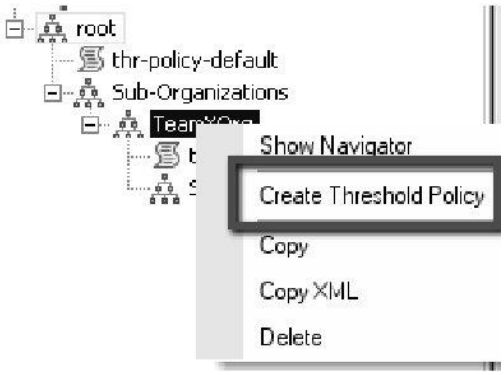
Step 5: Click **OK** to confirm creation of your organization.



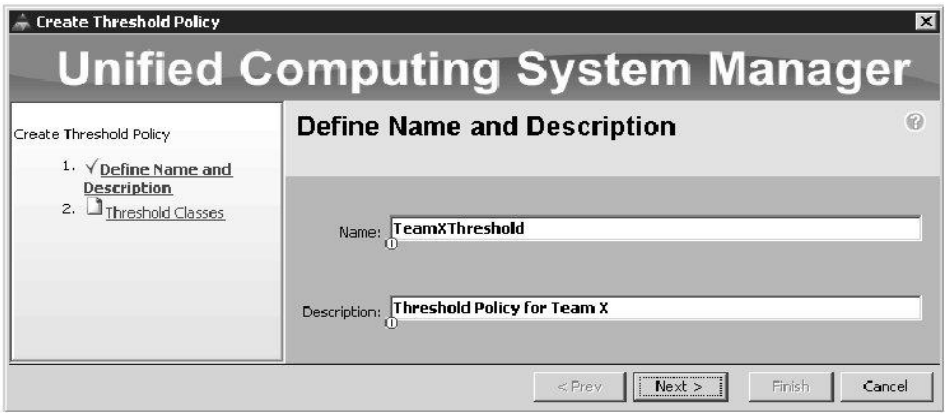
Step 6: Verify that your organization now appears under the root organization. You might need to expand the root organization to see yours.



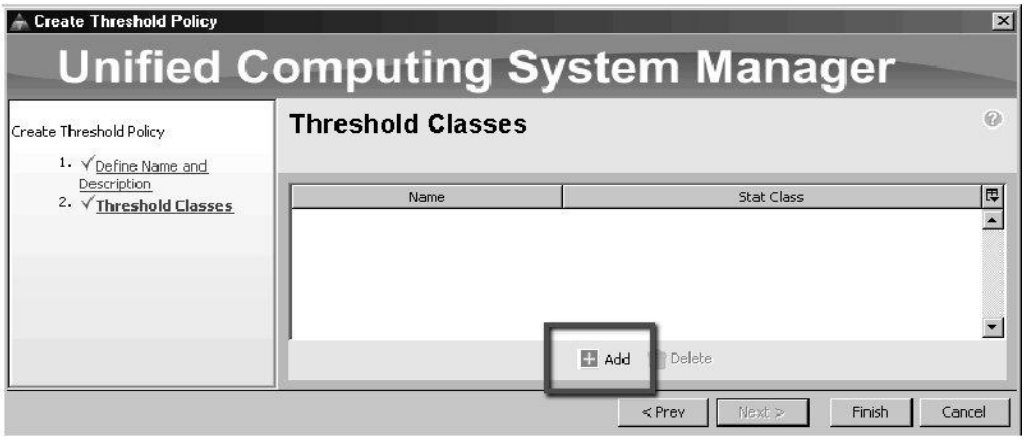
Step 7: Right-click your organization icon and choose **Create Threshold Policy.**



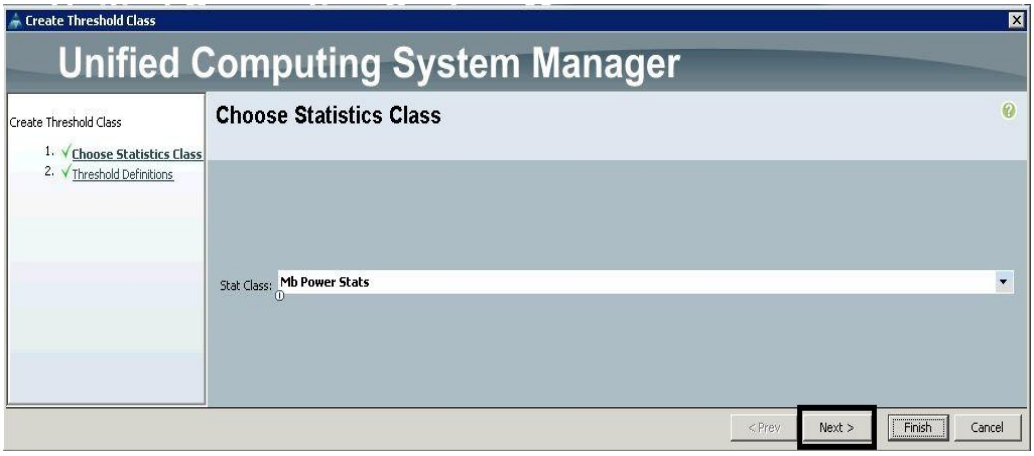
Step 8: Name your threshold policy **TeamXThreshold,** replacing X with your team number. Optionally provide a description. Click **Next.**



Step 9: Click **Add** to add a threshold class to your policy.

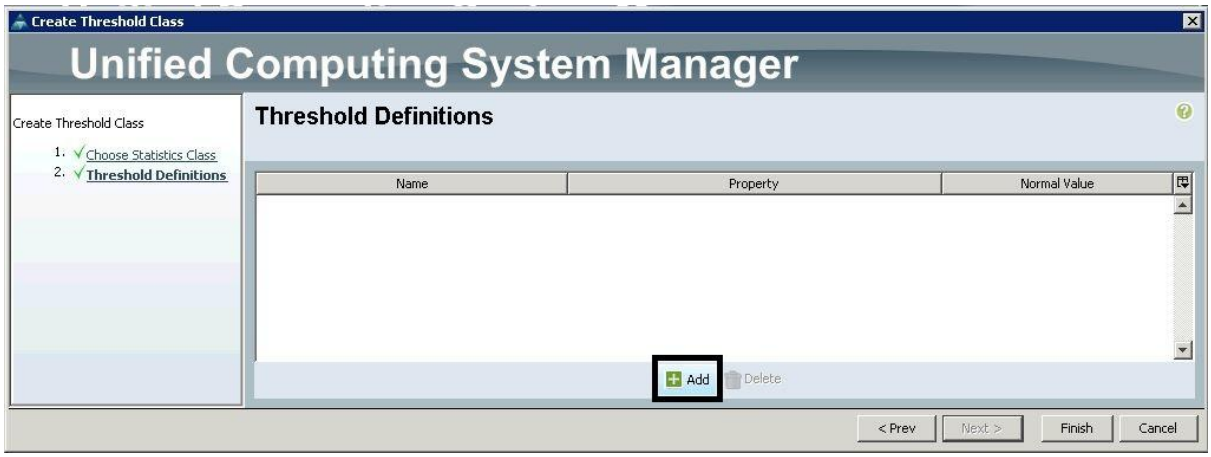


Step 10: Choose the **mb-power-stats** class and click **Next.**

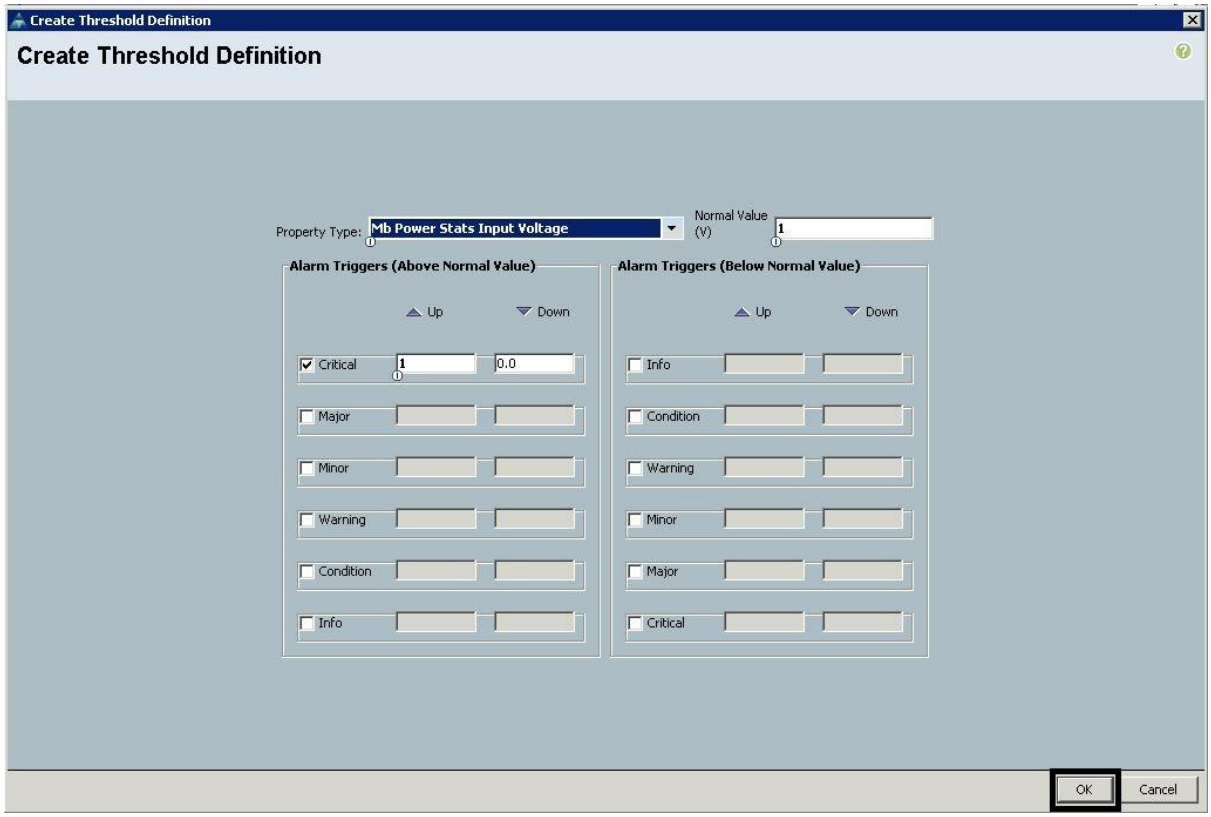


Note: This example will be creating a threshold policy with artificially low thresholds to ensure that it triggers and provides output for the student to review. The values in this example should not be considered reasonable in a production environment.

Step 11: Click **Add** to add threshold definition to your policy.

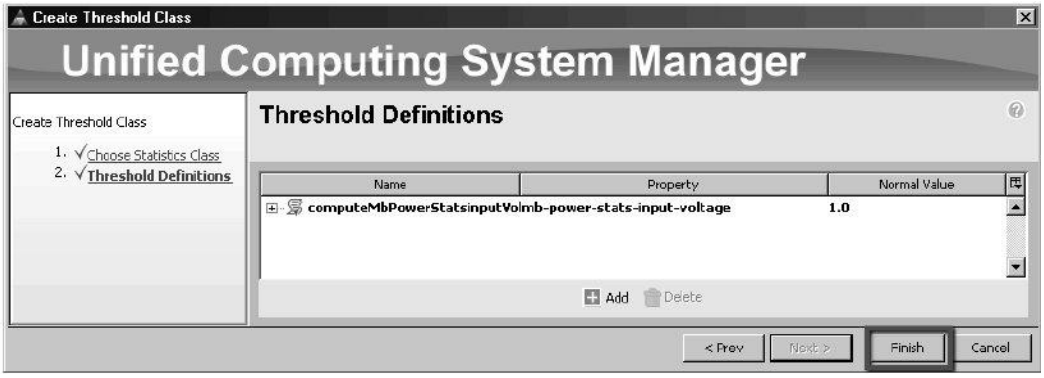


Step 12: Set the Property Type field to **mb-power-stats-input-voltage.** Set the normal value at **1.** Define a Critical trigger in the Up direction of **2.** Click **OK.**

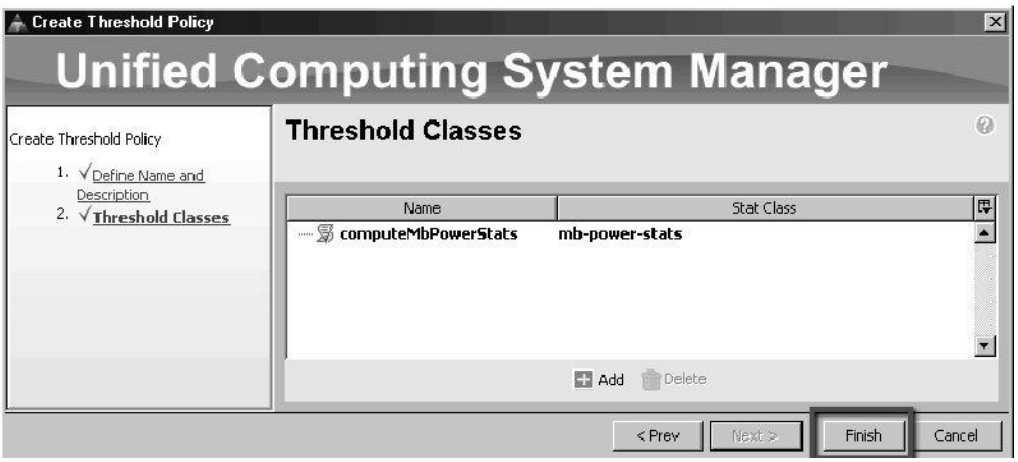


Note: This definition establishes the expected input voltage at 1 volt. Further, it defines a Critical fault if the input voltage is 1 volt higher than normal (2 volts). Because the normal input voltage to a Cisco UCS motherboard is 12 volts, this will always be triggered allowing us to see the effects of a match.

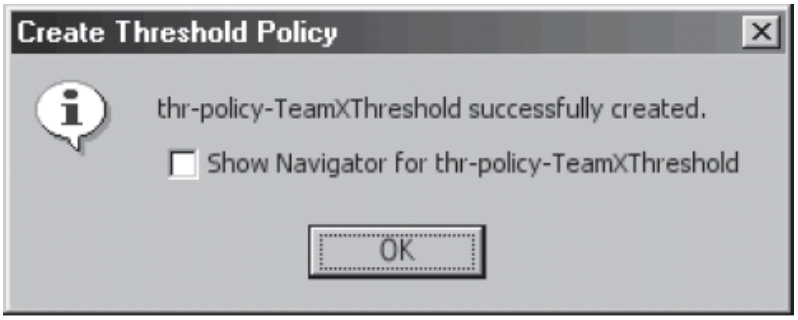
Step 13: Verify that your definition has been added to the table. Click **Finish.**



Step 14: Click **Finish.**

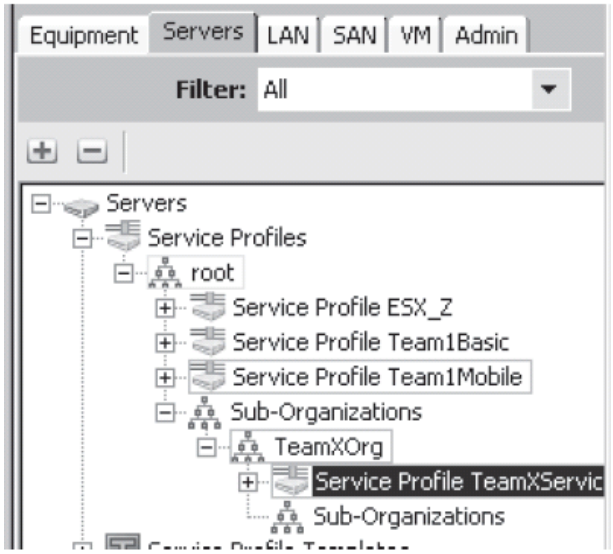


Step 15: Click **OK** to confirm creation of the threshold policy.

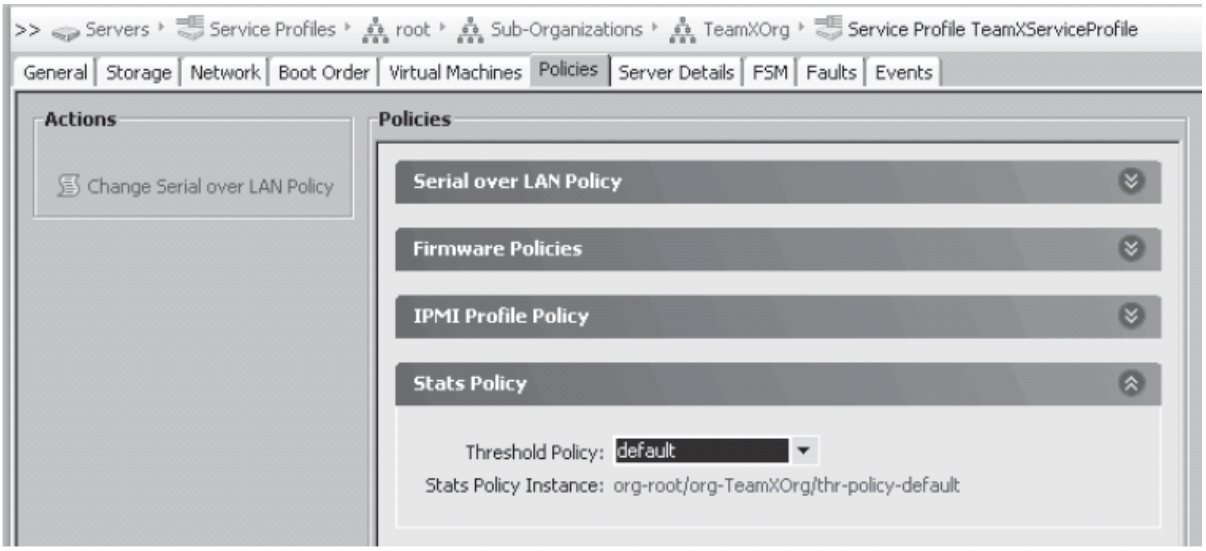


Step 16: *Be sure that you create your service profile under your team's organization that was created in this task.* Create a simple service profile by using any method that you prefer (template, simplified wizard, and expert wizard) and deploy it to your team server. The service profile need not be complex; in fact, no vNICs or vHBAs are required. You simply need a service profile that is deployed to a blade.

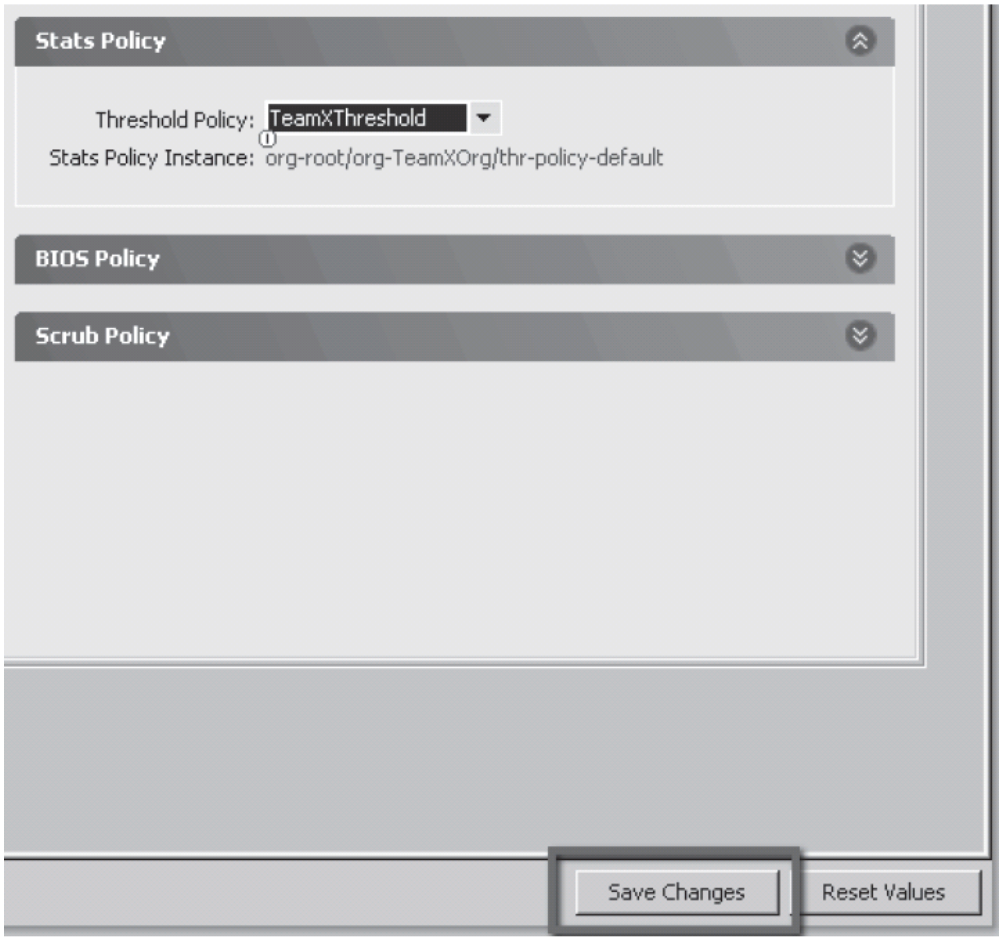
Step 17: In the navigation pane, choose the **Servers** tab and navigate to your team Service Profile.



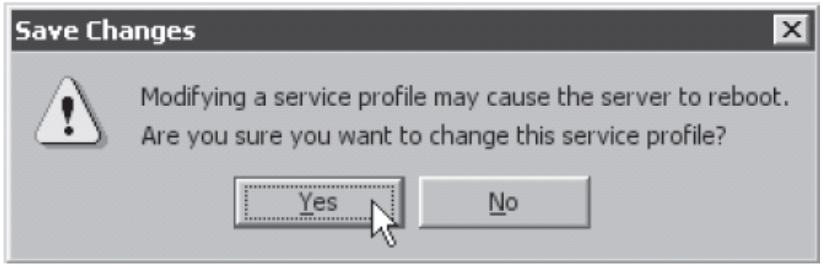
Step 18: In the content pane, choose the **Policies** tab and expand the **Stats Policy** section.



Step 19: Choose your team threshold policy from the choices, and then click **Save Changes.**



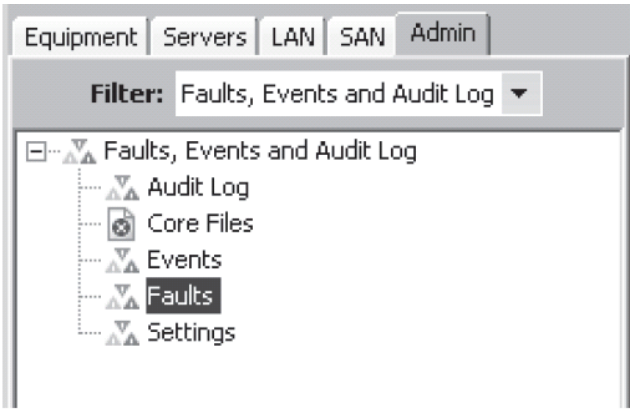
Step 20: If you receive a warning as shown here, click **Yes.**



Note: Some modifications to service policies will cause the service profile to reboot; however, modifying the threshold policy selection will not.

Step 21: Click **OK** to confirm the modification to the service profile.

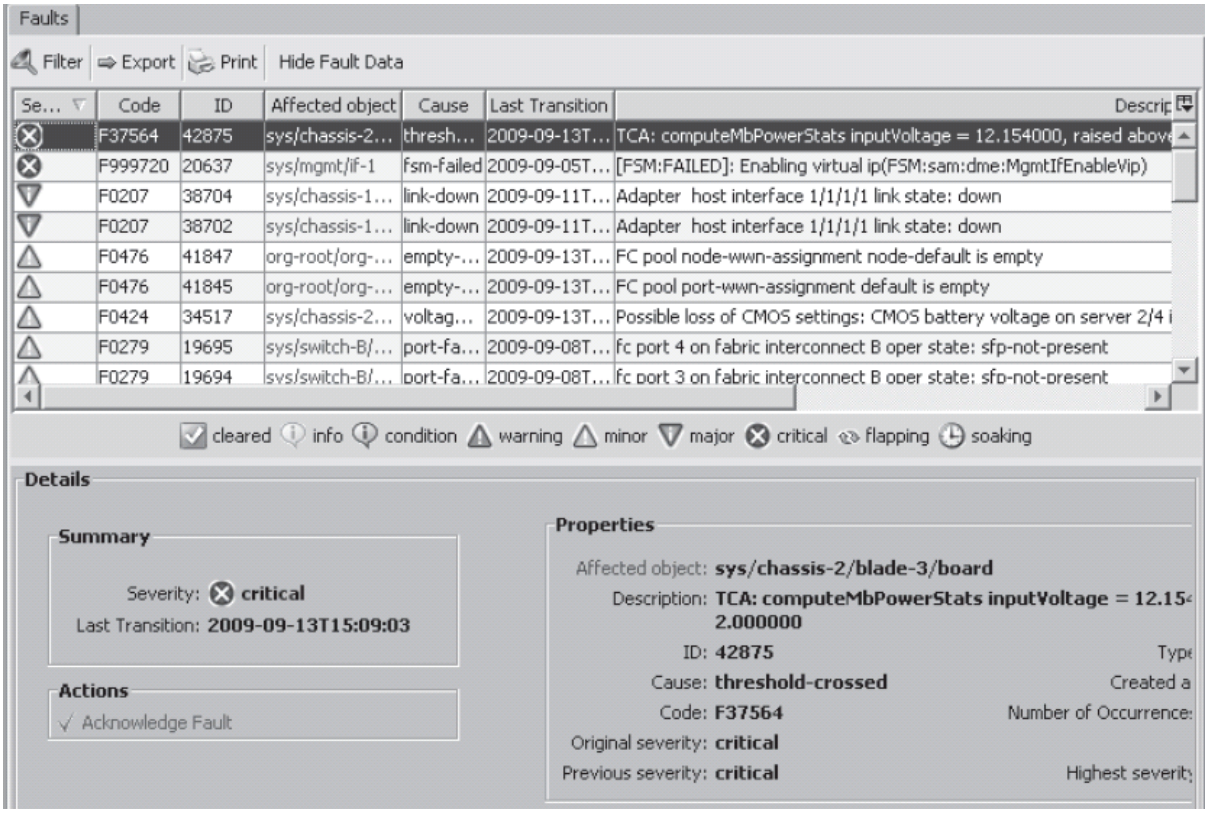
Step 22: Change the Filter field to **Faults, Events, and Audit Log** and choose the **Faults** icon.



Step 23: In the content pane, click the **Severity** column so that faults are sorted by severity. Scroll through the list until the Critical faults (a red circle with a white X) are visible.

Step 24: Due to the reporting interval, it may take up to 30 minutes for the fault to be reported in this screen. You can continue with the remainder of the tasks in this lab, returning periodically to check for your blade to report the fault.

Step 25: When your blade has reported a fault that is based on your threshold policy, you have completed this task.



Task 2: Explore Call Home Configuration

In this task, you will configure the Call Home feature.

Activity Procedure

Complete these steps:

Step 1: Login to 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 Services** for the following steps. Choose the **Call Home** icon.

Step 3: In the content pane, check to see the Admin state is **Off.**

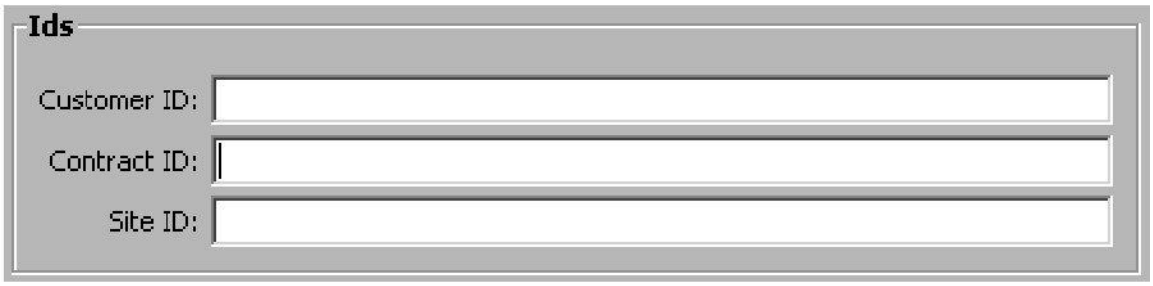
Note:	It is possible that the Admin state will be on if another student has enabled it and saved the configuration. If so, simply skip the next step.

Step 4: Change the Admin state to **On.**

Step 5: Experiment with various values in the Contact Information fields. Are any fields required? Are any formats enforced?

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 "+" and followed by a country code. The Email field enforces only very loose checking of two alphanumeric values separated by the @ symbol.

Step 6: Experiment with various values in the IDs fields. Are any fields required? Are any formats enforced?



Note: All fields in the IDs section are optional. These values will be included in any Call Home messages.

