

DCUCT

Troubleshooting Cisco Data Center Unified Computing

Version 5.0

Lab Guide

Text Part Number: 97-3219-01



Americas Headquarters

Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters

Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters

Cisco Systems International BV Amsterdam,
The Netherlands

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

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

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

Table of Contents

Lab Guide	1
Overview	1
Outline	1
Lab 1-1: Cisco UCS Network Baseline Documentation	2
Activity Objective	2
Visual Objective	2
Required Resources	3
Command List	3
Job Aids	4
Task 1: Verify Cisco UCS B-Series Equipment Using Cisco UCSM GUI	5
Task 2: Verify Cisco UCS C-Series Equipment Using Cisco IMC	6
Task 3: Examine LAN and SAN Network Topology	7
Lab 1-2: Cisco UCS Management and Service Profile Deployment	10
Activity Objective	10
Visual Objective	10
Required Resources	10
Job Aids	10
Trouble Ticket	12
Lab 1-3: Troubleshoot Cisco UCS B-Series Server Boot from SAN	13
Activity Objective	13
Visual Objective	13
Required Resources	13
Job Aids	14
Command List	14
Trouble Ticket	15
Lab 1-4: Troubleshoot LAN Connectivity: Part 1	16
Activity Objective	16
Visual Objective	16
Required Resources	16
Job Aids	17
Trouble Ticket	18
Lab 1-5: Troubleshoot LAN Connectivity: Part 2	19
Activity Objective	19
Visual Objective	19
Required Resources	19
Job Aids	20
Trouble Ticket	21
Lab 1-6: Troubleshoot Failover Connectivity: Part 1	22
Activity Objective	22
Visual Objective	22
Required Resources	22
Job Aids	23
Trouble Ticket	24
Lab 1-7: Troubleshoot Failover Connectivity: Part 2	25
Activity Objective	25
Visual Objective	25
Required Resources	25
Job Aids	26
Trouble Ticket	27
Lab 2-1: Troubleshoot Cisco UCS C-Series Server Boot from SAN	28
Activity Objective	28
Visual Objective	28
Required Resources	28
Job Aids	29
Command List	29
Trouble Ticket	30

Lab 2-2: Troubleshoot Network Connectivity	32
Activity Objective	32
Visual Objective	32
Required Resources	32
Job Aids	33
Command List	33
Trouble Ticket	34
Answer Key	35
Lab 1-1 Answer Key: Cisco UCS Network Baseline Documentation	35
Lab 1-2 Answer Key: Cisco UCS Management and Service Profile Deployment	48
Lab 1-3 Answer Key: Troubleshoot Cisco UCS B-Series Server Boot from SAN	53
Lab 1-4 Answer Key: Troubleshoot LAN Connectivity: Part 1	57
Lab 1-5 Answer Key: Troubleshoot LAN Connectivity: Part 2	60
Lab 1-6 Answer Key: Troubleshoot Failover Connectivity: Part 1	64
Lab 1-7 Answer Key: Troubleshoot Failover Connectivity: Part 2	66
Lab 2-1 Answer Key: Troubleshoot Cisco UCS C-Series Server Boot from SAN	68
Lab 2-2 Answer Key: Troubleshoot Network Connectivity	70

Lab Guide

Overview

This guide presents the instructions and other information concerning the lab activities for this course. You can find the solutions in the lab activity Answer Key.

Outline

This guide includes these activities:

- Lab 1-1: Cisco UCS Network Baseline Documentation
- Lab 1-2: Cisco UCS Management and Service Profile Deployment
- Lab 1-3: Troubleshoot Cisco UCS B-Series Server Boot from SAN
- Lab 1-4: Troubleshoot LAN Connectivity: Part 1
- Lab 1-5: Troubleshoot LAN Connectivity: Part 2
- Lab 1-6: Troubleshoot Failover Connectivity: Part 1
- Lab 1-7: Troubleshoot Failover Connectivity: Part 2
- Lab 2-1: Troubleshoot Cisco UCS C-Series Server Boot from SAN
- Lab 2-2: Troubleshoot Network Connectivity

Lab 1-1: Cisco UCS Network Baseline Documentation

Complete this lab activity to practice using support tools that are available for Cisco UCS systems and to determine equipment available in the lab.

Activity Objective

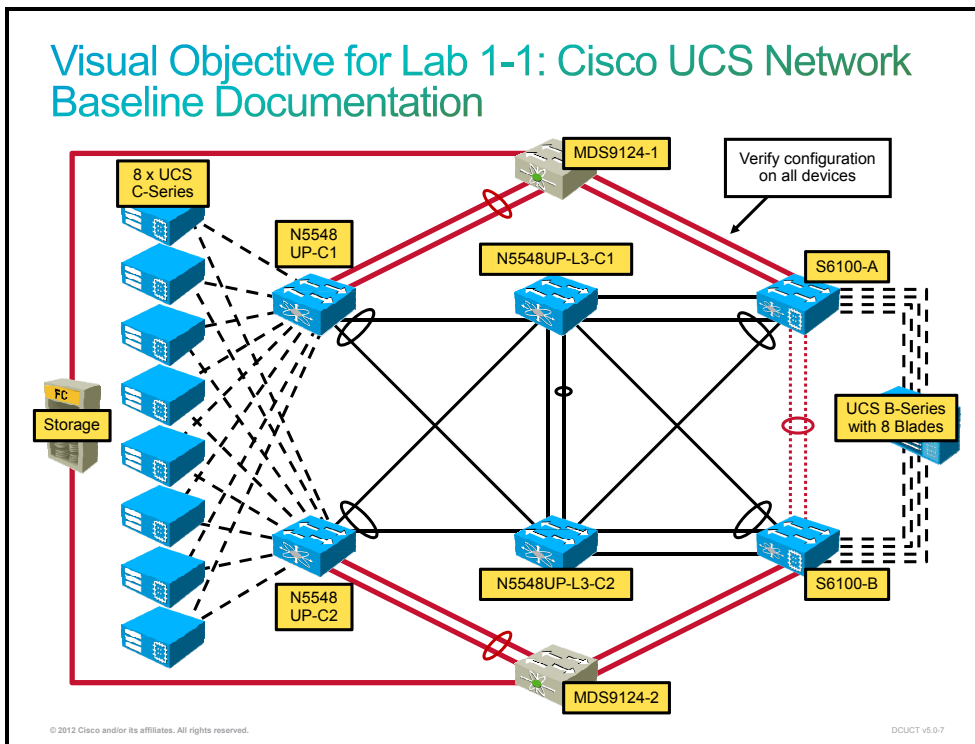
In this activity, you will use the CLI or GUI to log in to the equipment in your pod. After completing this activity, you will be able to meet these objectives:

- Check that you can access the lab environment
- Examine Cisco UCS B-Series server equipment using the Cisco UCSM GUI
- Examine Cisco UCS C-Series server equipment using the Cisco IMC
- Examine LAN and SAN network topology

Caution Do not reload the equipment or erase the configurations because it can take more than 20 minutes to complete the reload.

Visual Objective

The figure illustrates your lab topology.



Required Resources

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

- Instructor to provide the access details for lab equipment
- A computer and network access
- Two Cisco Nexus 5548UP switches with Layer 3 module
- Two Cisco Nexus 5548UP switches
- Eight Cisco UCS C-Series servers
- Two Cisco MDS 9124 switches
- Disk array
- Two Cisco UCS 6120XP servers
- One Cisco UCS 5108 server
- Eight Cisco UCS B-Series servers

Command List

The table describes the commands that are used in this activity.

Cisco UCSM and NX-OS Commands

Command	Description
<code>connect local-mgmt</code>	Connects to the local management port
<code>connect nxos</code>	Connects to NX-OS CLI
<code>scope license</code>	Enters the license mode
<code>show cdp neighbor</code>	Displays neighbor information obtained by Cisco Discovery Protocol
<code>show cluster state</code>	Displays cluster information
<code>show interface brief</code>	Displays brief overview of interfaces
<code>show interface status</code>	Displays interface status
<code>show usage detail</code>	Displays license usage for a Fabric Interconnect
<code>show version</code>	Displays Cisco NX-OS version

Job Aids

These job aids are available to help you complete the lab activity.

Management IP Addressing

Device	Interface	Device IP	Default Gateway	Username	Password
UCS cluster	Mgmt0	192.168.10.200	192.168.10.254	admin	NXos12345
s6100-A	Mgmt0	192.168.10.101	192.168.10.254	admin	NXos12345
s6100-B	Mgmt0	192.168.10.102	192.168.10.254	admin	NXos12345
MDS9124-1	Mgmt0	192.168.10.2	192.168.10.254	admin	NXos12345
MDS9124-2	Mgmt0	192.168.20.2	192.168.20.254	admin	NXos12345
N5548UP-L3-C1	Mgmt0	192.168.100.1	192.168.100.254	admin	NXos12345
N5548UP-L3-C2	Mgmt0	192.168.100.2	192.168.100.254	admin	NXos12345
N5548UP-C1	Mgmt0	192.168.10.91	192.168.100.254	admin	NXos12345
N5548UP-C2	Mgmt0	192.168.10.92	192.168.100.254	admin	NXos12345
C200-M2-1	Mgmt0	192.168.10.41	192.168.100.254	admin	NXos12345
C200-M2-2	Mgmt0	192.168.10.42	192.168.100.254	admin	NXos12345
C200-M2-3	Mgmt0	192.168.10.43	192.168.100.254	admin	NXos12345
C200-M2-4	Mgmt0	192.168.10.44	192.168.100.254	admin	NXos12345
C200-M2-5	Mgmt0	192.168.10.45	192.168.100.254	admin	NXos12345
C200-M2-6	Mgmt0	192.168.10.46	192.168.100.254	admin	NXos12345

Task 1: Verify Cisco UCS B-Series Equipment Using Cisco UCSM GUI

In this task, you will examine Cisco UCS B-Series server equipment using Cisco UCS Manager (UCSM) GUI.

Activity Procedure

Complete these steps:

- Step 1** On your assigned management PC, open Cisco UCSM.
- Step 2** On the web page, select Cisco UCSM and log in using username *admin* with password *NXos12345*. The Equipment topology page appears.
- Step 3** Select the Equipment tab in the left pane.
- Step 4** Select **Chassis**, and in the right pane, select the server assigned to your pad.
- Step 5** Right-click on your server and select **Show Navigator**.
- Step 6** In the right pane, select the **Inventory** tab.
- Step 7** By navigating over different sub-tabs, determine and write down the server inventory in student notes.

Note By double-clicking on different elements, you can access additional properties. For some requested information, that might be necessary.

- Step 8** Write down any other information regarding your server that you might need for troubleshooting purposes.
- Step 9** In the left pane, select **Chassis 1** and then **IO Modules**. Expand the view in the right pane by clicking on the + sign. Write down the IO modules model in your chassis, the port types, and the number of ports.

Student Notes

Use this Student Notes section to write down all information instructed in the activity procedure.

BIOS firmware version: _____

Cisco IMC running version: _____

Number of CPUs and type: _____

CPU speed: _____

Number of cores per CPU: _____

Number of memory DIMMs and total memory capacity: _____

Number and type of adapters: _____

IO Module number and model: _____

Activity Verification

You have completed this task when you attain this result:

- Requested information is written down in the Student Notes section.

Task 3: Examine LAN and SAN Network Topology

In this task, you will examine LAN and SAN network topology.

Activity Procedure

Complete these steps:

- Step 1** On your assigned management PC, open Cisco UCSM.
- Step 2** On the web page, select Cisco UCSM and log in using username *admin* with password *NXos12345*. The Equipment topology page appears.
- Step 3** Select the **Equipment** tab in the left pane.
- Step 4** Select **Fabric Interconnect** and then, in the right pane, select the **Fabric Interconnects** tab.
- Step 5** Expand the view by clicking on the + sign.
- Step 6** Write down number of uplink, server, and Fibre Channel ports on each Fabric Interconnect. Also, write down the number of unconfigured Ethernet ports.
- Step 7** By navigating over different tabs, determine and write down the server inventory in your student notes.
- Step 8** Connect to Cisco UCSM using SSH protocol. Connect by using PuTTY or a similar terminal client. Use IP address 192.168.10.200. Log in using username *admin* with password *NXos12345*.
- Step 9** By using Cisco Discovery Protocol, determine neighboring devices and ports used for connection. Write that information into the student notes.
- Step 10** Determine and write down the Cisco NX-OS version running on the Fabric Interconnect.
- Step 11** Determine and write down the module types and the number installed on the Fabric Interconnect.
- Step 12** Determine and write down the number and type of FEXs attached to the Fabric Interconnect.
- Step 13** Determine and write down the number of interfaces and their status.
- Step 14** Determine and write down the cluster status.
- Step 15** Determine and write down the license usage on the Fabric Interconnect.
- Step 16** Fill in the interface assignments in the table. Get the required information by logging in to the devices.

Student Notes

Use this Student Notes section to write down all information instructed in the activity procedure.

FI-A:

Uplink ports: _____

Server ports: _____

Fibre Channel ports: _____

Unconfigured Ethernet ports: _____

FI-B:

Uplink ports: _____

Server ports: _____

Fibre Channel ports: _____

Unconfigured Ethernet ports: _____

Cisco Discovery Protocol neighbors: _____

Cisco NX-OS version: _____

Fabric Interconnect modules: _____

FEX information: _____

Device	Interfaces	Comment
FI-A		Connection to N5548UP-L3-C1
FI-A		Connection to N5548UP-L3-C2
FI-A		Connection to MDS9214-1
FI-A		Connection to MDS9214-2
FI-A		Connection to UCS chassis 5108

Device	Interfaces	Comment
FI-B		Connection to N5548UP-L3-C1
FI-B		Connection to N5548UP-L3-C2
FI-B		Connection to MDS9214-1
FI-B		Connection to MDS9214-2
FI-B		Connection to UCS chassis 5108
N5548UP-L3-C1		Connection to N5548UP-L3-C2
N5548UP-L3-C1		Connection to N5548UP-C1
N5548UP-L3-C1		Connection to N5548UP-C2
N5548UP-L3-C2		Connection to N5548UP-L3-C1
N5548UP-L3-C2		Connection to N5548UP-C1
N5548UP-L3-C2		Connection to N5548UP-C2
N5548UP-C1		Connection to UCS C-Series server 1
N5548UP-C1		Connection to UCS C-Series server 2
N5548UP-C1		Connection to UCS C-Series server 3
N5548UP-C1		Connection to UCS C-Series server 4
N5548UP-C1		Connection to UCS C-Series server 5
N5548UP-C1		Connection to UCS C-Series server 6
N5548UP-C1		Connection to MDS9214-1
N5548UP-C2		Connection to UCS C-Series server 1
N5548UP-C2		Connection to UCS C-Series server 2
N5548UP-C2		Connection to UCS C-Series server 3
N5548UP-C2		Connection to UCS C-Series server 4
N5548UP-C2		Connection to UCS C-Series server 5
N5548UP-C2		Connection to UCS C server 6
N5548UP-C2		Connection to MDS9214-2
MDS9214-1		Connection to Storage Array
MDS9214-2		Connection to Storage Array

Activity Verification

You have completed this task when you attain this result:

- Requested info is written down in the Student Notes section.

Lab 1-2: Cisco UCS Management and Service Profile Deployment

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

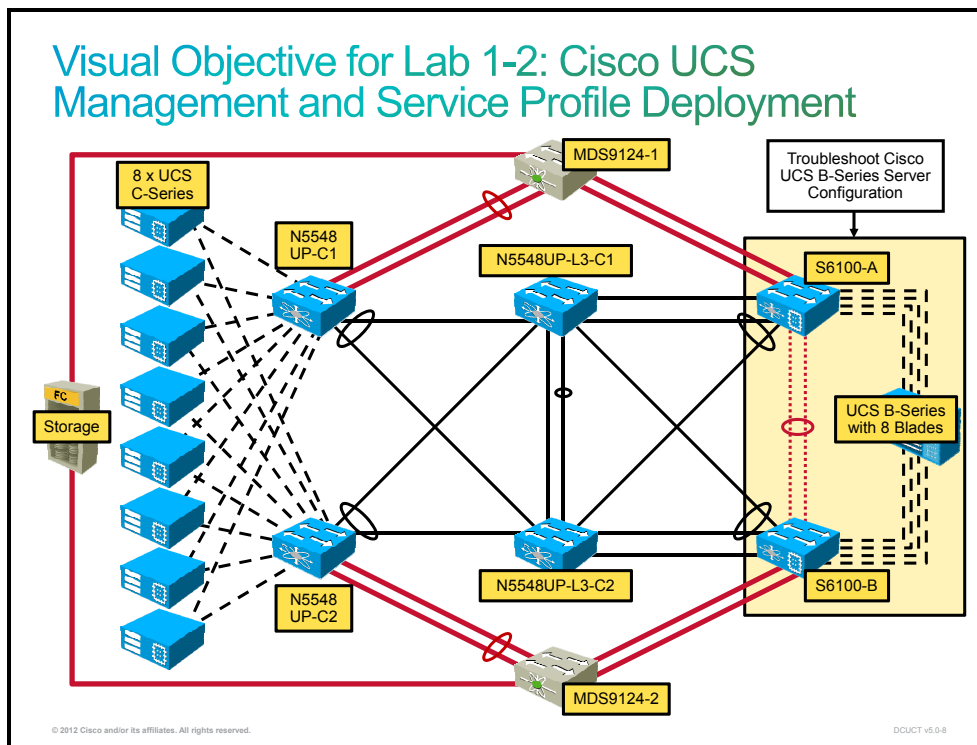
Activity Objective

In this activity, you will troubleshoot service profiles. After completing this activity, you will be able to meet these objectives:

- Perform trouble analysis and identify the cause of the problem
- Resolve the issue
- Successfully associate the service profile created from the service profile template

Visual Objective

The figure illustrates your lab topology.



Required Resources

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

- Two Cisco UCS 6120XP servers
- One Cisco UCS 5108 server
- Eight Cisco UCS B-Series servers

Job Aids

These job aids are available to help you complete the lab activity.

Server per Pod Assignment (where X is your pod number)

Pod	Blade
PODX	Server 1/X

UUID Addresses (where X is your pod number)

UUID Prefix	UUID Suffix
010025b5-0003-4100	0001-0000b200e20X

WWNN Values (where X is your pod number)

WWNN Addresses
20:00:00:25:B5:11:50:BX

WWPN Addresses (where X is your pod number)

HBA	WWPN Addresses
HBA - a	20:00:00:25:B5:A1:50:BX
HBA - b	20:00:00:25:B5:B1:50:BX

KVM Management IP Addresses

Pod	IP Management Pool
POD1	192.168.10.110
POD2	192.168.10.111
POD3	192.168.10.112
POD4	192.168.10.113

Trouble Ticket

The customer has deployed a new Cisco UCS and is in the process of deploying new ESXi hosts. The customer would like to use a service profile template to create their service profile. They have already configured a service profile template. When they create a service profile template from the service profile, they receive an error and they do not know how to solve the problems.

The customer has problems with accessing the KVM console.

The customer also wants to fix the problems that they had with previous service profiles in the testing deployments. When they applied some changes to the service profile, the system would reboot the servers without warning, leading to downtime. They want to fix this issue.

Activity Procedure

Complete these steps:

- Step 1** On your assigned management PC, open Internet Explorer and connect to the Cisco UCS Manager at IP address 192.168.10.200. If a security warning appears that the security certificate is not recognized, click **Continue to this website** (not Activity Verification).
- Step 2** Log in with username *admin* with password *NXos12345*. Cisco UCS manager appears.
- Step 3** From the UCS Manager Server tab, navigate to **Servers > Service Profile Templates > DCUCT > PODX** (where X is your pod number). From your service profile template, create one service profile.
- Step 4** Start troubleshooting.

Activity Verification

You have completed this task when you attain these results:

- Service profile does not have any errors and the association of your service profile to the blade is successful.
- Your server does not automatically reboot when you make some changes on the service profile templates.
- You can access your blade KVM console.

Lab 1-3: Troubleshoot Cisco UCS B-Series Server Boot from SAN

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

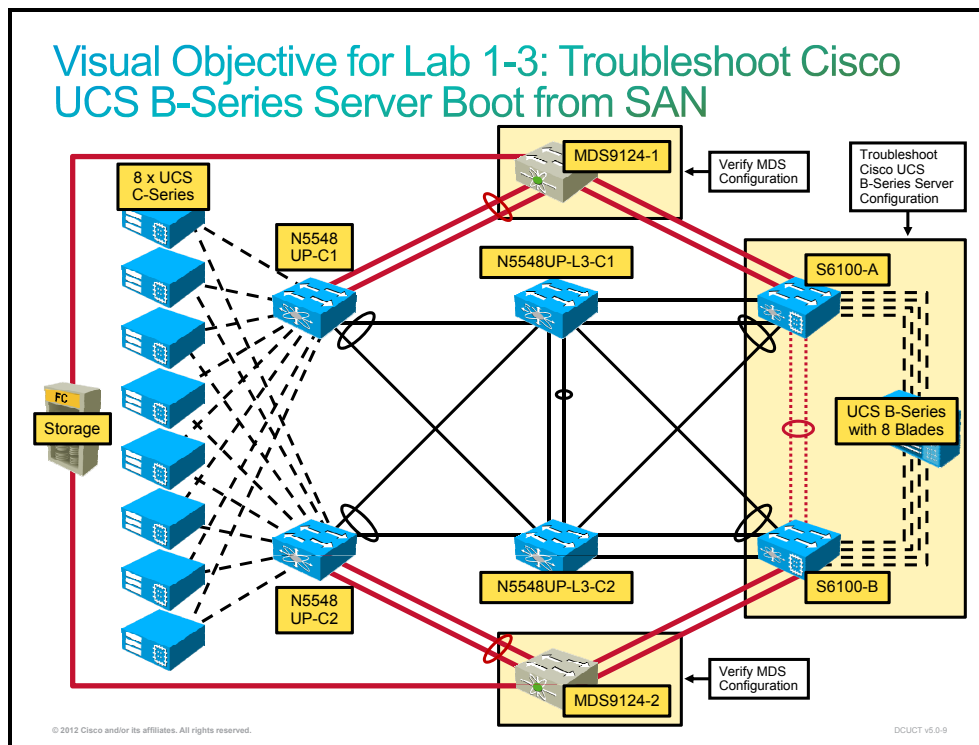
Activity Objective

In this activity, you will troubleshoot a bootup from the SAN. After completing this activity, you will be able to meet these objectives:

- Perform trouble analysis and identify the cause of the problem
- Resolve the issue
- Boot the ESXi server from the SAN

Visual Objective

The figure illustrates your lab topology.



Required Resources

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

- Two Cisco UCS 6120XP servers
- One Cisco UCS 5108 server
- Eight UCS B-Series servers
- Two MDS switches
- One storage array

Job Aids

These job aids are available to help you complete the lab activity.