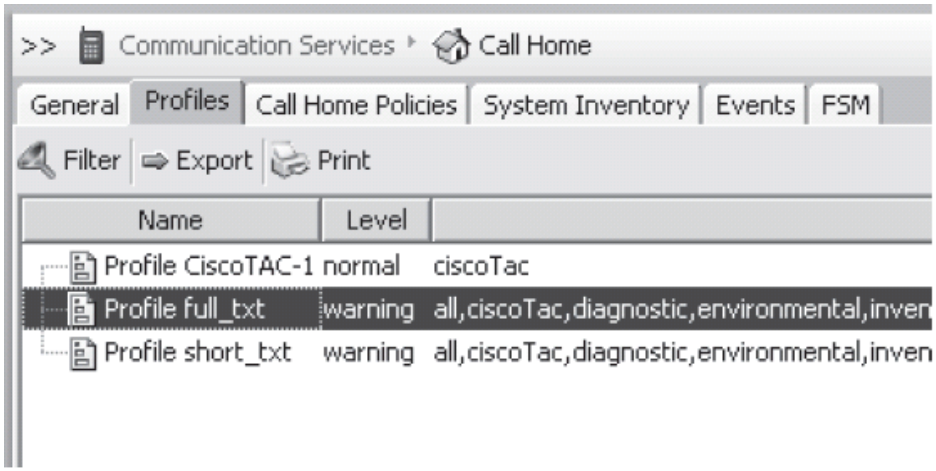
Step 7: Experiment with various values in the Email Addresses fields. Are any fields required? Are any formats enforced?

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 or "bounced" Call Home messages.

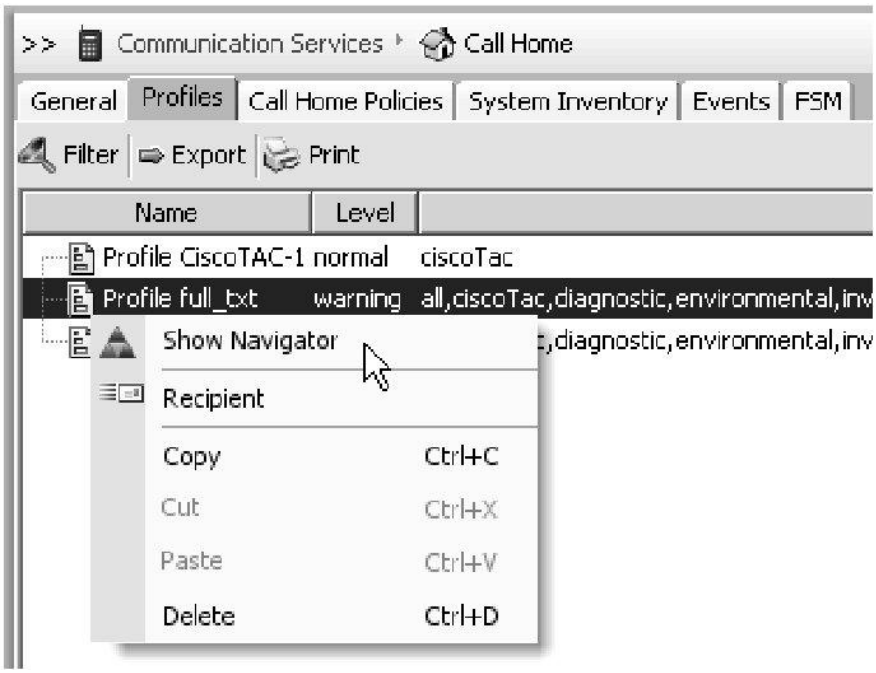
Step 8: Review the options available in the SMTP Server section.

Step 9: Do not save the Call Home configuration. As the lab is a shared environment, each student will review the settings but not save them. Return the Admin state to **Off.**

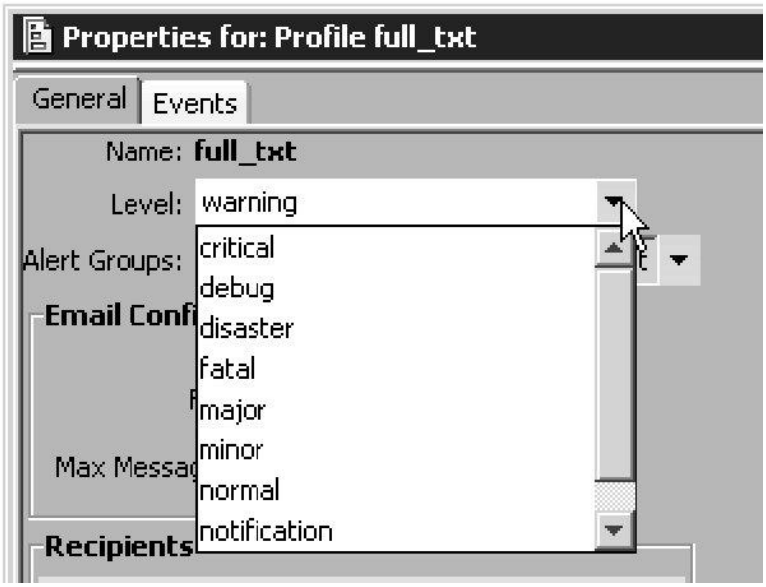
Step 10: In the content pane, choose the **Profiles** tab, and click the **full_txt** profile.



Step 11: Right-click the **full_txt** profile and choose **Show Navigator.**

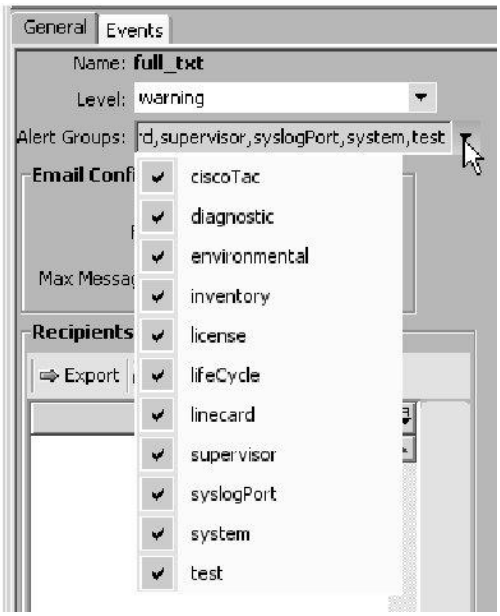


Step 12: Take a moment to review the message levels available. This setting dictates that all messages of the selected level and above (meaning more severe) will be sent to recipients of this profile.

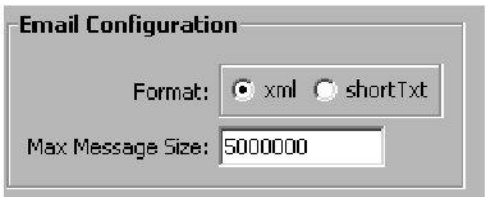


Note: The levels in this field are listed alphabetically, not by severity. The actual severity order, from least severe to most severe, is debug, notification, normal, warning, minor, major, critical, fatal, disaster.

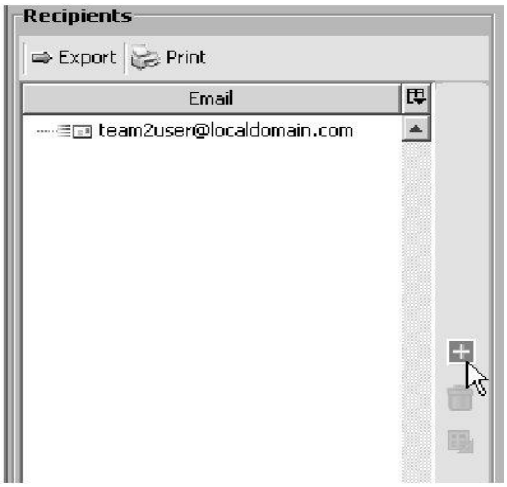
Step 13: Take a moment to review the Alert Groups that are available. This setting dictates which category of messages will trigger this profile.



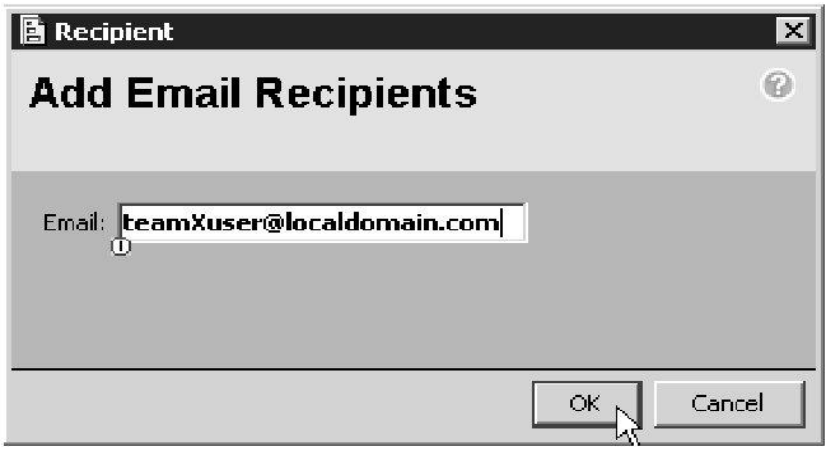
Step 14: Review the Email Configuration section. This section allows you to choose the format of messages that are sent to recipients of this profile, as well as set a maximum message size (in bytes). Any data above this size will be truncated.



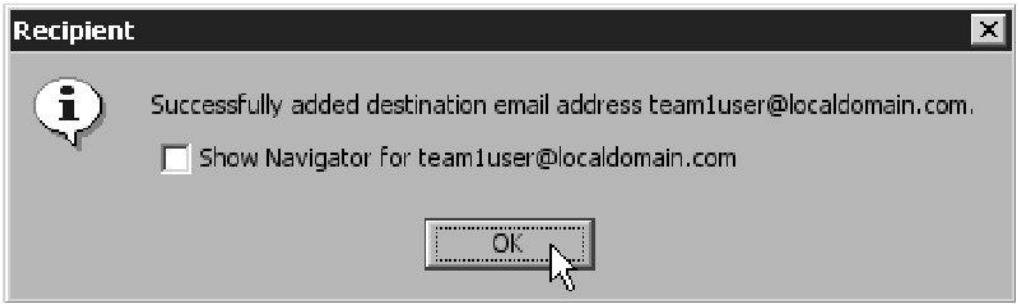
Step 15: The recipients section may already have users from other teams. Click the "+" button to add a recipient to this profile.



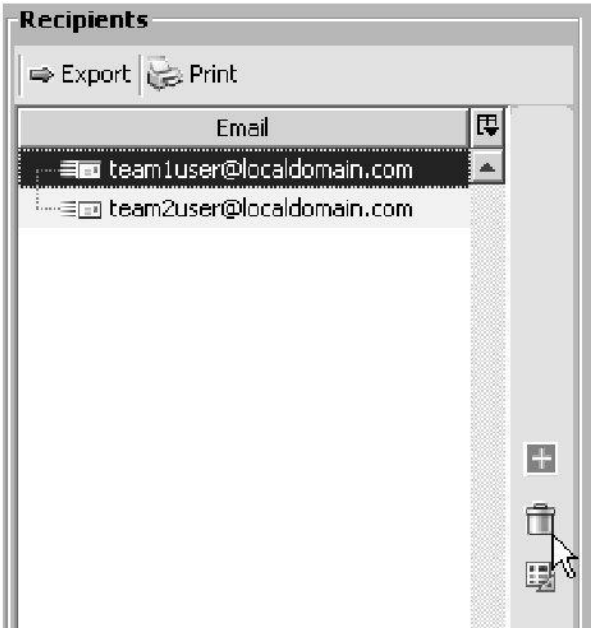
Step 16: Add a recipient of your choosing. The address that you specify does not matter as long as it passes the syntax checking of Cisco UCS Manager. Click **OK.**



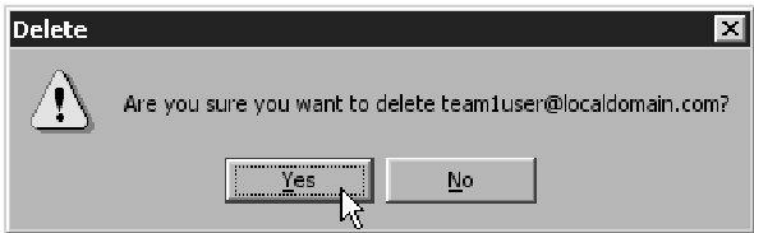
Step 17: Click **OK** to confirm creation of the recipient.



Step 18: Optionally, delete the recipient that you created. Highlight the recipient that you created and click the **trashcan** icon.

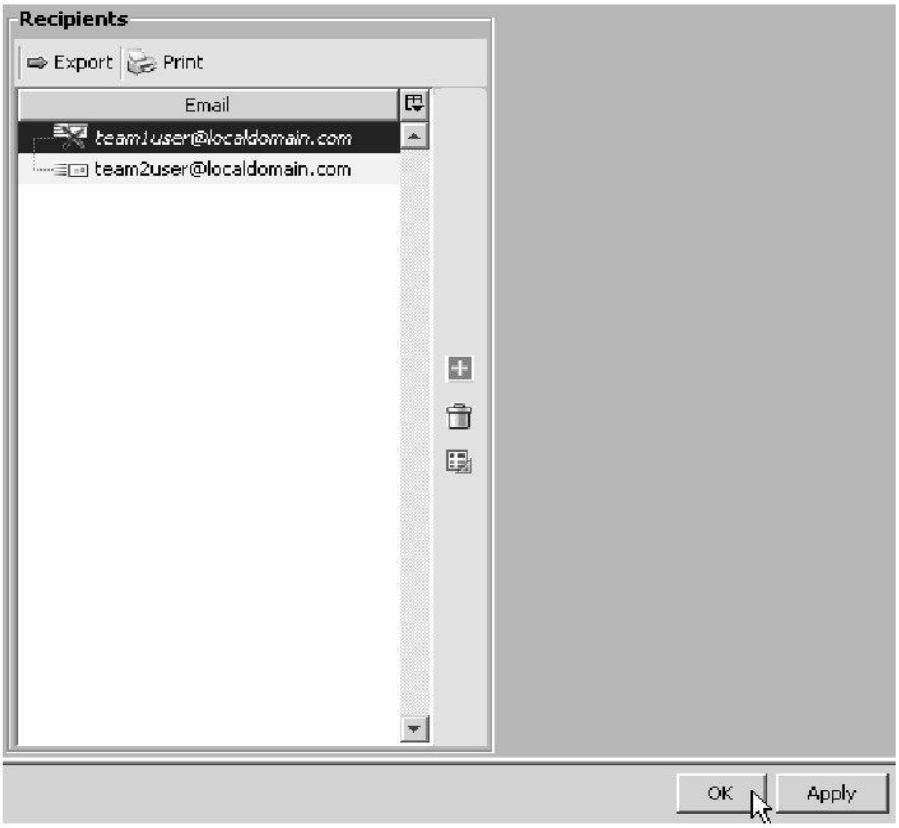


Step 19: Click **Yes** to delete the recipient.



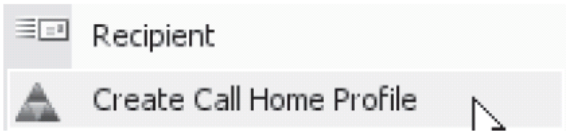
Step 20: Note that the recipient is not immediately removed from the list. The recipient line in the table will be grayed out and italicized, indicating that it will be removed.

Step 21: Click **OK** to complete removal of the user and close the properties window.

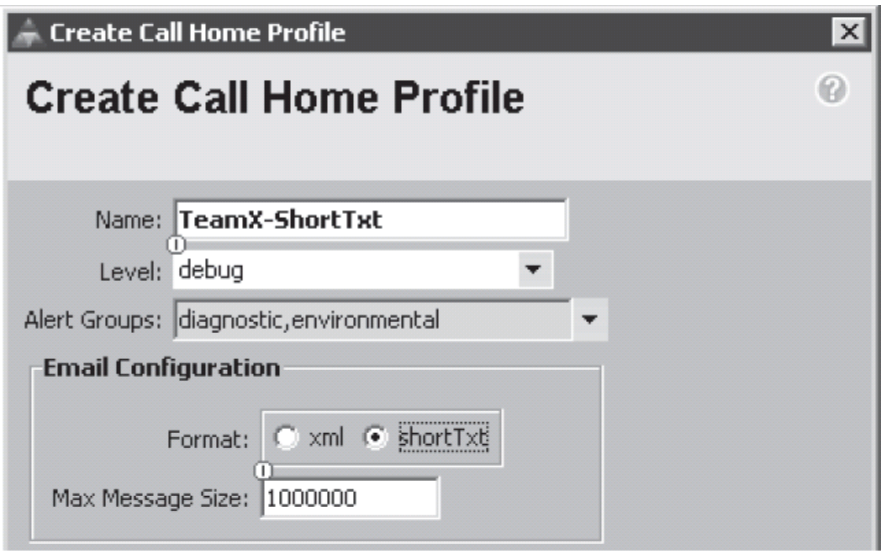


Step 22: Click the “+” button to add a new Call Home profile.

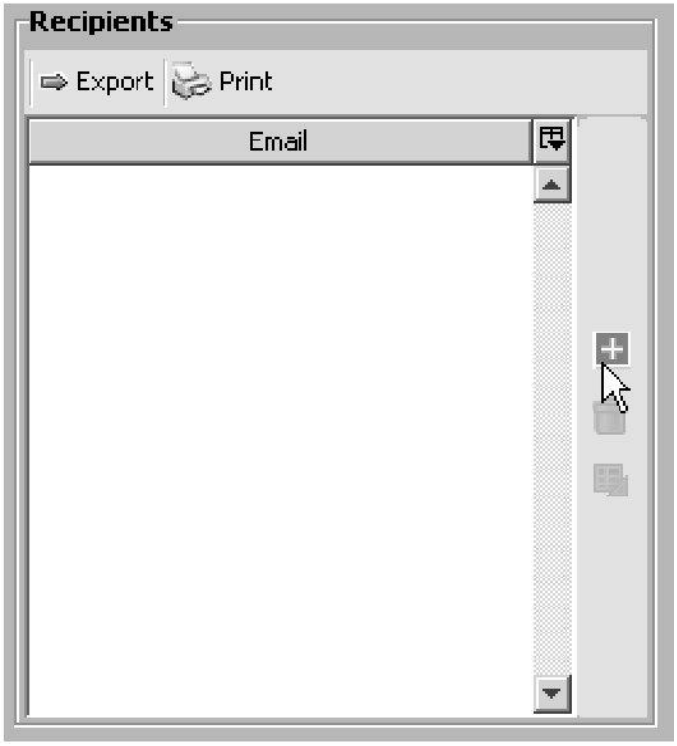
Step 23: Click Create Call Home Profile.



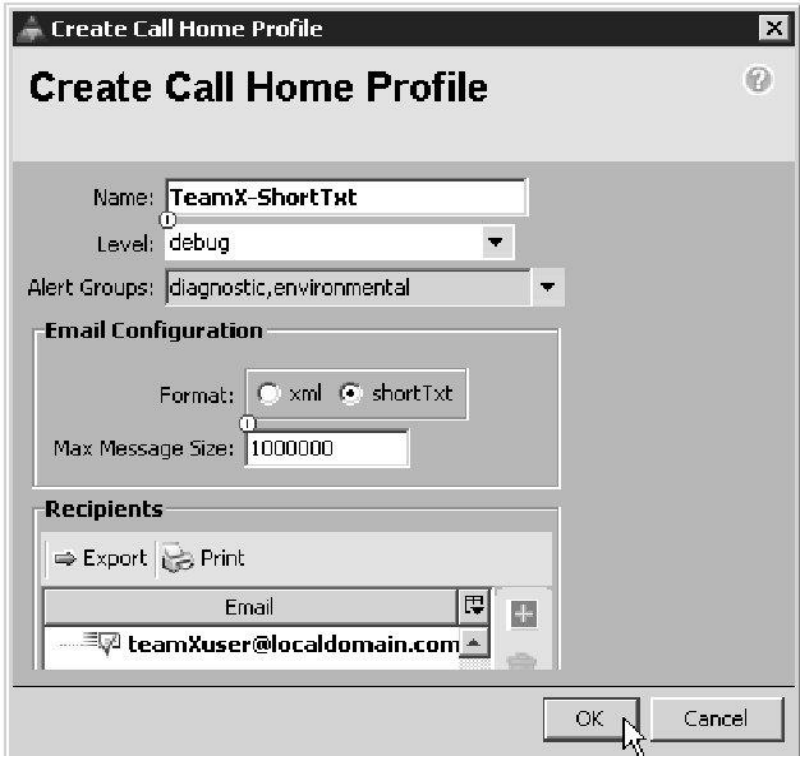
Step 24: Name your profile **TeamX-ShortTxt,** replacing X with your team number. Set the Level and Alert Groups fields to any values that you wish. Set the Format to **shortTxt** and leave the Max Message Size value at default.



Step 25: Add a recipient in the same manner as you did in the earlier steps.

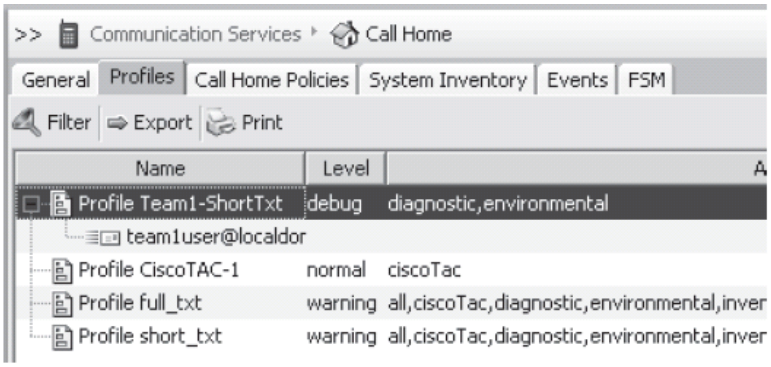


Step 26: Click **OK** to save your Call Home profile.

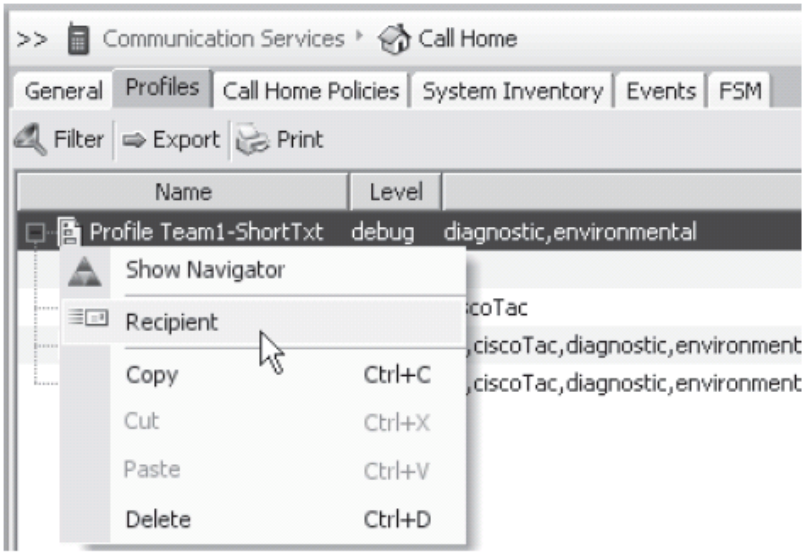


Step 27: Click **OK** to confirm creation of your profile.

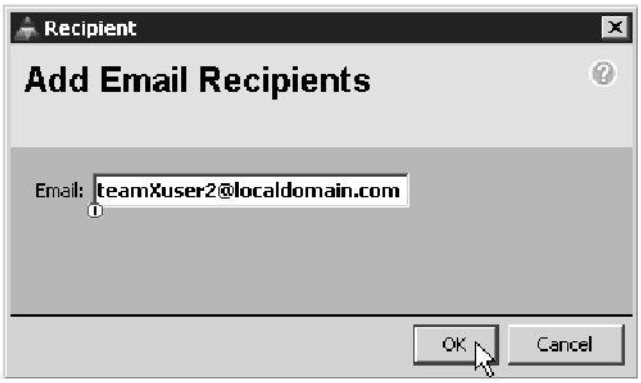
Step 28: Expand your profile icon and verify that the recipient that you configured is listed.



Step 29: Right-click your profile icon and choose **Recipient.**

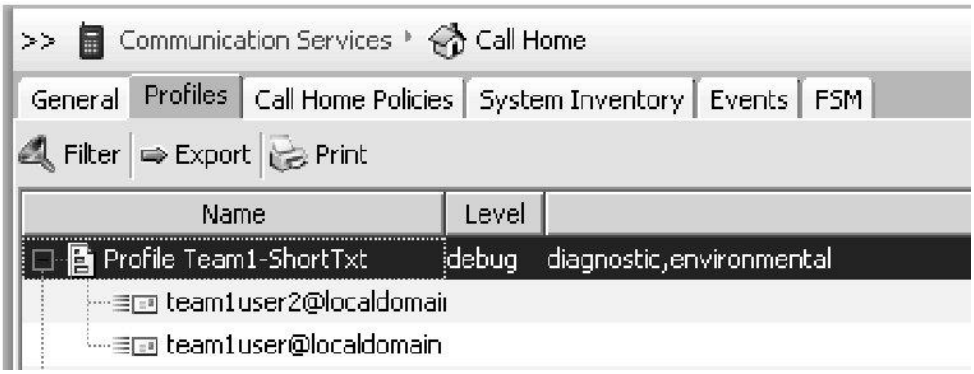


Step 30: Provide another, different recipient address to create another recipient under this profile.



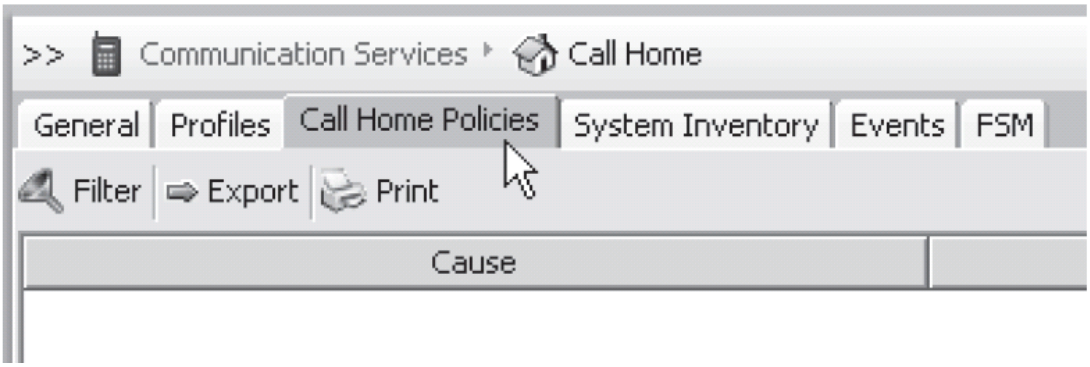
Step 31: Click **OK** to confirm addition of the recipient.

Step 32: Verify that both recipients now appear under your team's profile icon.

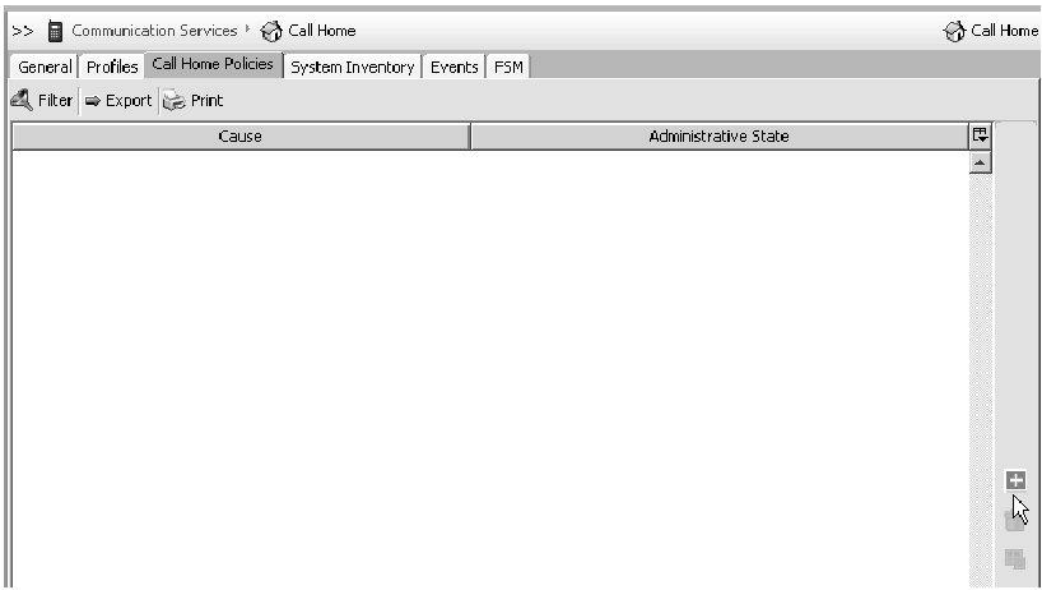


Note: Recipients can be added in this manner or through the profile properties window. Both accomplish the same result, but this method provides a quick and easy way to add recipients to a profile.

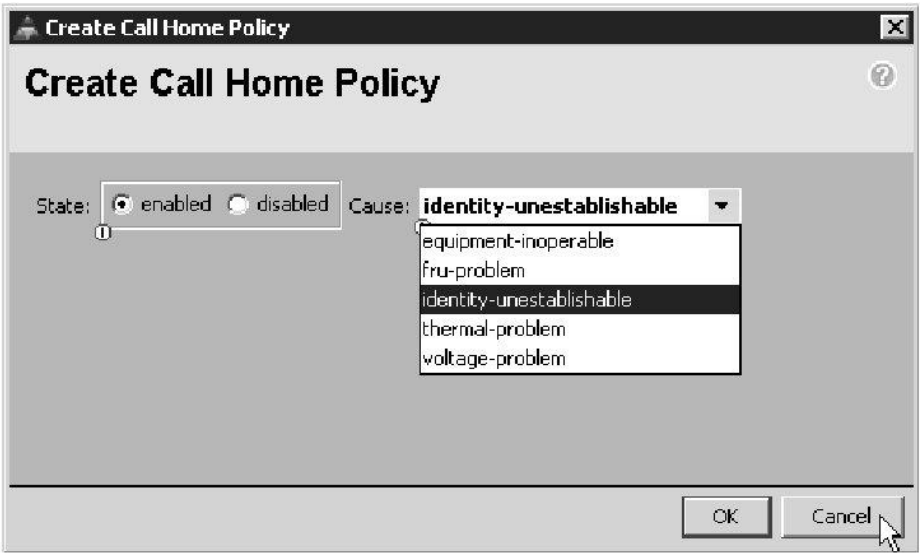
Step 33: In the content pane, click the **Call Home Policies** tab.



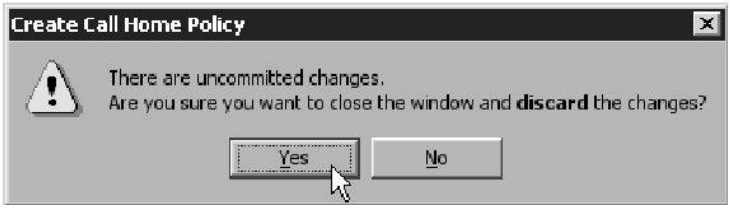
Step 34: Click the "+" button to add a new Call Home Policy.



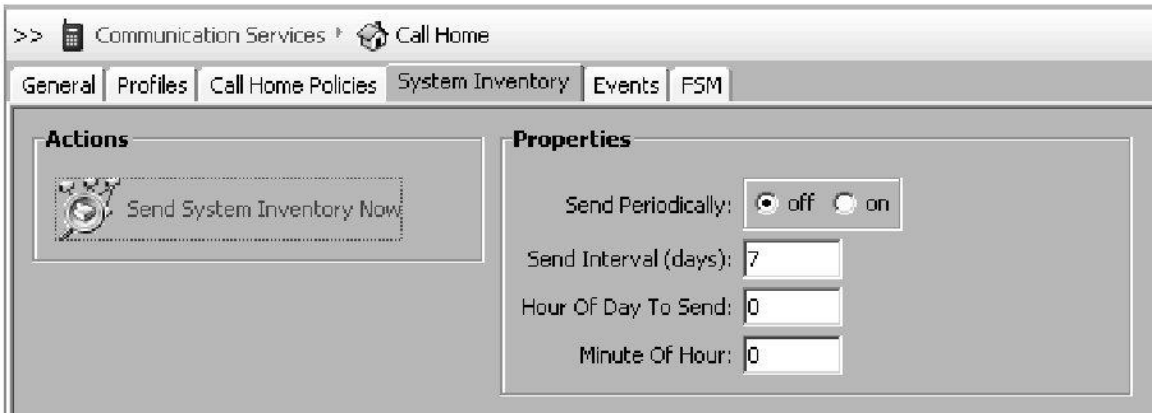
Step 35: Explore the options for creating a new Call Home Policy. When you have reviewed the options available, click **Cancel.** Only one of each policy can be created. As the lab is a shared environment, if multiple teams attempt to create the same policy, errors might occur.



Step 36: If you receive a warning regarding committed changes, click **Yes** to confirm discarding the changes.



Step 37: 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 UCS 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 3: Configure External Logging

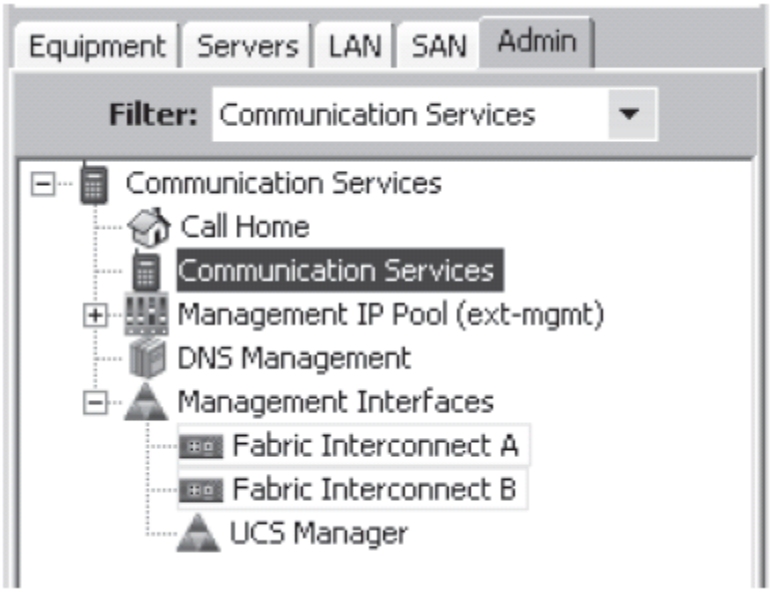
In this task, you will configure options for remote logging.

Activity Procedure

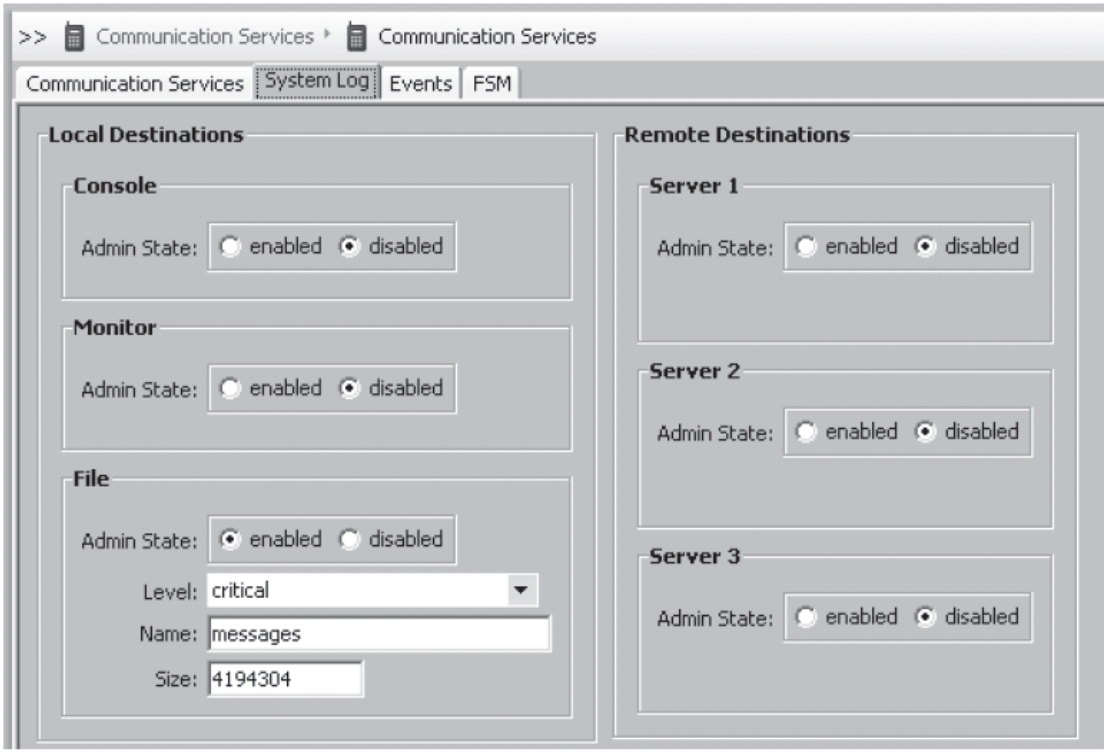
Complete these steps:

Step 1: Log into Cisco UCS Manager if necessary.

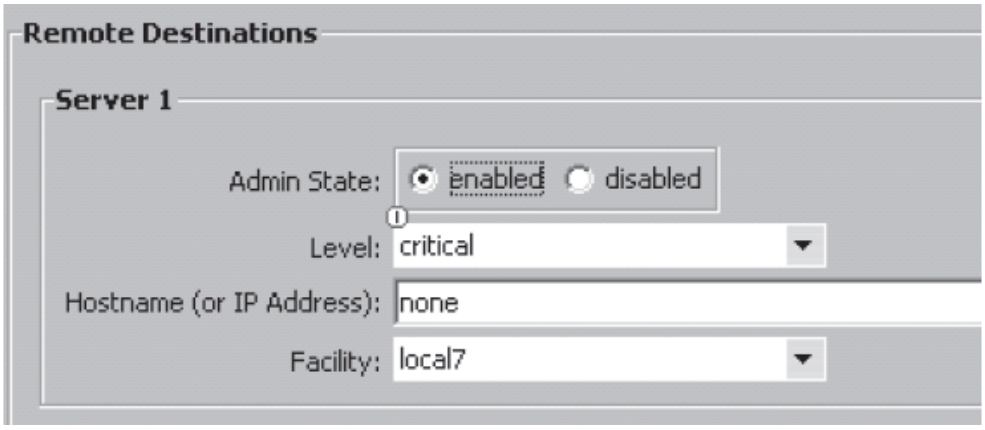
Step 2: Choose the **Admin** tab in the navigation pane. It may be helpful to change the **Filter** field to **Communication Services** for the following steps. Choose the **Communication Services** sub icon.



Step 3: In the content pane, choose the System Log tab. Review the options available for logging.



Step 4: In the Remote Destinations section, click the **Enabled** radio button for one of the servers. Review the settings available for a remote syslog server.



Note: The Level value specifies which severity of messages and above will be sent to the remote syslog server. The Hostname value specifies the remote syslog server. The Facility value specifies which syslog "facility" the remote syslog server will use to categorize the messages of this Cisco UCS deployment. The administrator of the syslog server will likely specify which facility value to use.

Step 5: Return the Admin state of your chosen remote server to **disabled.**

Task 4: Export Events and Faults

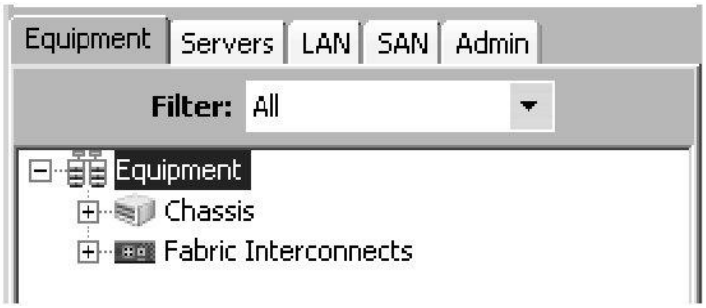
In this task, you will export event and fault data from Cisco UCS Manager.

Activity Procedure

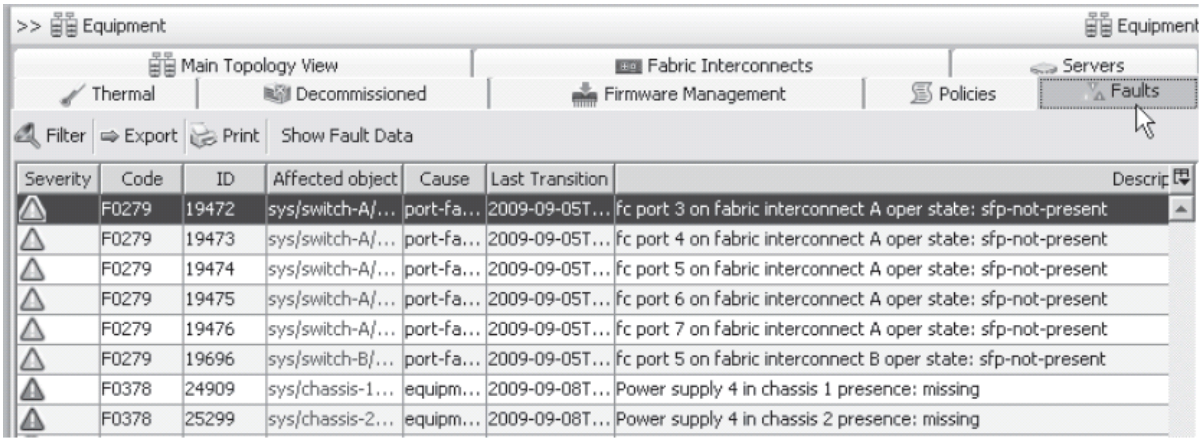
Complete these steps:

Step 1: Log into Cisco UCS Manager if necessary.

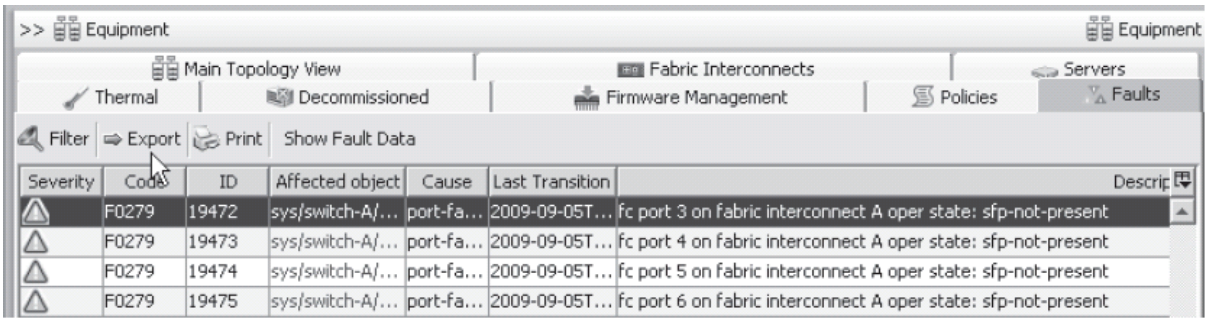
Step 2: Choose the **Equipment** tab in the navigation pane.



Step 3: In the content pane, choose the **Faults** tab.

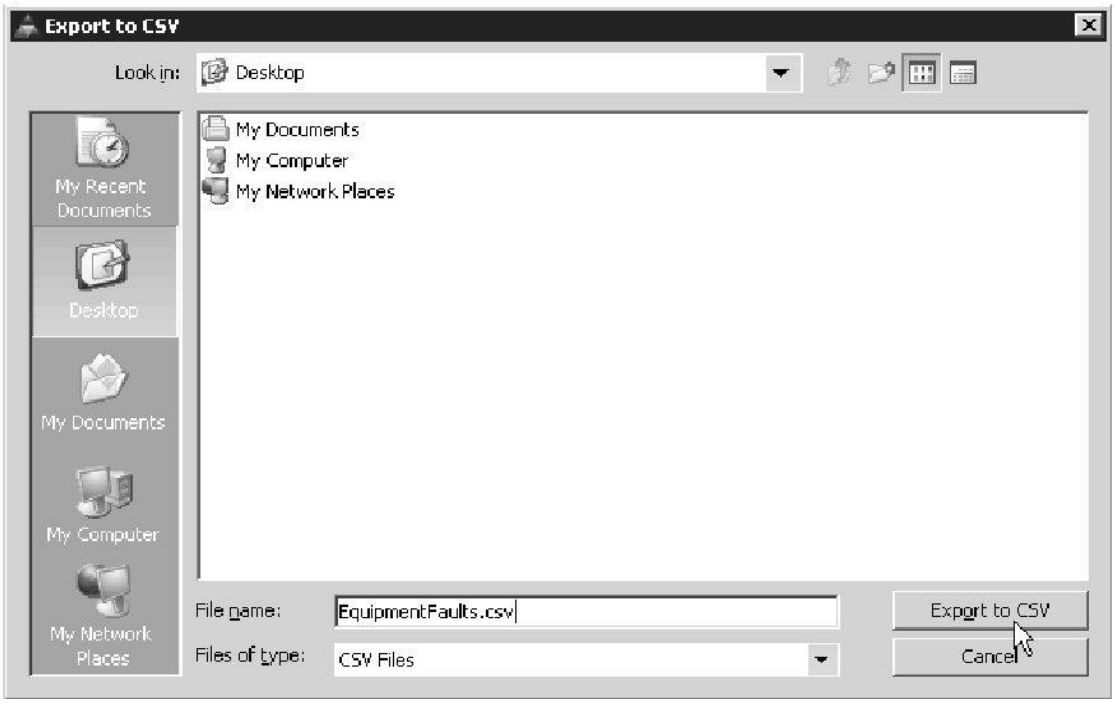


Step 4: Click **Export.**

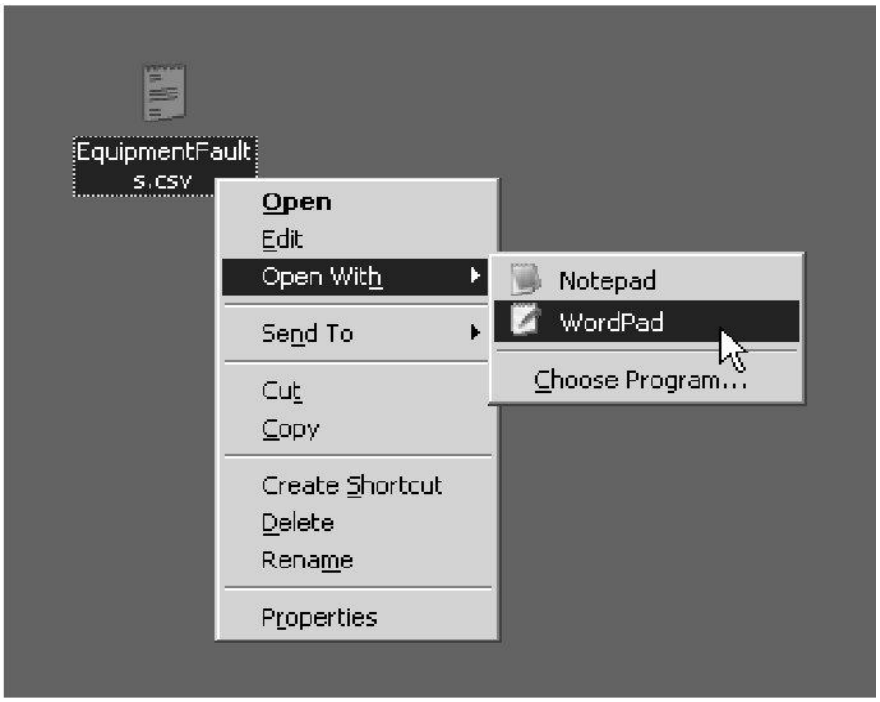


Note: Virtually any table of data in Cisco UCS Manager can be exported in this manner. This exercise is exporting Fault data just as an example.

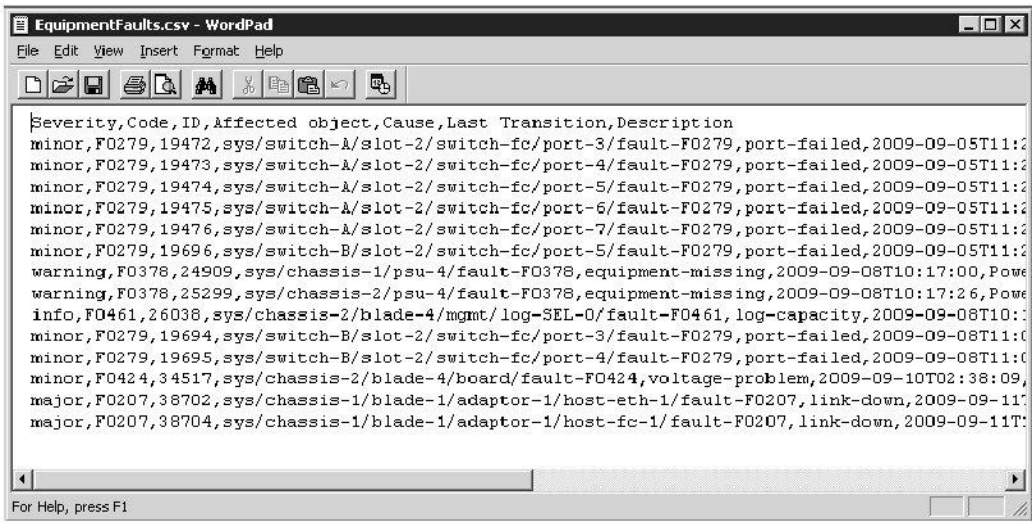
Step 5: Choose the **Desktop** icon in the left navigation pane, name the file **EquipmentFaults.csv,** and click **Export to CSV.**



Step 6: Minimize the Cisco UCS Manager windows and find the file that you created on the desktop. Right-click the file and choose **Open With** and **WordPad.**



Step 7: Spend a few minutes reviewing the content of the file. Note that the first line contains the key to the values.



Note: Reviewing a CSV file in WordPad is not generally very useful. Typically, this data would be imported into Excel or an analysis tool for further manipulation.

Step 8: When you have completed reviewing the contents of the exported data, close the WordPad window. Delete the export file by dragging it to the Recycle Bin on the desktop.

Step 9: Explore some of the other tables of data within Cisco UCS Manager and try exporting and reviewing them by using the same process. Some useful examples would include the Installed Firmware tab under Equipment and Firmware Management; the Audit Log under Faults, Events; and Audit Log in the Admin tab.

Lab 9-1: Installing ESXi and vCenter Server

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

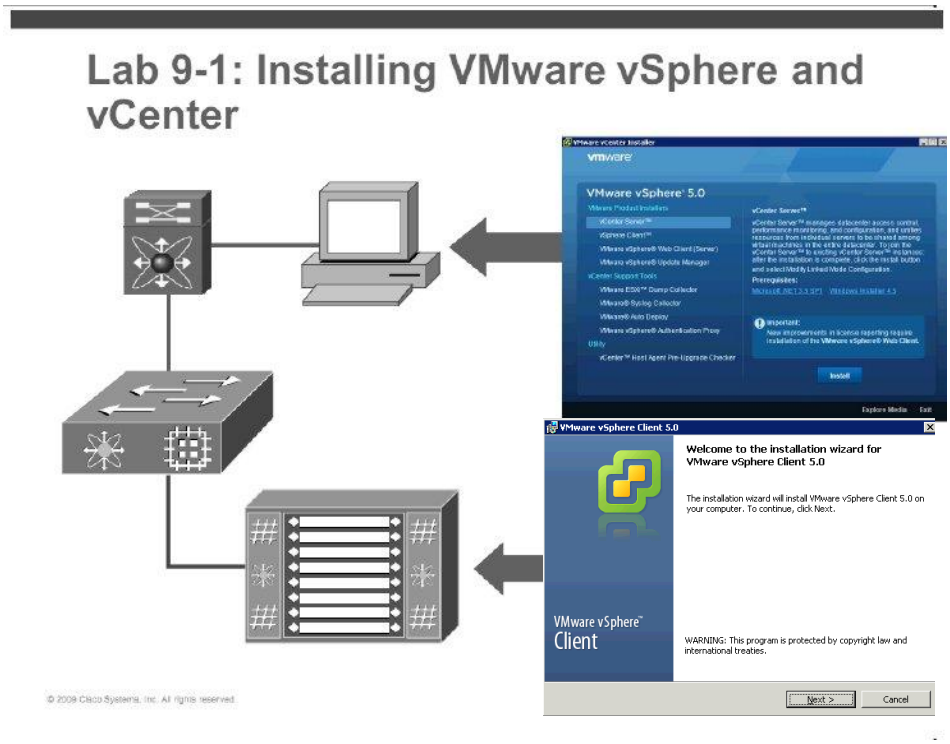
Activity Objective

In this activity, you will install VMware ESXi 5.0 on a Cisco UCS blade server. You will then install vCenter on your student desktop and configure it to manage your ESX host. After performing this lab, you should be able to:

- Demonstrate the process for creating a service profile
- Install vSphere 5.0 on your team's service profile
- Install vCenter on your student desktop to manage your ESX 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:

- Configured Cisco UCS environment
- Student desktop with network access and VMware vSphere client
- VMware ESXi 5.0 ISO image
- VMware vCenter installation media

Task 1: Install VSphere Client & Vcenter Server

In the task, you will do a default installation of v Sphere Client and vCenter Server onto your student desktop.

Activity Procedure

Complete these steps:

Step 1: From your desktop computer, launch D:\Autorun.exe

Step 2: For every option, accept the defaults.

Step 3: For organization enter UCS.

Step 4: When files start to copy, move on to Task 2.

Task 2: Create a Service Profile

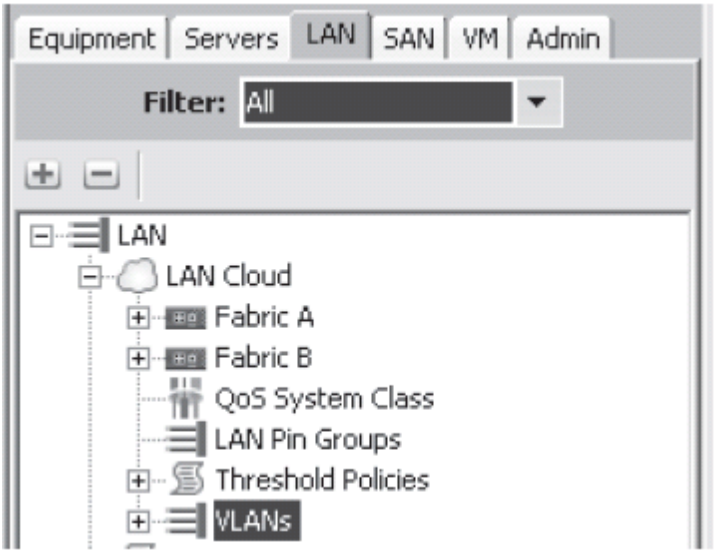
In the task, you will create a service profile to use in your Cisco Nexus 1000V implementation.

Activity Procedure

Complete these steps:

Step 1: Log into Cisco UCS Manager if necessary.

Step 2: In the navigation pane, choose the LAN tab. Drill down to LAN > LAN Cloud > Right-click on VLANs and select “Create VLAN(s)”



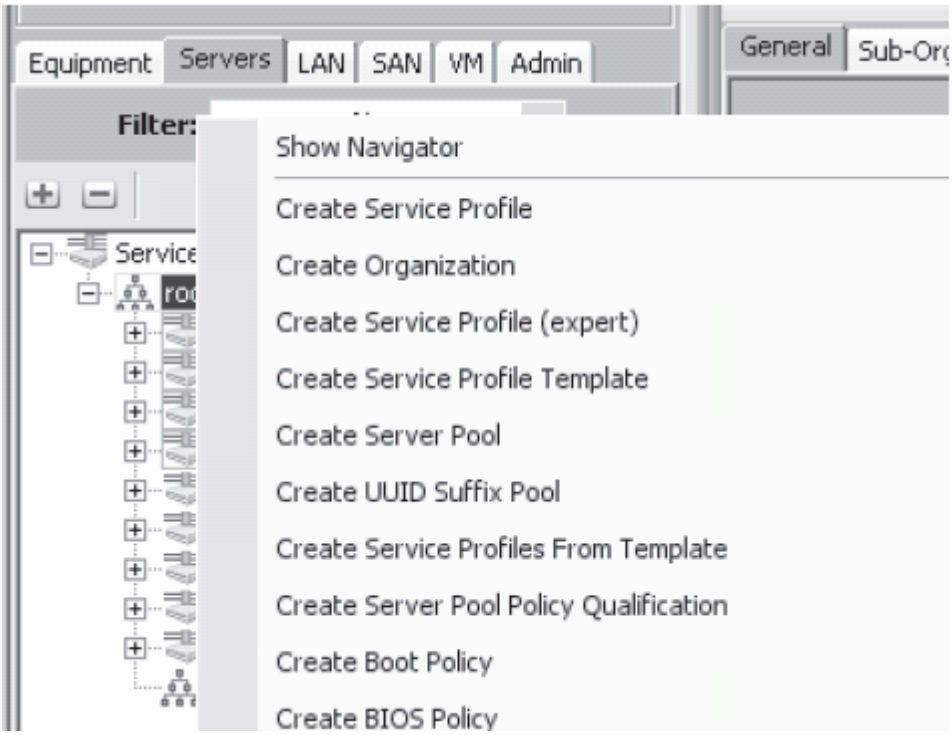
Step 3: Right-click on VLANs to create the following VLANs, (where X is your team number.)