Server per Pod Assignment (where X is your pod number)

Pod	Blade
PODX	Server 1/X

UUID Values (where X is your pod number)

UUID Prefix	UUID Suffix
010025b5-0003-4100	0001-0000b200e20X

WWNN Values (where X is your pod number)

WWNN Pools
20:00:00:25:B5:11:50:BX

WWPN Values (where X is your pod number)

HBA	WWPN Pool
HBA-a	20:00:00:25:B5:A1:50:BX
HBA-b	20:00:00:25:B5:B1:50:BX

Boot from SAN Parameters for All Pods

Boot Position	Device	VSAN	WWPN	LUN ID
SAN Target primary	HBA-a	11	50:06:01:60:41:e0:9f:5b	0
SAN Target secondary	HBA-a	11	50:06:01:69:41:e0:9f:5b	0
SAN Target primary	HBA-b	12	50:06:01:68:41:e0:9f:5b	0
SAN Target secondary	HBA-b	12	50:06:01:61:41:e0:9f:5b	0

Command List

The table describes the commands used in this activity.

Command	Description
<code>connect nx-os</code>	Connects to Cisco NX-OS CLI
<code>fcping</code>	Performs Fibre Channel Ping to connected neighbor
<code>feature npiv</code>	Enables feature NPIV
<code>show features</code>	Displays enabled features on MDS switch
<code>show flogi database</code>	Displays the FLOGI table
<code>show npvflogi-table</code>	Shows FLOGI table on the Cisco UCS NX-OS
<code>show vsan</code>	Displays the VSANs
<code>show zone active</code>	Displays active zones
<code>show zoneset active</code>	Displays active zonesets

Trouble Ticket

The customer is having a problem with booting the ESXi server from the SAN. The storage engineer has already configured the zoning and LUN masking. On the boot LUN, the customer has already installed the operating system, which was achieved with LUN copy functionality provided by the storage array. They want to fix the issue and they need your help.

Activity Procedure

Complete these steps:

Step 1 Open the KVM of your service profile, created in a previous lab.

Step 2 Verify that your operating system does not boot.

```
Reboot and Select proper Boot device  
or Insert Boot Media in selected Boot device and press a key_
```

Step 3 Log in to the Cisco UCS and both MDS switches and then start troubleshooting.

Note Zoning on the MDS switches and LUN masking on the storage array is already pre-configured. You do not need to configure anything there.

Activity Verification

You have completed this task when you attain these results:

- You successfully booted the ESXi server.
- You see on both MDS switches your service profile HBA.

Lab 1-4: Troubleshoot LAN Connectivity: Part 1

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

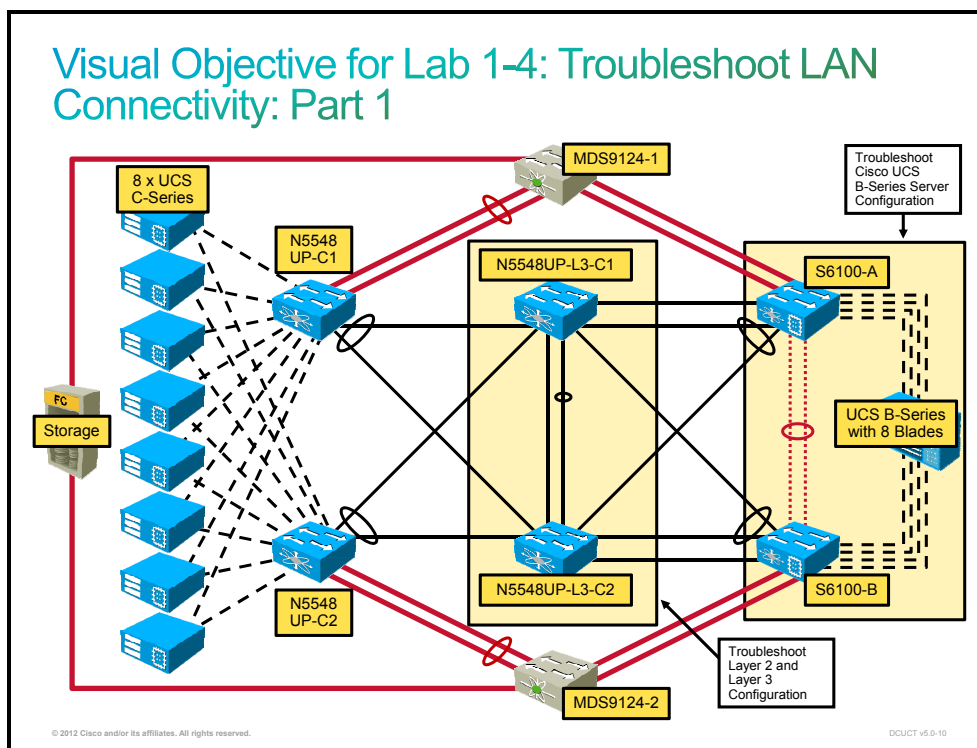
Activity Objective

In this activity, you will troubleshoot network connectivity. After completing this activity, you will be able to meet these objectives:

- Perform trouble analysis and identify the cause of the problem
- Resolve the issue
- Ping or access the management interface of the host

Visual Objective

The figure illustrates your lab topology.



Required Resources

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

- Two Cisco Nexus 5548 switches with Layer 3 module
- Two Cisco UCS 6120XP servers
- One Cisco UCS 5108 server
- Eight Cisco UCS B-Series servers

Job Aids

These job aids are available to help you complete the lab activity.

Server per Pod Assignment (where X is your pod number)

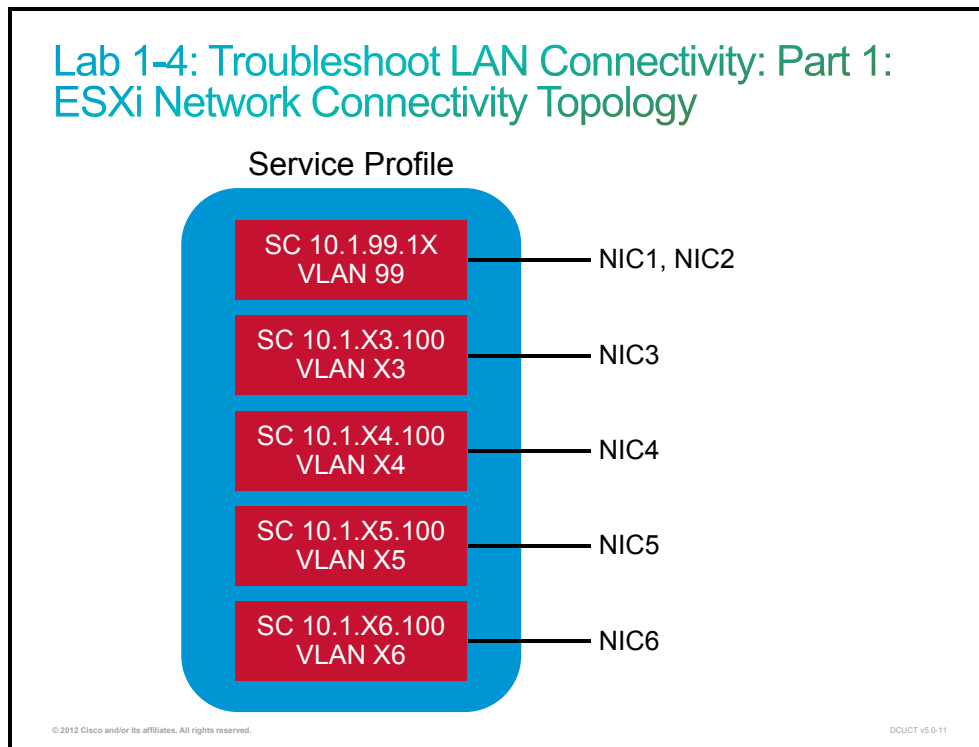
POD	Blade
PODX	Server 1/X

ESXi Server NICs Used in This Exercise

ESXi NIC	Management IP	VLAN	Detail information
NIC1	10.1.99.1X	VLAN 99	Replace X with your POD number
NIC2			

ESXi Network Connectivity Topology

Each ESXi server has five management IP addresses, where each is connected to a different uplink NIC, as shown in the figure.



MAC Addresses (where X is your pod number)

NIC	MAC address
NIC1	00:25:B5:01:01:BX
NIC2	00:25:B5:02:01:BX
NIC3	00:25:B5:03:01:BX
NIC4	00:25:B5:04:01:BX
NIC5	00:25:B5:05:01:BX
NIC6	00:25:B5:06:01:BX

NIC	MAC address
NIC7	00:25:B5:07:01:BX
NIC8	00:25:B5:08:01:BX

Trouble Ticket

The customer is having problems with the network connectivity of the newly configured ESXi servers. The management interface of the ESXi server is not reachable. The customer also noticed that NICs are not presented to the server in the correct order. The management network is configured on vSwitch0 with the uplink of NIC1 and NIC2.

Activity Procedure

Complete these steps:

- Step 1** From your assigned management PC, try to ping or connect vSphere client (use username *root* and password *NXos12345*) to your VMware ESXi host with the IP address 10.1.99.1X (where X is your pod number).
- Step 2** Verify that management IP address (10.1.99.1X) on the ESXi, which is connected to the first two NICs (NIC1 and NIC2 in the service profile), is not reachable.
- Step 3** Connect to both upstream N5548 switches, to the Cisco UCS, and to the console of the ESXi server. Start troubleshooting the connectivity.

Activity Verification

You have completed this task when you are able to connect to ESXi console with the vSphere client to the management ESXi IP address 10.1.99.1X (where X is your pod number).

Lab 1-5: Troubleshoot LAN Connectivity: Part 2

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

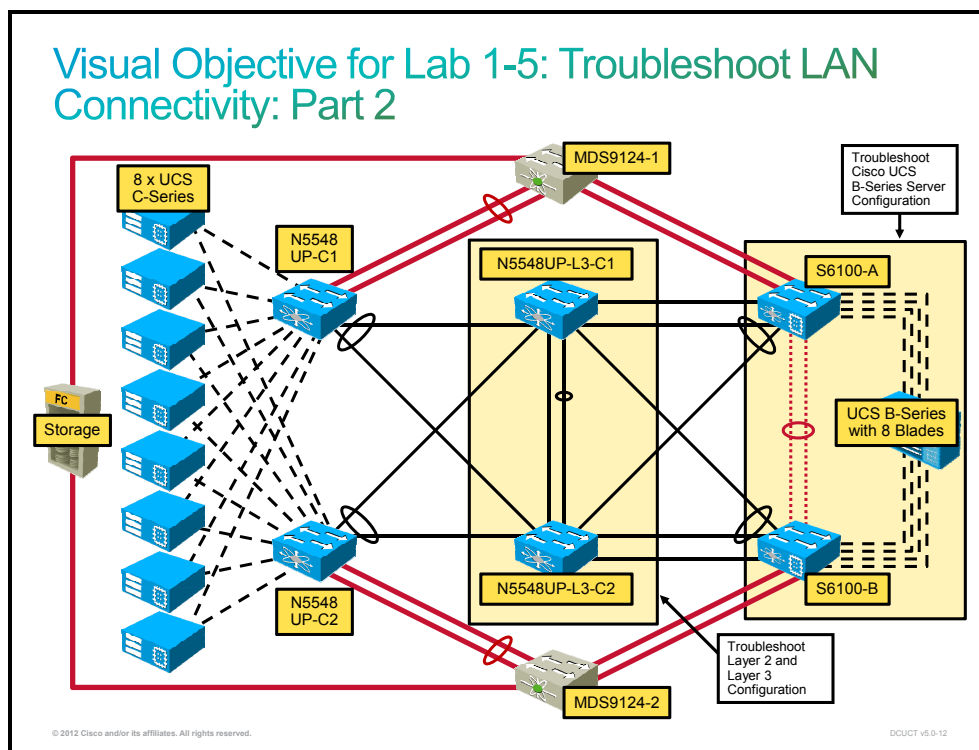
Activity Objective

In this activity, you will troubleshoot network connectivity. After completing this activity, you will be able to meet these objectives:

- Perform trouble analysis and identify the cause of the problem
- Resolve the issue
- Ping or access the management interface of the ESXi host

Visual Objective

The figure illustrates your lab topology.



Required Resources

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

- Two Cisco Nexus 5548 switches
- Two Cisco UCS 6120XP servers
- One Cisco UCS 5108 server
- Eight Cisco UCS B-Series servers

Job Aids

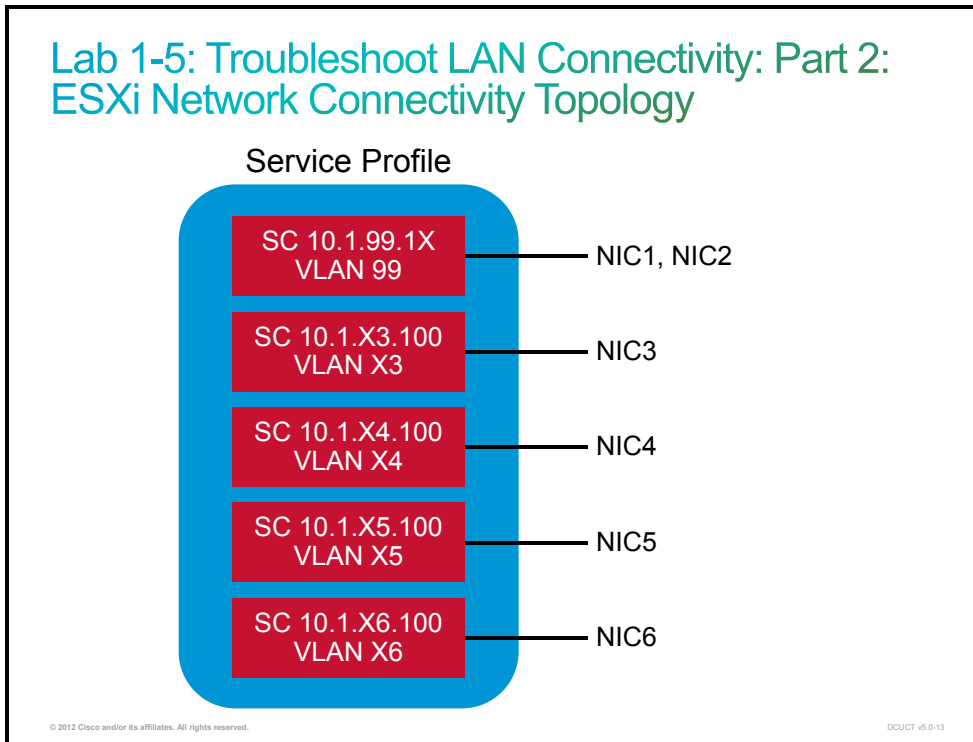
These job aids are available to help you complete the lab activity.

ESXi Server NICs Needed in this Exercise

ESXi NIC	Management IP	VLAN	Detail information
NIC1	10.1.99.1X	VLAN 99	Replace X with your POD number
NIC2			
NIC3	10.1.X3.100	VLAN X3	

ESXi Network Connectivity Topology

Each ESXi server has five management IP addresses, where each is connected to a different uplink NIC, as shown in the figure.



Trouble Ticket

The customer is having problems with the network connectivity of the newly configured ESXi servers. The management interface of the ESXi server is reachable on the 10.1.99.1X, which you fixed it in the previous lab. The customer is now having problems with the management IP address configured on the vSwitch1 with the uplink NIC3.

Activity Procedure

Complete these steps:

- Step 1** From your assigned management PC, connect the vSphere client (use username *root* and password *NXos12345*) to your VMware ESXi host with the IP address 10.1.99.1X (where X is your pod number).
- Step 2** Verify that management IP 10.1.X3.100 on the ESXi is connected to the NIC3 and that it is not reachable.
- Step 3** Connect both upstream Cisco Nexus N5548 switches to the Cisco UCS and to the ESXi server. Start troubleshooting the connectivity.

Activity Verification

You have completed this task when you are able to ping from the ESXi SSH shell to the default gateway 10.1.X3.1 (where X is your pod number) or ping the management IP from your student PC.

Lab 1-6: Troubleshoot Failover Connectivity: Part 1

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

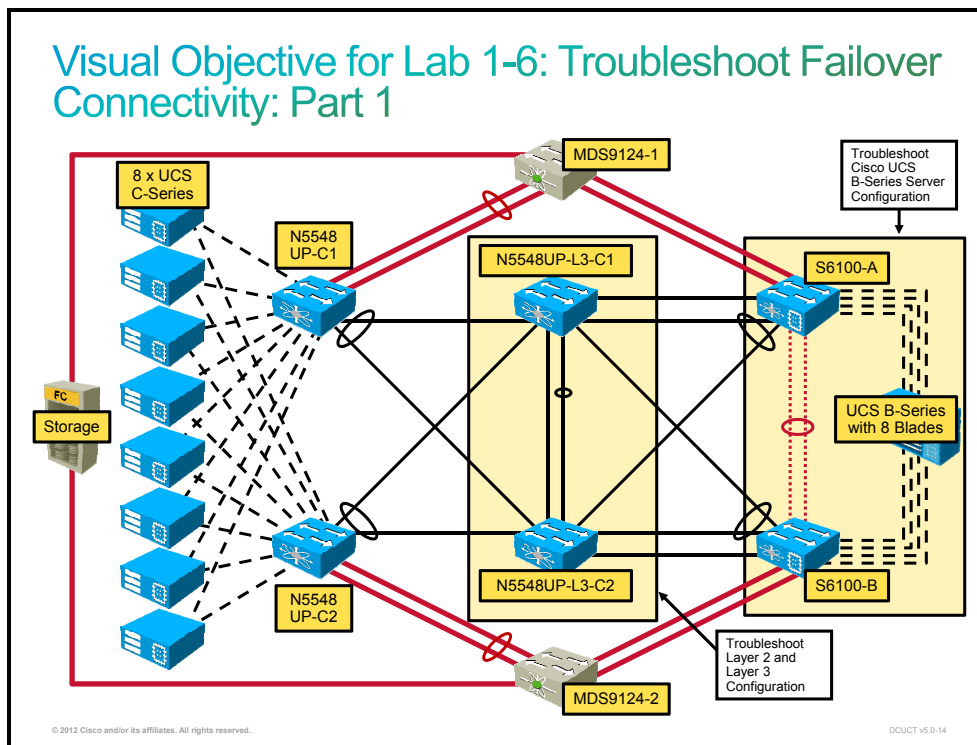
Activity Objective

In this activity, you will troubleshoot network connectivity in a failover scenario. After completing this activity, you will be able to meet these objectives:

- Perform trouble analysis and identify the cause of the problem
- Resolve the issue
- Ping or access the management interface of the ESXi host

Visual Objective

The figure illustrates your lab topology.



Required Resources

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

- Two Cisco Nexus 5548 switches with Layer 3 module
- Two Cisco UCS 6120XP servers
- One Cisco UCS 5108 server
- Eight Cisco UCS B-Series servers

Job Aids

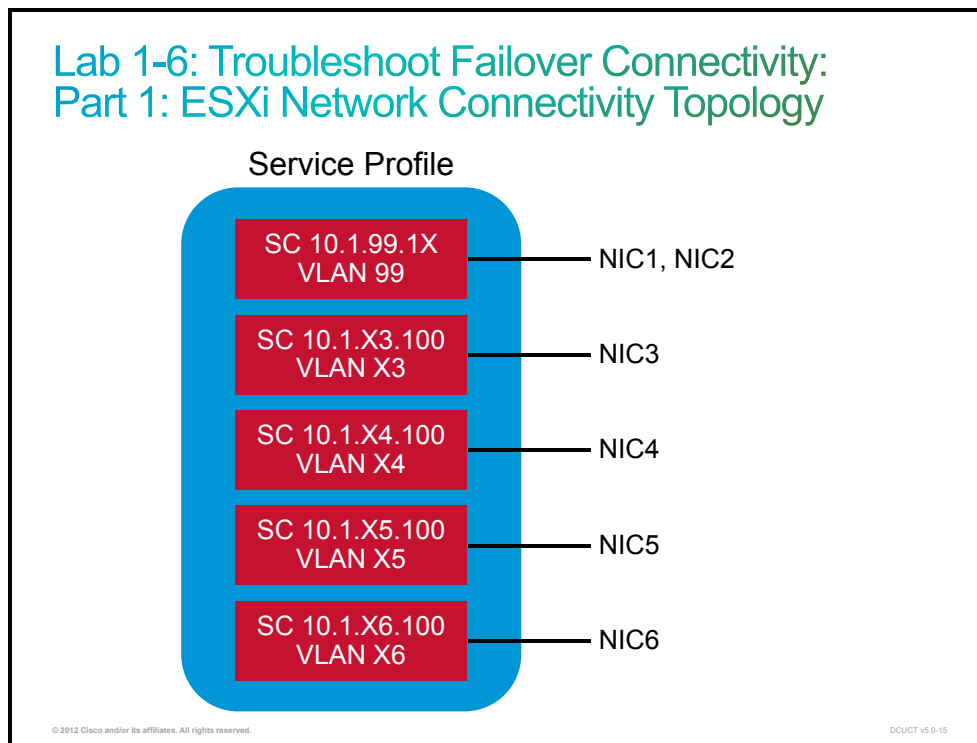
These job aids are available to help you complete the lab activity.

ESXi NICs Needed in This Exercise

ESXi NIC	Management IP	VLAN	Detail information
NIC1	10.1.99.1X	VLAN 99	Replace X with your POD number
NIC2			
NIC4	10.1.X4.100	VLAN X4	

ESXi Network Connectivity Topology

Each ESXi server has five service consoles (management IP addresses), where each is connected to a different uplink NIC, as shown in the figure.



Trouble Ticket

Now you are assigned a case where you need to resolve the LAN connectivity problems that the customer is experiencing with their UCS deployment. The customer has issues with accessing the ESXi hosts from the core LAN in the event of failover. The management interface of the ESXi server is reachable on the 10.1.99.1X (where X is your pod number).

The customer has problems with network connectivity when there is failover on the NIC4. The symptom is that all the virtual machines connected to virtual switch vSwitch2 become unreachable.

Activity Procedure

Complete these steps:

- Step 1** From your assigned management PC, connect the vSphere client (use username *root* and password *NXos12345*) to your VMware ESXi host with the IP address 10.1.99.1X (where X is your pod number).
- Step 2** Verify that management IP 10.1.X4.100 on the ESXi is connected to the NIC4 and that in case of a failover the management is unreachable.
- Step 3** Connect to both upstream Cisco Nexus N5548 switches, to the Cisco UCS, and to the ESXi server. Start troubleshooting the connectivity.

Activity Verification

You have completed this task when you are able to ping from the ESXi SSH shell to the default gateway 10.1.X4.1 (where X is your pod number) or ping the management IP from your student PC.