Type	VLAN ID	Name
Management	X0	TeamXMGMTVlan
Control	X1	TeamXCTRLVlan
Packet	X2	TeamXPKTVlan
Data	X3	TeamXDATVlan

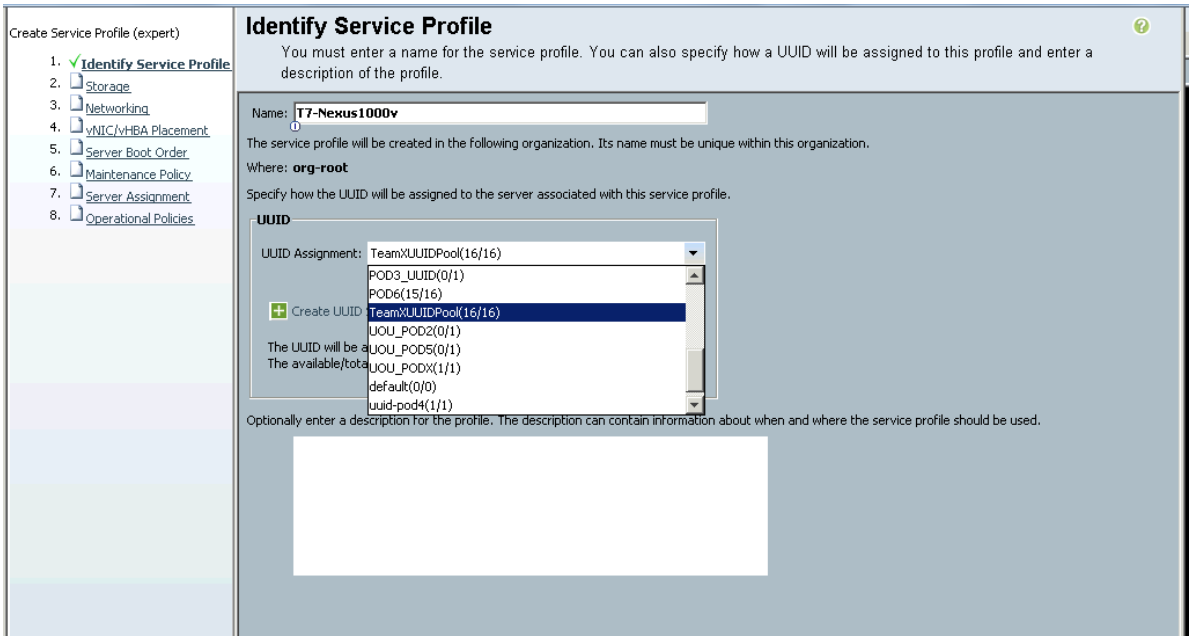
By default, the Cisco Nexus 1000V requires three VLANs for Control, Management and Packet traffic between the VSM and VEMs. In this lab, each team will use VLAN 1 as native / default VLAN.

Step 4: In the navigation pane, choose the Servers tab, and choose the Service Profiles icon. Before creating any new service profiles please delete and disassociate any previous service profiles from the server blade. Once done continue with the exercise.

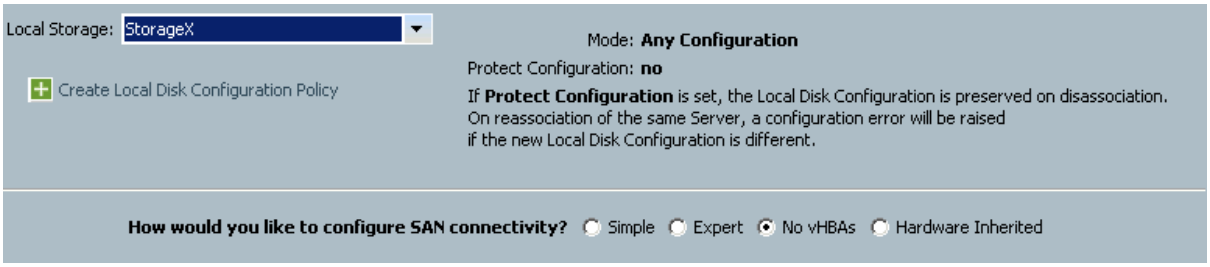
Step 5: Right-click the Service Profiles icon and choose Create Service Profile (expert).



Step 6: Name the profile TX-Nexus1000V. Choose UUID Profile "TeamXUUIDPool" created earlier. Click Next. Wherever necessary replace X with your team number.

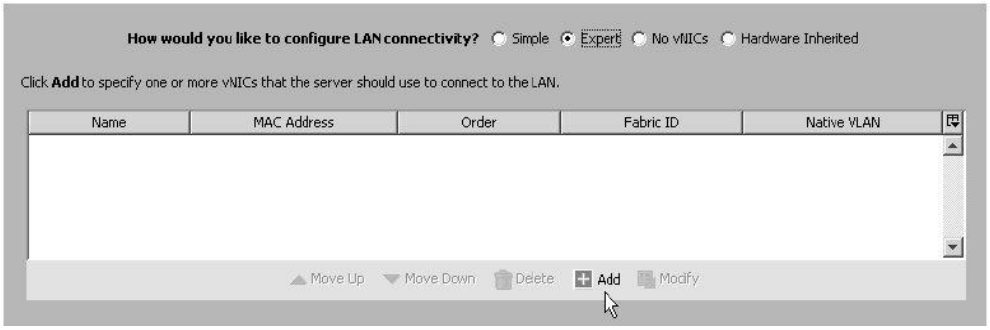


Step 7: Choose Local Storage Profile "StorageX" created from earlier lab and No vHBAs. Click Next.

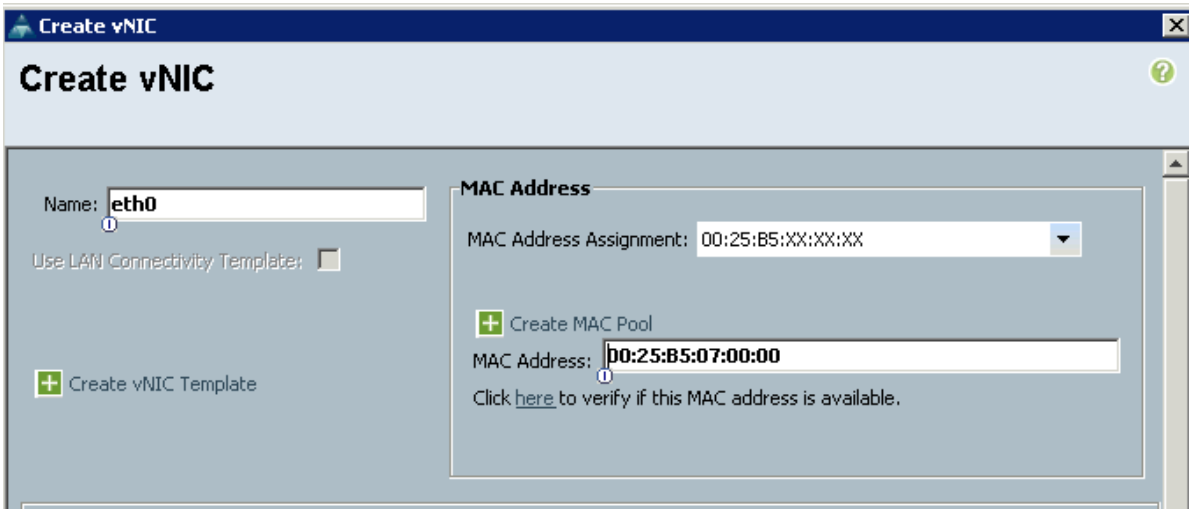


This step is very important to ensure that other lab resources are not disturbed during this exercise.Ensure that No vHBAs is selected.

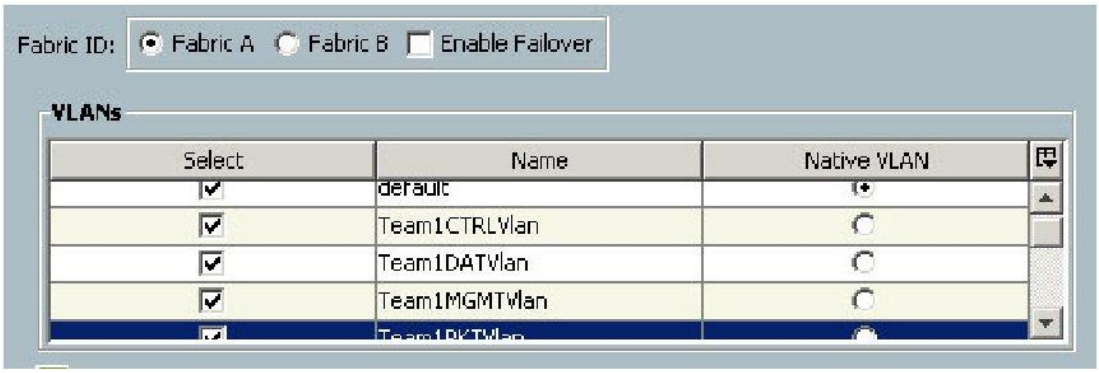
Step 8: From the Networking page, Select the "Expert" radio button and then click Add to add a vNIC to the profile.



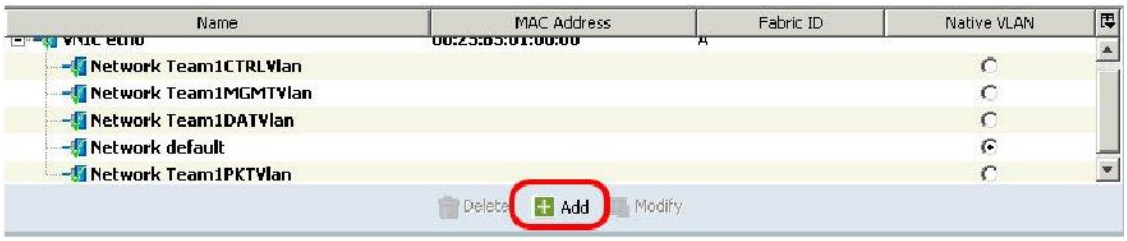
Step 9: Name the vNIC eth0, and choose Manual Using OUI for the MAC Address Assignment. Specify the MAC address of 00:25:B5:0X:00:00, replacing X with your team number.



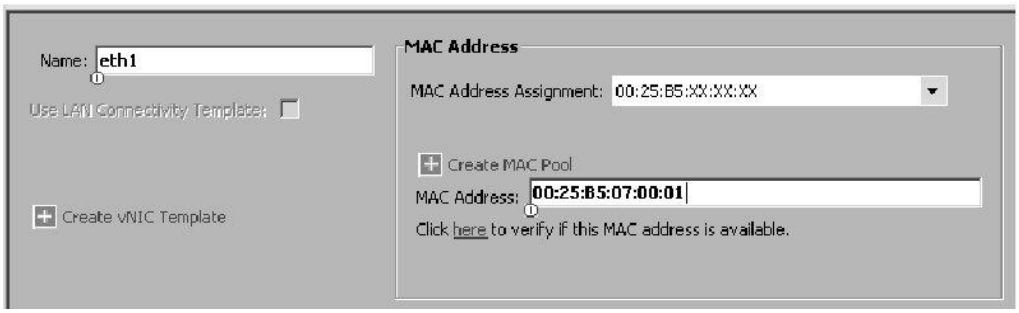
Step 10: Choose Fabric A; select the "VLAN Trunking" Yes radio button; select the default, TeamXCTRLVlan, TeamXMGMTVlan, TeamXPKTVlan, TeamXDATVlan VLAN's that were created in Step 3; do not select a Native VLAN and click OK to continue.



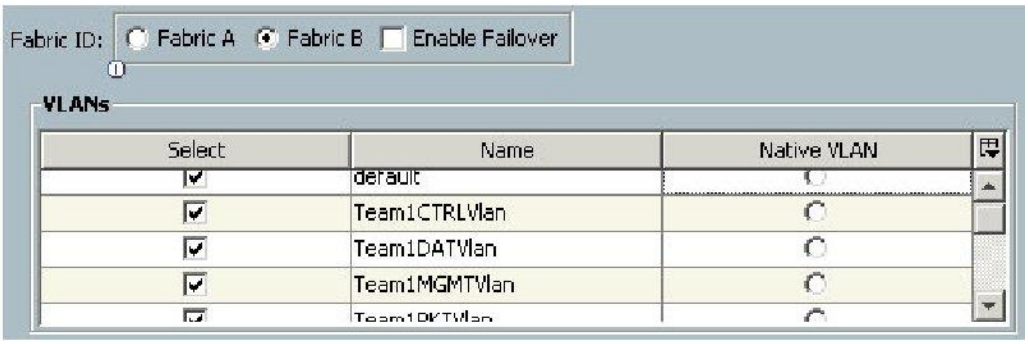
Step 11: From the Networking page, click Add to add another vNIC to the profile.



Step 12: Name the vNIC eth1, and choose Manual Using OUI for the MAC Address Assignment. Specify the MAC address of 00:25:B5:0X:00:01 (where X is your team number.)



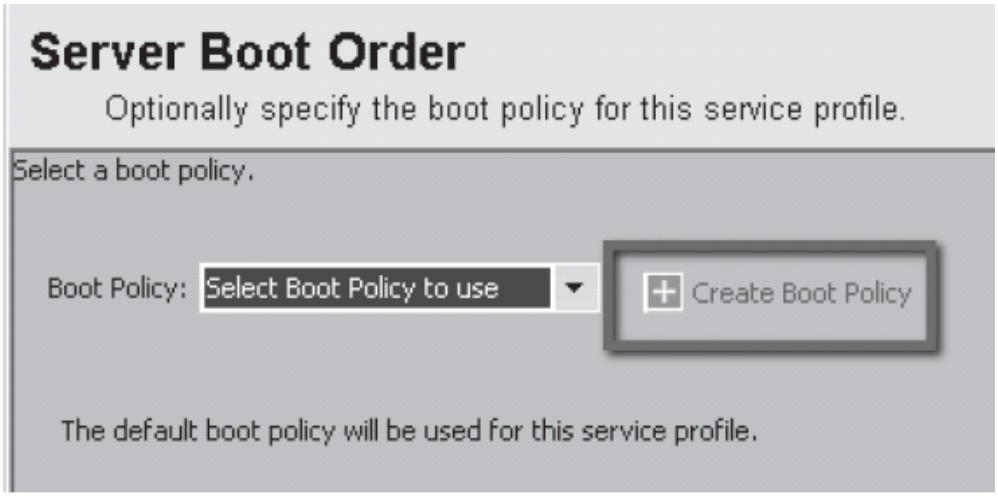
Step 13: Choose Fabric **B;** select the "VLAN Trunking" Yes radio button; select the default TeamXCTRLVlan, TeamXMGMTVlan, TeamXPKTVlan, TeamXDATVlan VLAN's that were created in Step 3; do not select a Native VLAN and click OK to continue.



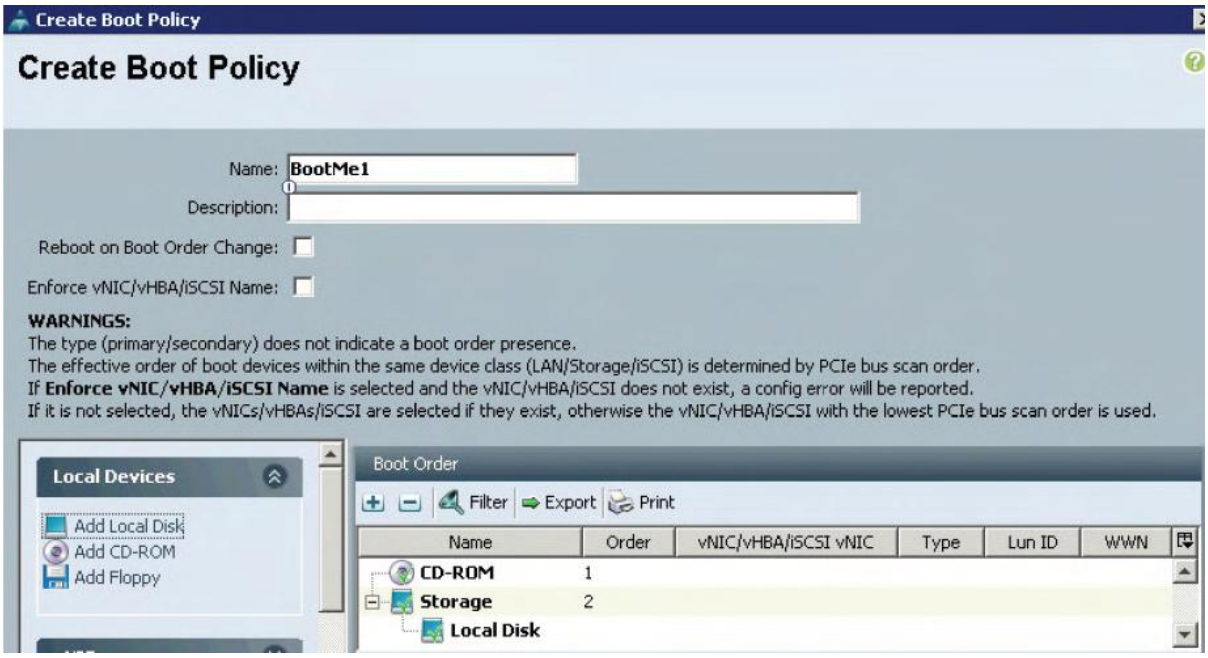
Step 14: On the Networking page, verify that your vNIC configuration is correct and click Next to continue.

Step 15: On the vNIC/vHBA Placement page, leave the default setting and click Next to continue.

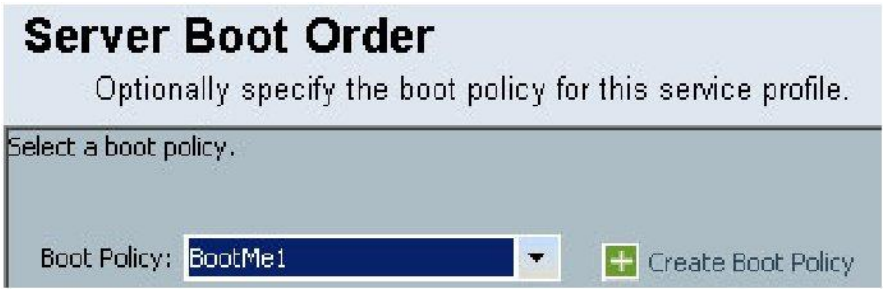
Step 16: On the Server Boot Order page, Click the “Create Boot Policy” link to create and save a Boot Policy



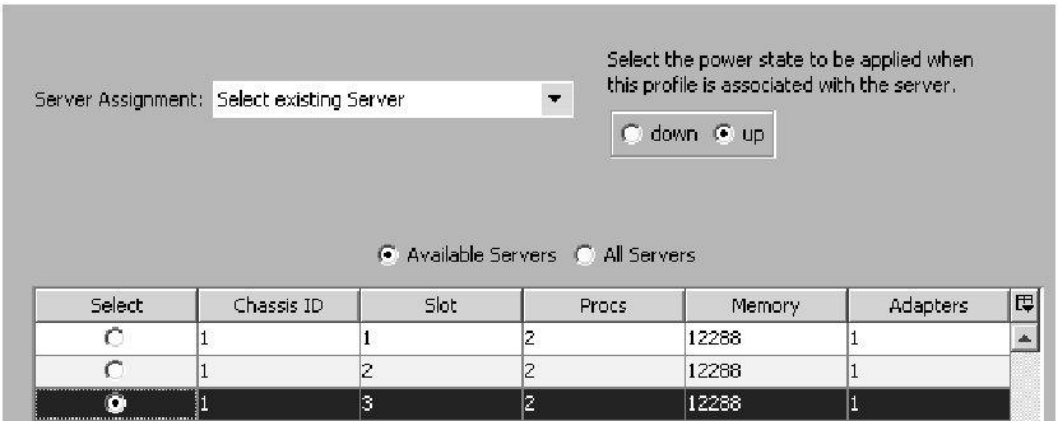
Step 17: Create a Boot Policy named BootMeX (where X is your team name) that consists of the CD-ROM and Local Disk objects and click OK to save it.



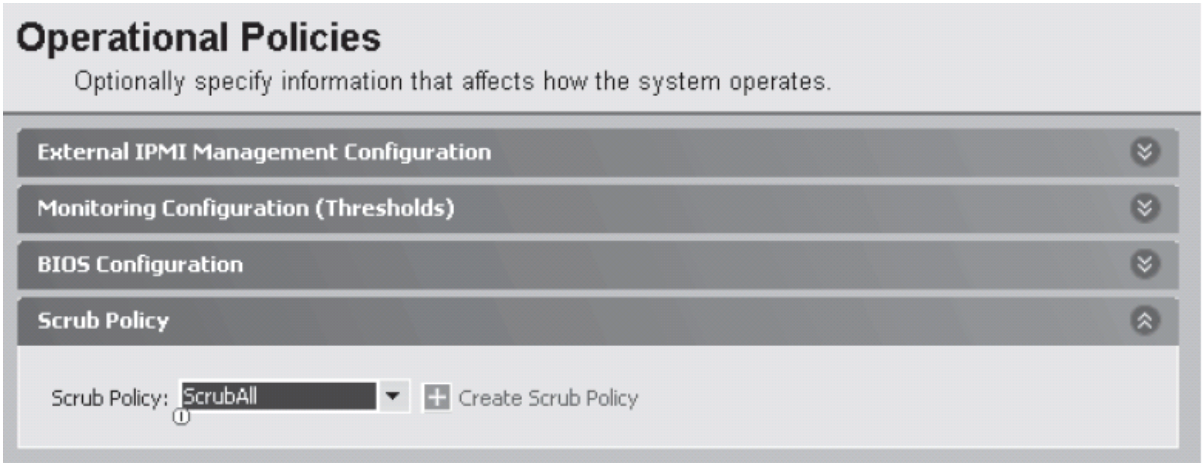
Step 18: On the Server Boot Order page, select BootMeX from the Boot Policy drop down list and click Next to continue



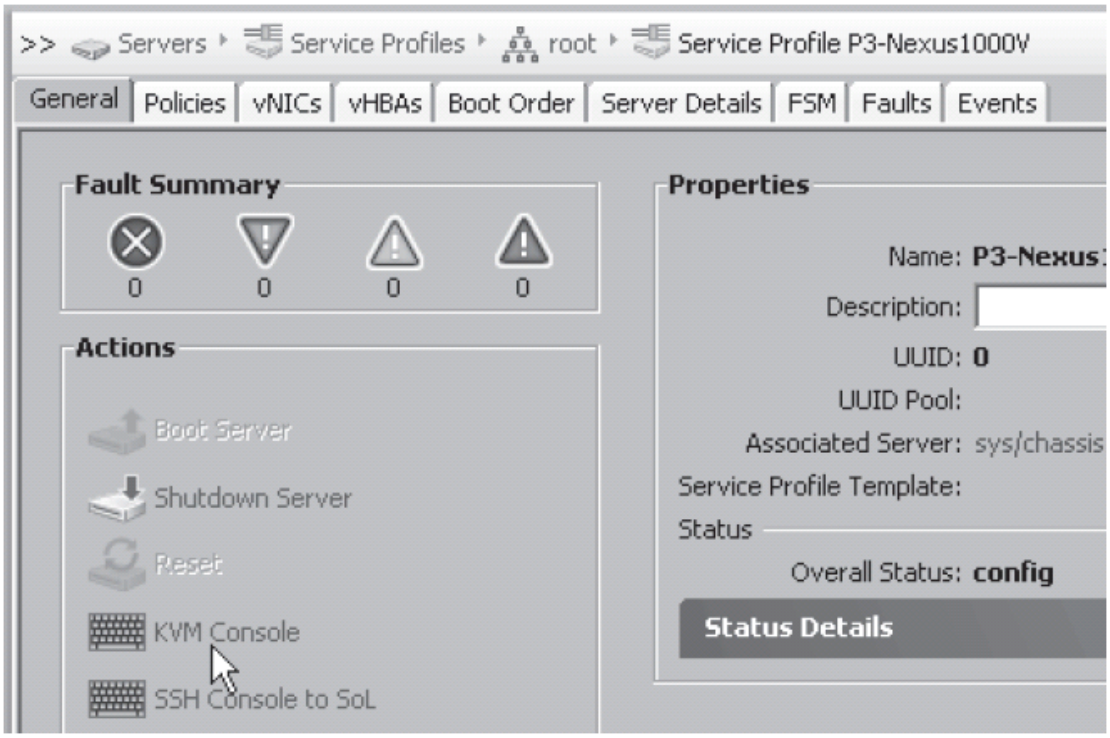
Step 19: On the Server Assignment page, choose your team server and click Next to continue.



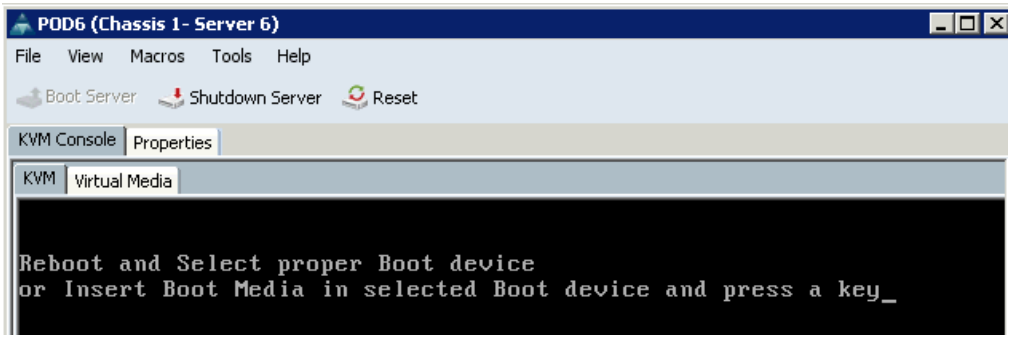
Step 20: On the Operational Policies page, expand Scrub Policy and select ScrubAll from the Scrub Policy drop down list. (If it does not exist, create the ScrubAll policies with Disk Scrub set to YES and Bios scrub set to NO.) Click Finish



Step 21: Choose your team's service profile. In the content pane, click KVM Console.



Step 22: Watch your server configure in the KVM window. When configuration is complete, the KVM should look like this:



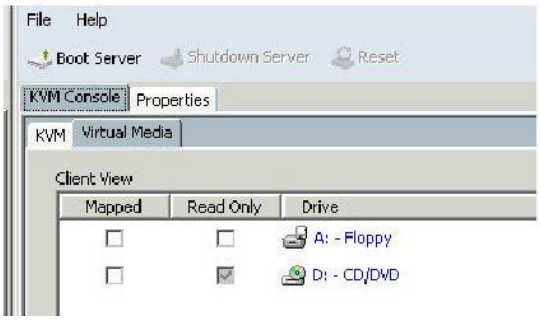
Task 3: Install vSphere ESXi 5.0

In this task, you will install vSphere (ESXi) 5.0 on your team's service profile.

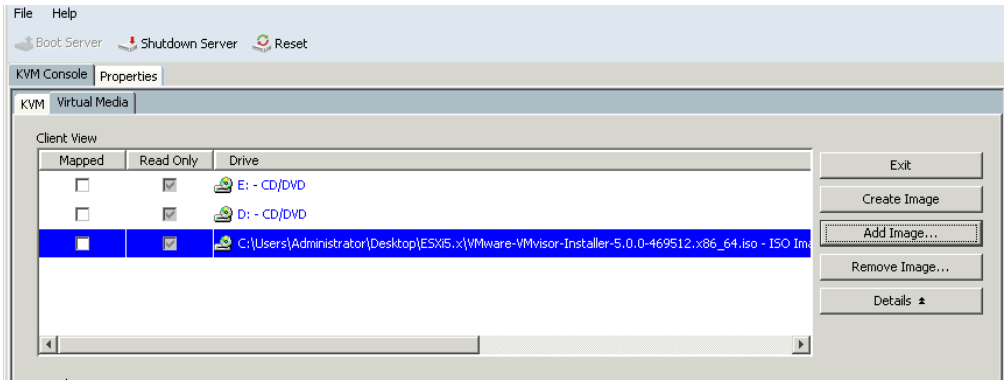
Activity Procedure

Complete these steps:

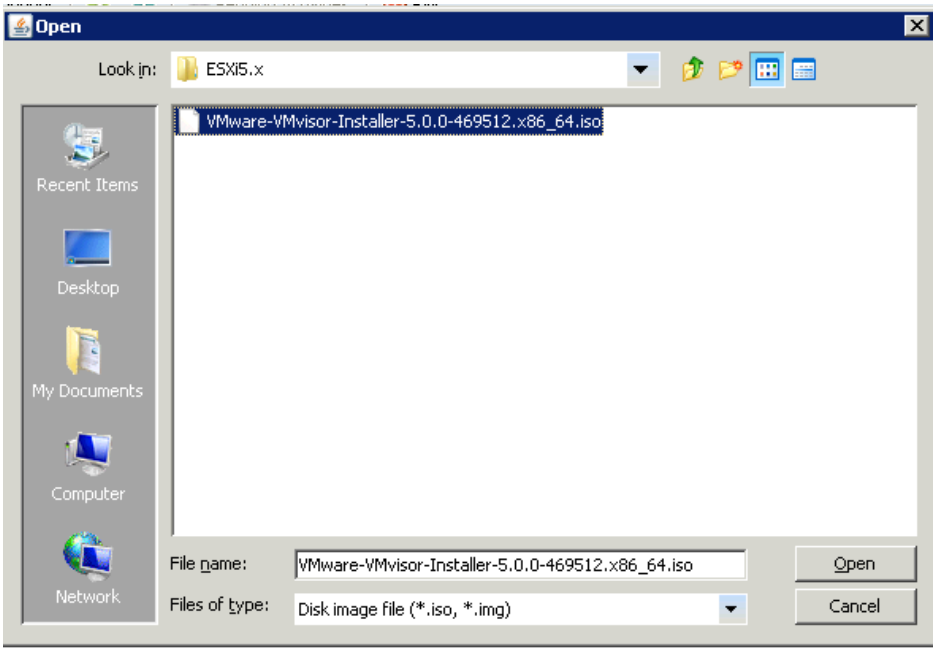
Step 1: Click Virtual Media.



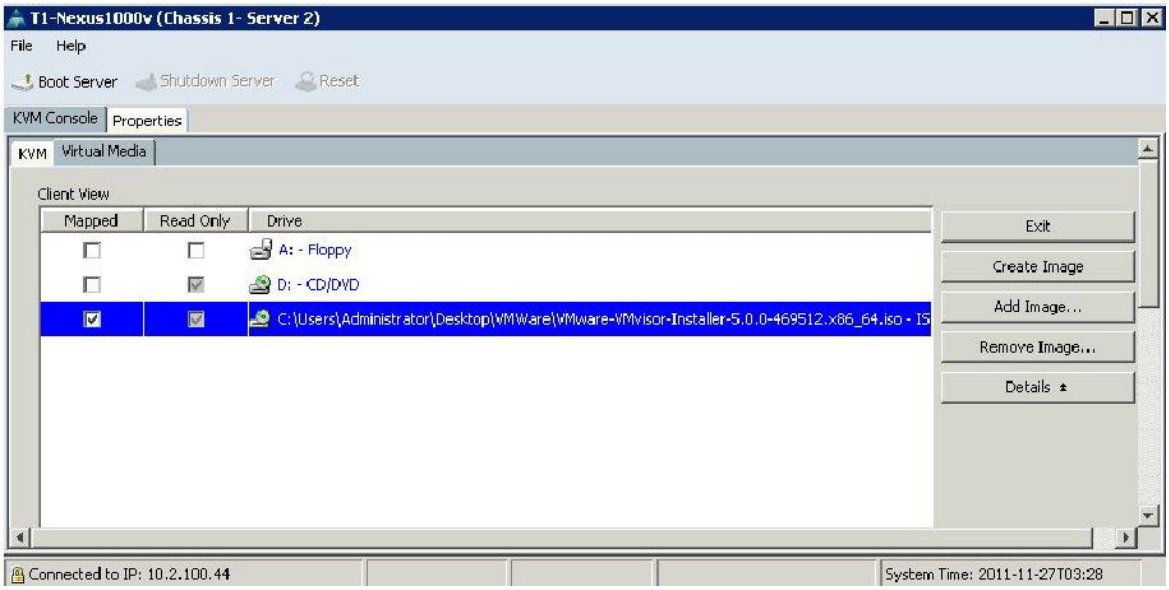
Step 2: Click Add Image.



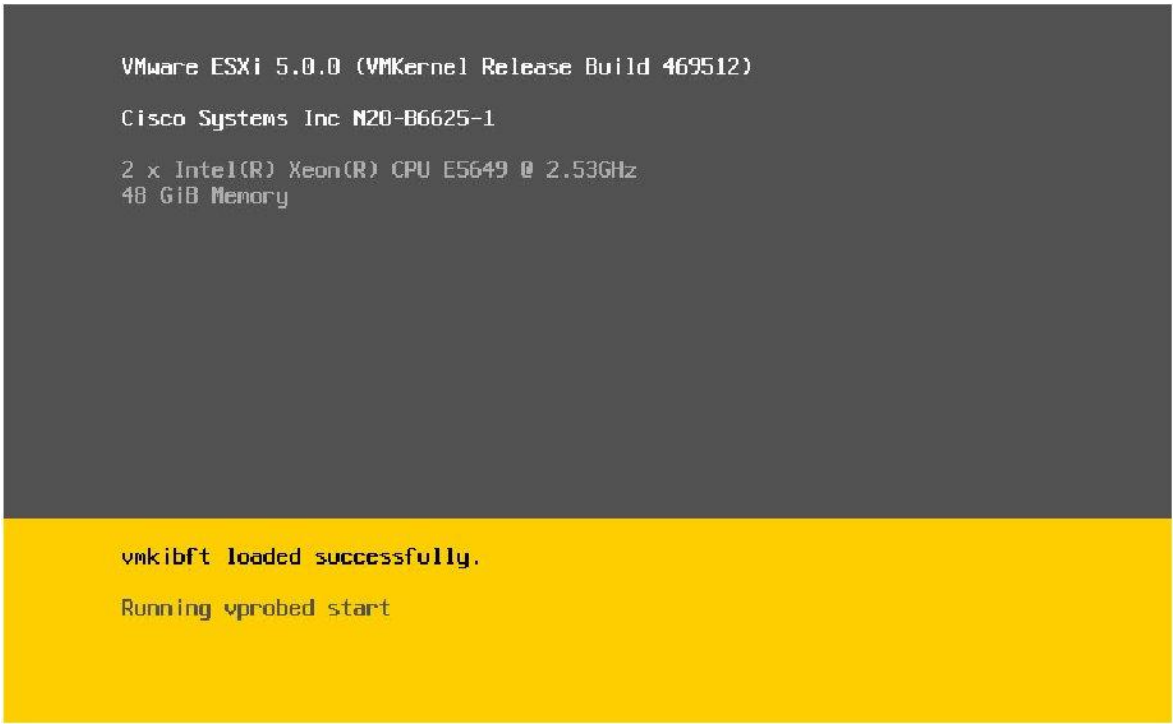
Step 23: The ISO is located on the desktop in ESXi5.x folder. Choose the ESX ISO (vMvisor) image and click Open.



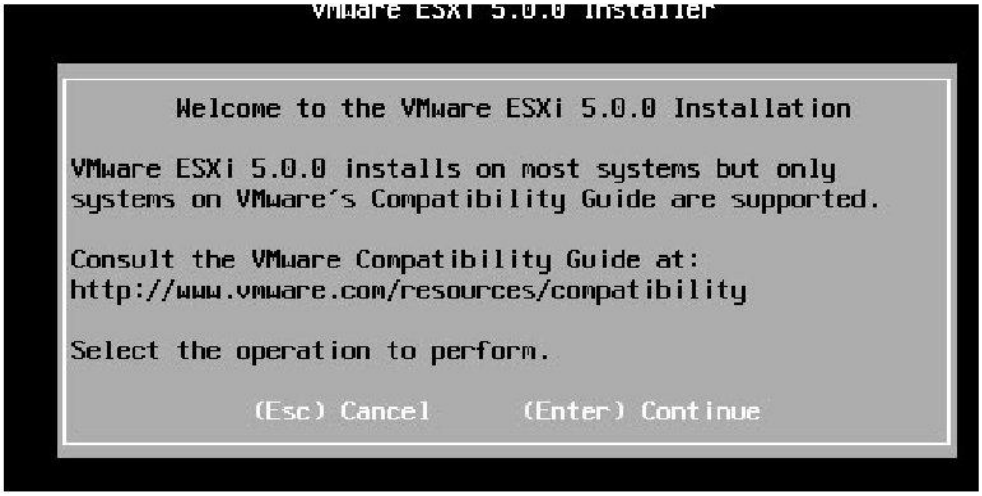
Step 24: Click the Mapped checkbox next to your ISO file.



Step 25: Now click the KVM tab and press any key or Boot Server if it is not. The ESXi 5.0 installer should launch. After the initial blue screen and loading text, you should see a similar screen as below.

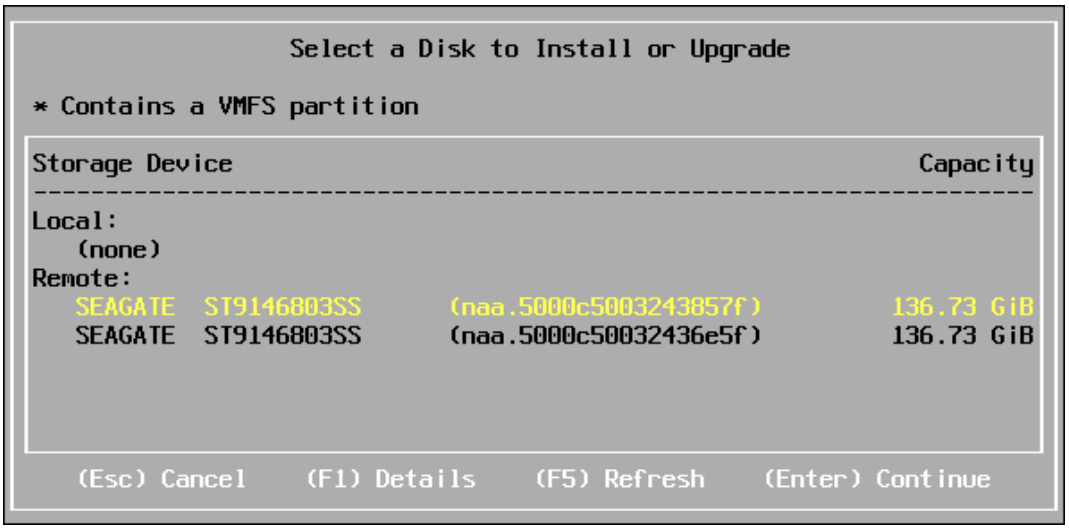


Step 26: After a short delay, you should see the ESXi Installer page. Press Enter.

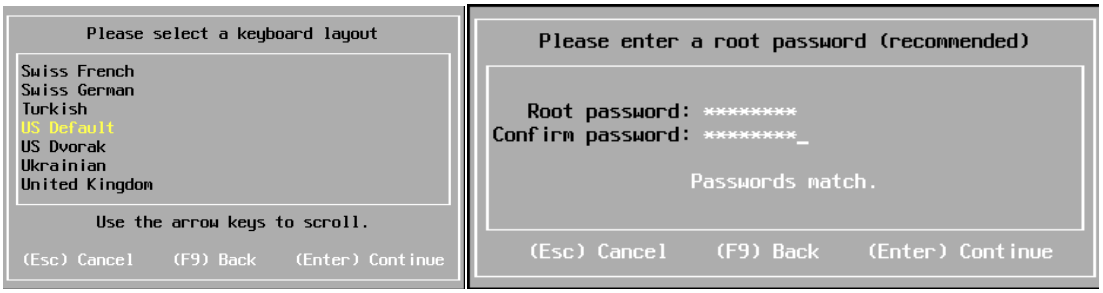


Step 27: End User License Agreement. Press F11.

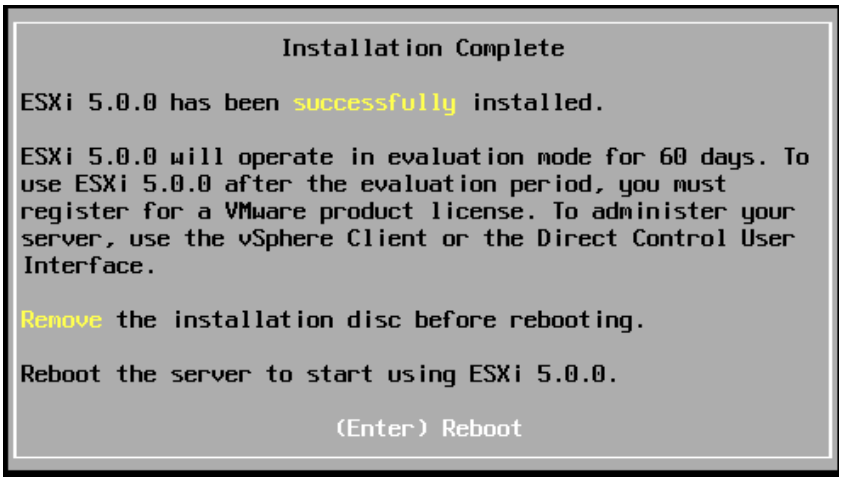
Step 28: Select the Remote hard drive (if they are 2 then choose the first) and press Enter.



Step 29: Select the default keyboard layout and set the root password to be "cisco123" and reconfirm it.

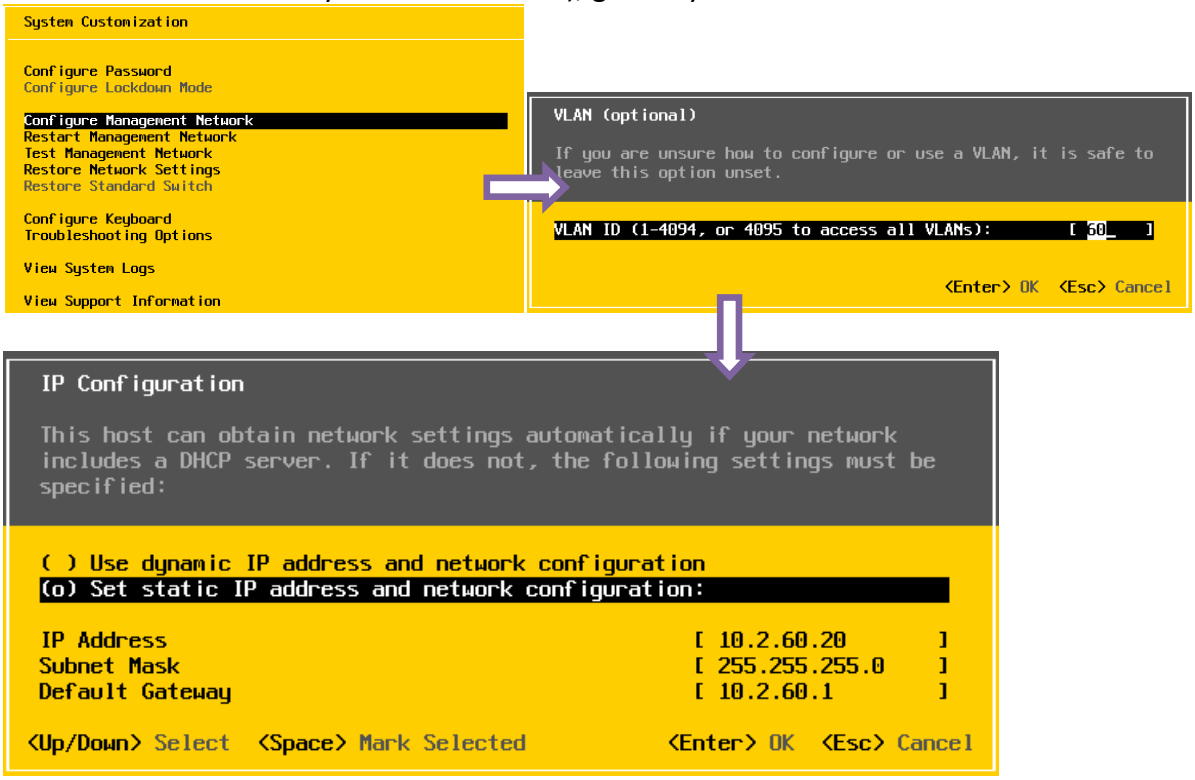


Step 30: The device will be rescan again. Once done, press F11 to install and the process installation will begin. After the installation is complete, press Enter to Reboot.



Step 31: Press F2 and Login as ROOT with password "cisco123".

Step 32: For this lab, we will use the static address. Press F2 to customise and choose Configure Management Network and implement the IP address assigned to your ESXi server: 10.2.X0.20 / 24 (X corresponds to your team number), gateway to 10.2.X0.1 and VLAN to X0.



Step 33 Press the Esc key to exit configuration of the management network.

Step 34 Press the Y key to accept the management network configuration.

Step 35 Press the down-arrow key to choose the Test Management Network element on the System Configuration screen.

Step 36 On the Test Management Network screen, press the Enter key. You should see OK as the result code from pinging the default gateway, if not please contact your instructor.

Task 4: Add ESXi Host to vCenter Server

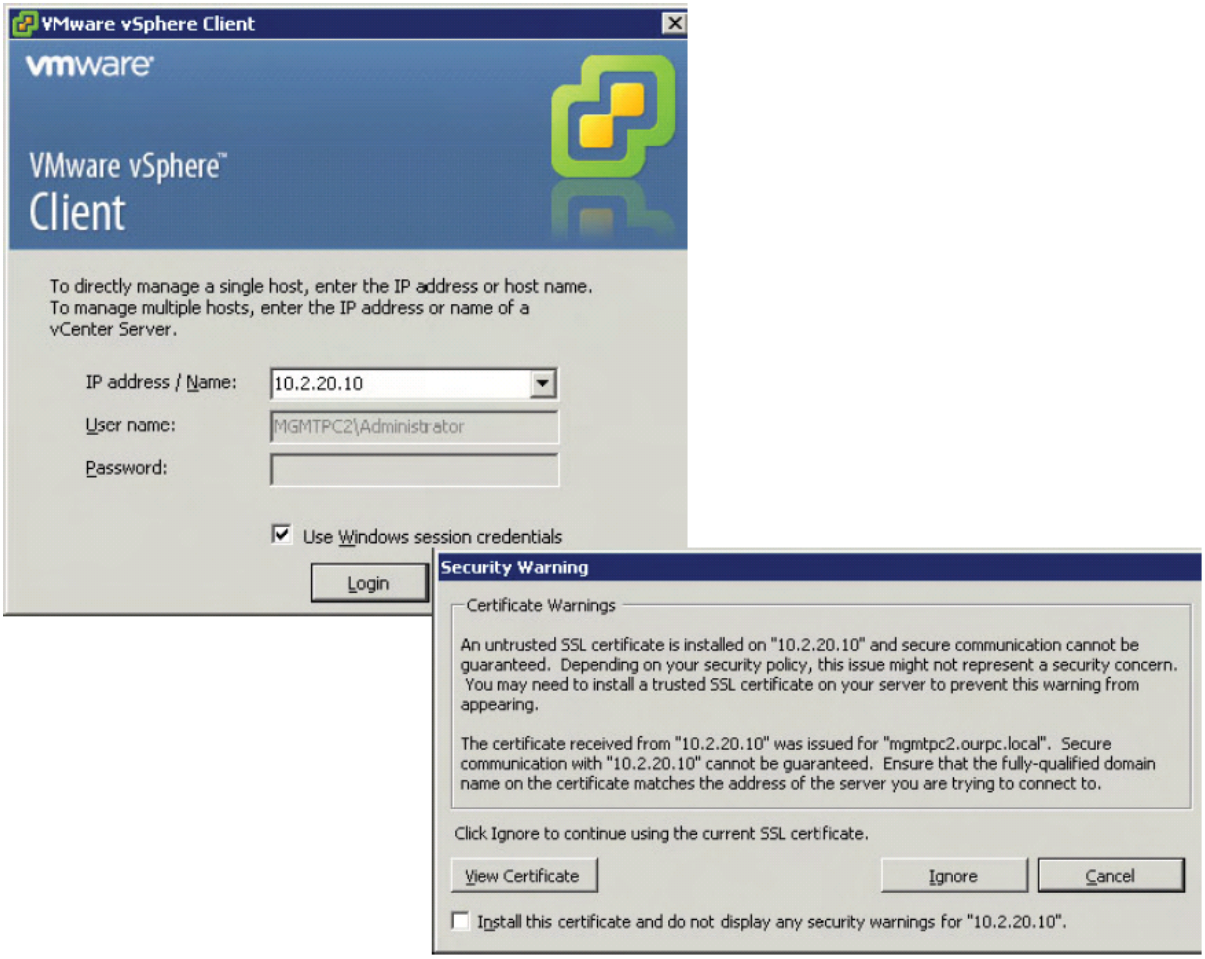
In this task, you will import two virtual machines and a VEM image for use in later exercises.

Activity Procedure

Complete these steps:

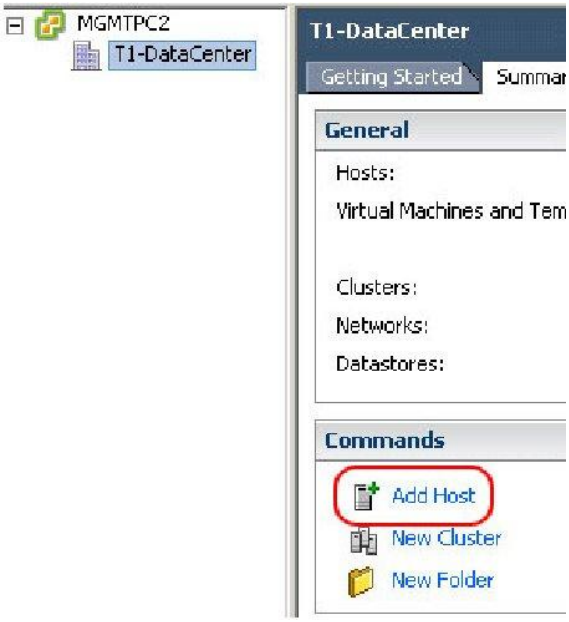
Step 1: Minimize the KVM console window and return to the student desktop. Find and launch the VMware vSphere Client icon.

Step 2: Connect to the vCenter Server using the its local IP address (10.2.X0.10). If prompted, install the security certificate and click ignore. (This will take a couple of minutes to connect and the X corresponds to your team number)

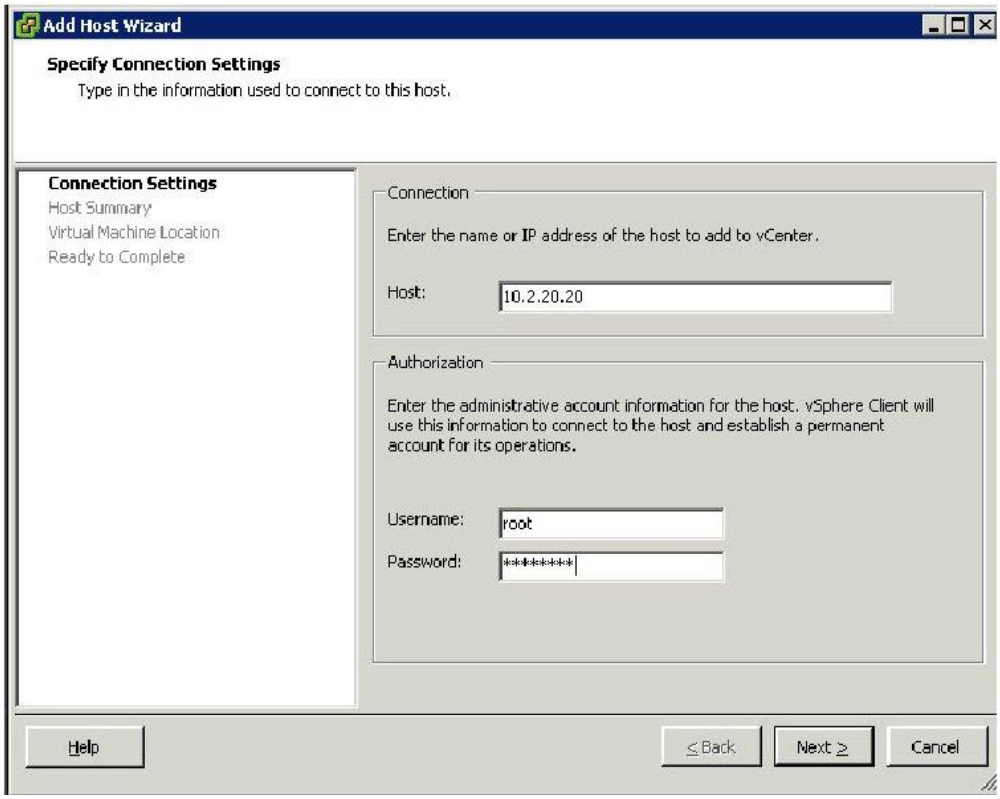


Step 3: Right Click on the vCenter object and create a Datacenter called TX-DataCenter (where X is you team number)

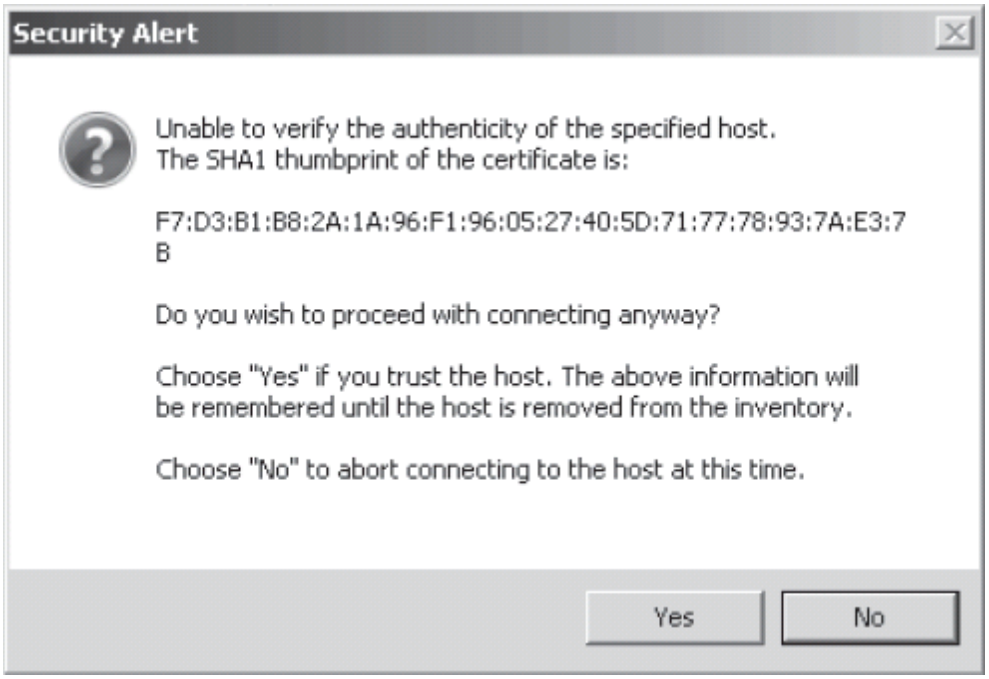
Step 4: Select the TX-DataCenter Datacenter and select Add Host



Step 5: Enter the IP address of your ESXi host. Use the username **root** and the password **cisco123**. Click Next.



Step 6: On the Security Alert window, click Yes.



: :

Step 7: On the Host Information page, click Next to continue

Step 8: On the Assign License page, leave the defaults and click Next to continue

Step 9: On the Configure Lockdown Mode, leave the defaults and click Next to continue

Step 10: On the Virtual Machine Location page, click Next to continue

Step 11: On the Ready to complete page, click Finish and monitor progress in the Recent Task section of the vSphere Client.

Lab 9-2: Installing a Cisco Nexus 1000V VSM

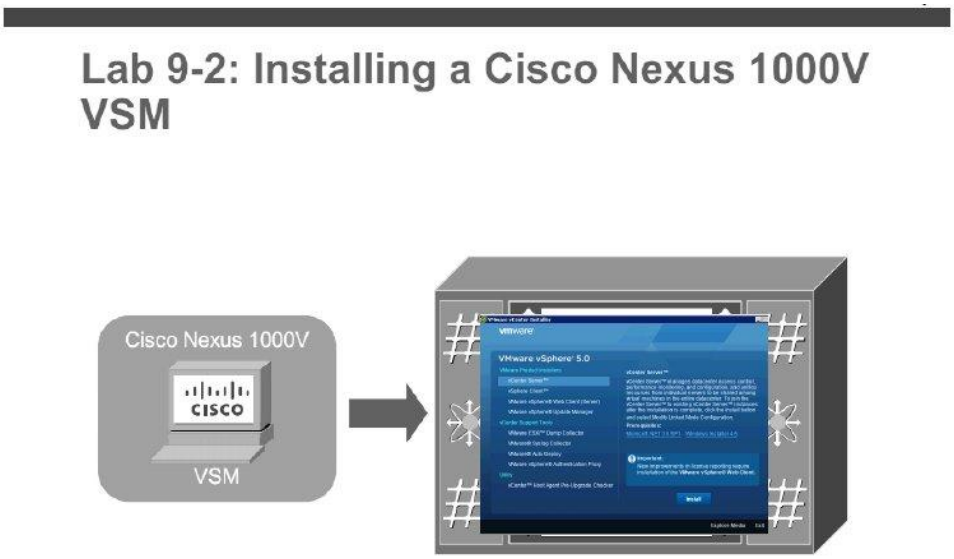
Complete this lab activity to practice what you learned in the related lesson.

Activity Objective

In this activity, you will configure a Cisco Nexus 1000V Virtual Supervisor Module (VSM) in the Cisco UCS environment. After performing this lab, you should be able to import a Cisco Nexus 1000V VSM into the ESX host's inventory.