Lab 1-7: Troubleshoot Failover Connectivity: Part 2

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

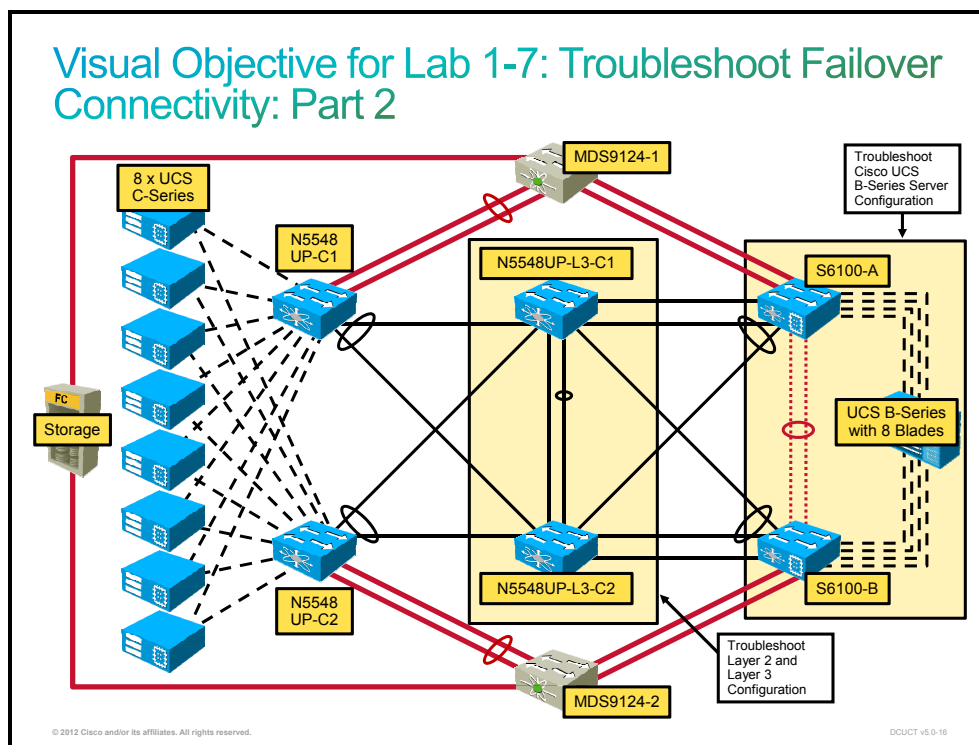
Activity Objective

In this activity, you will troubleshoot network connectivity. After completing this activity, you will be able to meet these objectives:

- Perform trouble analysis and identify the cause of the problem
- Resolve the issue
- Ping or access the management interface of the ESXi host

Visual Objective

The figure illustrates your lab topology.



Required Resources

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

- Two Cisco Nexus 5548 switches with Layer 3 module
- Two Cisco UCS 6120XP servers
- One Cisco UCS 5108 server
- Eight Cisco UCS B-Series servers

Job Aids

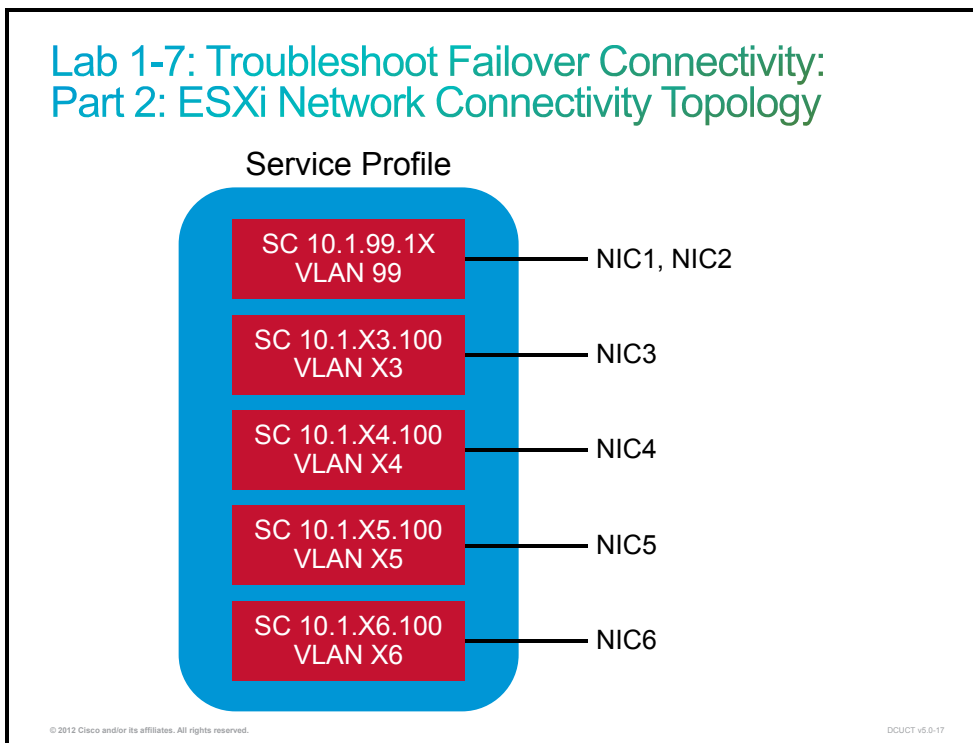
These job aids are available to help you complete the lab activity.

ESXi NICs Needed in This Exercise

ESXi NIC	Management IP	VLAN	Detail information
NIC1	10.1.99.1X	VLAN 99	Replace X with your POD number
NIC2			
NIC5	10.1.X5.100	VLAN X5	

ESXi Network Connectivity Topology

Each ESXi server has five service consoles (management IP addresses), where each is connected to a different uplink NIC, as shown in the figure.



Trouble Ticket

Now you are assigned a case in which you need to resolve the LAN connectivity problems that the customer is experiencing with their UCS deployment. The customer has issues with accessing the ESXi hosts from the core LAN in the event of failover. The management interface of the ESXi server is reachable on the 10.1.99.1X (where X is your pod number).

The customer has problems with network connectivity when there is failover on the NIC5. The symptom is that all the virtual machines connected to virtual switch vSwitch3 become unreachable.

Activity Procedure

Complete these steps:

- Step 1** From your assigned management PC, connect with the vSphere client (use username *root* and password *NXos12345*) to your VMware ESXi host with the IP address 10.1.99.1X (where X is your pod number).
- Step 2** Verify that management IP 10.1.X5.100 on the ESXi is connected to the NIC5 and that in case of a failover, the management is unreachable.
- Step 3** Connect to both upstream Cisco Nexus N5548 switches, to the Cisco UCS, and to the ESXi server. Start troubleshooting the connectivity.

Activity Verification

You have completed this task when you are able to ping from the ESXi SSH shell to the default gateway 10.1.X5.1 (where X is your pod number) or ping the management IP from your student PC.

Lab 2-1: Troubleshoot Cisco UCS C-Series Server Boot from SAN

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

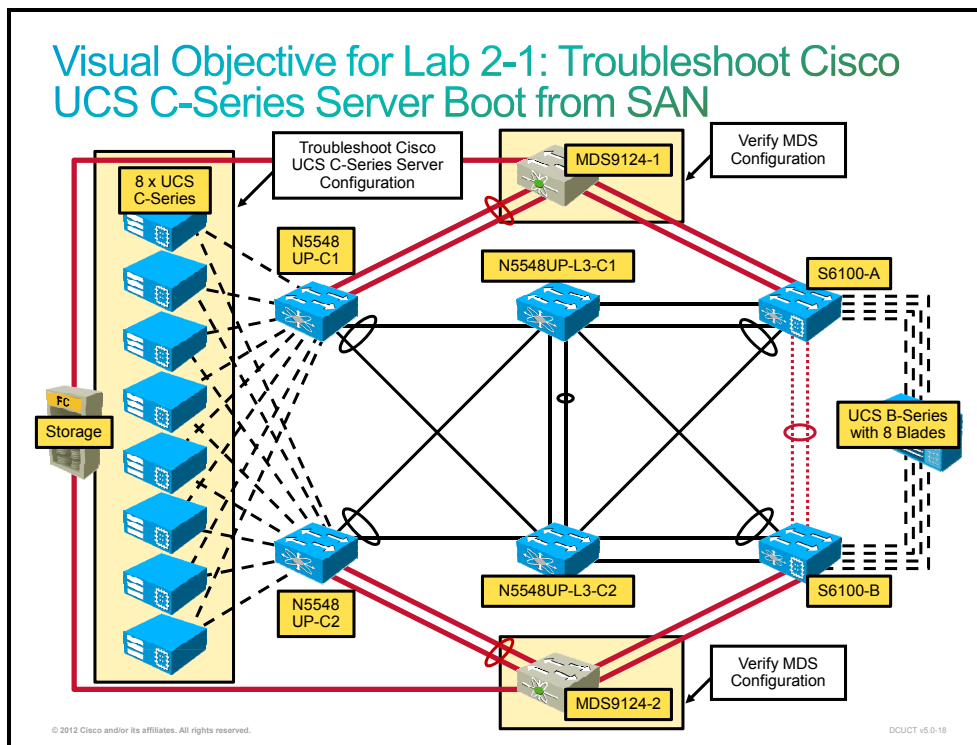
Activity Objective

In this activity, you will troubleshoot the bootup from the SAN. After completing this activity, you will be able to meet these objectives:

- Perform trouble analysis and identify the cause of the problem
- Resolve the issue
- Boot ESXi server from the SAN

Visual Objective

The figure illustrates your lab topology.



Required Resources

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

- Six Cisco UCS C-Series servers
- Six Cisco Nexus 5548UP switches
- Two Cisco MDS 9124 switches
- One disk array

Job Aids

These job aids are available to help you complete the lab activity.

Management IP Addressing

Pod	Management IP	Credentials
N5548-1	192.168.10.91	admin / NXos12345
N5548-2	192.168.10.92	admin / NXos12345
N5548-3	192.168.10.93	admin / NXos12345
N5548-4	192.168.10.94	admin / NXos12345
N5548-5	192.168.10.99	admin / NXos12345
N5548-6	192.168.10.100	admin / NXos12345
MDS9124-1	192.168.10.2	admin / C1sco123
MDS9124-2	192.168.10.3	admin / NXos12345
C200-1	192.168.10.41	admin / NXos12345
C200-2	192.168.10.42	admin / NXos12345
C200-3	192.168.10.43	admin / NXos12345
C200-4	192.168.10.44	admin / NXos12345
C200-5	192.168.10.45	admin / NXos12345
C200-6	192.168.10.46	admin / NXos12345

SAN Information:

	Pod 1	Pod 2	Pod 3	Pod 4	Pod 5	Pod 6
VSAN	11	12	11	12	11	12
FCoE VLAN	1011	1012	1011	1012	1011	1012
vHBA used	fc0	fc0	fc0	fc0	fc0	fc0
Device-alias	dcuci-c1	dcuci-c2	dcuci-c3	dcuci-c4	dcuci-c5	dcuci-c6
Boot target WWPN	50:06:01:60:41:e0:9f:5b	50:06:01:68:41:e0:9f:5b	50:06:01:60:41:e0:9f:5b	50:06:01:68:41:e0:9f:5b	50:06:01:60:41:e0:9f:5b	50:06:01:68:41:e0:9f:5b
Boot target LUN	0	0	0	0	0	0

Command List

The table describes the commands used in this activity.

Command	Description
<code>show device-alias database</code>	Displays the device-alias database
<code>show fcns database</code>	Displays the contents of the FCNS database
<code>show flogi database</code>	Displays information about FLOGI sessions

Command	Description
<code>show hardware internal fc-mac slot-number port port-number statistics</code>	Gives all non-zero statistics for the port
<code>show interface brief</code>	Displays a table with interface statuses
<code>show interface fc slot/port</code>	Displays the configuration information of a Fiber Channel interface
<code>show license usage</code>	Displays license usage
<code>show vsan membership</code>	Displays VSAN membership information
<code>show zone</code>	Displays all configured zones
<code>show zoneset active</code>	Displays the active zoneset

Trouble Ticket

The customer would like to bootup from the SAN. The Cisco UCS C-Series server should be able to boot ESXi from the SAN, but cannot connect to the storage array. It is your task to figure out what is wrong and correct it.

Activity Procedure

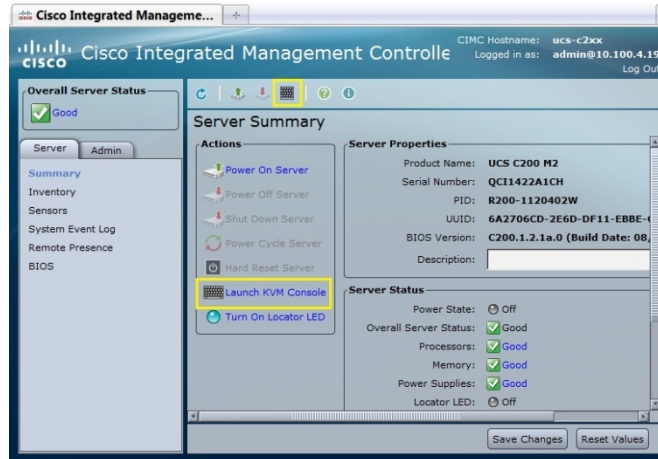
Complete these steps:

- Step 1** Open a web browser and log in to the IP address of the Cisco IMC of the Cisco UCS C-Series server (192.168.10.4X, where X is your pod number).



- Step 2** From the Cisco Integrated Management Controller summary screen, click the **Power On Server** link or **Power Cycle Server** in the Actions area of the screen. Click **OK** when prompted to confirm powering on or power cycling the server.

- Step 3** Open a KVM Console window inside the Cisco IMC and observe the boot process. When possible, enter the boot order menu (by pressing **F6**).



- Step 4** Verify that there is no option to boot from the SAN.

- Step 5** Start troubleshooting.

Activity Verification

You have completed this task when you attain these results:

- The network is operational and your Cisco UCS C-Series server successfully boots an ESXi from the SAN.
- The FCNS database (**show fcns database**) on both Nexus 5548 and MDS switches is populated with entries from the disk array and Cisco UCS C-Series server.
- All issues have been properly identified, documented, and resolved.

Lab 2-2: Troubleshoot Network Connectivity

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

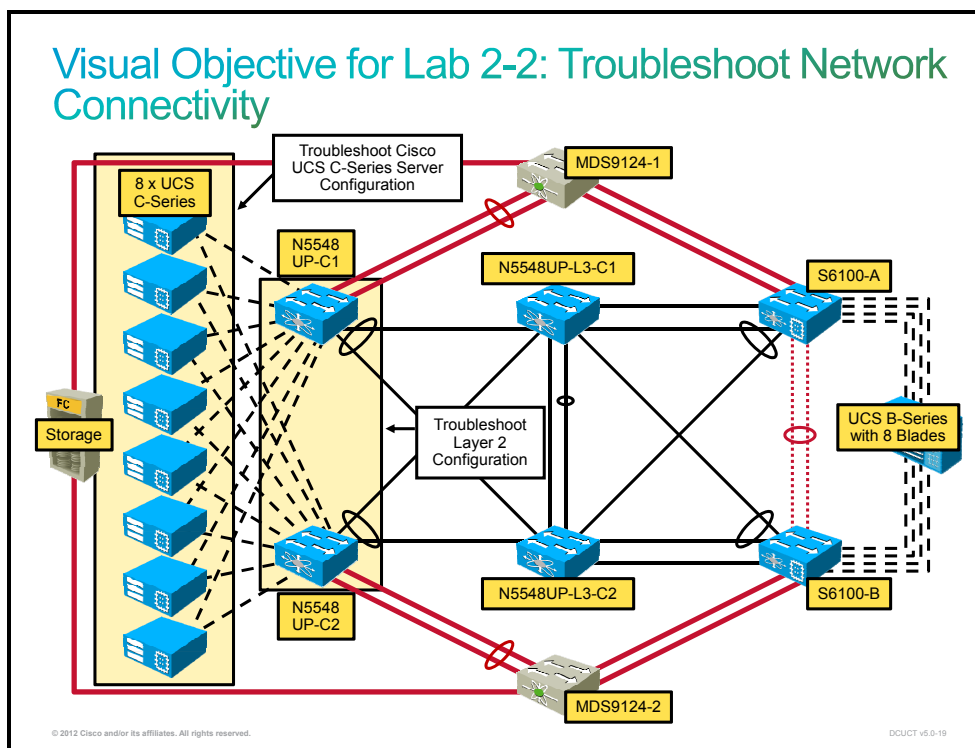
Activity Objective

In this activity, you will troubleshoot network connectivity of the Cisco UCS C-Series server. After completing this activity, you will be able to meet these objectives:

- Perform trouble analysis and identify the cause of the problem
- Resolve the issue
- Ping the ESXi server from your student laptop

Visual Objective

The figure illustrates your lab topology.



Required Resources

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

- Six Cisco UCS C-Series servers
- Six Cisco Nexus 5548UP switches
- One disk array

Job Aids

These job aids are available to help you complete the lab activity.

Management IP Addressing

Device	Interface	Device IP	Default Gateway	Username	Password
N5548UP-L3-C1	Mgmt0	192.168.100.1	192.168.100.254	admin	NXos12345
N5548UP-L3-C2	Mgmt0	192.168.100.2	192.168.100.254	admin	NXos12345
N5548UP-C1	Mgmt0	192.168.10.91	192.168.100.254	admin	NXos12345
N5548UP-C2	Mgmt0	192.168.10.92	192.168.100.254	admin	NXos12345

Command List

The table describes the commands used in this activity.

Command	Description
<code>interface fc slot/port</code>	Configures a Fiber Channel interface
<code>interface san-port-channel channel</code>	Configures a SAN Port Channel interface
<code>show fcns database</code>	Displays the contents of the FCNS database
<code>show flogi database</code>	Displays information about FLOGI sessions
<code>show hardware internal fc-mac slot-number port port-number statistics</code>	Gives all non-zero statistics for the port
<code>show interface brief</code>	Displays a table with interface statuses
<code>show interface fc slot/port</code>	Displays the configuration information of a Fiber Channel interface
<code>show license usage</code>	Displays license usage
<code>show vsan membership</code>	Displays VSAN membership information
<code>switchport mode mode</code>	Sets the Layer 2 interface type
<code>switchport speed</code>	Sets the speed parameters on an interface
<code>switchport trunk</code>	Configures trunking parameters on an interface
<code>vsanvsan interface interface</code>	Adds interface to VSAN
<code>vsan database</code>	Enters the VSAN configuration mode

Trouble Ticket

The customer is having problems with the network connectivity of the newly configured ESXi hosts on the Cisco UCS C-Series servers. The management interface of the ESXi server is unreachable. The customer also noticed that NICs are not presented to server in the correct order. The management network is configured on vSwitch0 with the uplink of NIC1. It is your task to figure out what is wrong and correct it.

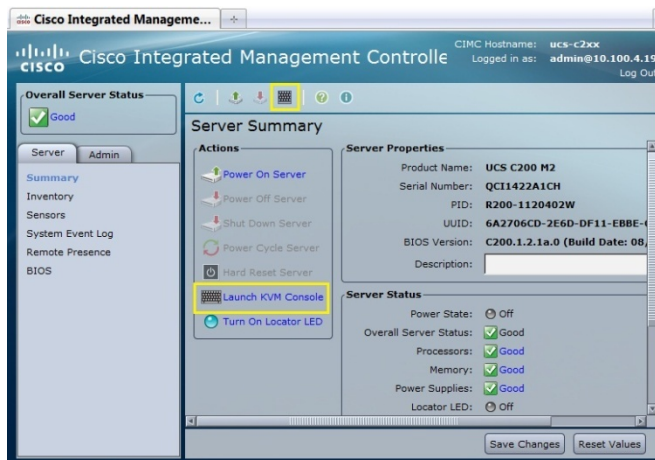
Activity Procedure

Complete these steps:

- Step 1** Open a web browser and log in to the IP address of the Cisco IMC of your pod Cisco UCS C-Series server (192.168.10.4X, where X is your pod number).



- Step 2** Open a KVM Console window inside the Cisco IMC and observe the boot process. When possible, enter the boot order menu (by pressing **F6**).



- Step 3** Verify that there is a problem pinging your ESXi server with the IP address 10.1.99.1X, where X is your pod number.

- Step 4** Start troubleshooting.

Activity Verification

- You have completed this task when you are able to ping from the ESXi SSH shell to the default gateway 10.1.99.1X (where X is your pod number) or ping the management IP from your student PC.

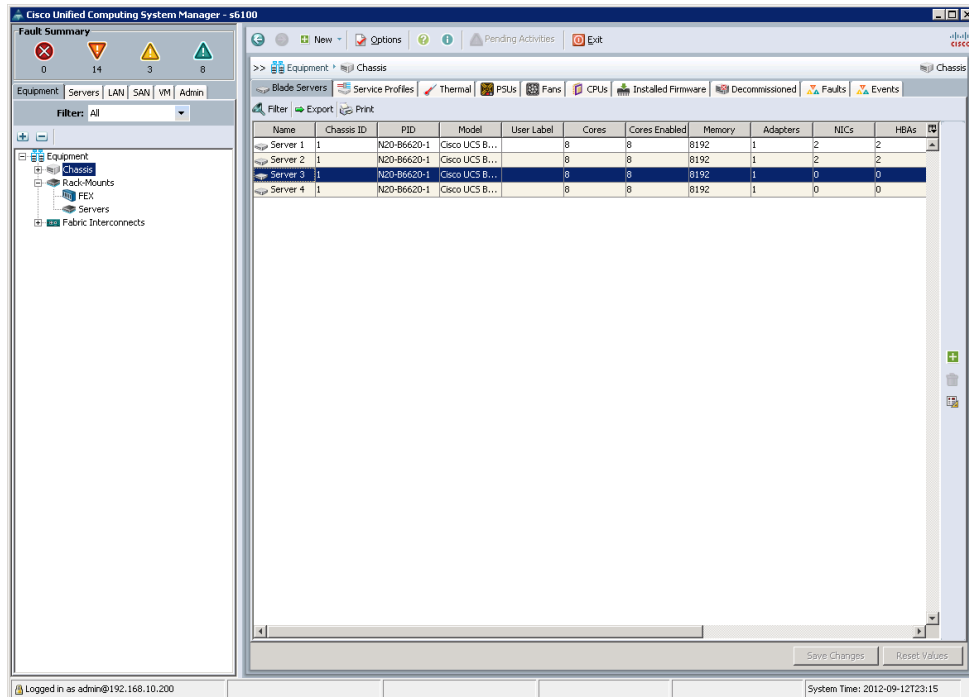
Answer Key

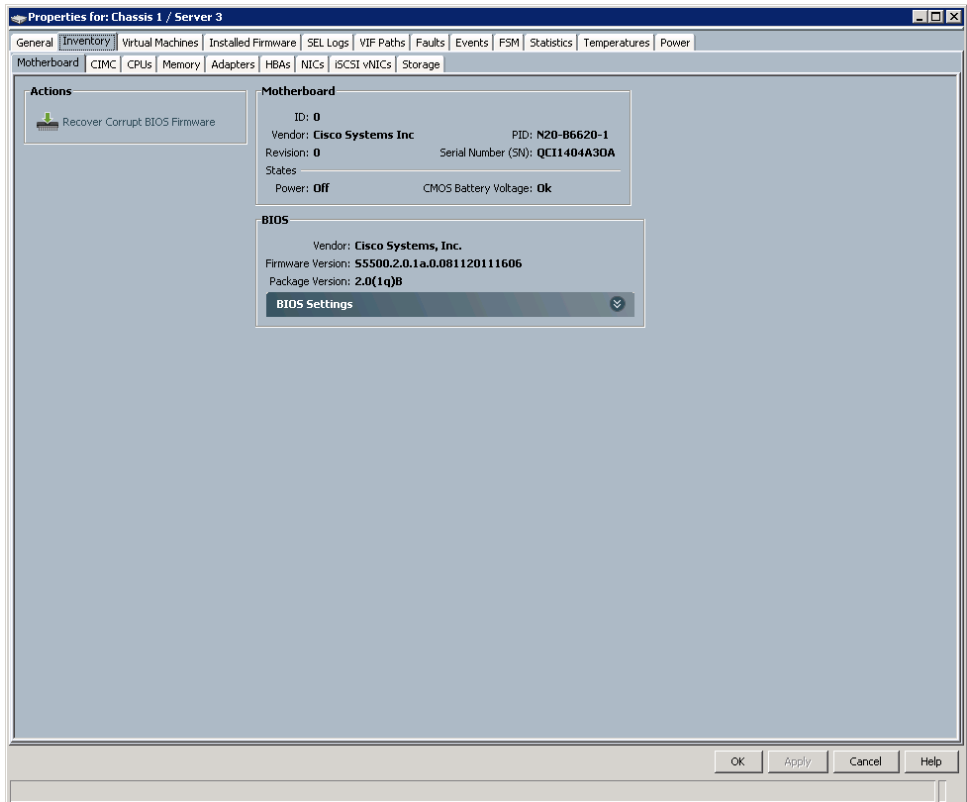
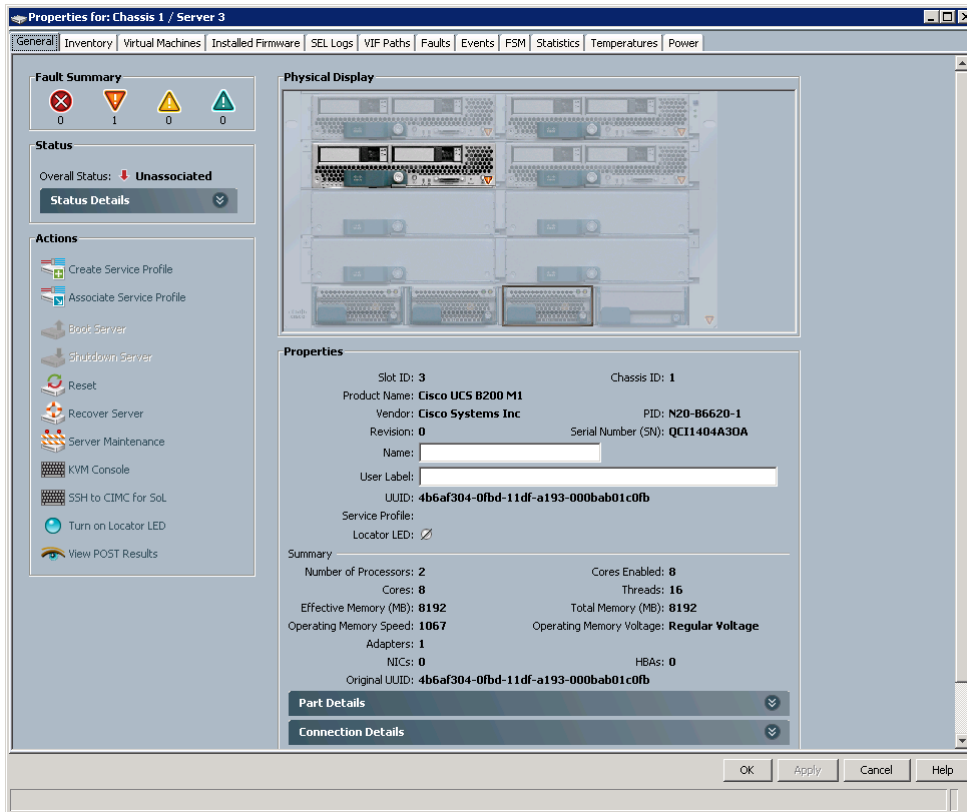
The steps needed for requested activities that are described in this guide appear here.

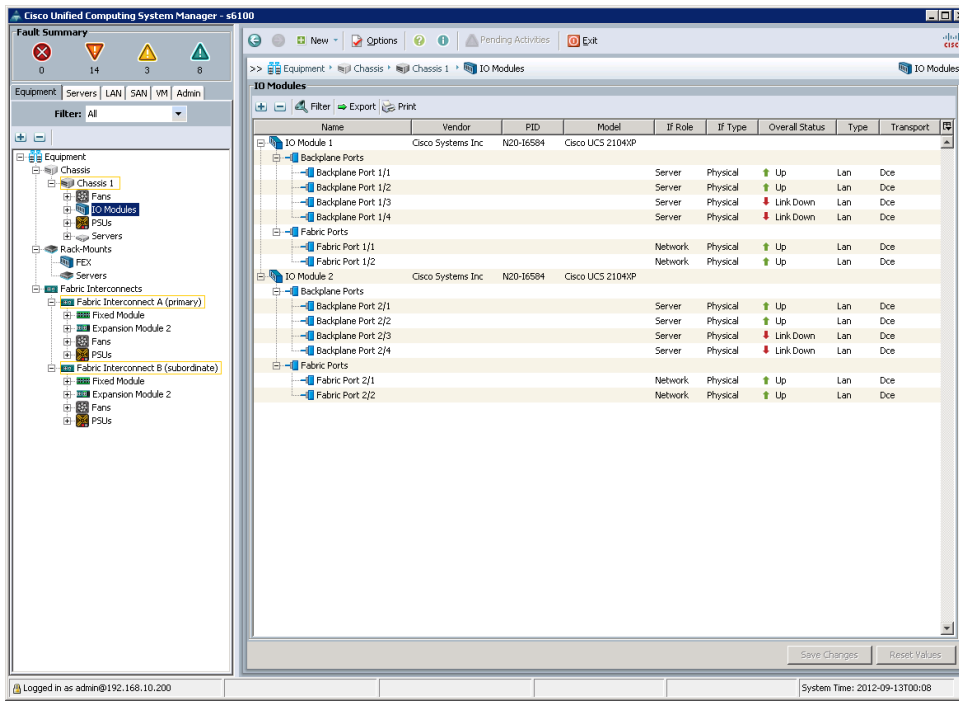
Note Depending on your lab configuration, screenshots and printouts presented here might be different from the actual screenshots and printouts that you have in your lab.

Lab 1-1 Answer Key: Cisco UCS Network Baseline Documentation

Task 1: Verify Cisco UCS B-Series Equipment Using Cisco UCSM GUI

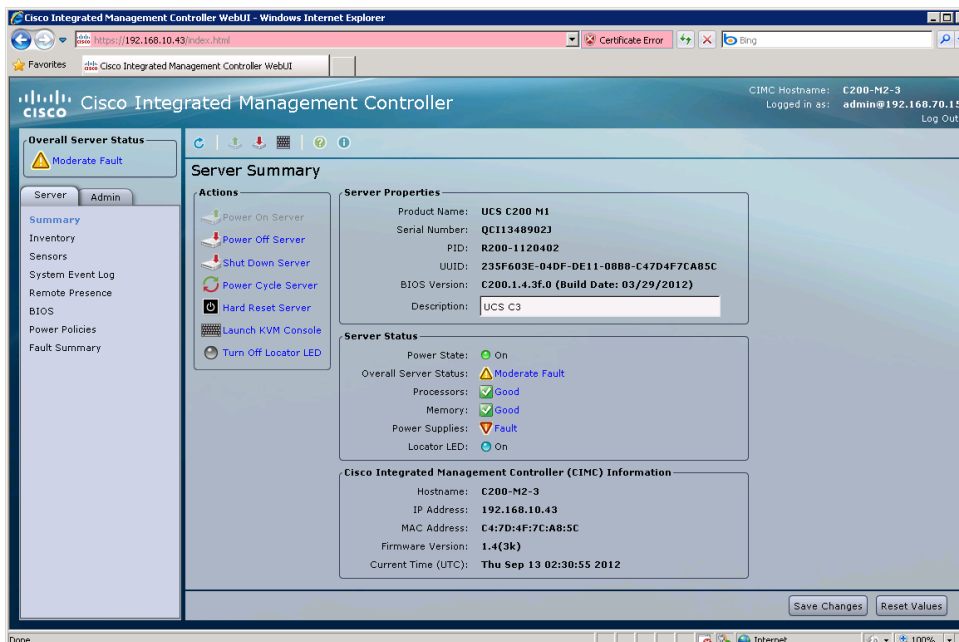






- BIOS firmware version: S5500.2.0.1a.0.081120111606
- Cisco IMC running version: 2.0(1q)
- Number of CPUs and type: Two Intel(R) Xeon(R) E5520
- CPU speed: 2.266
- Number of cores per CPU: Four
- Number of memory DIMMs and total memory capacity: Two 4-GB, 8-GB
- Number and type of adapters: N20-AC0002
- IO Module number and model: Cisco UCS 2104XP

Task 2: Verify Cisco UCS C-Series Equipment Using Cisco CIMC



Cisco Integrated Management Controller WebUI - Windows Internet Explorer

https://192.168.10.43/index.html

Certificate Error

Cisco Integrated Management Controller

CIMC Hostname: C200-M2-3
Logged in as: admin@192.168.70.151
Log Out

Overall Server Status
Moderate Fault

Server Admin

Summary
Inventory
Sensors
System Event Log
Remote Presence
BIOS
Power Policies
Fault Summary

Inventory

CPU Memory Power Supplies Network Adapters Storage PCI Adapters

CPU1

Socket Name: CPU1 Vendor: Intel(R) Corporation
Status: Enabled Family: Xeon
Speed(Mhz): 2266 Version: Intel(R) Xeon(R) CPU E5520 @ 2.27GHz
Number of Cores: 4 Signature: Type 0, Family 6, Model 26, Stepping 5
Number of Threads: 8

CPU2

Socket Name: CPU2 Vendor: N/A
Status: Unpopulated Family: N/A
Speed(Mhz): N/A Version: N/A
Number of Cores: N/A Signature: N/A
Number of Threads: N/A

Save Changes Reset Values

Cisco Integrated Management Controller WebUI - Windows Internet Explorer

https://192.168.10.43/index.html

Certificate Error

Cisco Integrated Management Controller

CIMC Hostname: C200-M2-3
Logged in as: admin@192.168.70.151
Log Out

Overall Server Status
Moderate Fault

Server Admin

Summary
Inventory
Sensors
System Event Log
Remote Presence
BIOS
Power Policies
Fault Summary

Adapter Cards

CPU Memory Power Supplies Network Adapters Storage PCI Adapters

PCI Slot	Product Name	Serial Number	Product ID	Vendor	CIMC Management Enabled
1	UCS VIC P81E	QC11523A80X	N2XX-ACPCI01	Cisco Systems Inc	no

Adapter Card 1

General vNICs VM FEXs vHBAs

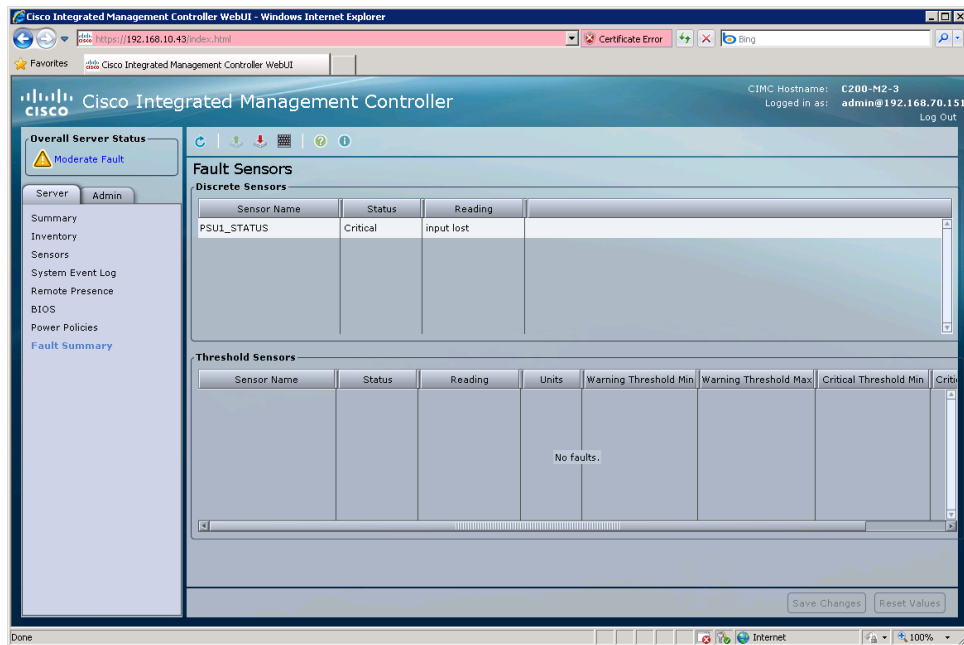
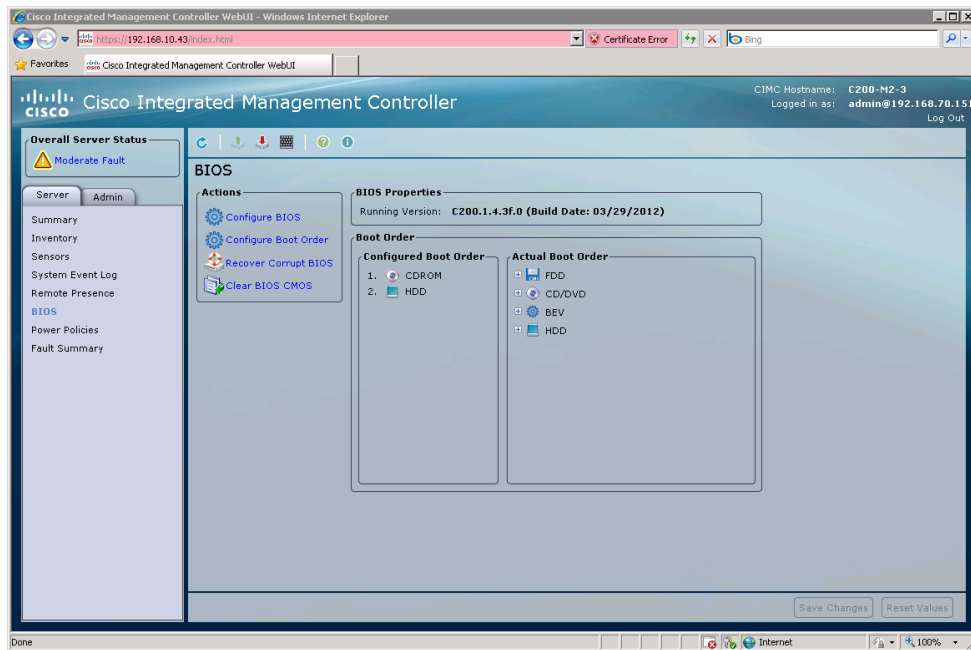
Actions

- Modify Adapter Properties
- Export Configuration
- Import Configuration
- Install Firmware
- Activate Firmware
- Reset To Defaults

Adapter Card Properties

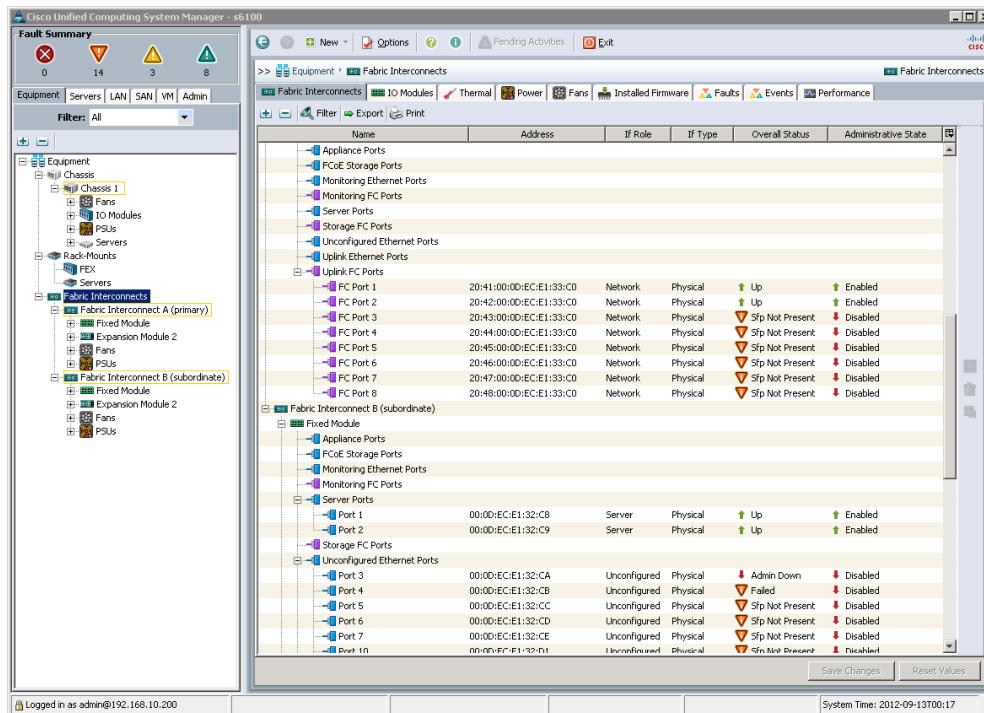
PCI Slot: 1
Vendor: Cisco Systems Inc
Product Name: UCS VIC P81E
Product ID: N2XX-ACPCI01
Serial Number: QC11523A80X
Version ID: V01
Hardware Revision: 4
CIMC Management Enabled: no
Configuration Pending: no
Description:

Save Changes Reset Values



- Number of CPUs, speed, and number of cores: Two E5506 @ 2.13GHz
- Number of DIMMs and total amount of memory: Two 4-GB, 8-GB
- Number of power supplies and current state of power inputs: One
- Number and type of network adapters: UCS VIC P81E
- Local storage information: LSI MegaRAID SAS 9260-4I
- Number and type of PCI adapters: 2, LSI MegaRAID, UCS VIC
- Examine and write down server BIOS version and configuration: 200.1.4.3h.0 (Build Date: 07/18/2012)
- Examine and write down server fault status: No faults

Task 3: Examine LAN and SAN Network Topology



Step 1 Log in to Fabric Interconnect A (192.168.10.101) with PuTTY client and get the information about the connected devices with the **show cdp neighbors** command and fill the table in Step 8.

```
s6100-A#connect nxos a
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
```

```
s6100-A(nxos)#show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
S - Switch, H - Host, I - IGMP, r - Repeater,
V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute
```

Device ID	Local	Intrfce	Hldtme	Capability	Platform	Port ID
N5548UP-L3-C1 (SSI16010PVG)	Eth1/1	173	R S I s	N5K-C5548UP	Eth1/1	
N5548UP-L3-C1 (SSI16010PVG)	Eth1/2	173	R S I s	N5K-C5548UP	Eth1/2	
N5548UP-L3-C1 (SSI16010PVG)	Eth1/3	173	R S I s	N5K-C5548UP	Eth1/3	
N5548UP-L3-C1 (SSI16010PVG)	Eth1/4	173	R S I s	N5K-C5548UP	Eth1/4	
N5548UP-L3-C1 (SSI16010PVG)	Eth1/5	173	R S I s	N5K-C5548UP	Eth1/5	
N5548UP-L3-C1 (SSI16010PVG)	Eth1/6	173	R S I s	N5K-C5548UP	Eth1/6	
N5548UP-L3-C1 (SSI16010PVG)	Eth1/7	173	R S I s	N5K-C5548UP	Eth1/7	
N5548UP-L3-C1 (SSI16010PVG)	Eth1/8	173	R S I s	N5K-C5548UP	Eth1/8	
N5548UP-L3-C1 (SSI16010PVG)	Eth1/19	173	R S I s	N5K-C5548UP	Eth1/9	
N5548UP-L3-C2 (SSI16010Q23)	Eth1/20	173	R S I s	N5K-C5548UP	Eth1/10	

```
s6100-A#connect nxos b
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>

s6100-A(nxos)#**show cdp neighbors**

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
 S - Switch, H - Host, I - IGMP, r - Repeater,
 V - VoIP-Phone, D - Remotely-Managed-Device,
 s - Supports-STP-Dispute

Device ID	Local Intrfce	Hldtme	Capability	Platform	Port ID
N5548UP-L3-C2 (SSI16010Q23)	Eth1/1	173	R S I s	N5K-C5548UP	Eth1/1
N5548UP-L3-C2 (SSI16010Q23)	Eth1/2	173	R S I s	N5K-C5548UP	Eth1/2
N5548UP-L3-C2 (SSI16010Q23)	Eth1/3	173	R S I s	N5K-C5548UP	Eth1/3
N5548UP-L3-C2 (SSI16010Q23)	Eth1/4	173	R S I s	N5K-C5548UP	Eth1/4
N5548UP-L3-C2 (SSI16010Q23)	Eth1/5	173	R S I s	N5K-C5548UP	Eth1/5
N5548UP-L3-C2 (SSI16010Q23)	Eth1/6	173	R S I s	N5K-C5548UP	Eth1/6
N5548UP-L3-C2 (SSI16010Q23)	Eth1/7	173	R S I s	N5K-C5548UP	Eth1/7
N5548UP-L3-C2 (SSI16010Q23)	Eth1/8	173	R S I s	N5K-C5548UP	Eth1/8
N5548UP-L3-C2 (SSI16010Q23)	Eth1/19	173	R S I s	N5K-C5548UP	Eth1/9
N5548UP-L3-C1 (SSI16010PVG)	Eth1/20	173	R S I s	N5K-C5548UP	Eth1/10

Step 2 Display the running version of the Fabric Interconnect.

s6100-A(nxos)#**show version**

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 herein are owned by
 other third parties and are used and distributed under license.
 Some parts of this software are covered under the GNU Public
 License. A copy of the license is available at
<http://www.gnu.org/licenses/gpl.html>.

Software

```

BIOS:          version 1.5.0
loader:        version N/A
kickstart:     version 5.0(3)N2(2.1q)
system:        version 5.0(3)N2(2.1q)
power-seq:     Module 1: version v1.2
BIOS compile time:      11/30/10
kickstart image file is: bootflash:/installables/switch/ucs-6100-k9-
kickstart.5.0.3.N2.2.1q.bin
kickstart compile time: 10/13/2011 22:00:00 [10/14/2011 07:50:42]
system image file is:   bootflash:/installables/switch/ucs-6100-k9-
system.5.0.3.N2.2.1q.bin
system compile time:    10/13/2011 22:00:00 [10/14/2011 09:53:32]

```

Hardware

```

cisco UCS 6100 Series Fabric Interconnect ("20x10GE/Supervisor")
Intel(R) Celeron(R) M CPU with 3633996 kB of memory.
Processor Board ID JAF1339AKET

```