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:

- Configured Cisco UCS environment Installed VMware ESX and
- vCenter instances from Lab 9-1

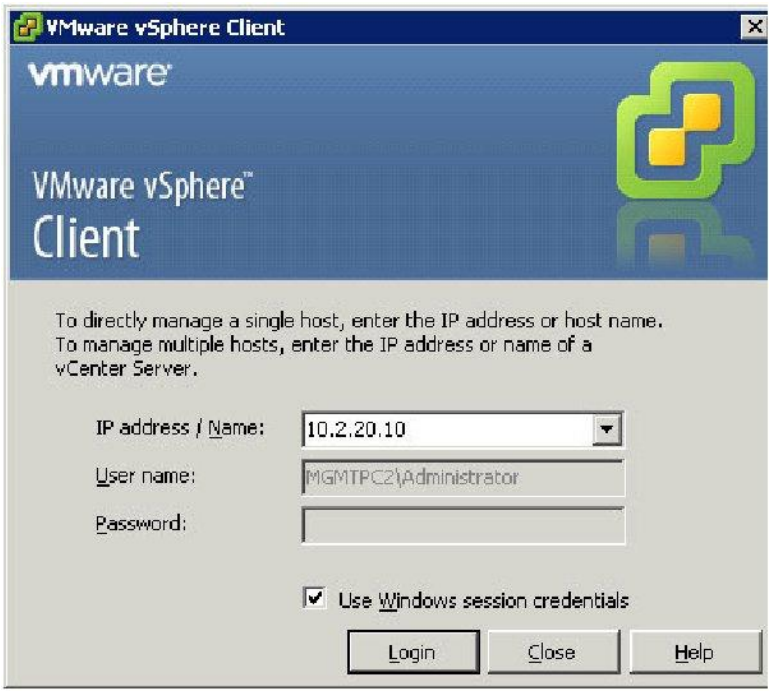
Task 1: Update the ESXi Host's Network Configuration

In this task, you will add Virtual Machine Port Groups to the ESXi host's configuration to accommodate the installation of the Cisco Nexus 1000v VSM.

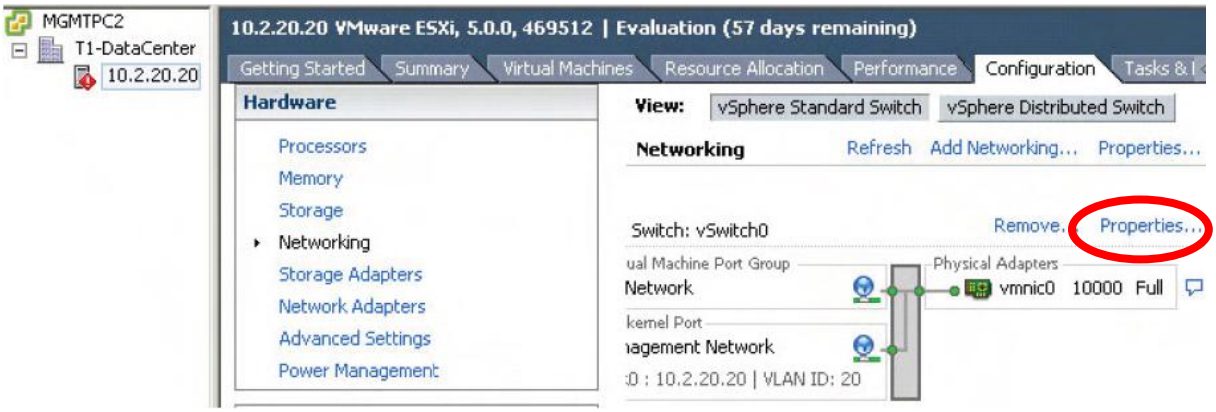
Activity Procedure

Complete these steps:

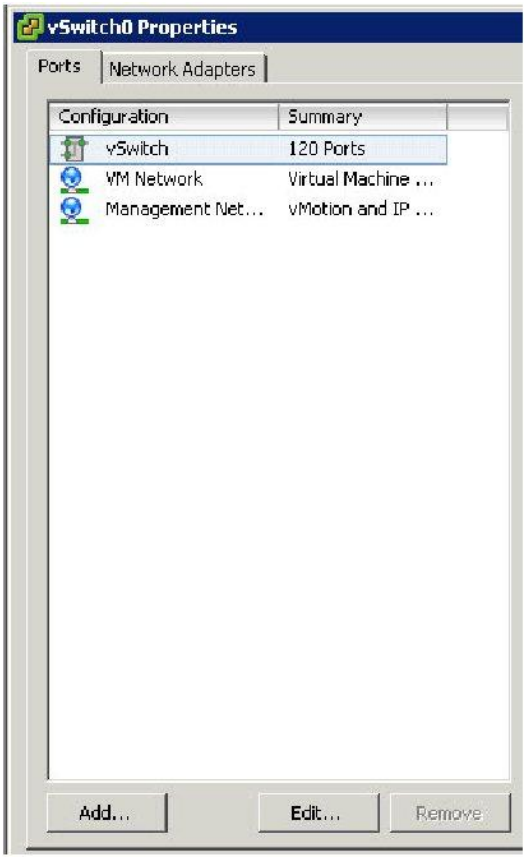
Step 1: Log into the vSphere client if necessary. Log into localhost, using the Windows session credentials.



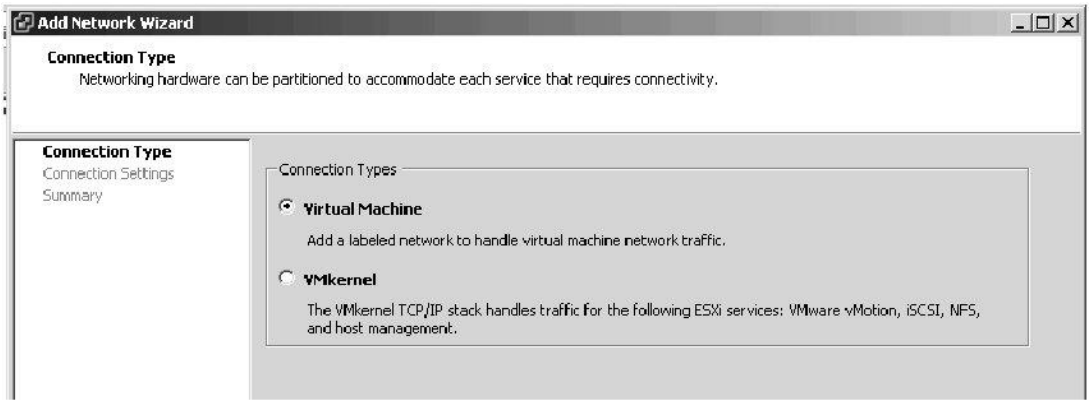
Step 2: Open the Configuration > Networking view for your ESX host, and click Properties for vSwitch0.



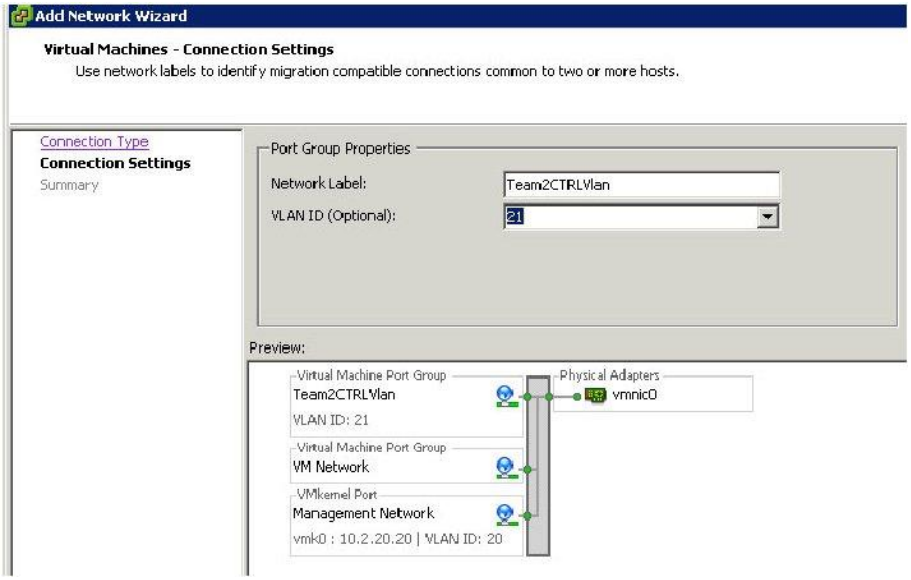
Step 3: Click Add.



Step 4: Choose Virtual Machine and click Next.



Step 5: Name the network TeamXCTRLVlan and set the VLAN ID to X1 replacing X with your team number.



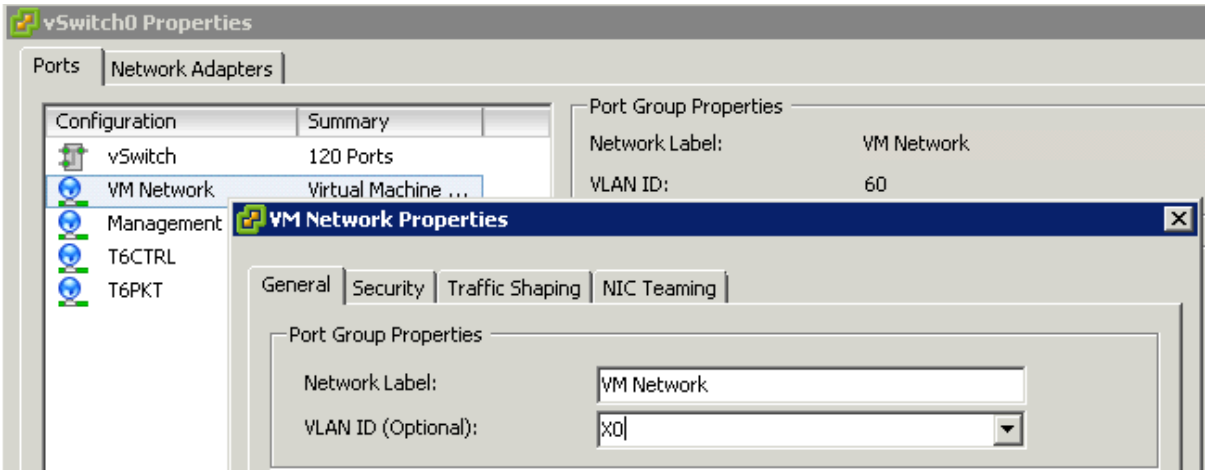
Step 6: Click Next.

Step 7: Verify and click Finish.

Step 8: Repeat Steps 3- 7 to create a Virtual Machine Port Group with a Network Label of Team2PKTVlan and a VLAN ID of X2, replacing X with your team number.

These Port groups will be used while adding the VSM Virtual Machine.

Step 9: Edit VM Network and change its Vlan ID to X0



Step 10: Click Close.

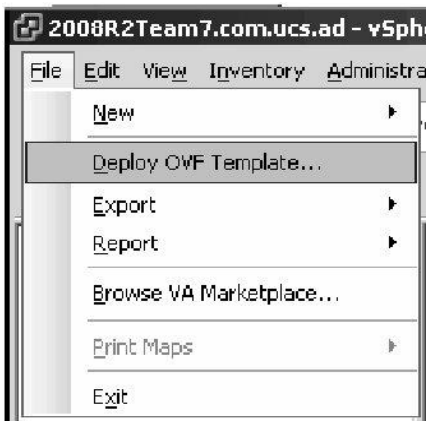
Task 2: Deploy the Cisco Nexus 1000v VSM Virtual Machine

In this task, you will add Virtual Machine Port Groups to the ESXi host's configuration to accommodate the installation of the Cisco Nexus 1000v VSM.

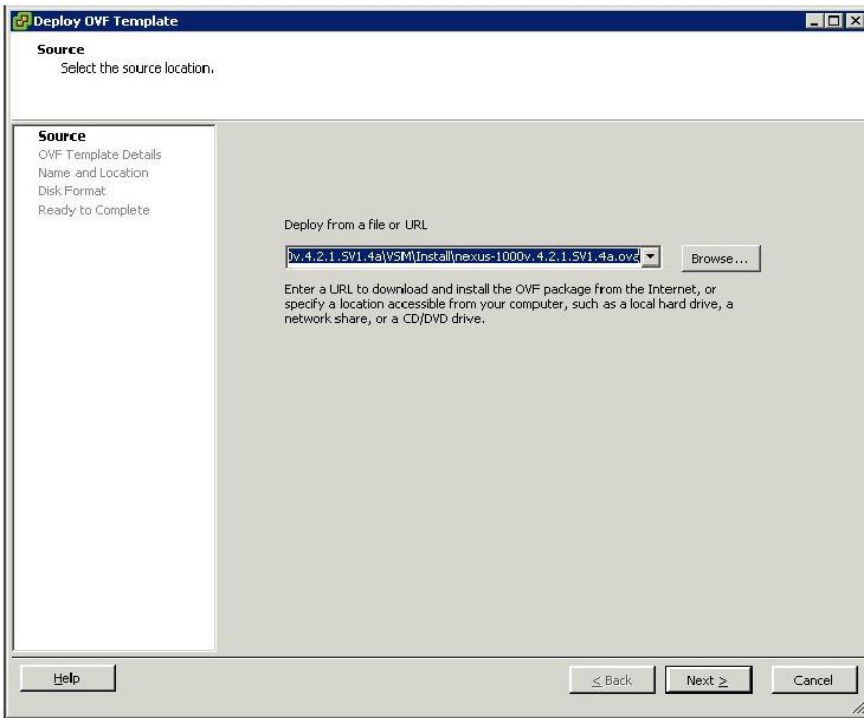
Activity Procedure

Complete these steps:

Step 1: From the VSphere Client, choose File > Deploy OVF Template.



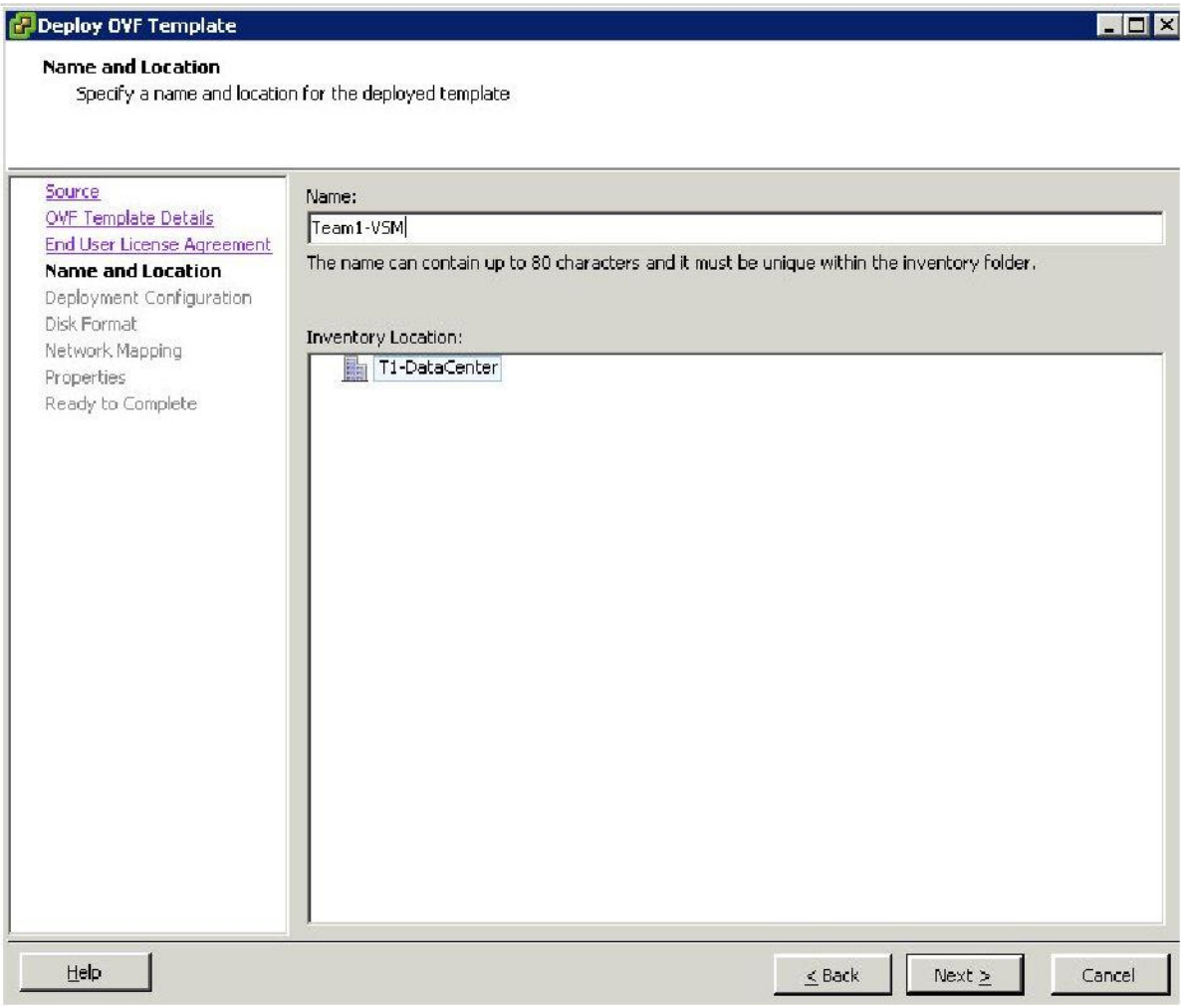
Step 2: From the Source window, either use the Browse button, or enter the path to the OVA template file as shown below, press the Next button. Desktop\VMWare\Nexus1000v.4.2.1.SV1.4a\VSM\Install\nexus-1000v.4.2.1.SV1.4a.ova



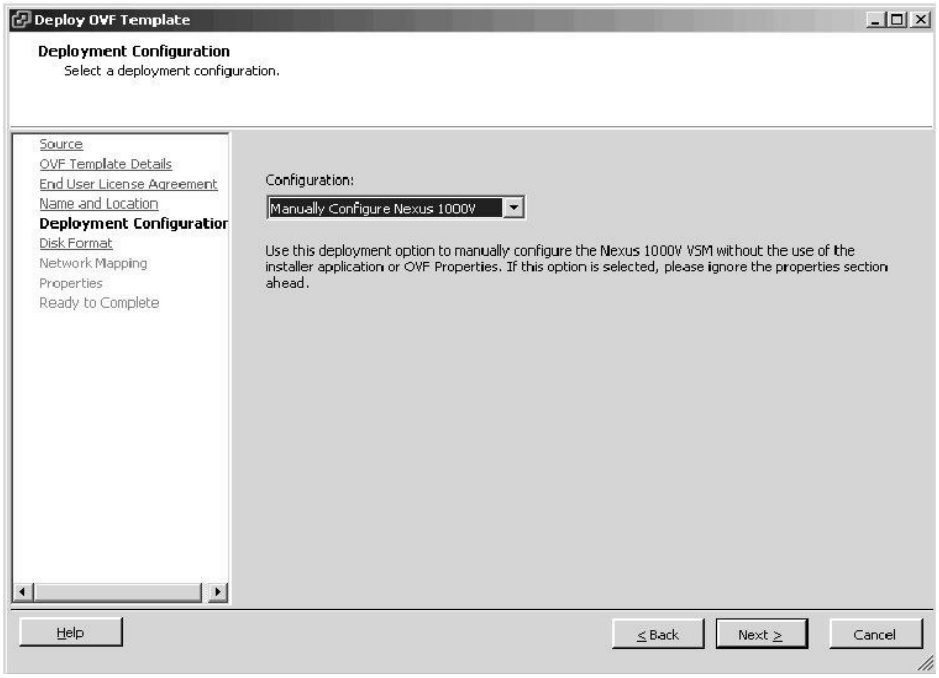
Step 3: From the OVF Template Details window, press the Next button and proceed to the End User License Agreement window.

Step 4: From the End User License Agreement window, select Accept and press the Next button to proceed to the Name and Location window.

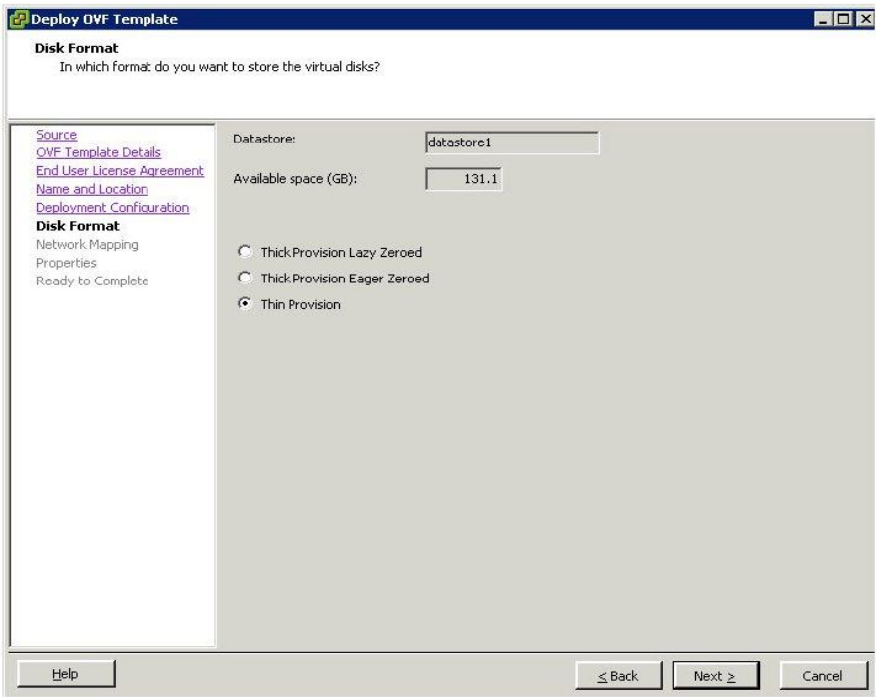
Step 5: From the Name and Location window, enter TeamX-VSM in the Name field and select your Datacenter in the Inventory Location field, then click the Next button to proceed to the Deployment Configuration window.



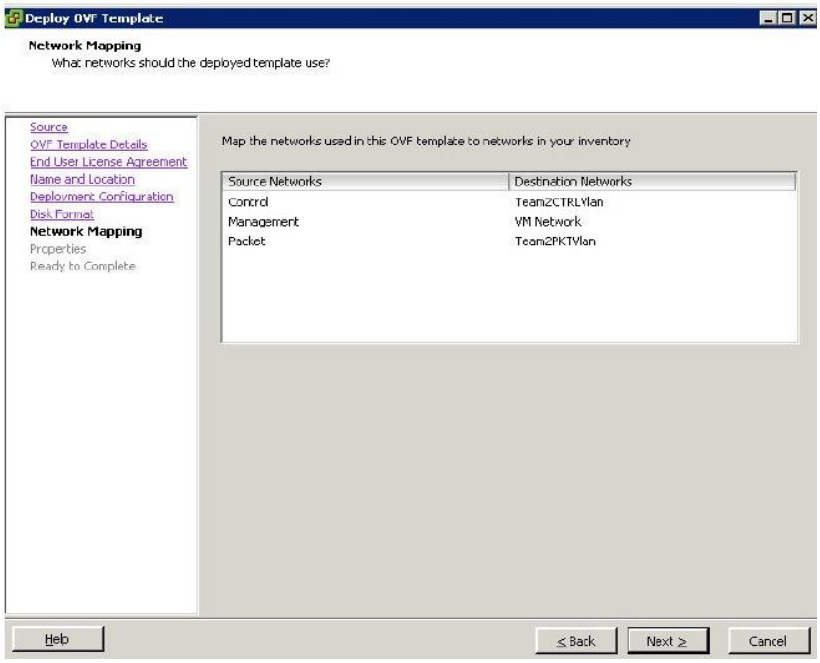
Step 6: From the Deployment Configuration window, select "Manually Configure Nexus 1000v" from the Configuration drop-down list and then click the Next button to proceed to the Disk Format window



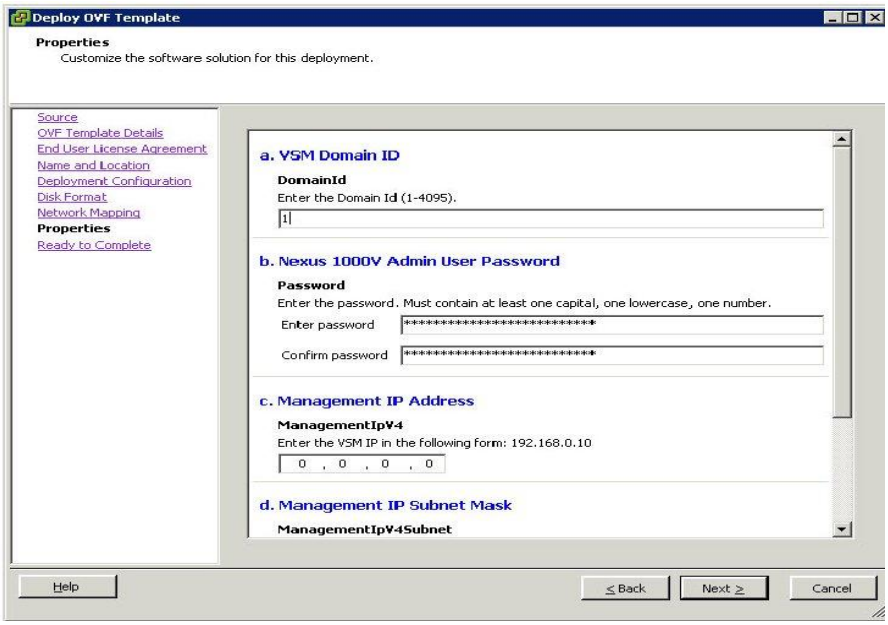
Step 7: From the Disk Format window, select the "Thin provisioning format" radio button and then click the Next button to proceed to the Network Mapping window.



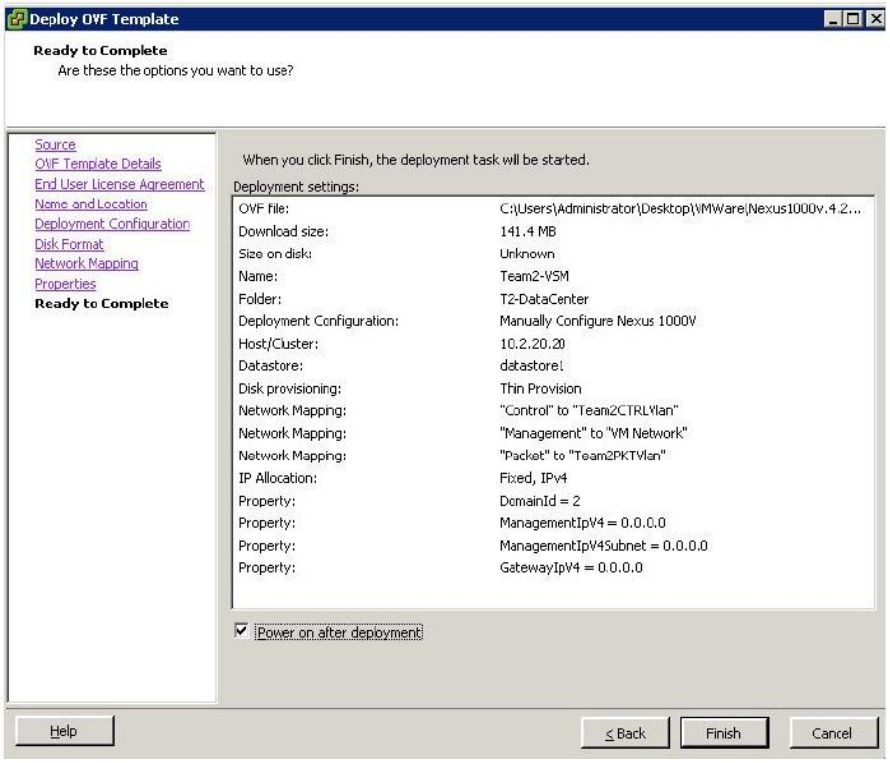
Step 8: From the Network Mapping window, map the Control and Packet Source Networks to the Control and Packet Destination Networks, respectively; and map the Management network to the VM Network Destination Network. Click the Next button to proceed to the Properties window.



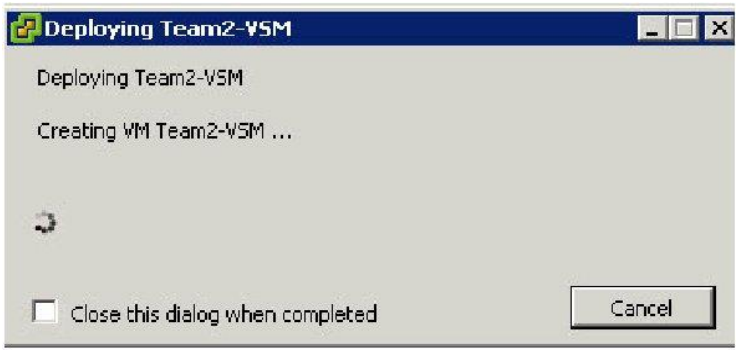
Step 9: On the Properties window, do not make any changes; except for Domain ID, enter your team number. Click the Next button to process to the Ready to Complete window.



Step 10: From the Ready to Complete window, check the "Power on after Deployment" and click Finish.



The installation of the VSM Virtual Machine should take less than 90 seconds



Step 11: Click the Close button with the deployment is completed.

Task 3: Configure the Cisco Nexus 1000v VSM Virtual Machine

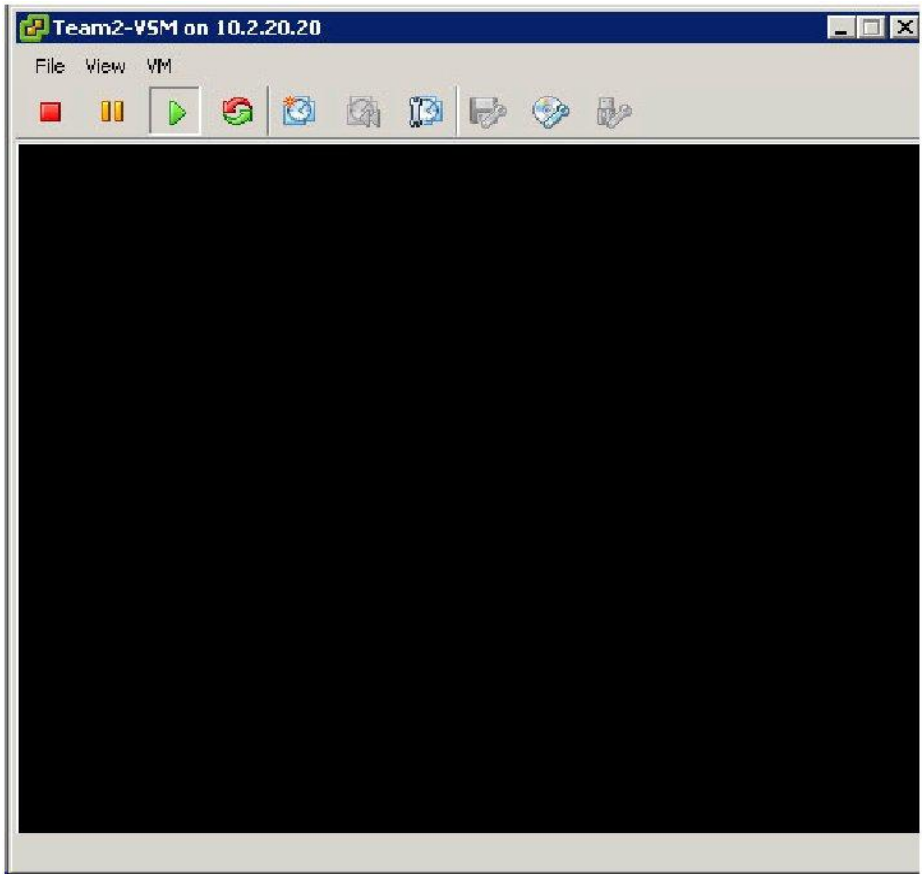
In this task, you will Power on and configure the Cisco Nexus 1000v VSM.

Activity Procedure

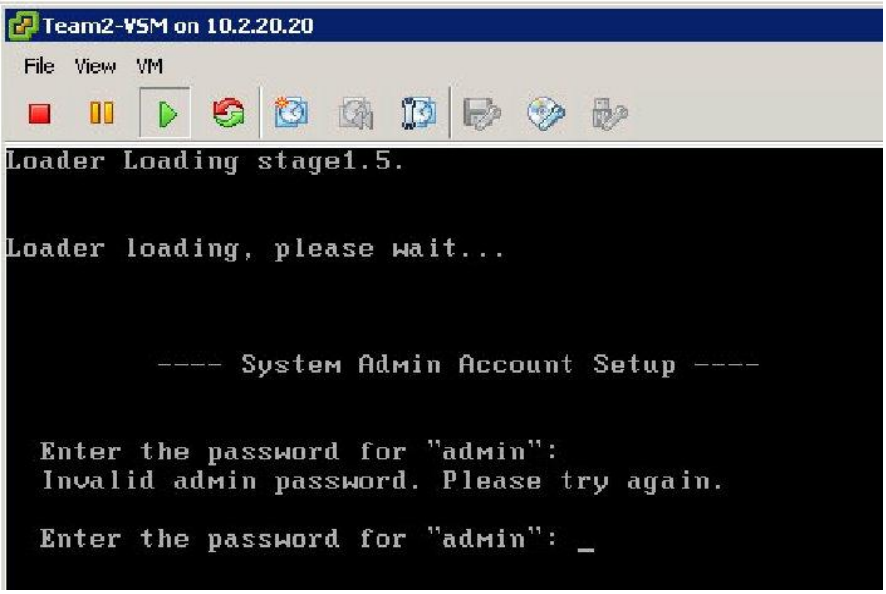
Complete these steps:

Step 1: From the VSphere Client, Right-click on the VSM and Choose Open Console

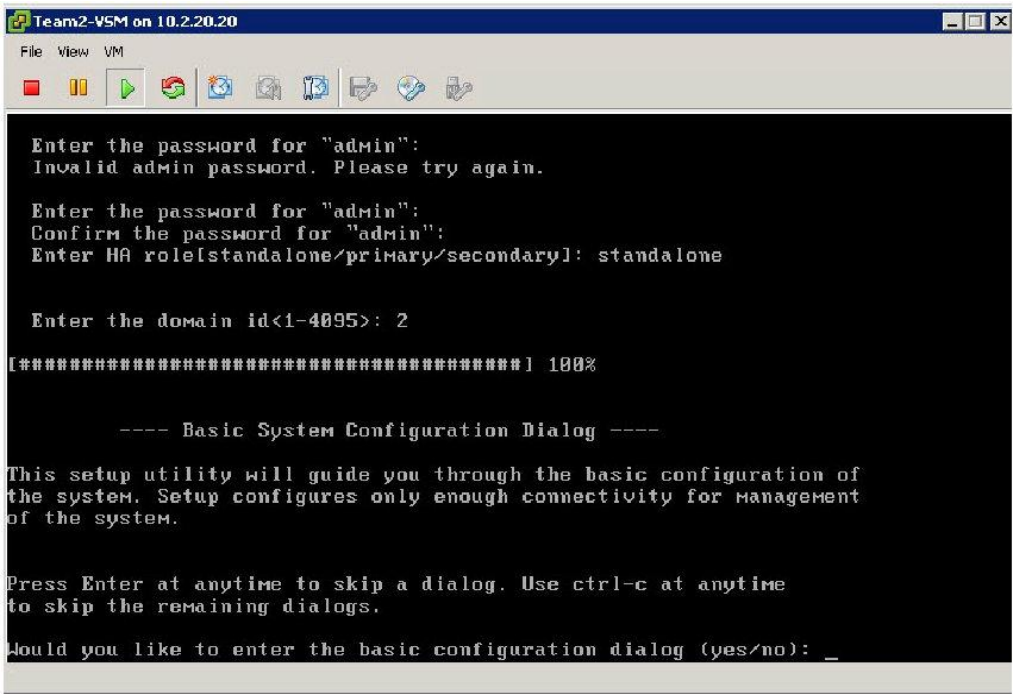
Step 2: From the VSM Console window, click the green arrow to Power On if it is not switched on.



Step 3: When the VSM VM powers on for the first time, the System Admin Account Setup script will run. Enter and reenter to confirm **1234Qwer** for the "admin" password. (No character entry will be visible in the console.)



Step 4: Next you will need to enter **standalone** for the HA role and enter your team number for the domain id. After which, those settings will be saved and you will be given the option to enter the Basic System Configuration Dialog. Type **yes** to proceed.



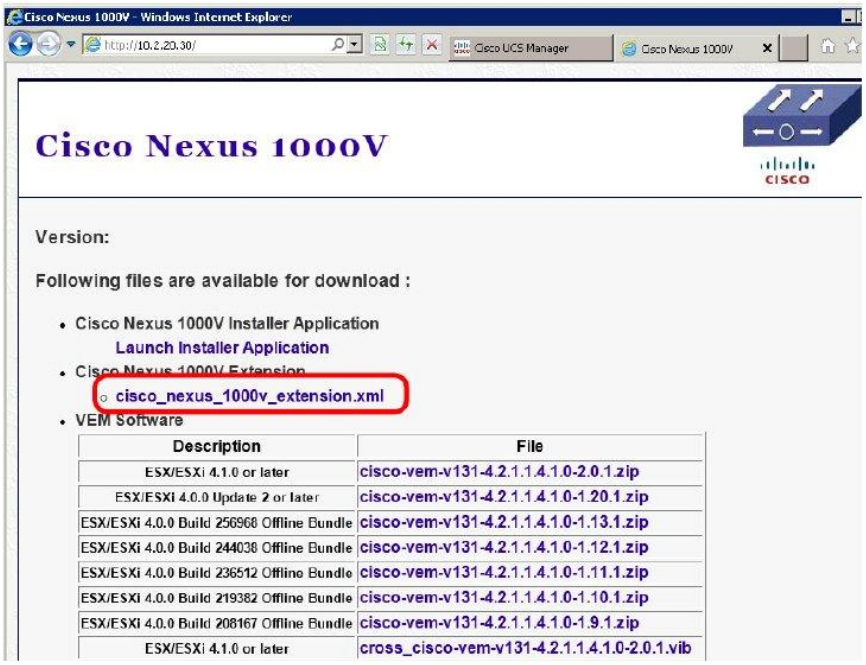
Step 5: Answer the following configuration questions as indicated by the bold text. Numeric responses use X to denote Team number.

```
Press Enter at anytime to skip a dialogueto skip the remaining dialogs.
Use ctrl-c at anytime
Would you like to enter the basic configuration dialog (yes/no): yes
Create another login account (yes/no) [n]: no
Configure read-only SNMP community string (yes/no) [n]: no
Configure read-write SNMP community string (yes/no) [n]: no
Enter the switch name: TeamX-N1Kv
Continue with Out-of-band (mgmt0) management configuration? [yes/no]: yes
Mgmt0 IPv4 address: 10.2.X0.30 (Where X is team number)
Mgmt0 IPv4 netmask: 255.255.255.0
Configure the default-gateway? (yes/no) [y]: yes
Default-gateway address: 10.2.X0.1
Configure Advanced IP options? (yes/no)? [n]: no
Enable the telnet service? (yes/no) [y]: no
Enable the ssh service? (yes/no) [n]: yes
Type of ssh key you would like to generate (dsa/rsa) : rsa
Number of key bits <768-2048> : 768
Configure the NTP Server? (yes/no) [n]: no
Vem feature level will be set to 4.0(4)SV1(3), Do you want to reconfigure?
(yes/no) [n]: no
Configure svs domain parameters? (yes/no) [y]: yes
Enter SVS Control mode (L2/L3): L2
Enter control vlan <1-3967, 4048-4093>: X1 (Where X is team number)
Enter packet vlan <1-3967, 4048-4093>: X2 (Where X is team number)

The following configuration will be applied:
switchname Team7-N1Kv
interface mgmt0
ip address 10.2.X0.30 255.255.255.0
no shutdown
no telnet server enable
vrf context management
ip route 0.0.0.0/0 10.2.X0.1
telenet server enable
ssh key rsa 768 force
ssh server enable
svs-domain
svs mode L2
control vlan X1
packet vlan X2
domain id X
vlan X1
vlan X2

Would you like to edit the configuration? (yes/no) [n]: no
Use this configuration and save it? 9yes/no) [y]: yes
[########################################] 100%
User Access Verification
TeamX-N1Kv login:
```

Step 6: Press Ctrl + Alt to release the cursor from the console window.

Step 7: From the desktop computer, open a web browser window and browse to the mgmt0 address of the Cisco Nexus VSM mgmt0 IP 10.2.X0.30.

Step 8: Right-click the cisco_nexus1000v_extension.xml and choose Save Target As, or Save Link As, depending on your browser.

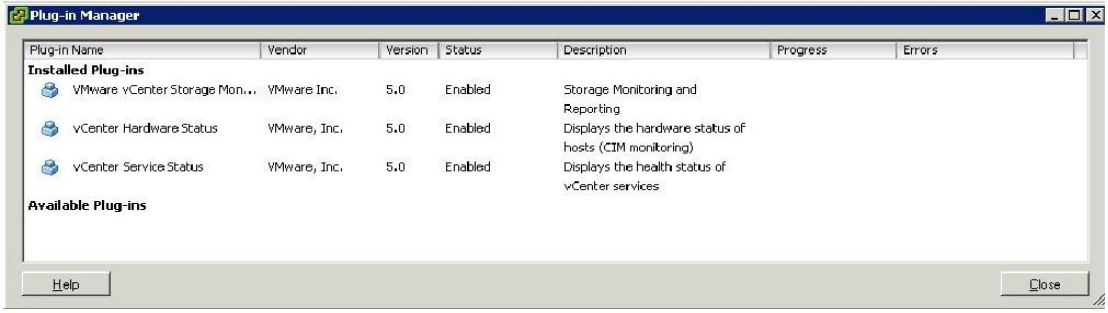


Step 9: Choose a safe location, such as your desktop, and click Save and close the browser window.

This file will be installed in vCenter to authenticate the VSM.

Step 10: Return to the vSphere client.

Step 11: From the file menu, choose Plug-Ins > Manage Plug-Ins.



Step 12: Right-click the white space and choose New Plug-In.

You might have to expand the window to obtain blank space at the bottom of the window.

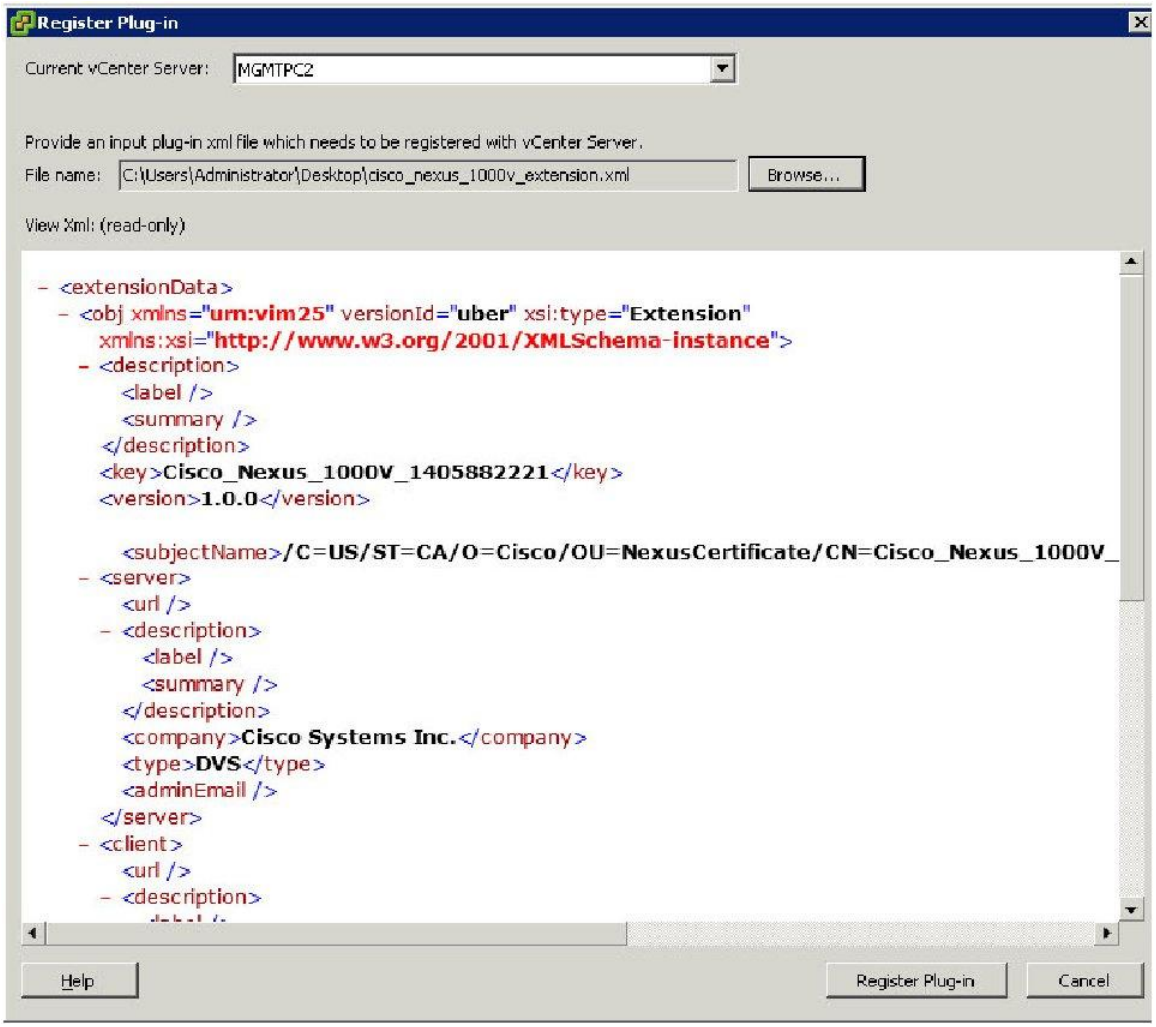
Step 13: Click Browse.

Step 14: Click Desktop.

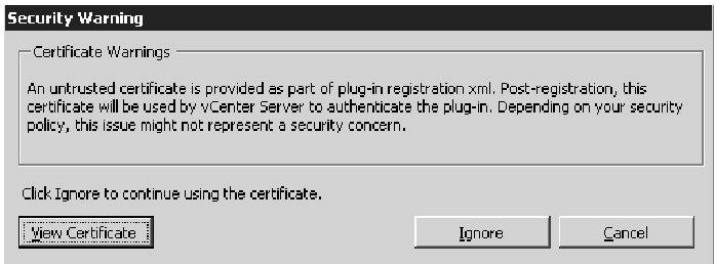
Step 15: Locate and choose the xml file that you saved to the desktop.

Step 16: Click Open.

Step 17: Click Register Plug-In.

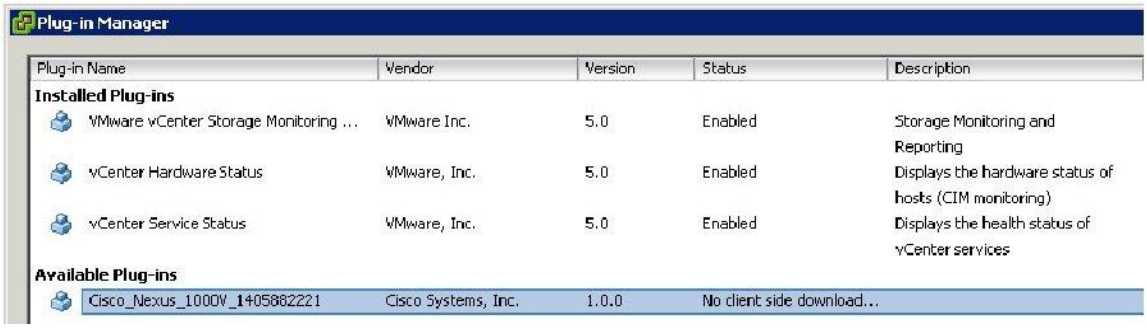


Step 18: If prompted with a security warning, choose Ignore.

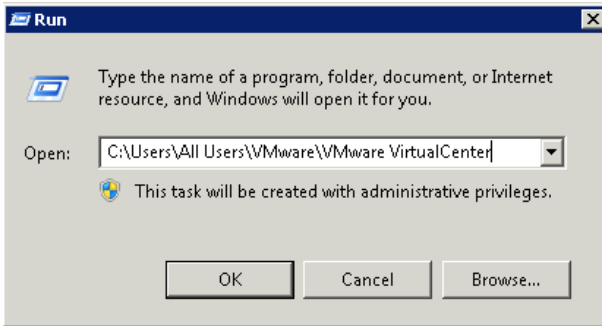


Step 19: If prompted with a security warning, choose Ignore.

Step 20: Click OK on the Plug-in success message.



Step 21: Click on Windows "Start" Button and choose "RUN". Type in the following "C:\Users\All Users\VMware\VMware VirtualCenter" and press "**OK"** button.



Step 22: Right-click the proxy.xml file and choose Open With.

Step 23: Choose Notepad.

Step 24: Click OK.

Step 25: Choose Edit > Find.

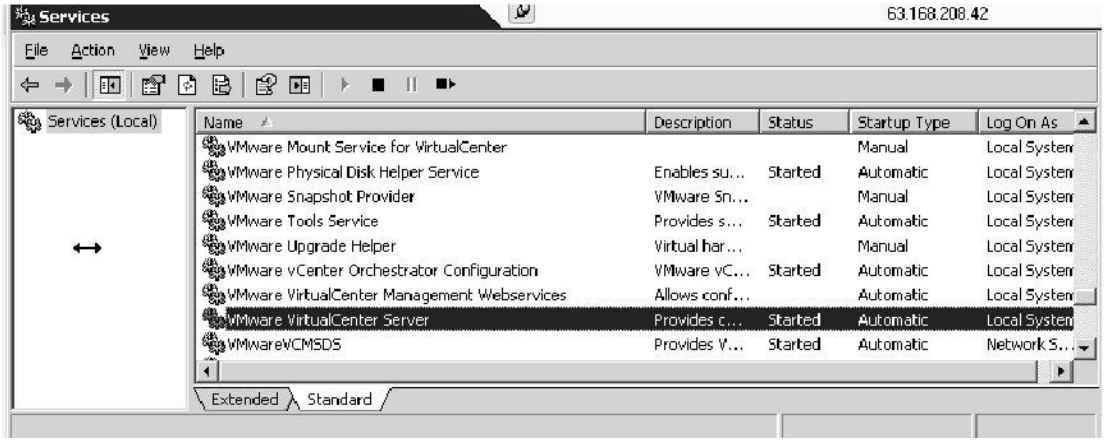
Step 26: Enter :8089 and click Find Next.

Step 27: Ensure that the vCenter server address of your pod is correct as shown here.
<serverNamespace>10.2.X0.10:8089</serverNamespace>

Step 28: If changes were made, choose File > Save.

Step 29: Close the file and the folder.

Step 30: If changes were made, open services.msc and restart the VMware VirtualCenter Server Service.



Step 31: If presented with an error restarting the service, close the error message and continue.

Step 32: Ensure that the VSM VM console is open by using the following credentials:
User Name: admin
Password: 1234Qwer

Step 33: Configure the VCenter connection:

```
TeamX-N1Kv# configure
TeamX-N1Kv(config)# svs connection TX-DataCenter (Where X is your
team
number)
TeamX-N1Kv(config-svs-conn)# vmware dvs datacenter-name TX-DataCenter
(Where X is your team number)
TeamX-N1Kv(config-svs-conn)# protocol vmware-vim
TeamX-N1Kv(config-svs-conn)# remote ip address 10.2.X0.10 (Where X is
your team number)
TeamX-N1Kv(config-svs-conn)# connect
TeamX-N1Kv(config-svs-conn)# copy run start
[########################################] 100%
```

Step 34: Verify the configuration.

```
TeamX-N1Kv(config-svs-conn)# show svs connection

connection TX-DataCenter:
ip address: 10.2.20.10
protocol: vmware-vim https
certificate: default
datacenter name: TX-DataCenter
DVS uuid: a4 b6 3e 50 33 9c 50 69-fc 30 ec 27 78 e4 a7 d2
config status: Enabled
operational status: Connected
sync status: Complete
version: VMware vCenter Server 5.0.0 build-258902
```

The UUID will vary. This is the unique identifier for this VSM.

```
TeamX-N1Kv(config-svs-conn)# show interface brief
--------------------------------------------------------------------------------
Port         VRF   Status IP Address       Speed MTU
--------------------------------------------------------------------------------
mgmt0        --    up 10.2.20.3      0     1000  1500
--------------------------------------------------------------------------------
Port         VRF   Status IP Address       Speed MTU
--------------------------------------------------------------------------------
Control0     --    up --                   1000  1500
```

No interfaces exist because they have not been added from vCenter.

```
TeamX-N1Kv(config-svs-conn)# show svs domain
SVS domain config:
Domain id:
Control vlan: X1
Packet vlan: X2
L2/L3 Control mode: L2
L3 Control Interface: NA
Status: Config push to VC successful.
```

Step 35: Release the mouse by pressing Ctrl + Alt.

Step 36: Close the console window.

Any ports not specifically placed in a port group will be placed in the “Quarantine” port groups.

Lab 9-3: Configuring Port Profiles

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

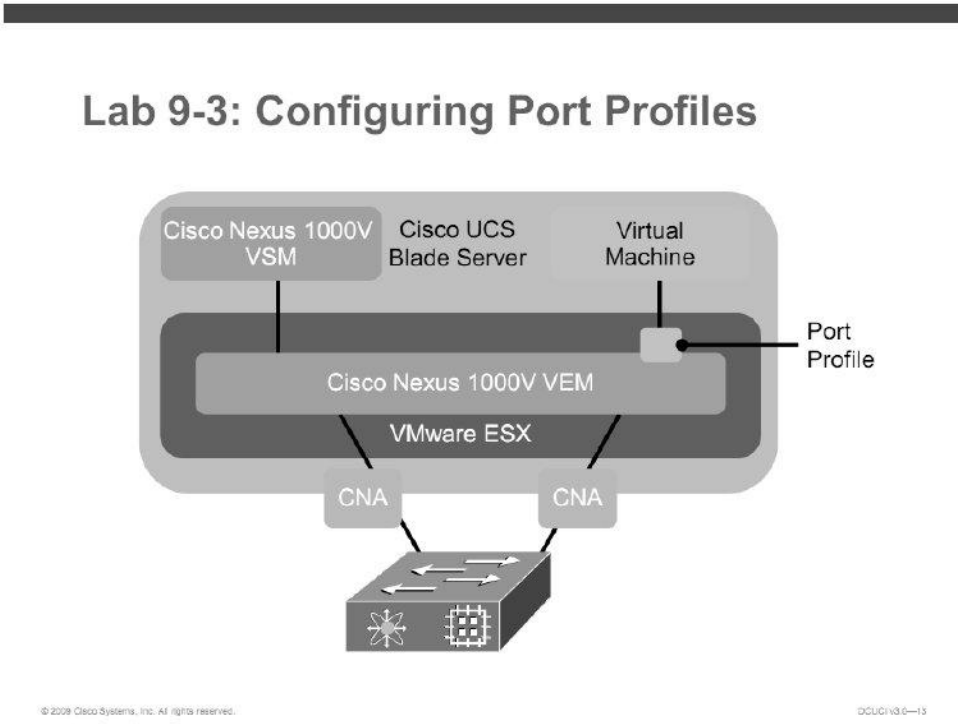
Activity Objective

In this activity, you will configure Cisco Nexus 1000V port profiles and install a Cisco Nexus 1000V VEM. After performing this lab, you should be able to:

- Create a port profile for the Cisco Nexus 1000V uplinks
- Create a Cisco Nexus 1000V virtual machine data port profile
- Add hosts to a Cisco Nexus 1000V VSM
- Add a host to a Cisco Nexus 1000V port group and validate the functionality of the virtual Ethernet ports

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:

- Configured Cisco UCS environment
- Installed Cisco Nexus 1000V VSM from Lab 9-2
- Windows 2003 VM and Cisco Nexus 1000V VEM images from Lab 9-2

Task 1: Create a System Uplink Port Profile

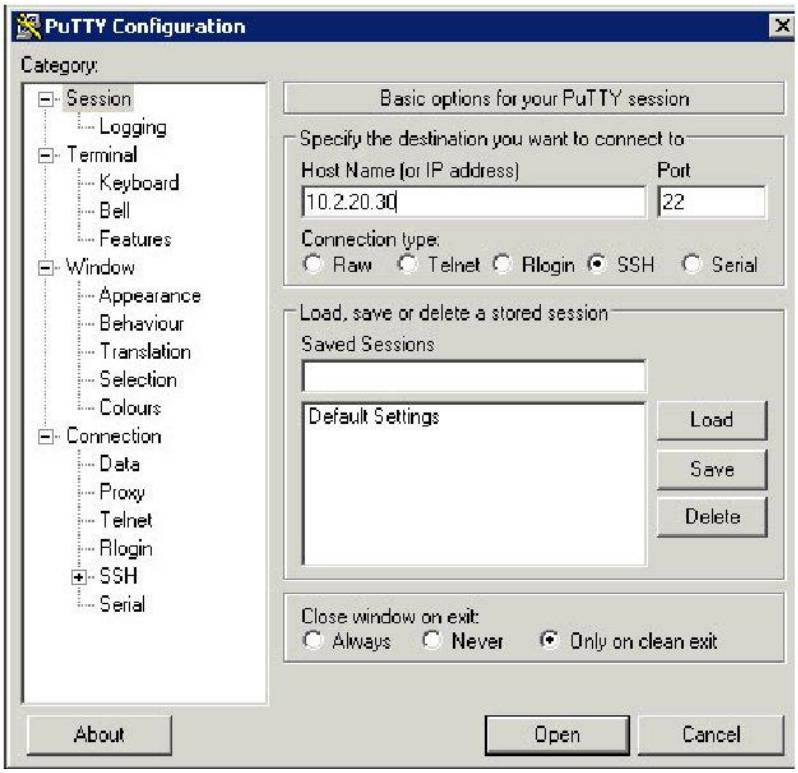
In this task, you will create a port profile for the Nexus 1000V distributed switch uplinks.