```

Device name: s6100-A
bootflash: 15728640 kB

```

Kernel uptime is 309 day(s), 12 hour(s), 47 minute(s), 45 second(s)

Last reset at 530086 usecs after Tue Nov 8 12:06:50 2011

Reason: Reset Requested by CLI command reload
System version: 5.0(3)N2(2.1q)
Service:

plugin

Core Plugin, Ethernet Plugin, Fc Plugin, Virtualization Plugin

Step 3 Display installed modules in the Fabric Interconnect.

s6100-A(nxos)#show module

Mod	Ports	Module-Type	Model	Status
-	-	-	-	-
1	20	20x10GE/Supervisor	N10-S6100-SUP	active *
2	8	8x1/2/4G FC Module	N10-E0080	ok

Mod	Sw	Hw	World-Wide-Name(s) (WWN)
-	-	-	-
1	5.0(3)N2(2.1q)	1.2	--
2	5.0(3)N2(2.1q)	1.0	20:41:00:0d:ec:e1:33:c0 to 20:48:00:0d:ec:e1:33:c0

Mod	MAC-Address(es)	Serial-Num
-	-	-
1	000d.ece1.33c8 to 000d.ece1.33ef	JAF1339AKET
2	000d.ece1.33f0 to 000d.ece1.33f7	JAF1337AKPR

Step 4 Display FEX details.

s6100-A(nxos)#show fex detail

FEX: 1 Description: FEX0001 state: Online
FEX version: 5.0(3)N2(2.1q) [Switch version: 5.0(3)N2(2.1q)]
FEX Interim version: 5.0(3)N2(2.1q)
Switch Interim version: 5.0(3)N2(2.1q)
Chassis Model: N20-C6508, Chassis Serial: FOX1334G68T
Extender Model: N20-I6584, Extender Serial: QCI133400A4
Part No: 73-11623-05
Card Id: 67, Mac Addr: 00:26:51:08:de:04, Num Macs: 10
Module Sw Gen: 12594 [Switch Sw Gen: 21]
post level: complete
pinning-mode: static Max-links: 1
Fabric port for control traffic: Eth1/1
Fabric interface state:
Eth1/1 - Interface Up. State: Active
Eth1/2 - Interface Up. State: Active

Fex Port	State	Fabric Port
Eth1/1/1	Up	Eth1/1
Eth1/1/2	Up	Eth1/2
Eth1/1/3	Down	Eth1/1
Eth1/1/4	Down	Eth1/2
Eth1/1/5	Down	None
Eth1/1/6	Down	None
Eth1/1/7	Down	None
Eth1/1/8	Down	None
Eth1/1/9	Up	Eth1/2

Logs:
09/11/2012 10:19:19.442586: Module register received
09/11/2012 10:19:19.443887: Registration response sent
09/11/2012 10:19:19.676322: Module Online Sequence
09/11/2012 10:19:24.974421: Module Online

Step 5 Display interface brief.

s6100-A(nxos) #show interface brief

Interface	Vsan	Admin Mode	Admin Trunk Mode	Status	SFP	Oper Mode	Oper Speed (Gbps)	Port Channel
fc2/1	11	NP	off	up	sw1	NP	2	1
fc2/2	11	NP	off	up	sw1	NP	2	1
fc2/3	11	NP	off	sfpAbsent	--	--	--	--
fc2/4	11	NP	off	sfpAbsent	--	--	--	--
fc2/5	11	NP	off	sfpAbsent	--	--	--	--
fc2/6	11	NP	off	sfpAbsent	--	--	--	--
fc2/7	11	NP	off	sfpAbsent	--	--	--	--
fc2/8	11	NP	off	sfpAbsent	--	--	--	--

Ethernet Port Interface	VLAN	Type	Mode	Status	Reason	Speed
					Ch #	
Eth1/1	1	eth	fabric	up	none	10G(D) --
Eth1/2	1	eth	fabric	up	none	10G(D) --
Eth1/3	1	eth	access	down	SFP not inserted	10G(D) --
Eth1/4	1	eth	access	down	SFP not inserted	10G(D) --
Eth1/5	1	eth	access	down	SFP not inserted	10G(D) --
Eth1/6	1	eth	access	down	SFP not inserted	10G(D) --
Eth1/7	1	eth	access	down	SFP not inserted	10G(D) --
Eth1/8	1	eth	trunk	up	none	1000(D) --
Eth1/9	1	eth	trunk	down	SFP not inserted	10G(D) --
Eth1/10	1	eth	access	down	SFP not inserted	10G(D) --
Eth1/11	1	eth	access	down	SFP not inserted	10G(D) --
Eth1/12	1	eth	access	down	SFP not inserted	10G(D) --
Eth1/13	1	eth	access	down	SFP not inserted	10G(D) --
Eth1/14	1	eth	access	down	SFP not inserted	10G(D) --
Eth1/15	1	eth	access	down	SFP not inserted	10G(D) --
Eth1/16	1	eth	access	down	SFP not inserted	10G(D) --
Eth1/17	1	eth	access	down	SFP not inserted	10G(D) --
Eth1/18	1	eth	access	down	SFP not inserted	10G(D) --
Eth1/19	1	eth	trunk	up	none	10G(D) --
Eth1/20	1	eth	trunk	up	none	10G(D) --

Interface	Vsan	Admin Trunk Mode	Status	Oper Mode	Oper Speed (Gbps)	IP Address
san-port-channel 1	11	off	up	NP	4	--

Port	VRF	Status	IP Address	Speed	MTU
mgmt0	--	down	192.168.10.101	100	1500

Vethernet	VLAN	Type	Mode	Status	Reason	Speed
Veth1553	1	eth	trunk	down	nonPartcipating	auto
Veth1576	1	eth	trunk	down	nonPartcipating	auto
Veth9747	1011	eth	access	down	nonPartcipating	auto
Veth9770	1011	eth	access	down	nonPartcipating	auto
Veth32770	1	eth	access	down	nonPartcipating	auto

Interface	Vsan	Admin	Admin	Status	SFP	Oper	Oper	Port
-----------	------	-------	-------	--------	-----	------	------	------

		Mode	Trunk Mode		Mode	Speed	Channel (Gbps)
vfc1555	11	F	on	BoundIfDown	--	--	--
vfc1578	11	F	on	BoundIfDown	--	--	--

Ethernet Port Interface	VLAN	Type	Mode	Status	Reason	Ch #	Speed
Eth1/1/1	1	eth	vntag	up	none		10G(D) --
Eth1/1/2	1	eth	vntag	up	none		10G(D) --
Eth1/1/3	1	eth	vntag	down	Link not connected		10G(D) --
Eth1/1/4	1	eth	vntag	down	Link not connected		10G(D) --
Eth1/1/5	1	eth	access	down	Administratively down		10G(D) --
Eth1/1/6	1	eth	access	down	Administratively down		10G(D) --
Eth1/1/7	1	eth	access	down	Administratively down		10G(D) --
Eth1/1/8	1	eth	access	down	Administratively down		10G(D) --
Eth1/1/9	4044	eth	trunk	up	none		10G(D) --

Step 6 Connect to local-mgmt.

```
s6100-A(nxos)#exit
s6100-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

s6100-A(local-mgmt)#show cluster extended-state
Cluster Id: 0x98adfd5209fa11e1-0xb823000dece133c4

Start time: Tue Nov  8 12:57:27 2011
Last election time: Tue Nov  8 12:58:05 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: FOX1334G68T, state: active
```

Step 7 Display the license.

```
s6100-A(local-mgmt)#exit
s6100-A#scope license
s6100-A /license #show usage
Feat Name                               Scope Default Total Quant Used Quant State
Peer Count Comparison Grace Used
-----
ETH_PORT_ACTIVATION_PKG                 A                8                8                6 License Ok
Matching                                0
ETH_PORT_ACTIVATION_PKG                 B                8                8                6 License Ok
Matching                                0
```

Step 8 Log in to all Cisco Nexus N5548 Fabric Interconnects and issue a **show cdp neighbors** command. From the output, you can populate the table. Log in to the MDS switches and check the connected devices with the **show flogi database** command. From the Fabric Interconnect, you already have the Cisco Discovery Protocol neighbors.

```
N5548UP-L3-C1# show cdp neighbors
```

```
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
```

```
S - Switch, H - Host, I - IGMP, r - Repeater,
V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute
```

Device-ID	Local Infrfce	Hldtme	Capability	Platform	Port ID
s6100-A(SS113360G3X)	Eth1/1	141	S I s	N10-S6100	Eth1/1
s6100-A(SS113360G3X)	Eth1/2	141	S I s	N10-S6100	Eth1/2
s6100-A(SS113360G3X)	Eth1/3	141	S I s	N10-S6100	Eth1/3
s6100-A(SS113360G3X)	Eth1/4	141	S I s	N10-S6100	Eth1/4
s6100-A(SS113360G3X)	Eth1/5	141	S I s	N10-S6100	Eth1/5
s6100-A(SS113360G3X)	Eth1/6	141	S I s	N10-S6100	Eth1/6
s6100-A(SS113360G3X)	Eth1/7	141	S I s	N10-S6100	Eth1/7
s6100-A(SS113360G3X)	Eth1/8	141	S I s	N10-S6100	Eth1/8
s6100-A(SS113360G3X)	Eth1/19	141	S I s	N10-S6100	Eth1/9
s6100-B(SS113360G1W)	Eth1/19	141	S I s	N10-S6100	Eth1/10
N5548UP-C1	Eth1/11	141	S I s	N5K-C5548UP	Eth1/11
N5548UP-C2	Eth1/12	141	S I s	N5K-C5548UP	Eth1/12
N5548UP-L3-C2	Eth1/20	141	S I s	N5K-C5548UP	Eth1/20
N5548UP-L3-C2	Eth1/21	141	S I s	N5K-C5548UP	Eth1/21

```
N5548UP-L3-C2# show cdp neighbors
```

```
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
```

```
S - Switch, H - Host, I - IGMP, r - Repeater,
V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute
```

Device-ID	Local Infrfce	Hldtme	Capability	Platform	Port ID
s6100-B(SS113360G1W)	Eth1/1	141	S I s	N10-S6100	Eth1/1

```

s6100-B(SS113360G1W) Eth1/2      141   S I s      N10-S6100   Eth1/2
s6100-B(SS113360G1W) Eth1/3      141   S I s      N10-S6100   Eth1/3
s6100-B(SS113360G1W) Eth1/4      141   S I s      N10-S6100   Eth1/4
s6100-B(SS113360G1W) Eth1/5      141   S I s      N10-S6100   Eth1/5
s6100-B(SS113360G1W) Eth1/6      141   S I s      N10-S6100   Eth1/6
s6100-B(SS113360G1W) Eth1/7      141   S I s      N10-S6100   Eth1/7
s6100-B(SS113360G1W) Eth1/8      141   S I s      N10-S6100   Eth1/8
s6100-B(SS113360G1W) Eth1/20     141   S I s      N10-S6100   Eth1/9
s6100-A(SS113360G3X) Eth1/20     141   S I s      N10-S6100   Eth1/10
N5548UP-C1           Eth1/11     141   S I s      N5K-C5548UP Eth1/11
N5548UP-C2           Eth1/12     141   S I s      N5K-C5548UP Eth1/12
N5548UP-L3-C1        Eth1/20     141   S I s      N5K-C5548UP Eth1/20
N5548UP-L3-C1        Eth1/21     141   S I s      N5K-C5548UP Eth1/21

```

M9124-1# sh flogi database

```

-----
INTERFACE      VSAN      FCID      PORT NAME      NODE NAME
-----
fc1/           11  0xee0000  50:06:01:60:41:e0:9f:5b  50:06:01:60:c1:e0:9f:5b
                        [CX3-SPA]
fc1/8         11  0xee0500  50:06:01:69:41:e0:9f:5b  50:06:01:60:c1:e0:9f:5b
                        [CX3-SPB-1]
po1           11  0xee0100  24:01:00:0d:ec:e1:33:c0  20:0b:00:0d:ec:e1:33:c1

```

Total number of flogi = 3.

M9124-2# sh flogi database

```

-----
INTERFACE      VSAN      FCID      PORT NAME      NODE NAME
-----
fc1/7         12  0xee0100  50:06:01:68:41:e0:9f:5b  50:06:01:60:c1:e0:9f:5b
                        [CX3-SPB]
fc1/8         12  0xee0000  50:06:01:61:41:e0:9f:5b  50:06:01:60:c1:e0:9f:5b
                        [CX3-SPA]
po2           12  0xee0300  24:02:00:0d:ec:e1:32:c0  20:0c:00:0d:ec:e1:32:c1

```

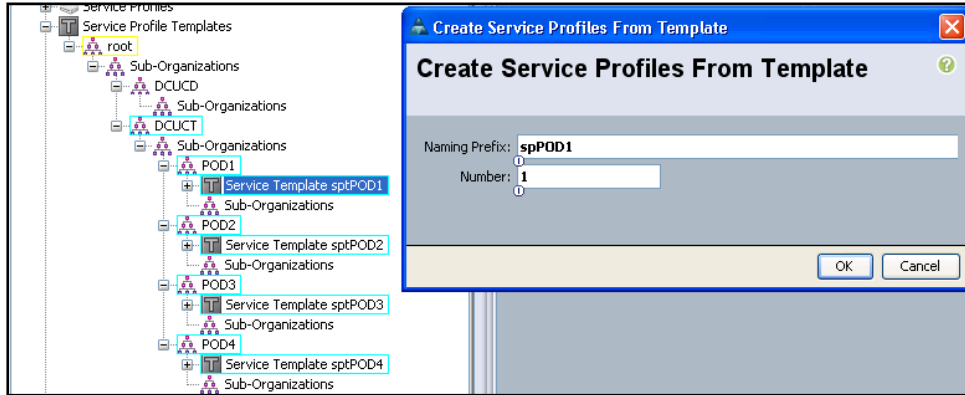
Device	Interfaces	Comment
FI-A	Eth1/1-8, Eth1/19	Connection to N5548UP-L3-C1
FI-A	Eth1/20	Connection to N5548UP-L3-C2
FI-A	fc2/1-2	Connection to MDS9214-1
FI-A	-	Connection to MDS9214-2
FI-A	eth1/10-11	Connection to UCS chassis 5108
FI-B	Eth1/19	Connection to N5548UP-L3-C1

Device	Interfaces	Comment
FI-B	Eth1/1-8, Eth1/20	Connection to N5548UP-L3-C2
FI-B	-	Connection to MDS9214-1
FI-B	fc2/1-2	Connection to MDS9214-2
FI-B	eth1/10-11	Connection to UCS chassis 5108
N5548UP-L3-C1	Eth1/20-21	Connection to N5548UP-L3-C2
N5548UP-L3-C1	Eth1/11	Connection to N5548UP-C1
N5548UP-L3-C1	Eth1/12	Connection to N5548UP-C2
N5548UP-L3-C2	Eth1/20-21	Connection to N5548UP-L3-C1
N5548UP-L3-C2	Eth1/11	Connection to N5548UP-C1
N5548UP-L3-C2	Eth1/12	Connection to N5548UP-C2
N5548UP-C1	Eth1/1	Connection to UCS C server 1
N5548UP-C1	Eth1/2	Connection to UCS C server 2
N5548UP-C1	Eth1/3	Connection to UCS C server 3
N5548UP-C1	Eth1/4	Connection to UCS C server 4
N5548UP-C1	Eth1/5	Connection to UCS C server 5
N5548UP-C1	Eth1/6	Connection to UCS C server 6
N5548UP-C1	fc1/30-31	Connection to MDS9214-1
N5548UP-C2	Eth1/1	Connection to UCS C server 1
N5548UP-C2	Eth1/2	Connection to UCS C server 2
N5548UP-C2	Eth1/3	Connection to UCS C server 3
N5548UP-C2	Eth1/4	Connection to UCS C server 4
N5548UP-C2	Eth1/5	Connection to UCS C server 5
N5548UP-C2	Eth1/6	Connection to UCS C server 6
N5548UP-C2	fc1/30-31	Connection to MDS9214-2
MDS9214-1	fc1/7-8	Connection to Storage Array
MDS9214-2	fc1/7-8	Connection to Storage Array

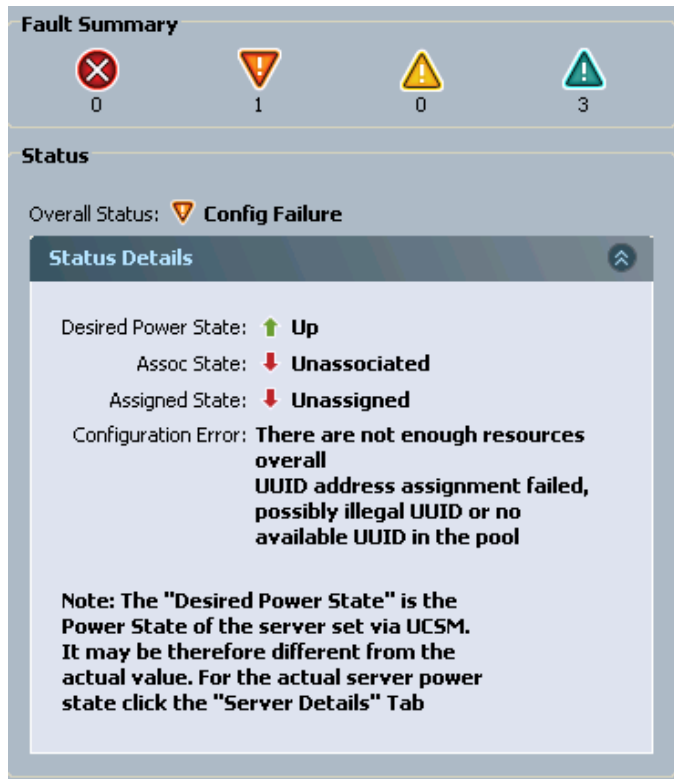
Lab 1-2 Answer Key: Cisco UCS Management and Service Profile Deployment

When you complete this activity, your solution will be similar to the results here, with differences that are specific to your device or workgroup:

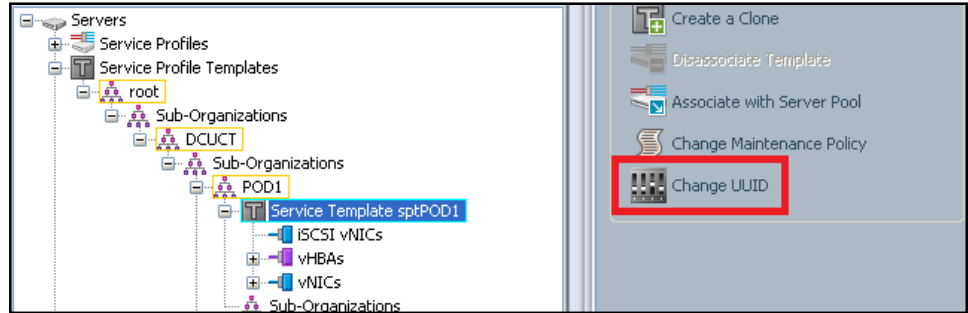
Step 1 Create a service profile from the template. The example is for Pod 1.



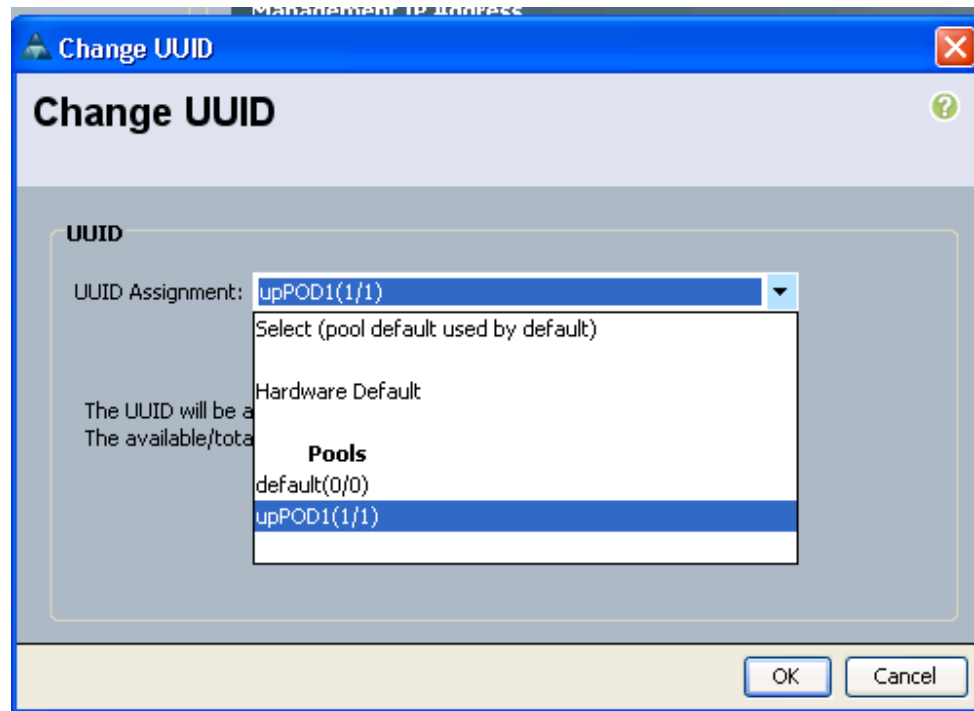
Step 2 When the service profile is created, you receive the following error.



Step 3 To resolve the issue with the UUID, go to the service profile template, sptPODX, by navigating to Service profile templates > Sub-organizations > DCUCT > PODX, and choose **Change UUID**. The example is for Pod 1.



Step 4 A Change UUID window will pop up. In the UUID Assignment, choose **upPODX** or type **UUID manual**. The example is for POD1.

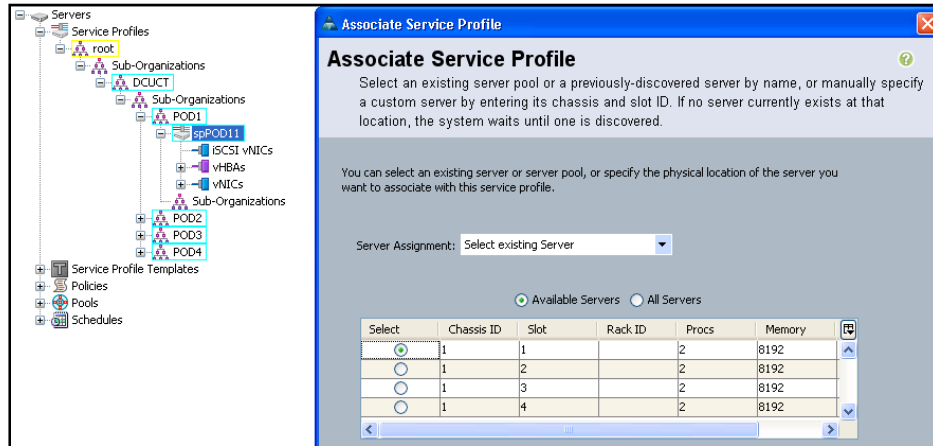


- UUID addresses (replace X with your pod number).

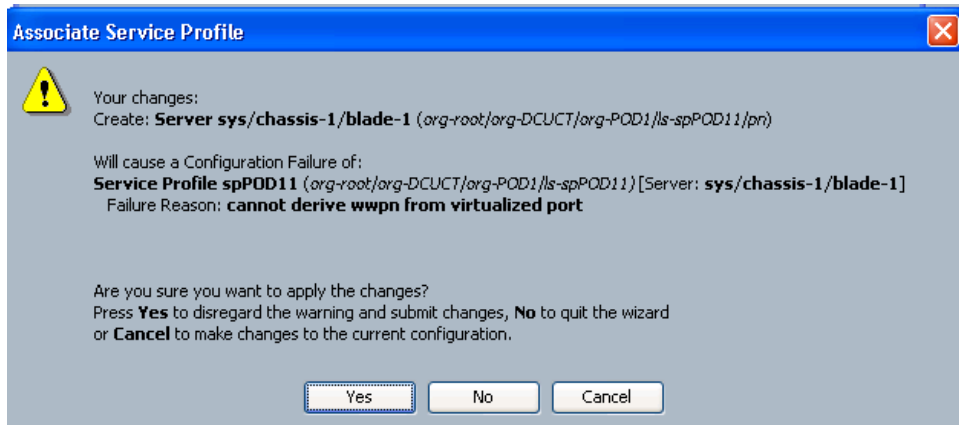
UUID Prefix	UUID Suffix
010025b5-0003-4100	0001-0000b200e20X

Step 5

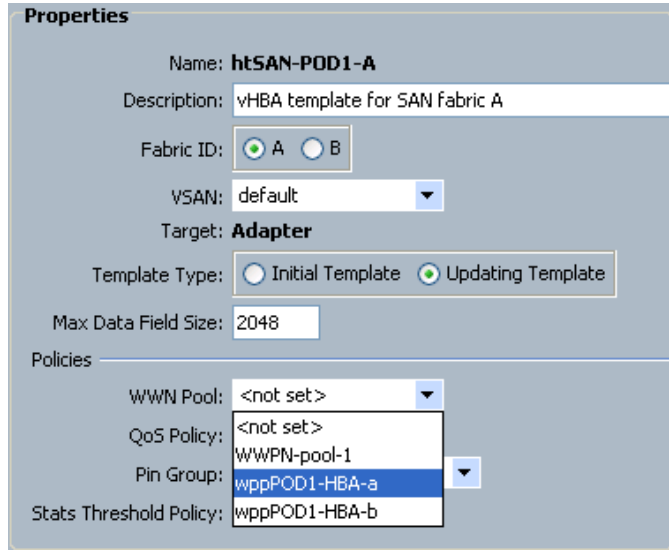
Step 6 Associate the service profile with blade X (where X is your pod number). The example is for POD1.



Step 7 When you try to associate the service profile, the following warning appears. Read the warning and click **No**.



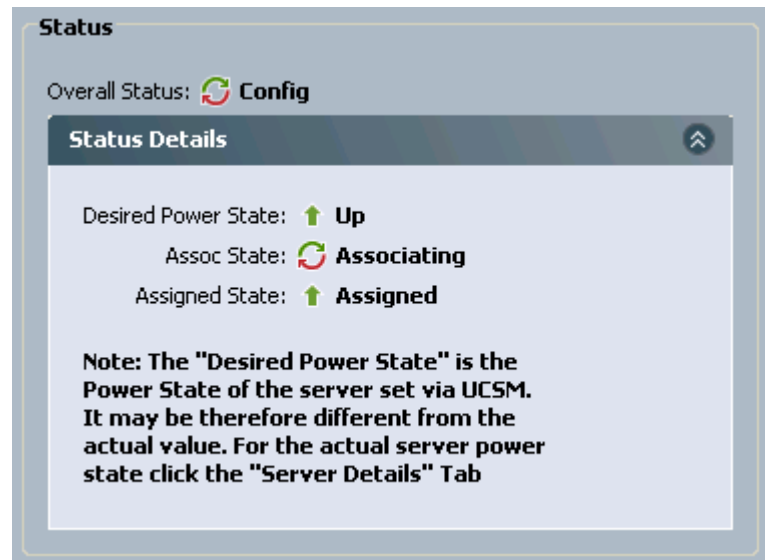
Step 8 The service profile cannot derive the WWPN. The problem is on the first HBA, which is created from the vHBA template. Under the SAN tab, go to Policies > Sub organizations > POD1 > vHBA Templates, and select HBA template **htSAN-PODX-A**. In the WWN pool, select **wppPODX-HBA-a** or enter the WWPN. The example is for POD1.



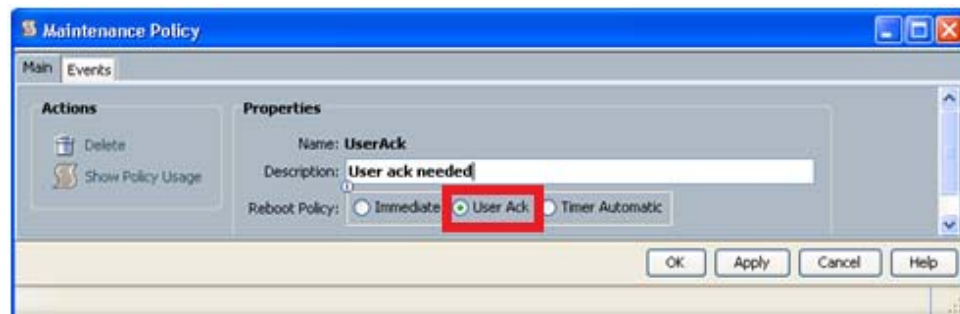
■ WWPN values (replace X with your pod number):

HBA	WWPN Pool
HBA - a	20:00:00:25:B5:A1:50:BX
HBA - b	20:00:00:25:B5:B1:50:BX

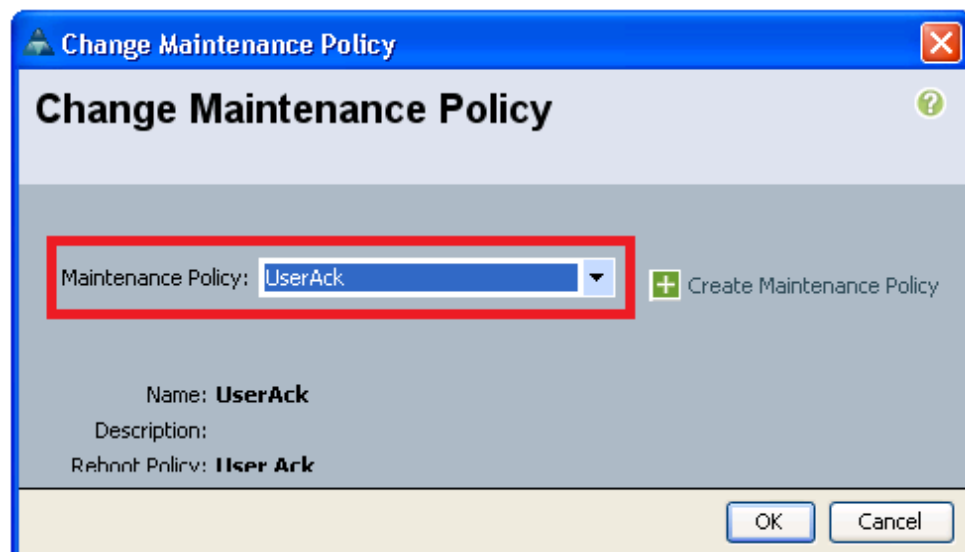
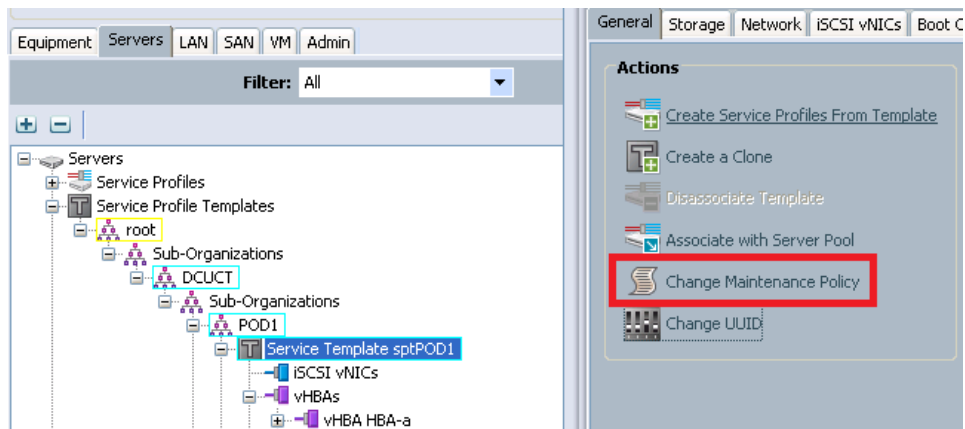
Step 9 Try to associate the blade. The association is successful.



- Step 10** To resolve the issue with automatic reboot of the server when some changes are made in the service profile template, you need to set the Maintenance Policy, located in the Server tab. Navigate to Server > Policies > root > Sub-organizations > DCUCT > POD1 > Maintenance Policy, and change it to **UserAck**.



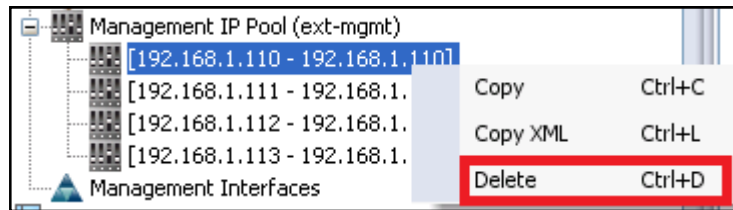
- Step 11** Apply the Maintenance Policy on the service profile template.



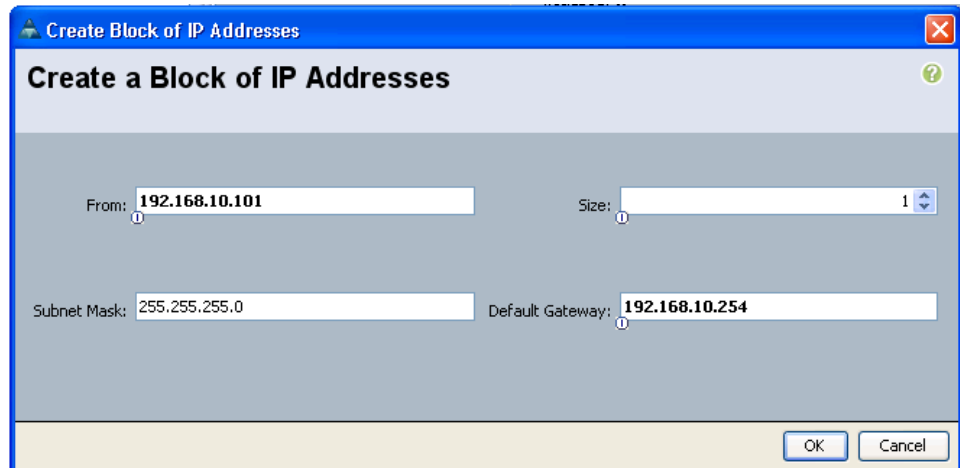
- Step 12** To resolve the issue with accessing the KVM console, you will have to change management IP addresses. Under the Admin tab, go to **Communication Management > Management IP Pool** and on the right side, under IP Addresses, search for your assigned management pool.

IP Address	Subnet	Default Gateway	Assigned	Assigned To	Prev Assigned To
192.168.1.110	255.255.255.0	192.168.1.254	yes	sys/chassis-1/blade-1/mgmt/ipv4-pooled-addr	sys/chassis-1/blade-1/mgmt/ipv4-pooled-addr
192.168.1.111	255.255.255.0	192.168.1.254	yes	sys/chassis-1/blade-3/mgmt/ipv4-pooled-addr	sys/chassis-1/blade-3/mgmt/ipv4-pooled-addr
192.168.1.112	255.255.255.0	192.168.1.254	yes	sys/chassis-1/blade-4/mgmt/ipv4-pooled-addr	sys/chassis-1/blade-4/mgmt/ipv4-pooled-addr
192.168.1.113	255.255.255.0	192.168.1.254	yes	sys/chassis-1/blade-2/mgmt/ipv4-pooled-addr	sys/chassis-1/blade-2/mgmt/ipv4-pooled-addr

Step 13 Delete your pool. The example is for POD1.



Step 14 Re-create the pool with the correct IP address.



■ KVM Management IP addresses

Pod	IP Management Pool
POD1	192.168.10.110
POD2	192.168.10.111
POD3	192.168.10.112
POD4	192.168.10.113

Lab 1-3 Answer Key: Troubleshoot Cisco UCS B-Series Server Boot from SAN

When you complete this activity, your solution will be similar to the results here, with differences that are specific to your device or workgroup:

Step 1 Log in to both MDS switches and check for your server. The example is for POD1.

```
M9124-1#show flogi database
```

```
-----
INTERFACE  VSAN FCID          PORT NAME          NODE NAME
-----
fc1/7      11  0xee0000  50:06:01:60:41:e0:9f:5b  50:06:01:60:c1:e0:9f:5b
                        [CX3-SPA]
fc1/8      11  0xee0500  50:06:01:69:41:e0:9f:5b  50:06:01:60:c1:e0:9f:5b
                        [CX3-SPB-1]
Po1        11  0xee0100  24:01:00:0d:ec:e1:33:c0  20:0b:00:0d:ec:e1:33:c1
```

```
Total number of flogi = 3.
```

M9124-2#show flogi database

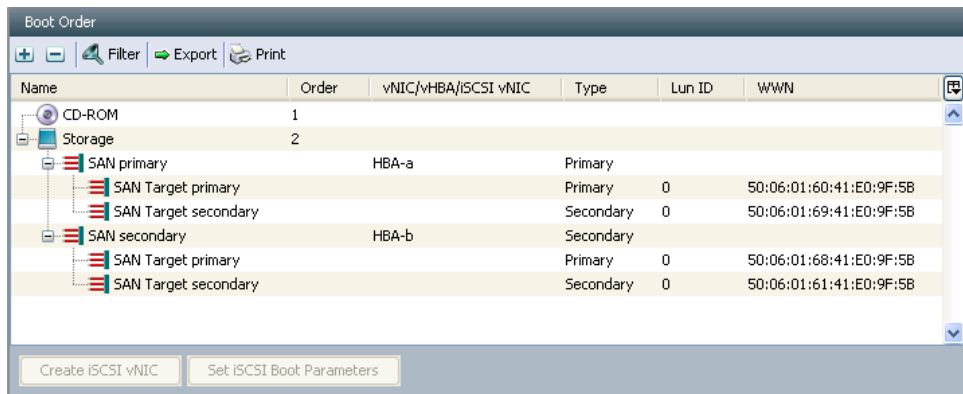
```

-----
INTERFACE  VSAN FCID          PORT NAME          NODE NAME
-----
fc1/7      12   0xee0100  50:06:01:68:41:e0:9f:5b 50:06:01:60:c1:e0:9f:5b
                                     [CX3-SPB]
fc1/8      12   0xee0000  50:06:01:61:41:e0:9f:5b 50:06:01:60:c1:e0:9f:5b
                                     [CX3-SPA]
Po2        12   0xee0300  24:02:00:0d:ec:e1:32:c0 20:0c:00:0d:ec:e1:32:c1

Total number of flogi = 3.

```

Step 2 Check the Boot Order in the service profile template and set it as shown in the figure. After changing the boot policy, your server will reboot.

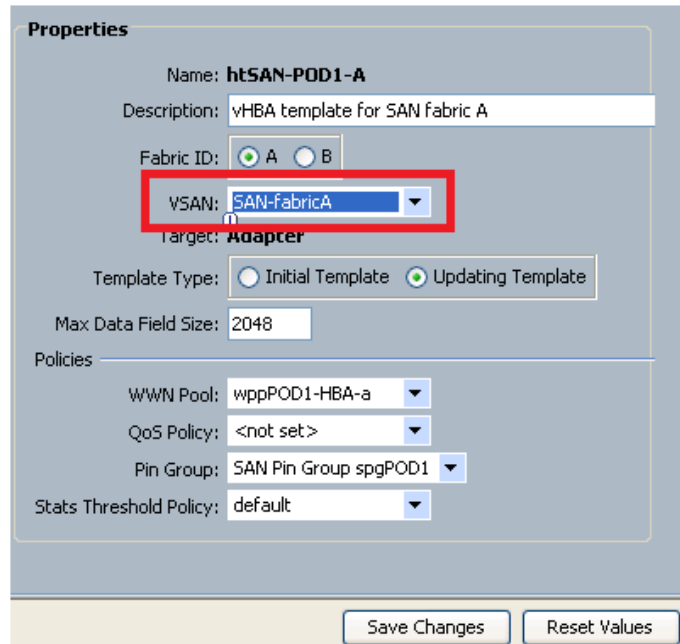


- Boot from SAN parameters for all pods:

Boot Position	Device	VSAN	WWPN	LUN ID
SAN target primary	HBA-a	11	50:06:01:60:41:e0:9f:5b	0
SAN target secondary	HBA-a	11	50:06:01:69:41:e0:9f:5b	0
SAN target primary	HBA-b	12	50:06:01:68:41:e0:9f:5b	0
SAN target secondary	HBA-b	12	50:06:01:61:41:e0:9f:5b	0

Step 3

Step 4 The server still does not boot from the SAN. Verify the HBA settings. First, you must fix the problem for the first HBA. Under the SAN tab, check the **htSAN-PODx-A**. The VSAN is set to default, which is wrong. Select the **SAN-FabricA**, which is in VSAN11. The example is for POD1.



Step 5 Check the FLOGI table on the MDS1 and verify that you can see your server. The example is for POD1.

M9124-1#**show flogi database**

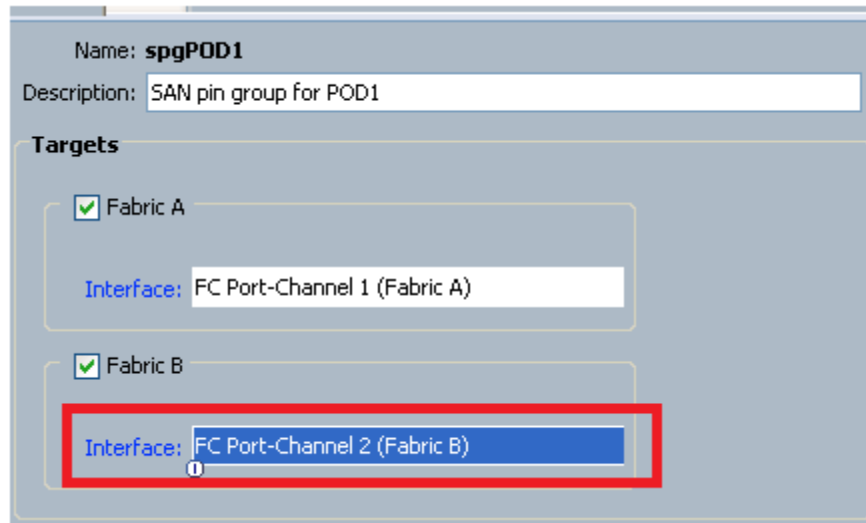
```