Activity Procedure

Complete these steps:

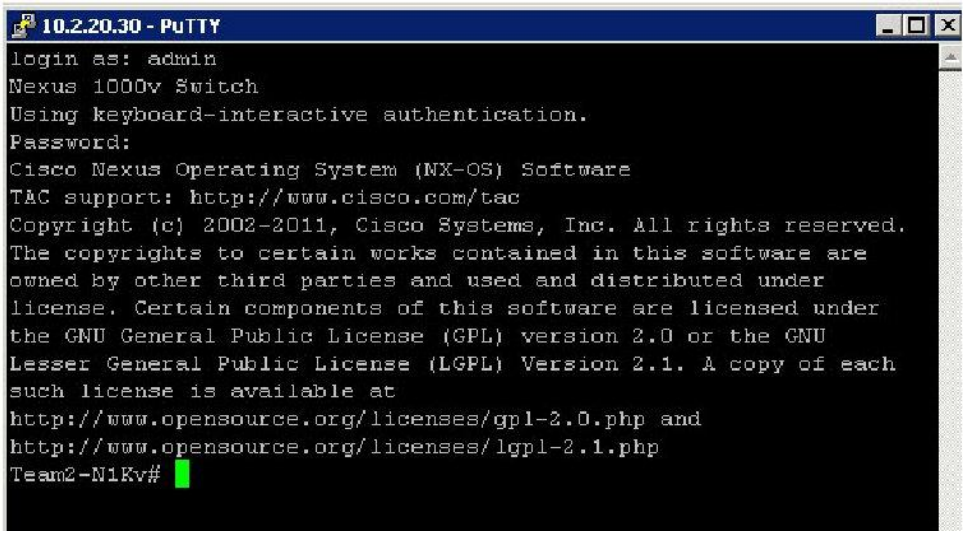
Step 1: From the desktop, open the PuTTY Client.

Step 2: Open an SSH session to your switch at IP Address 10.2.X0.30 (where X is your team number).



Step 3: Choose Yes if prompted to confirm the SSH key.

Step 4: Log in to the switch by using username admin, password 1234Qwer.



SSH is the recommended method to access the switch after you have installed the Cisco Nexus 1000V.

Step 5: Take some time to explore the switch and context sensitive help using show commands .

Step 6: Enter configuration mode.

```
TeamX-N1Kv# configure terminal (this can be shortened to conf)
TeamX-N1Kv(conf)#
```

Step 7: Configure a system port profile.

```
TeamX-N1Kv(config)# vlan X0-X3
TeamX-N1Kv(config)# port-profile type ethernet systemUplinkX (X is Team
Number)
TeamX-N1Kv(config-port-prof)# description System Uplink
TeamX-N1Kv(config-port-prof)# switchport mode trunk
TeamX-N1Kv(config-port-prof)# switchport trunk allowed vlan X0-X3
(where X is Team number)
TeamX-N1Kv(config-port-prof)# no shutdown
TeamX-N1Kv(config-port-prof)# system vlan X1,X2 (where X is Team #)
TeamX-N1Kv(config-port-prof)# vmware port-group
```

When using the **vmware port-group <name>** command, if no name is specified, the port profile name is used for the VMware port group.

```
TeamX-N1Kv(config-port-prof)# state enabled
```

Step 8: Save your configuration.

```
TeamX-N1Kv(config-port-prof)# copy run start
[########################################] 100%
```

This Port Profile will be used for communication between VSM and VEM and for outbound VM communication. Separate Port Profiles can also be used for these functions.

Step 9: Verify the system port profile configuration.

```
TeamX-N1Kv(config-port-prof)# show port-profile name systemUplinkX
port-profile systemUplinkX
description: System Uplink
type: ethernet
status: enabled
max-ports: 32
min-ports: 1
capability l3control: no
capability iscsi-multipath: no
system vlans: X2-X3
port-group: systemUplinkX
max-ports: -
inherit:
config attributes:
      switchport mode trunk
      switchport trunk allowed vlan X0-X4
      no shutdown
evaluated config attributes:
      switchport mode trunk
      switchport trunk allowed vlan X0-X4
      no shutdown
assigned interfaces:
```

No interfaces are shown because none have been assigned yet. Interfaces are assigned from the vSphere client.

Step 10: Exit the Port Profile configuration prompt:

```
TeamX-N1Kv(config-port-prof)# exit
TeamX-N1Kv(config)#
```

Task 2: Create Port Profiles for Management Ports

In this task, you will create a port profile for communication between the Nexus 1000V VSM and VEM's.

Activity Procedure

Complete these steps:

Step 1: Configure port profile for the Control port group.

```
TeamX-N1Kv(config)# port-profile ControlX1 (where X is Team number)
TeamX-N1Kv(config-port-prof)# description Control Port Group
TeamX-N1Kv(config-port-prof)# switchport mode access
TeamX-N1Kv(config-port-prof)# switchport access vlan X1 (where X is
Team number)
TeamX-N1Kv(config-port-prof)# no shutdown
TeamX-N1Kv(config-port-prof)# system vlan X1 (where X is Team #)
TeamX-N1Kv(config-port-prof)# vmware port-group
```

When using the **vmware port-group <name>** command, if no name is specified, the port profile name is used for the VMware port group.

```
TeamX-N1Kv(config-port-prof)# state enabled
```

Step 2: Save your configuration

```
TeamX-N1Kv(config-port-prof)# copy run start
[########################################] 100%
```

Step 3: Verify the port profile.

```
TeamX-N1Kv(config-port-prof)# show port-profile name ControlX1
port-profile ControlX1
description: Control Port Group
type: vethernet
status: enabled
capability l3control: no
pinning control-vlan: -
pinning packet-vlan: -
system vlans: X1
port-group: ControlX1
max-ports: 32
inherit:
config attributes:
      switchport mode access
      switchport access vlan X1
      no shutdown
evaluated config attributes:
      switchport mode access
      switchport access vlan X1
      no shutdown
assigned interfaces:
```

No interfaces are shown because none have been assigned yet. Interfaces are assigned from the vSphere client.

Step 4: Exit the Port Profile Configuration prompt:

```
TeamX-N1Kv(config-port-prof)# exit
TeamX-N1Kv(config)#
```

Step 5: Configure port profile for the Packet port group.

```
TeamX-N1Kv(config)# port-profile PacketX2 (where X is Team number)
TeamX-N1Kv(config-port-prof)# description Packet Port Group
TeamX-N1Kv(config-port-prof)# switchport mode access
TeamX-N1Kv(config-port-prof)# switchport access vlan X2 (where X is
Team number)
TeamX-N1Kv(config-port-prof)# no shutdown
TeamX-N1Kv(config-port-prof)# system vlan X2 (where X is Team #)
TeamX-N1Kv(config-port-prof)# vmware port-group
```

When using the **vmware port-group <name>** command, if no name is specified, the port profile name is used for the VMware port group.

```
TeamX-N1Kv(config-port-prof)# state enabled
```

Step 6: Save your configuration.

```
TeamX-N1Kv(config-port-prof)# copy run start
[########################################] 100%
```

This Port Profile will be used for communication between VSM and VEM and for outbound VM communication. Separate Port Profiles can also be used for these functions.

Step 7: Verify the port profile.

```
TeamX-N1Kv(config-port-prof)# show port-profile name PacketX2
port-profile PacketX2
      description: Packet Port Group
      type: vethernet
      status: enabled
      capability l3control: no
      pinning control-vlan: -
      pinning packet-vlan: -
      system vlans: X2
      port-group: PacketX2
      max-ports: 32
      inherit:
      config attributes:
            switchport mode access
            switchport access vlan X2
            no shutdown
      evaluated config attributes:
            switchport mode access
            switchport access vlan X2
            no shutdown
      assigned interfaces:
```

No interfaces are shown because none have been assigned yet. Interfaces are assigned from the vSphere client.

Step 8: Exit the Port Profile Configuration prompt:

```
TeamX-N1Kv(config-port-prof)# exit
TeamX-N1Kv(config)#
```

Task 3: Create a Data Port Profile

In this task, you will create a port profile for a virtual machine port group.

Activity Procedure

Complete these steps:

Step 1: Create the Management VLAN.

```
TeamX-N1Kv(config)# vlan X3 (where X is your team number)
```

Step 2: Create a VM data profile.

```
TeamX-N1Kv(config-vlan)# port-profile vmDataX (where X is team
number)
TeamX-N1Kv(config-port-prof)# description VM Data Port Group
TeamX-N1Kv(config-port-prof)# switchport mode access
TeamX-N1Kv(config-port-prof)# switchport access vlan X3 (where X is
team number)
TeamX-N1Kv(config-port-prof)# vmware port-group
```

Because a port group name is not specified, the port profile name will be used to export the profile to the vSphere server.

```
TeamX-N1Kv(config-port-prof)# no shutdown
TeamX-N1Kv(config-port-prof)# state enabled
```

Step 3: Save your configuration.

```
TeamX-N1Kv(config-port-prof)# copy run start
[########################################] 100%
```

Step 4: Verify the port profile configuration.

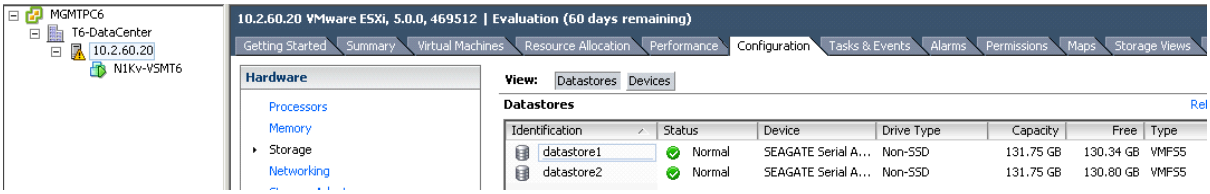
```
TeamX-N1Kv(config-port-prof)# show port-profile name vmDataX (Where
X is team number).
port-profile vmDataX
  description: VM Data Port Group
  type: vethernet
  status: enabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group: vmDataX
  max-ports: 32
  inherit:
  config attributes:
      switchport mode access
      switchport access vlan X3
      no shutdown
  evaluated config attributes:
      switchport mode access
      switchport access vlan X3
      no shutdown
  assigned interfaces:
```

Step 5: Return to the Datacenter Networking view. Your team's Port Groups should be visible.

Task 4a: Copy the VEM install package to your Host

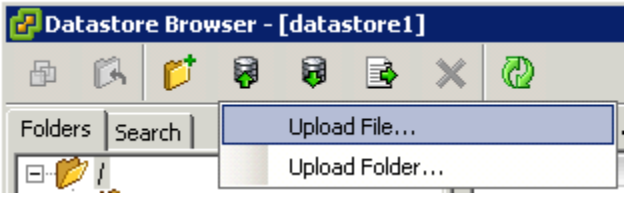
Step 1 If needed, open your vSphere client and connect to your vCenter Server as was originally explained in Lab 9, Task 4.

Step 2 Using your vSphere Client, expand on your "TeamX-DataCenter" so you may click on your ESXi host. Across the top-right click on the **Configuration** tab and then the **Storage** option beneath the "Hardware" section.



Step 3 Once there, right-click on the **datastore1** Datastore and choose "Browse Datastore". In this new window click on the folder icon with a green plus sign. That's the "Create New Directory" icon. Name this new directory **VEM**.

Step 4 Finally, we will upload the Nexus 1000V VSM install package to the newly created directory on your host's local datastore. Click on the "Upload to this Datastore" icon and browse to **DESKTOP\Nexus1000v\VEM** and select the **VEM500-201108271.zip** to upload it to the host's datastore.



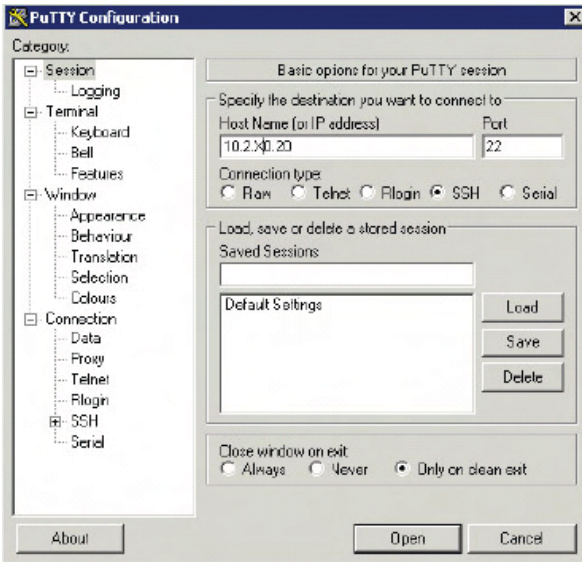
Task 4b: Install the VEM and Add Hosts to the Distributed Switch

In this task, you will install the Virtual Ethernet Module on the ESXi host and add the ESXi host to the Cisco Nexus 1000V Distributed Switch.

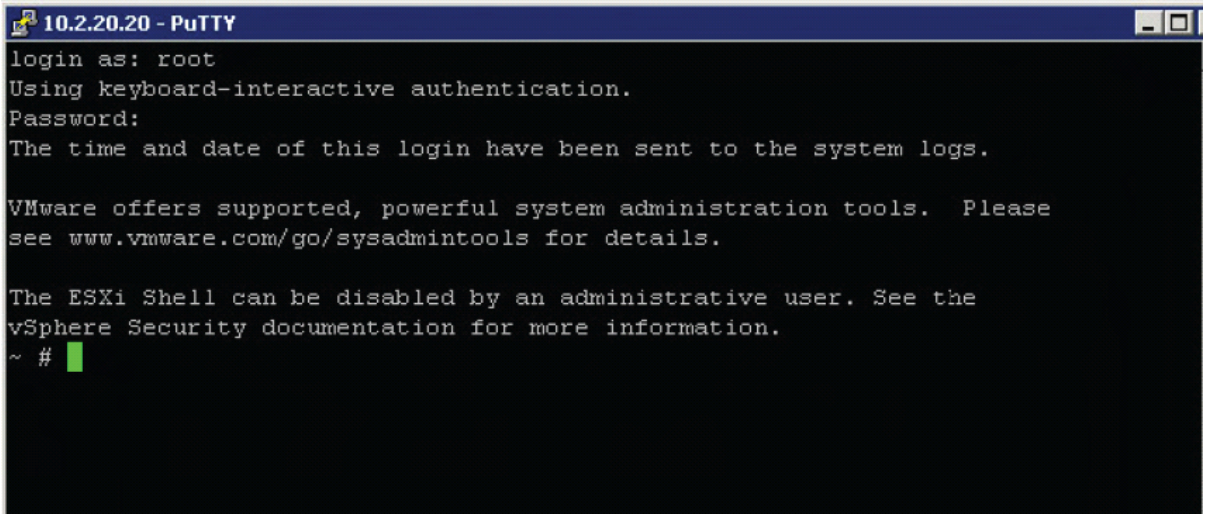
Activity Procedure

Complete these steps:

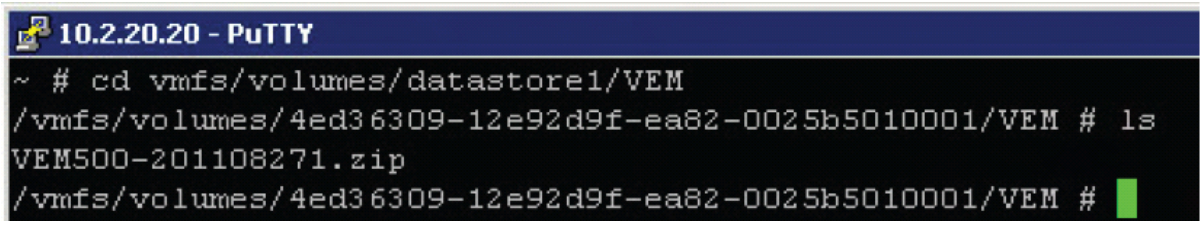
Step 1: From your student desktop, launch a PuTTY ssh session to your team's ESXi host's Tech Support mode console interface. It should be 10.2.X0.20, X being your Team group.



Step 2: Log in with username: root, password: cisco123.



Step 3: Navigate to the directory where the Cisco Nexus 1000V VEM file is located and perform a ls command to get the name of the current version.



Step 4: Install the Cisco Nexus 1000V VEM image into the ESX host.

Using the tab key after starting to type the filename will automatically complete it without having to type the entire filename.

```
/vmfs/volumes/4a65cce…00000667/VEM # esxcli software vib install
-d /vmfs/volumes/datastore1/VEM/VEM500-201108271.zip
```

Step 5: Verify that the DPA is running with the vem status command.

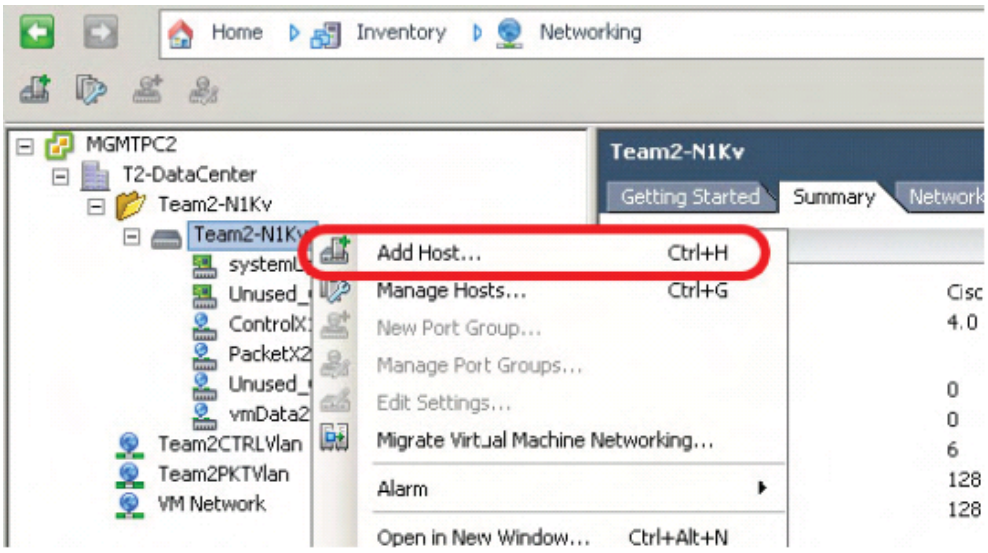
```
~ # vem status

VEM modules are loaded

Switch Name       Num Ports   Used Ports  Configured Ports  MTU
Uplinks
vSwitch0             128           6           128          1500
vmnic1

VEM Agent (vemdpa) is running
```

Step 6: Exit the console.

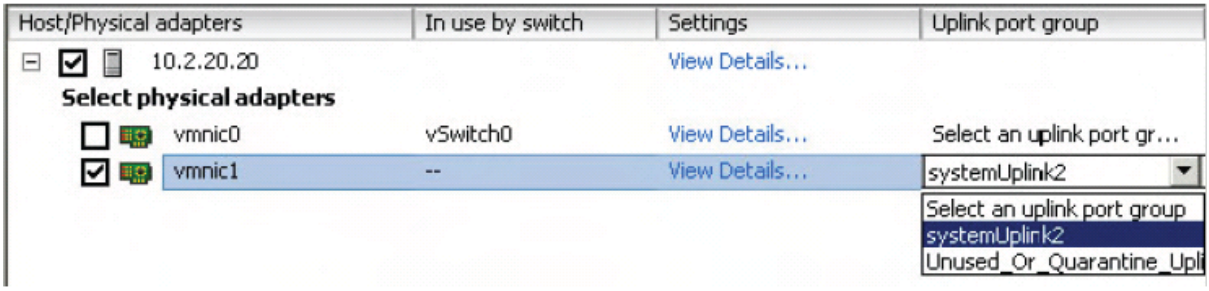
~ #exit

Step 7: Log into the VSphere client and connect to your VCenter Server instance.

Step 8: Open the Networking Inventory view, right-click the TeamX-N1Kv Distributed Switch and click Add Host.

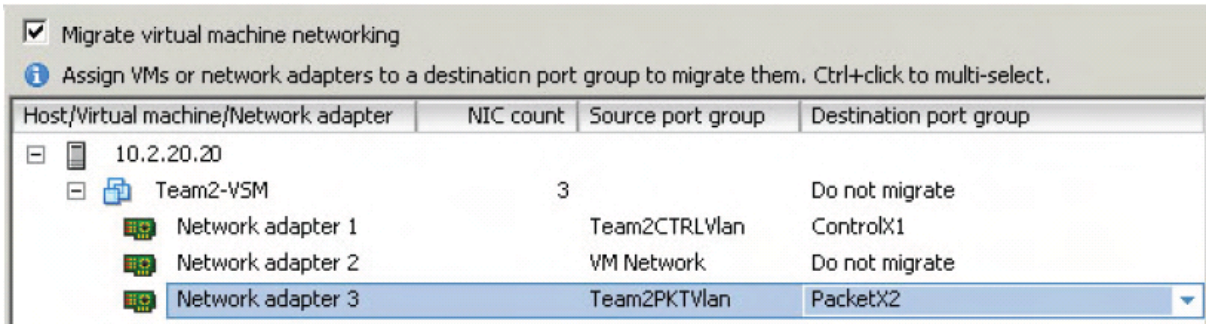


Step 9: In the "Select hosts and physical adapters" window, select your team's host; the vmnic that is currently NOT in use by a switch and the systemUplinkX port group and click Next> to continue.

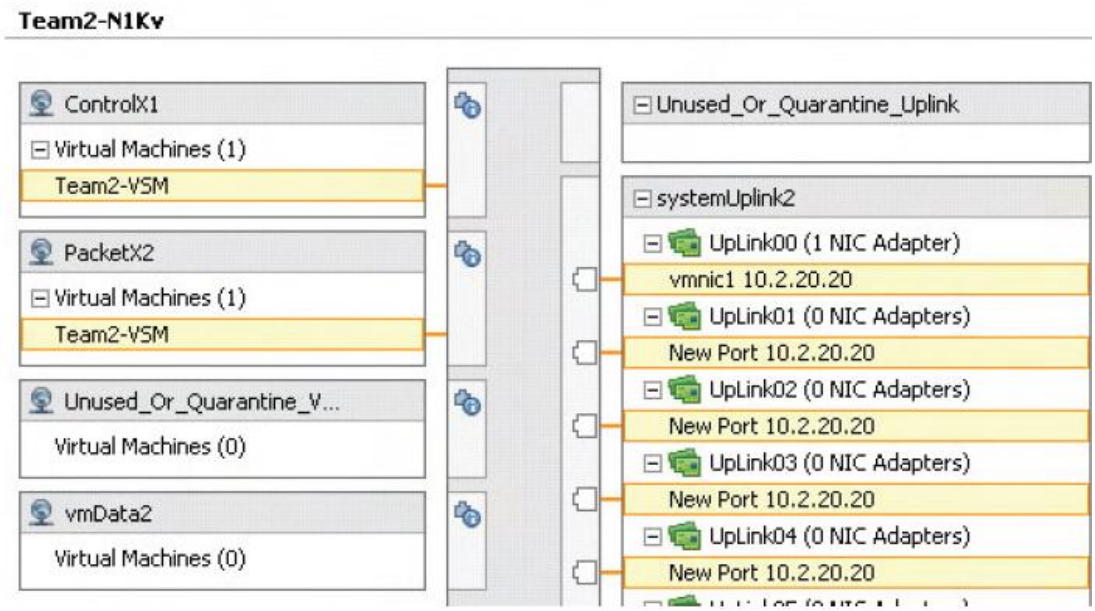


Step 10: Click Next to continue past the "Network connectivity" window. On the "Virtual machine networking" window, Check the "Migrate virtual machines networking box; expand out the VSM VM and migrate

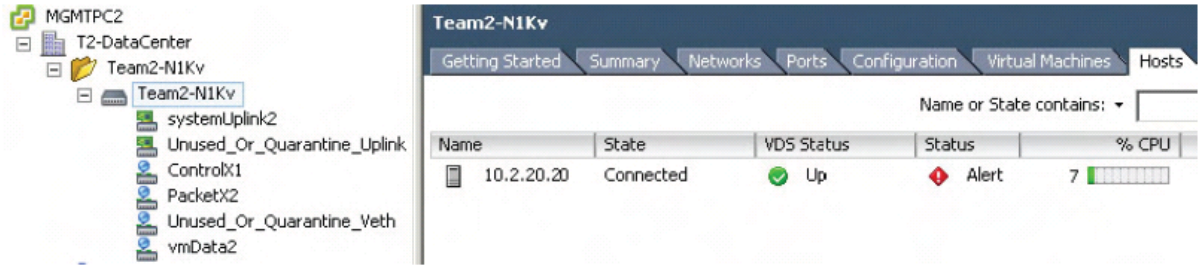
Network adapters from the Control and Packet port groups on vSwitch 0 to the ControlX1 and PacketX2 port groups on the TeamX-N1Kv Distributed Switch click Next to continue.



Step 11: Verify the settings and click Finish.



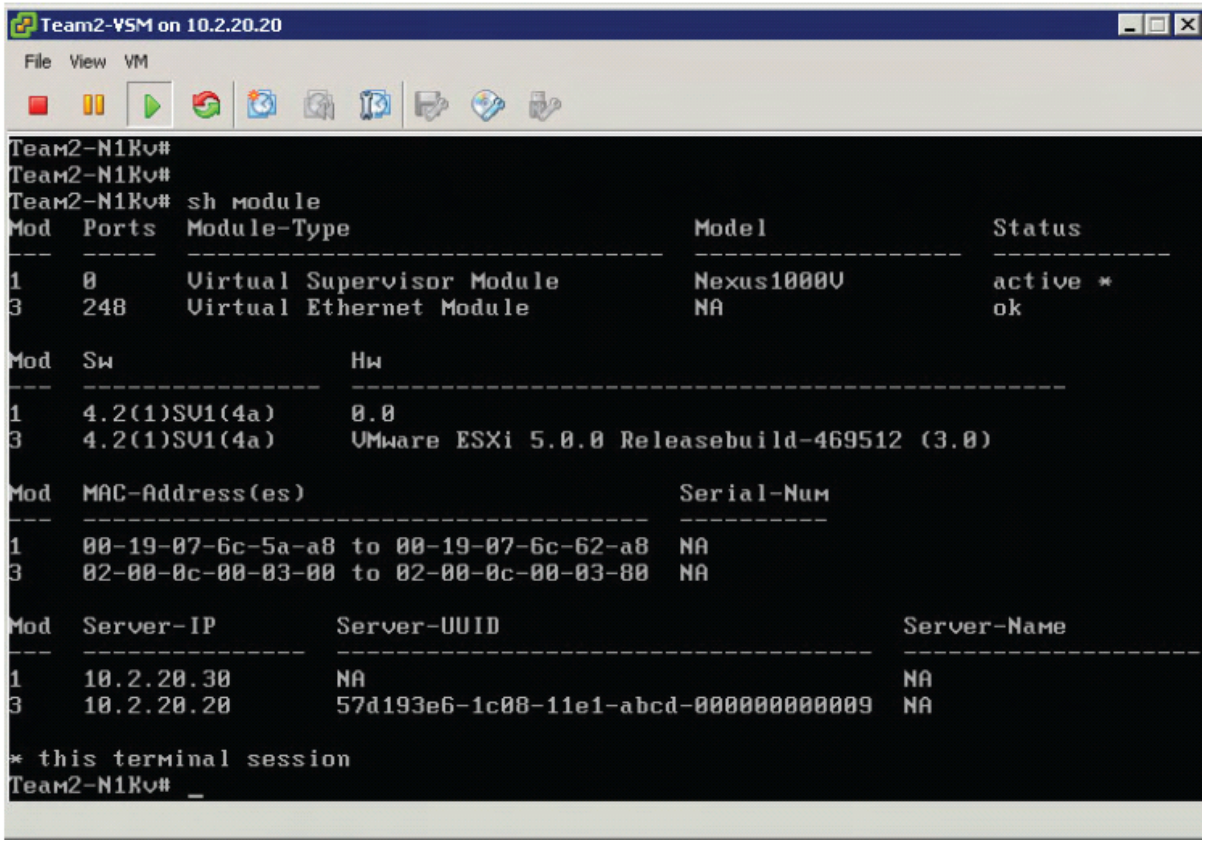
Step 12: With the TeamX-N1Kv DVS still selected, click on the Hosts tab and verify you're your host is present.

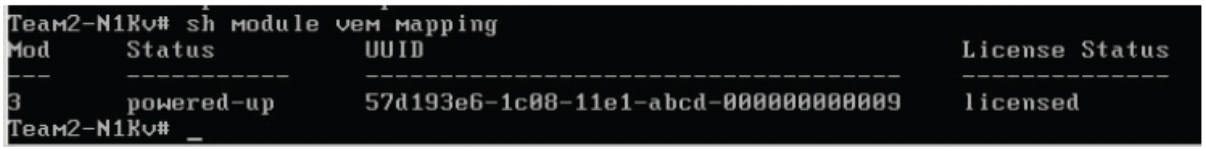


Step 13: Return to the PuTTY ssh session to the VSM to verify the configuration.

If you have closed the ssh session, open a PuTTY session from the desktop to your team's VSM, 10.2.20.30 , with username: admin and password: 1234Qwer.

Step 14: Verify that the Cisco Nexus 1000V VEM installed on the host is properly communicating with the Cisco Nexus 1000V VSM by using the show module and show module vem mappings commands. The output should look like this:





Step 15: Save your configuration and end the ssh session with the VSM

```
TeamX-N1Kv(config-port-prof)# copy run start
[########################################] 100%
TeamX-N1Kv(config-port-prof)# end
```