-----
INTERFACE  VSAN  FCID                PORT NAME                NODE NAME
-----
fc1/7      11    0xee0000            50:06:01:60:41:e0:9f:5b  50:06:01:60:c1:e0:9f:5b
                                     [CX3-SPA]
fc1/8      11    0xee0500            50:06:01:69:41:e0:9f:5b  50:06:01:60:c1:e0:9f:5b
                                     [CX3-SPB-1]
Po1        11    0xee0100            24:01:00:0d:ec:e1:33:c0  20:0b:00:0d:ec:e1:33:c1
Po1        11    0xee0101            20:00:00:25:b5:a1:50:b1  20:00:00:25:b5:11:50:b1
                                     [dcuct-b1-a]

```

Total number of flogi = 4.

Step 6 On the second MDS switch, you still do not see the second HBA. Under the SAN tab, check the **htSAN-PODx-B**. The VSAN settings are correct. The problem is with SAN pinning. Check the SAN pin group **spgPODx** and change the Target for Fabric B to point to FC Port-Channel 2. The example is for POD1.



Step 7 Then check the FLOGI table on the MDS2 and verify that you can see your server. The example is for POD1.

M9124-2#**show flogi database**

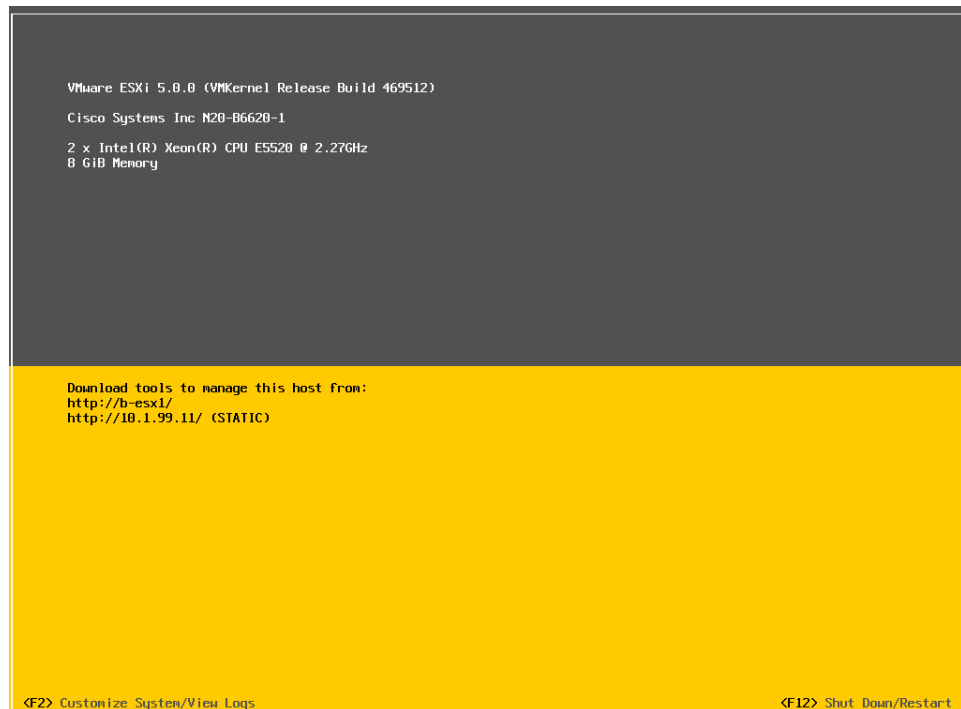
```
-----
INTERFACE  VSAN FCID          PORT NAME          NODE NAME
-----
fc1/7      12   0xee0100      50:06:01:68:41:e0:9f:5b 50:06:01:60:c1:e0:9f:5b
                    [CX3-SPB]
fc1/8      12   0xee0000      50:06:01:61:41:e0:9f:5b 50:06:01:60:c1:e0:9f:5b
                    [CX3-SPA]
Po2        12   0xee0300      24:02:00:0d:ec:e1:32:c0 20:0c:00:0d:ec:e1:32:c1
Po2        12   0xee0301      20:00:00:25:b5:b1:50:b1 20:00:00:25:b5:11:50:b1
                    [dcuct-b1-b]
-----
```

Total number of flogi = 4.

Step 8 When your server is seen on both MDS switches in the FLOGI table, reboot your server.



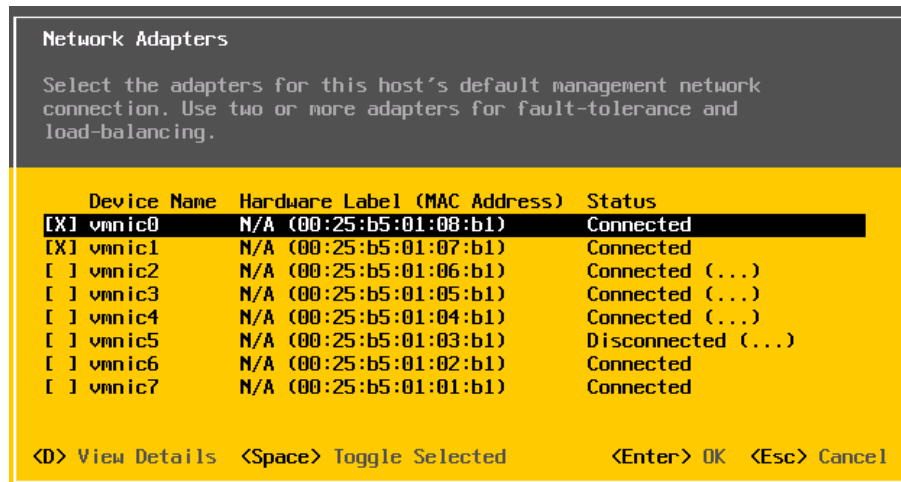
Step 9 The ESXi server booted successfully. The example is for POD1.



Lab 1-4 Answer Key: Troubleshoot LAN Connectivity: Part 1

When you complete this activity, your solution will be similar to the results here, with differences that are specific to your device or workgroup:

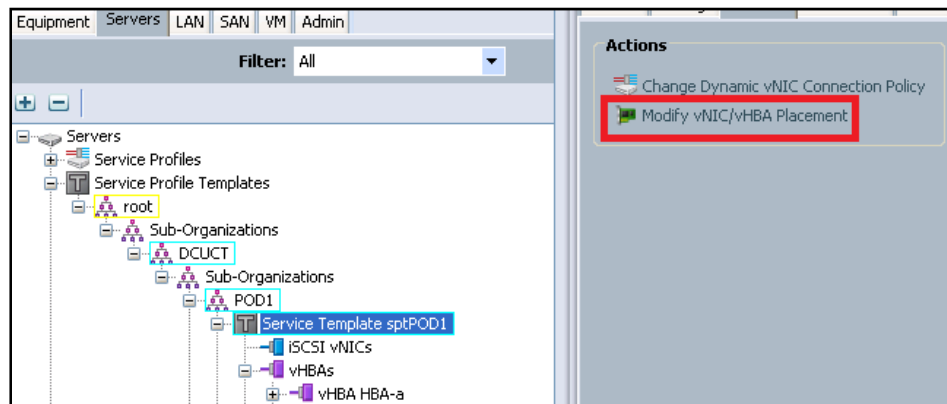
- Step 1** Try to ping the ESXi server on IP address 10.1.99.1X (where X is your pod number).
- Step 2** Open the KVM console of your ESXi host. Press **F2** inside the window and log in with the username *root* and password *NXos12345*. Then, select **Configure management network > network adapters** and check the interface order. The example is for POD1.



Step 3 According to the figure and table, which can be found in the lab aids, the order of the vNICs is not correct. Each ESXi server needs eight NICs.

NIC	MAC Address
NIC1	00:25:B5:01:01:BX
NIC2	00:25:B5:02:01:BX
NIC3	00:25:B5:03:01:BX
NIC4	00:25:B5:04:01:BX
NIC5	00:25:B5:05:01:BX
NIC6	00:25:B5:06:01:BX
NIC7	00:25:B5:07:01:BX
NIC8	00:25:B5:08:01:BX

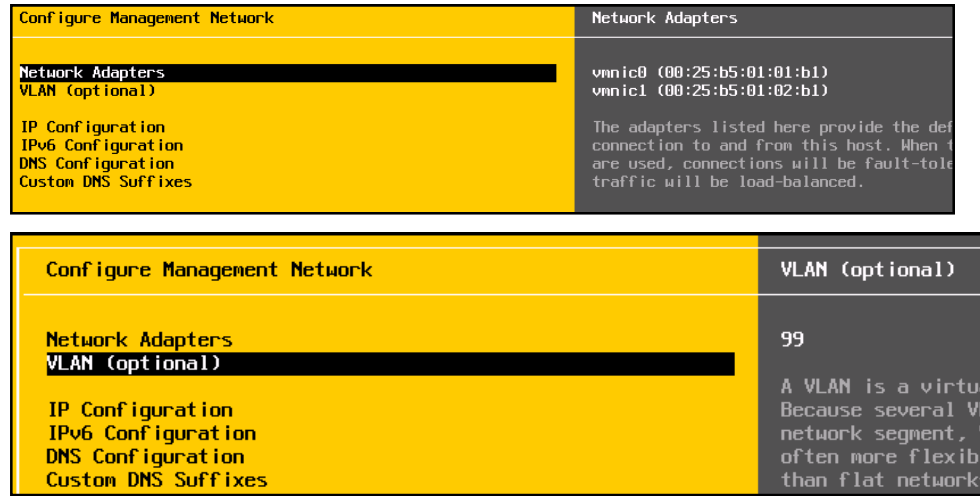
Step 4 Reorder the vNICs by going to your service profile template, select the Network tab in the right window and choose **Modify vNIC/vHBA Placement**. The example is for POD1.



Step 5 In the Modify vNIC/vHBA Placement window, set the NIC order as shown in the figure. With this change, and because you set user ACK policy, your server will need to be rebooted.

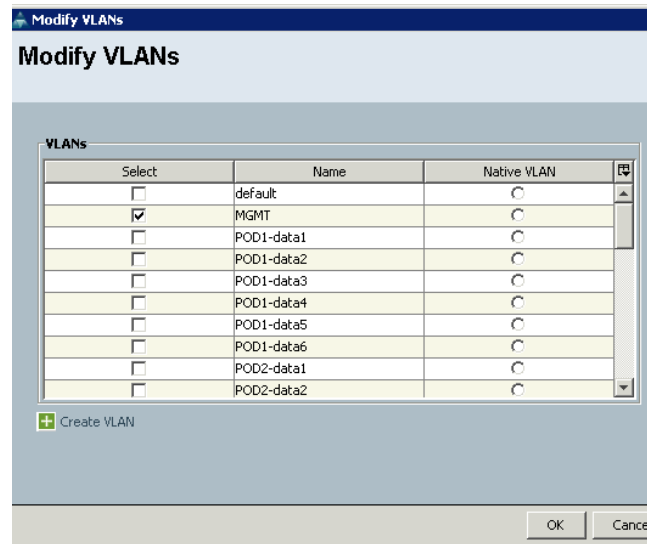
Name	MAC Address	Desired Order	Actual Order	Fabric ID
vNIC NIC1	Derived	1	Unspecified	A
vNIC NIC2	Derived	2	Unspecified	B
vNIC NIC3	Derived	3	Unspecified	A B
vNIC NIC4	Derived	4	Unspecified	A B
vNIC NIC5	Derived	5	Unspecified	A B
vNIC NIC6	Derived	6	Unspecified	A B
vNIC NIC7	Derived	7	Unspecified	A B
vNIC NIC8	Derived	8	Unspecified	A B

Step 6 After you reboot the server, the ping still does not work. Log in to the ESXi server console and verify whether the NIC order changes were applied, and check to determine which VLAN contains the management IP address. The example is for POD1.



The NIC1 and NIC2 with the MAC address (00:25:B5:01:01:B1, 00:25:B5:01:02:B1) are connected to vSwitch0. The management IP address is in VLAN 99.

Step 7 Next you must check the configuration for the first two NICs (NIC1 and NIC2) in the Cisco UCS Manager on the ntPODx-1 and ntPODx-2 templates. You must *deselect Native VLAN* at the management VLAN for both NICs, because the tagging is done on the ESXi. The other solution is also to remove the VLAN settings on the ESXi host.



Step 8 The ping should be successful.

```
C:\ Command Prompt
C:\Documents and Settings\Administrator>ping 10.1.99.11

Pinging 10.1.99.11 with 32 bytes of data:

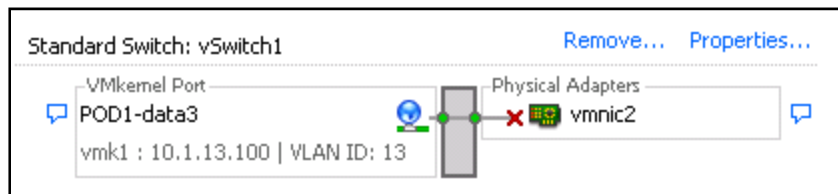
Reply from 10.1.99.11: bytes=32 time<1ms TTL=63
Reply from 10.1.99.11: bytes=32 time<1ms TTL=63
Reply from 10.1.99.11: bytes=32 time<1ms TTL=63
Reply from 10.1.99.11: bytes=32 time<1ms TTL=63

Ping statistics for 10.1.99.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Lab 1-5 Answer Key: Troubleshoot LAN Connectivity: Part 2

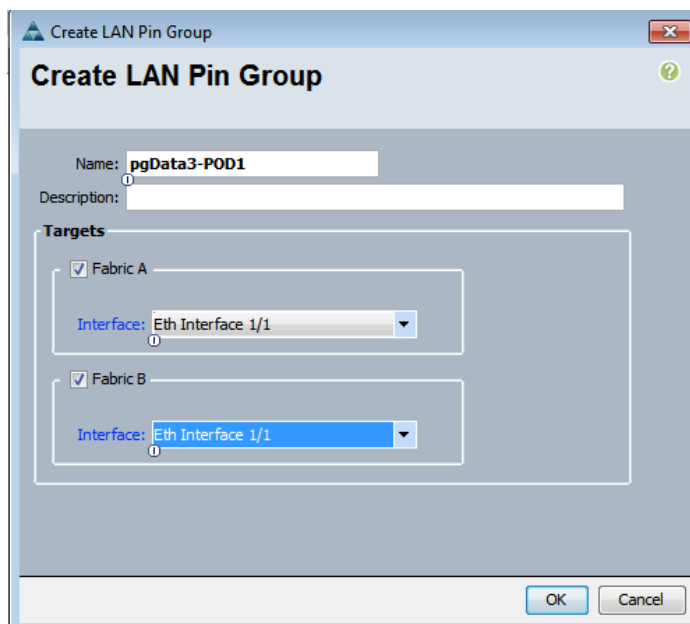
When you complete this activity, your solution will be similar to the results here, with differences that are specific to your device or workgroup:

Step 1 Log in to your ESXi server with the vSphere client using the username *root* and password *NXos12345*. Go to the Configuration tab and choose **Networking**. Locate vSwitch1 and notice the status of the interface. It is in shutdown state.



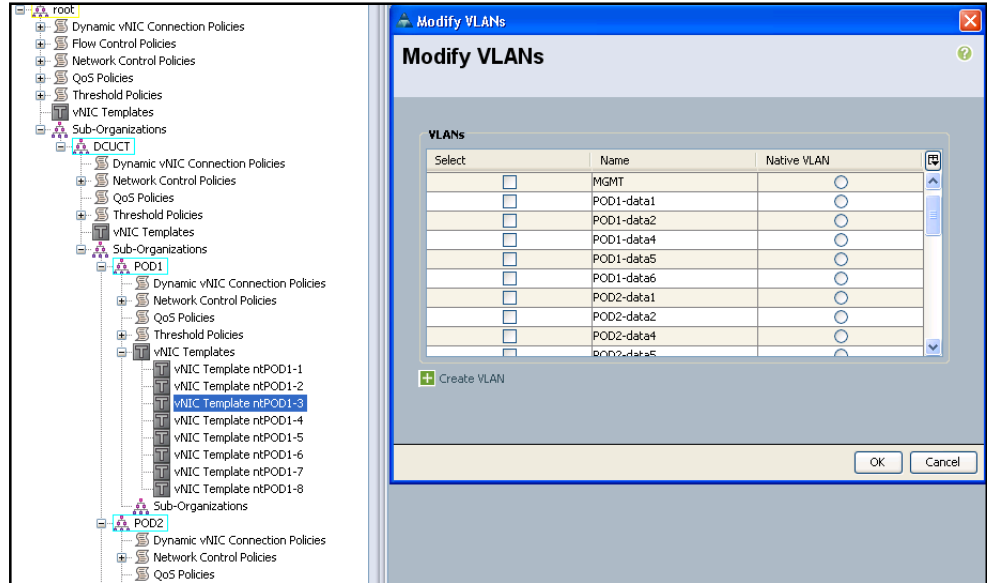
Step 2 If the NIC is in shutdown state on the ESXi host and Cisco UCS is working in EHV mode, this means that NIC3 is pinned to the uplink port, which is not working. Check the pinning settings for NIC template ntPODx-3.

Step 3 The pin group for NIC3 is configured to pgData3-PODX to the uplink ports, which are not working. Reconfigure the pin group to match your Pod settings (PODx must set targets on both Fabric Interconnects to Eth1/x). The example is for POD1.

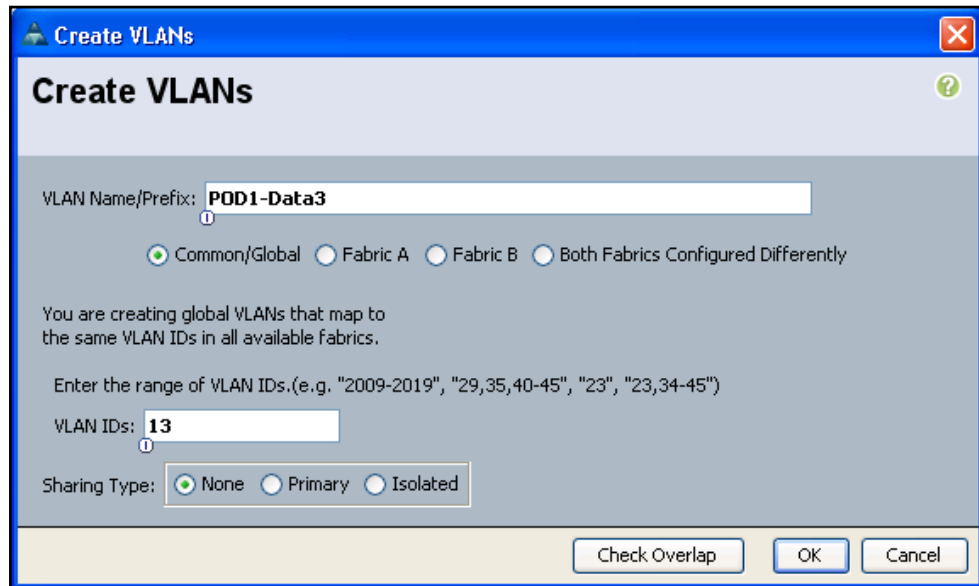


Step 4 The status of the interface on the ESXi host should become active. Next, try to ping the IP address 10.1.X3.100. The ping is still not working.

Step 5 The management IP address 10.1.X3.100 is in VLAN X3, where X is your pod number. First, check to determine if VLAN X3 is allowed on the NIC3. Go to ntPODX-3 template and choose **Modify VLAN**. The example is for POD1.

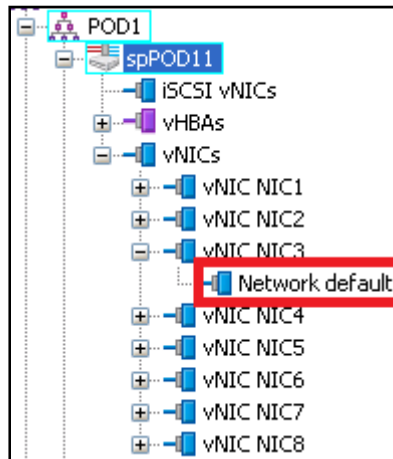


Step 6 There is no PODx-Data3 VLAN. You must create a new VLAN X3 with the name PODx-Data3 and allow that new VLAN on the NIC3. The example is for POD1.



Step 7 Try to ping the IP address 10.1.X3.100. The ping is still not working.

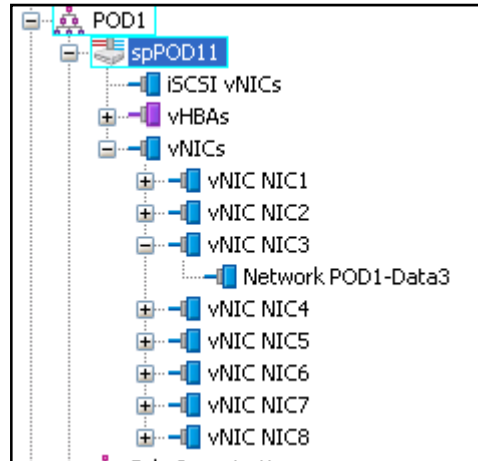
Step 8 The next step is to check to determine if the new VLAN was propagated to your service profile. Expand your service profile NIC3. There is no new VLAN X3.



Step 9 The new VLAN was not pushed to the service profile. You must check the NIC template used by the NIC3, named ntPODx-3. The changes you made in the previous step were not propagated to your service profile because the vNIC template is set to Initial Template. Change it to **Updating Template**.

The screenshot shows the 'Properties' configuration page for a vNIC template named 'ntPOD1-3'. The 'Description' is 'vNIC template for NIC3'. The 'Fabric ID' is set to 'Fabric A' with the 'Enable Failover' checkbox checked. The 'Target' section has 'Adapter' checked and 'VM' unchecked. The 'Template Type' is set to 'Updating Template', which is highlighted with a red box. The 'MTU' is set to '9000'. The 'Policies' section includes: 'MAC Pool' set to 'mpPOD1-3', 'QoS Policy' set to '<not set>', 'Network Control Policy' set to '<not set>', 'Pin Group' set to 'LAN Pin Group pgData3-POD1', and 'Stats Threshold Policy' set to 'default'.

Step 10 Verify that the changes were now pushed to your service profile. The example is for POD1.



Step 11 Try to ping the IP address 10.1.X3.100. The ping is still not working.

Step 12 The configuration on the ESXi host and Cisco UCS is now corrected. There must be something wrong on the core switch. Log in to N5548IP-L3-C1 and N5548IP-L3-C2 and check the configuration of the interface 1/x, where x is your pod number. The example is for all pods.

```
N5548IP-L3-C1 (config) #vlan X3
N5548IP-L3-C1 ((config-vlan) #name PODx-Data3
N5548IP-L3-C1 (config) #interface Ethernet1/1
N5548IP-L3-C1 (config-if) #switchport
N5548IP-L3-C1 (config-if) #switchport mode trunk
N5548IP-L3-C1 (config-if) #switchport trunk allowed vlan add X3
```

Step 13 The ping should be successful. The example is for POD1.

```
C:\ Command Prompt
C:\Documents and Settings\Administrator>ping 10.1.13.100

Pinging 10.1.13.100 with 32 bytes of data:

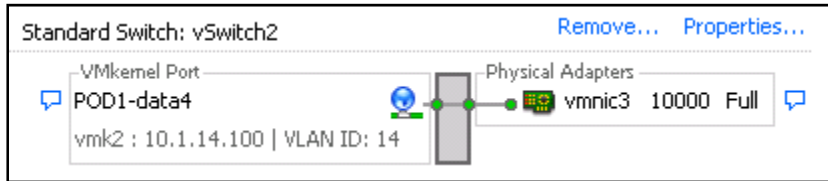
Reply from 10.1.13.100: bytes=32 time<1ms TTL=63
Reply from 10.1.13.100: bytes=32 time<1ms TTL=63
Reply from 10.1.13.100: bytes=32 time<1ms TTL=63
Reply from 10.1.13.100: bytes=32 time<1ms TTL=63

Ping statistics for 10.1.13.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Lab 1-6 Answer Key: Troubleshoot Failover Connectivity: Part 1

When you complete this activity, your solution will be similar to the results here, with differences that are specific to your device or workgroup:

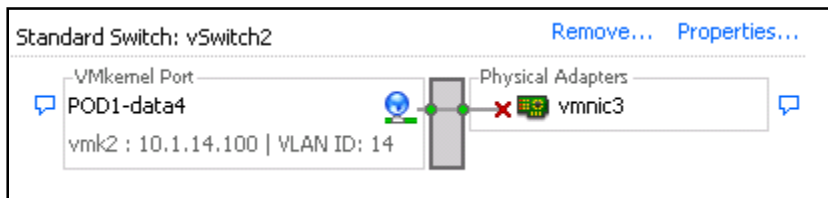
Step 1 Log in to your ESXi server with vSphere client using the username root and password *NXos12345*. Go to the Configuration tab and choose **Networking**. Locate vSwitch2 and notice the status of the physical adapter. The example is for POD1.



Step 2 Issue an infinite ping to the vmk2 and disable the NIC4 pinned uplink on the interface on FI-A.

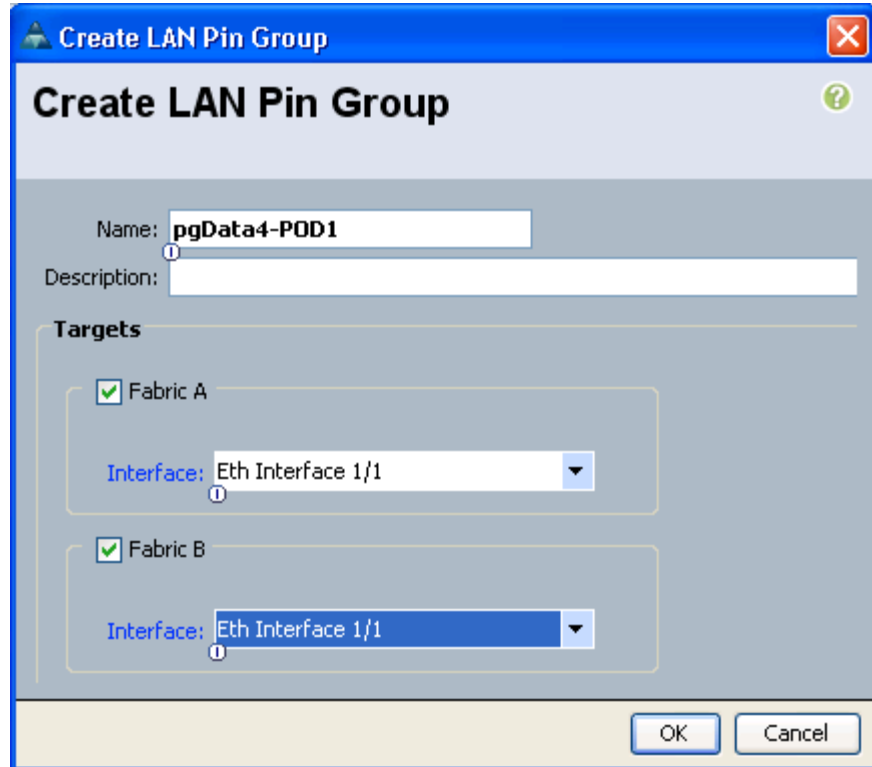
Pod	Uplink Pinned Interface on FI-A
POD1	Eth1/1
POD2	Eth1/2
POD3	Eth1/3
POD4	Eth1/4
POD5	Eth1/5
POD6	Eth1/6
POD7	Eth1/7
POD8	Eth1/8

Step 3 After the failover, the ping is not working anymore. Check the vmnic3 status on the ESXi host. The vmnic3 is in shutdown state. The example is for POD1.



Step 4 If the NIC is in shutdown state on the ESXi host and Cisco UCS is working in EHV mode, this means that NIC4 is pinned to the uplink port, which is not working. Check the pinning settings for NIC template ntPODx-4.

- Step 5** The pin group for NIC4 is configured to pgData4-PODX to the uplink ports, which are not working. Reconfigure the pin group to match your Pod settings (PODx must set targets on both Fabric Interconnects to Eth1/x). The example is for POD1.



- Step 6** After changing the pgData4-PODx pin group, the status of the vmnic3 must become active. Ping the management interface and verify if it is successful.
- Step 7** The ping is still not working. Check the VLAN trunking settings on the NIC template ntPODx-4.
- Step 8** Check the configuration on the N5548IP-L3-C2. First, verify if the VLAN is configured, then check the configuration of your PODs interface. The example is for POD1.

```
N5548IP-L3-C2 (config)#vlan X4
N5548IP-L3-C2 ((config-vlan)#name PODx-Data4
N5548IP-L3-C2 (config)#interface Ethernet1/1
N5548IP-L3-C2 (config-if)#switchport
N5548IP-L3-C2 (config-if)#switchport mode trunk
N5548IP-L3-C2 (config-if)#switchport trunk allowed vlan add X4
```

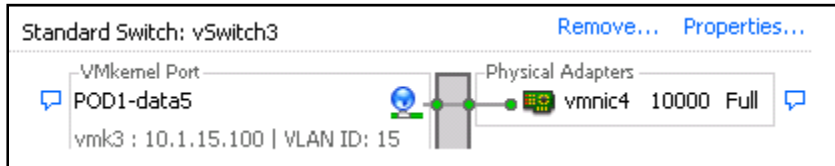
- Step 9** The ping should be now successful in case of failover.

```
Reply from 10.1.14.100: bytes=32 time<1ms TTL=63
Reply from 10.1.14.100: bytes=32 time<1ms TTL=63
Reply from 10.1.14.100: bytes=32 time<1ms TTL=63
Reply from 10.1.14.100: bytes=32 time<1ms TTL=63
Request timed out.
Reply from 10.1.14.100: bytes=32 time<1ms TTL=63
Reply from 10.1.14.100: bytes=32 time<1ms TTL=63
Reply from 10.1.14.100: bytes=32 time<1ms TTL=63
```

Lab 1-7 Answer Key: Troubleshoot Failover Connectivity: Part 2

When you complete this activity, your solution will be similar to the results here, with differences that are specific to your device or workgroup:

Step 1 Log in to your ESXi server with vSphere client with the username root and password *NXos12345*. Go to the Configuration tab and choose **Networking**. Locate vSwitch3 and notice the status of the physical adapter. The example is for POD1.

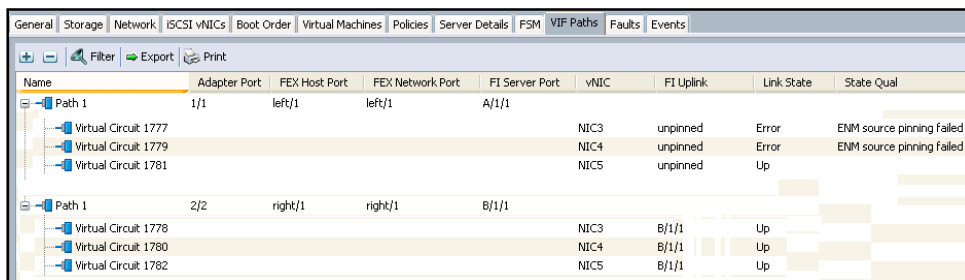


Step 2 Issue an infinite ping to the vmk2 and disable the NIC5 pinned uplink interface on FI-A.

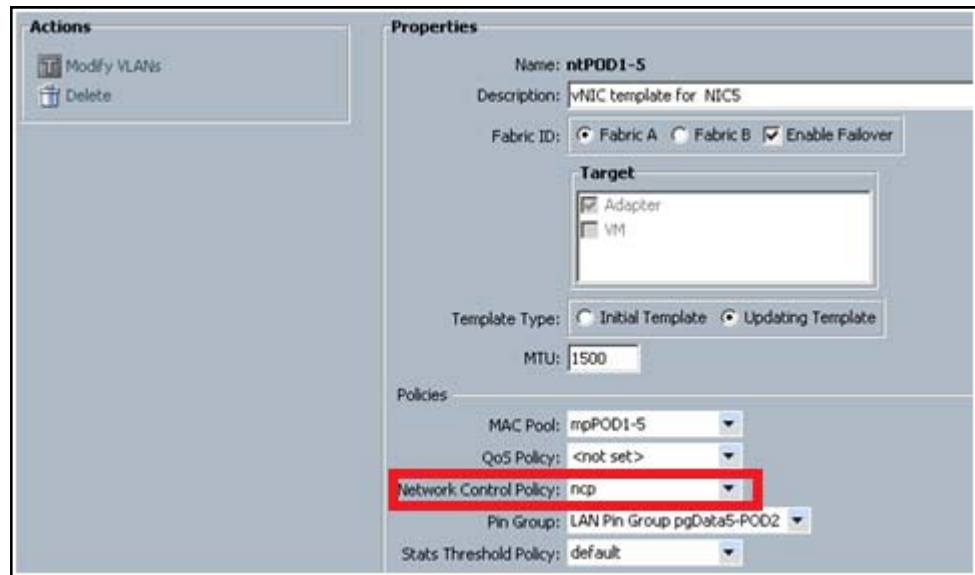
Pod	Uplink Pinned Interface on FI-A
POD1	Eth1/1
POD2	Eth1/2
POD3	Eth1/3
POD4	Eth1/4
POD5	Eth1/5
POD6	Eth1/6
POD7	Eth1/7
POD7	Eth1/8

Step 3 After the failover, the ping is not working anymore. Check the vmnic4 status on the ESXi host. The vmnic4 is still in UP state. The example is for POD1.

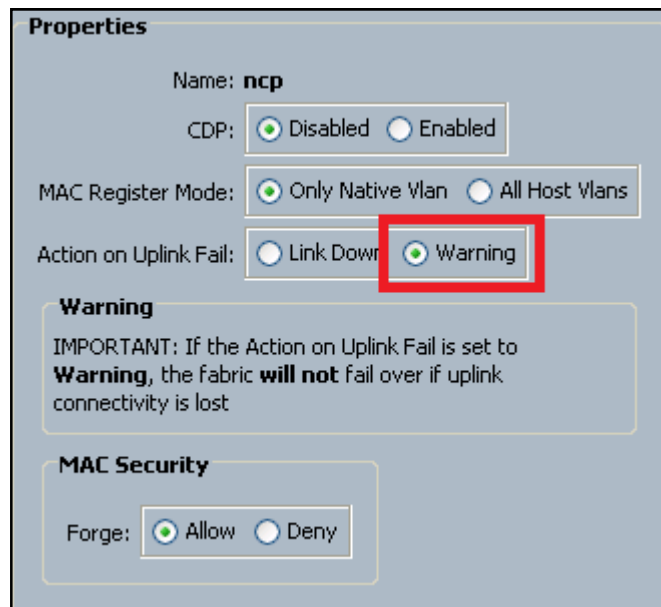
Step 4 Go to your service profile in the Cisco UCSM, select the **VIF Paths** tab, and check the pinning settings for NIC5. For NIC 5, there is no Error in the Link state, and the link state is UP.



- Step 5** The uplink interface is DOWN and vNIC is UP, which means that there is something strange configured on the NIC5. First, check the configuration of NIC5 template ntPODx-5. You will see that the Network Control Policy is configured as **ncp**.



- Step 6** Check the ncp policy configuration. The network control policy Action on uplink Fail is set to Warning, which means that if the uplink fails, only the warning will be seen in the UCSM.



- Step 7** Reconfigure the Action on Uplink Fail from Warning to **Link Down** in the network control policy.

- Step 8** Verify the VIF Paths again. Now there is an error, which means that the pinning was made to the second Fabric Interconnect.

Name	Adapter Port	FEX Host Port	FEX Network Port	FI Server Port	vNIC	FI Uplink	Link State	State Qual
Path 1	1/1	left/1	left/1	A/1/1				
Virtual Circuit 1777					NIC3	unpinned	Error	ENM source pinning failed
Virtual Circuit 1779					NIC4	unpinned	Error	ENM source pinning failed
Virtual Circuit 1781					NIC5	unpinned	Error	ENM source pinning failed
Path 2	2/2	right/1	right/1	B/1/1				
Virtual Circuit 1778					NIC3	B/1/1	Up	
Virtual Circuit 1780					NIC4	B/1/1	Up	
Virtual Circuit 1782					NIC5	B/1/1	Up	

- Step 9** The ping is still not working. Check the configuration on the N5548IP-L3-C2. First, verify if the VLAN is configured, then check the configuration of your Pod interface. The example is for POD1.

```
N5548IP-L3-C2 (config) #vlan X5
N5548IP-L3-C2 ( (config-vlan) #name PODx-Data4
N5548IP-L3-C2 (config) #interface Ethernet1/1
N5548IP-L3-C2 (config-if) #switchport
N5548IP-L3-C2 (config-if) #switchport mode trunk
N5548IP-L3-C2 (config-if) #switchport trunk allowed vlan add X5
```

- Step 10** The ping should now be successful in case of failover.

Lab 2-1 Answer Key: Troubleshoot Cisco UCS C-Series Server Boot from SAN

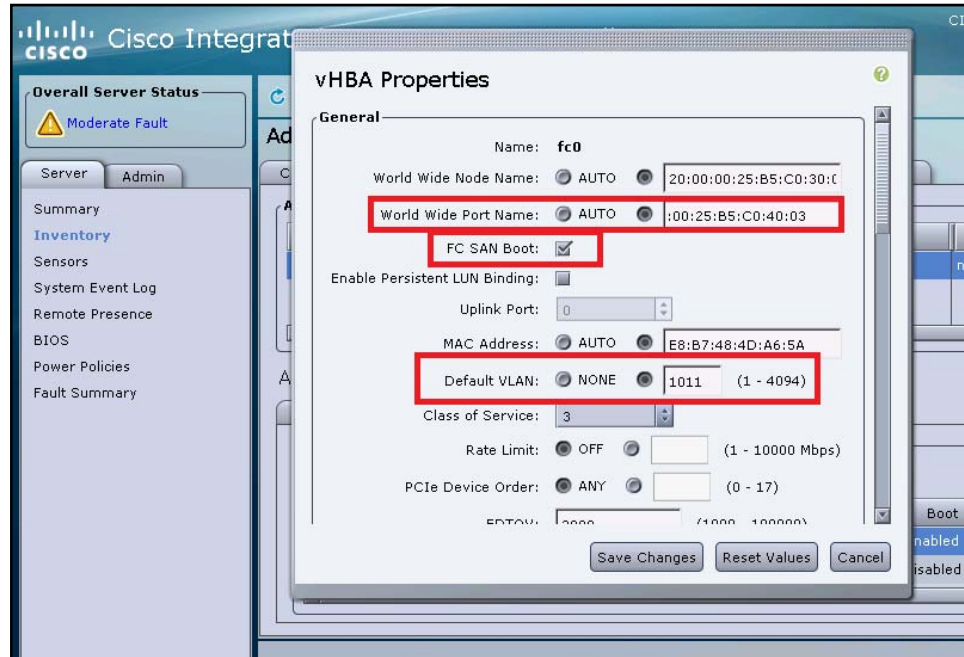
When you complete this activity, your solution will be similar to the results here, with differences that are specific to your device or workgroup:

- Step 1** The first thing to look for is that HBA fc0 has FC SAN Boot enabled. Navigate to Server > Inventory > Network Adapters > vHBAs > fc0 > Properties and enable **FC SAN Boot**.

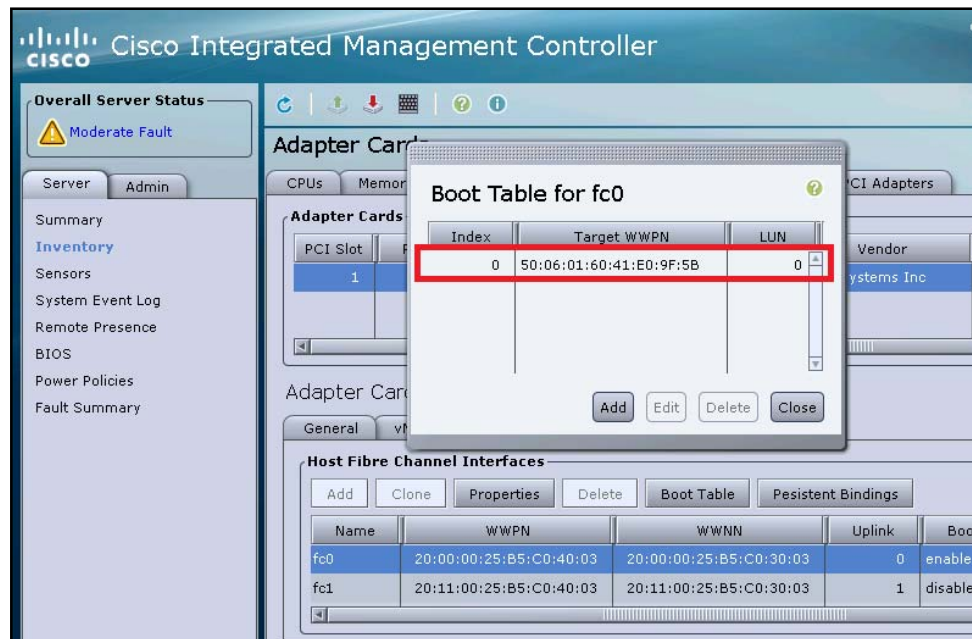
- Step 2** FCoE VLAN ID is also not configured—put in your Pod ID. If you observe the zoning output in the Cisco Nexus 5548 switch, you can see your pod WWPN. You can also check the device alias (use the **show device-alias database** command) on the Nexus 5548 to see the correct WWPN:

```
N5548-3#show device-alias database
device-alias name CX3-SPA pwwn 50:06:01:60:41:e0:9f:5b
device-alias name CX3-SPB pwwn 50:06:01:68:41:e0:9f:5b
device-alias name dcuci-c1 pwwn 20:00:00:25:b5:c0:40:01
device-alias name dcuci-c2 pwwn 20:00:00:25:b5:c0:40:02
device-alias name dcuci-c3 pwwn 20:00:00:25:b5:c0:40:03
device-alias name dcuci-c4 pwwn 20:00:00:25:b5:c0:40:04
<...rest of the output omitted...>
```

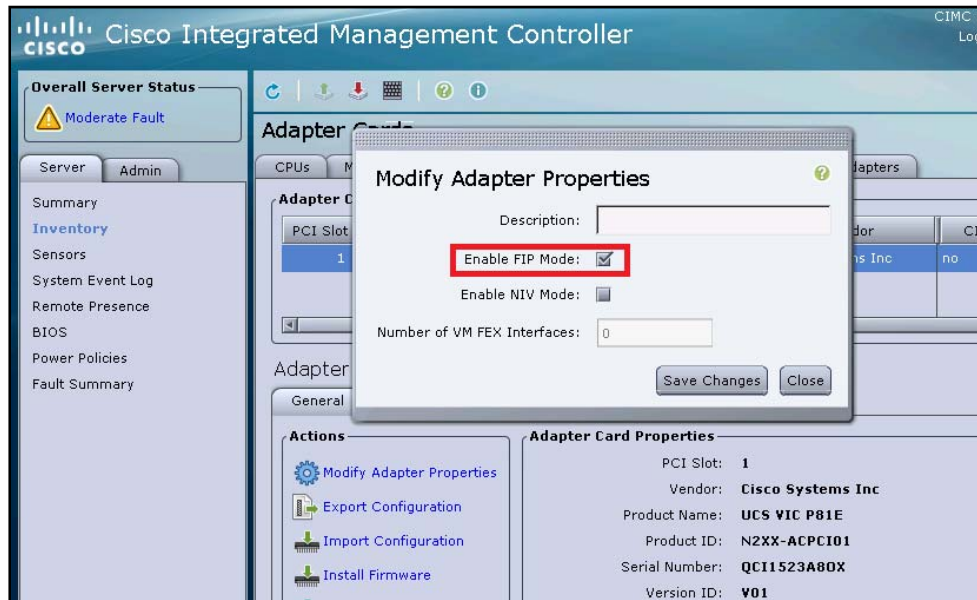
Step 3 Change the WWPN for your server to enable the correct zoning. You can see the example of all corrections for Pod 3 in the figure.



Step 4 The boot target that is configured in the vHBA is not the same as the target listed in the table in Job Aids. Navigate to Server > Inventory > Network Adapters > vHBAs > fc0 > Boot Table and change the boot target accordingly. The example is for POD3.



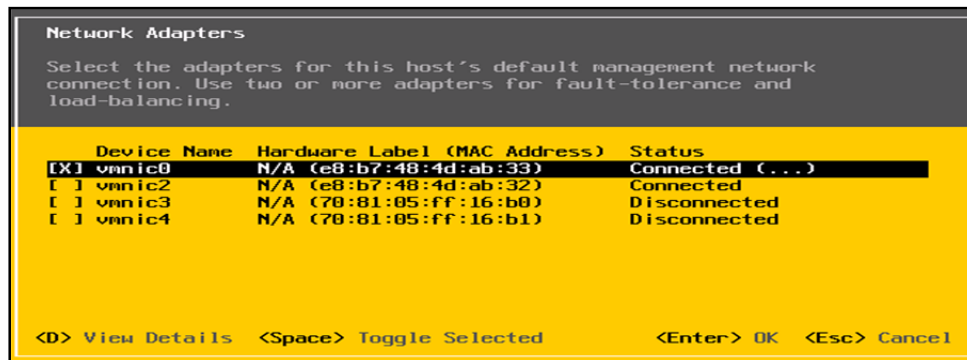
- Step 5** In addition, FIP mode is not enabled. Navigate to Server > Inventory > Network Adapters > General > Modify Adapter Properties, and enable **FIP Mode**.



- Step 6** Reboot the server to apply the changes. The server should boot successfully from the ESXi host. You will need that ESXi host in the next lab.

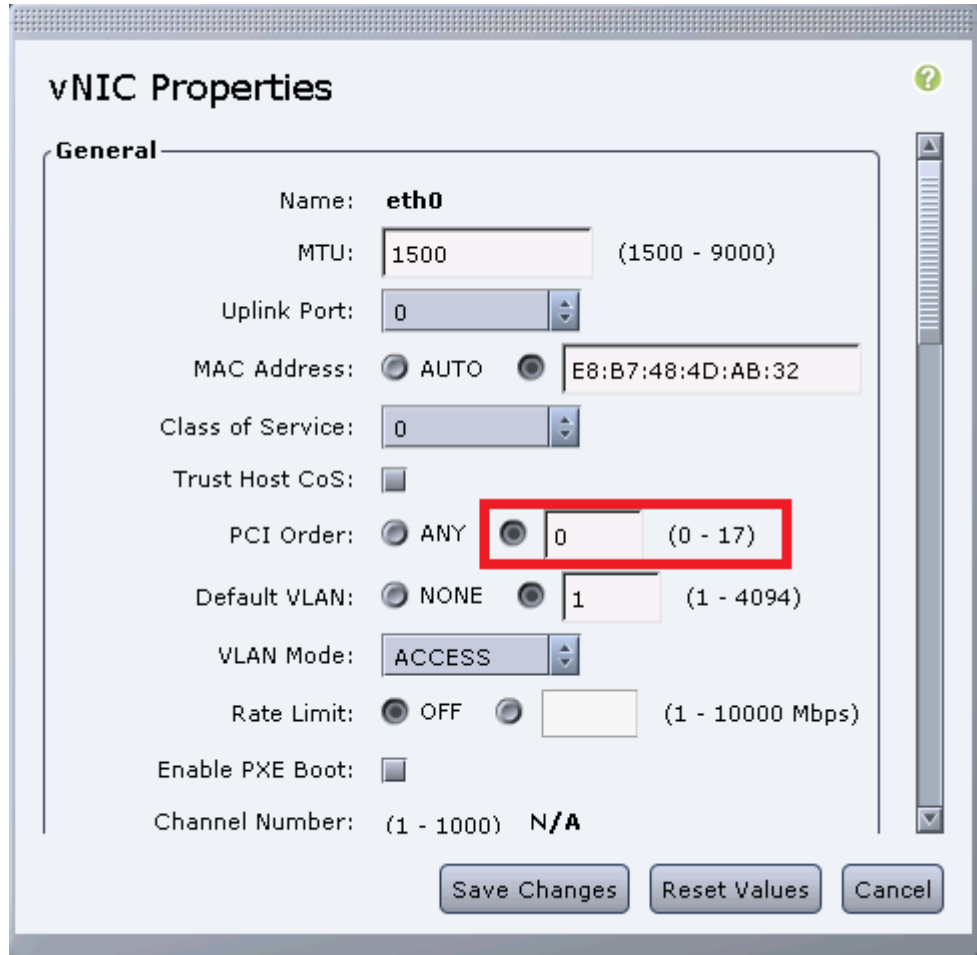
Lab 2-2 Answer Key: Troubleshoot Network Connectivity

- Step 1** Try to ping the ESXi server on the IP address 10.1.99.1X2.
- Step 2** Log in to the Cisco IMC on your Cisco UCS C-Series server with the IP address 192.168.10.4X, with username *admin* and password *NXos12345*.
- Step 3** Open the KVM console of your ESXi host on your Cisco UCS C-Series server. Press **F2** inside the window and log in with the username *root* and password *NXos12345*. Then go to Configure management network > network adapters, and check the interface order. The example is for POD1.

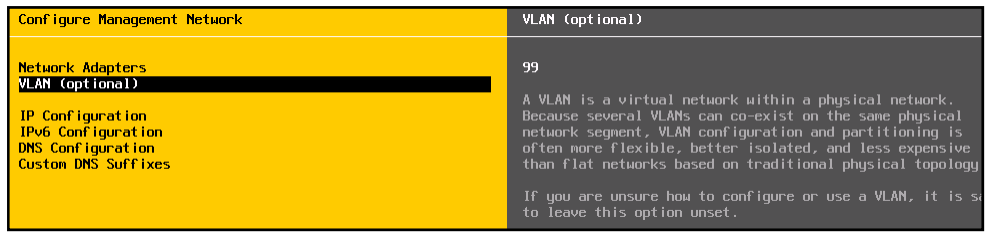


- Step 4** According to the figure and the information in the inventory on the Cisco IMC, the NIC order is wrong. NIC1 on the P81E should be presented as vmnic0 and NIC2 as second vmnic.

- Step 5** Reorder the vNICs by going in the Cisco IMC under the Server tab to Inventory > Network Adapters vNICs. Select **eth0** and change the PCI Order to 0. Example is for POD1.



- Step 6** To apply the changes, you must reboot the server.
- Step 7** When the server is back, the ping still does not work. Log in to the ESXi server console and verify whether the NIC order changes were applied, and check in which VLAN the management IP address is located. The example is for POD1.



The NIC1 with MAC address e8:b7:48:4d:ab:32 is connected to vSwitch0. The management IP address is in VLAN 99.

- Step 8** Next, you must check the configuration for the first NIC. Change the VLAN mode to **Trunk**, and default VLAN to **None**.

vNIC Properties

General

Name: **eth0**

MTU: (1500 - 9000)

Uplink Port:

MAC Address: AUTO

Class of Service:

Trust Host CoS:

PCI Order: ANY (0 - 17)

Default VLAN: **NONE** (1 - 4094)

VLAN Mode:

Rate Limit: OFF (1 - 10000 Mbps)

Enable PXE Boot:

Channel Number: (1 - 1000) **N/A**

- Step 9** To apply the changes, you must reboot the server.
- Step 10** When the server is back on line, try to ping the management IP again. It still does not work. The next step is to verify the configuration on the Cisco Nexus N5548 switches. Log in to the N5548UP-C1 and verify VLAN settings. VLAN 99 is not allowed to your server.

```
N5548UP-C1(config)# interface Ethernet1/1
N5548UP-C1(config-if)# switchport
N5548UP-C1(config-if)# switchport mode trunk
N5548UP-C1(config-if)# switchport trunk allowed vlan add 99
```

- Step 11** The ping should be successful.